Emmy Noether

Collected Mathematical Works in English

Complete Maintained English Corpus Edition

This linked reader brings together the complete substantive English corpus currently maintained by the project: numbered papers 1–43, retained scholarly apparatus, the 1929/30 lectures on hypercomplex quantities, the Kapferer paper and Noether supplement, bibliography, and short communications and reviews.

Editorial status. This is a machine-assisted working translation and typeset edition. It is complete in project coverage but is not a peer-reviewed translation or a critical edition. Source-language and target-language decisions, exact lineage, correction dispositions, and validation evidence are preserved separately in the accompanying editable-source and provenance archives.

German authority. NOETH-DE-AUTH-v051-20260811 / NOETH-DE-ED-0014. All 25 accepted authority deltas have an explicit English disposition; 20 required source or layout changes and 5 were already conformant.

English concept DOI: `10.5281/zenodo.21923145`
This version DOI: `10.5281/zenodo.21923146`
Zenodo record: `21923146`
Living repository: `https://github.com/KokunoYumeto/emmy-noether-en`

Release date: 2026-08-13

Contents

1. On the Formation of the Form System (1907) 1

2. On the Formation of the Form System (1908) 3

3. On the Invariant Theory of Forms in n Variables (1909) 40

4. On the Invariant Theory of Forms in n Variables (1911) 43

5. Rational Function Fields 63

6. Fields and Systems of Rational Functions 65

7. The Finiteness Theorem for the Invariants of Finite Groups 88

8. Polynomial Representation of Invariants 90

9. The Most General Domains from Integral Transcendental Numbers 96

10. The Functional Equations of the Isomorphic Mapping 110

11. Equations with Prescribed Group 116

12. Invariants of Arbitrary Differential Expressions 121

13. Invariant Variational Problems 125

14. The Arithmetic Theory of Algebraic Functions of One Variable 138

15. Finiteness of Integral Invariants of Binary Forms 149

16. On Series Expansion in Form Theory 160

17. Joint with Werner Schmeidler: Modules in Noncommutative Domains 164

18. On a Work in Elimination Theory by K. Hentzelt 185

19. Ideal Theory in Ring Domains 186

20. An Algebraic Criterion for Absolute Irreducibility 210

21. Formal Calculus of Variations and Differential Invariants 215

22. On the Theory of Polynomial Ideals and Resultants 218

23. Algebraic and Differential Invariants 233

24. Elimination Theory and General Ideal Theory 238

25. Elimination Theory and Ideal Theory 256

26. Abstract Construction of Ideal Theory in the Algebraic Number Field 259

27. Hilbert Numbers in Ideal Theory 260

28. Group Characters and Ideal Theory 261

29. Finiteness for Finite Linear Groups of Characteristic p 262

30. Abstract Construction of Ideal Theory in Number and Function Fields 266

31. The Discriminant Theorem for Orders **286**

32. Joint with R. Brauer: On Minimal Splitting Fields **300**

33. Hypercomplex Quantities and Representation Theory in Arithmetic Conception **305**

34. Hypercomplex Quantities and Representation Theory **307**

35. On Maximal Domains of Integral Functions **340**

36. Ideal Differentiation and the Different **346**

37. Normal Basis in Fields without Higher Ramification **347**

38. Jointly with R. Brauer and H. Hasse: A Main Theorem on Algebras **351**

39. Hypercomplex Systems, Commutative Algebra, and Number Theory **356**

40. Noncommutative Algebras **360**

41. The Principal Genus Theorem for Relative Galois Number Fields **377**

42. Split Crossed Products and Their Maximal Orders **383**

43. Ideal Differentiation and the Different **388**

RA10: scan-visible apparatus for Papers 40–43 **405**

Algebra of Hypercomplex Quantities: 1929/30 Lectures **409**

Kapferer: Multiplicity Conditions and Noether Supplement **451**

Bibliography **456**

Short Communications and Book Reviews **459**

1. On the Formation of the form System of the Ternary Biquadratic form

Reports of the Physical-Medical Society in Erlangen 39 (1907), pp. 176–179

(Extract from the author's dissertation.)

Work by Gordan, Maisano, and Pascal[1] deals with the form system of the ternary biquadratic form. Gordan sets up the complete form system, consisting of 54 formations, for the special automorphic form

$$f = x_1^3 x_2 + x_2^3 x_3 + x_3^3 x_1,$$

on the basis of principles similar to those which he had given for form systems in the binary domain.

In Maisano's work, for the general biquadratic form, the forms up to and including the fifth order[2] are set up, together with some invariants, covariants, and contravariants of higher order, according to the method used by Gordan in volume I of the *Mathematische Annalen* for the ternary cubic form. Pascal, using Maisano's results, is chiefly concerned with the question of the decomposition of the biquadratic form into factors[3].

The aim of my investigations is to set up the form system for the general ternary biquadratic form; to begin with, only the main foundations are given, and a so-called "relatively complete system"[4] is established.

The basic idea for forming systems of ternary forms is the same as in the binary domain. Starting from a first relatively complete system – the system of forms taken over from the binary case – one passes, according to a definite law, to systems with ever higher modulus, until either the system of a modulus – taking the modulus as ground form – becomes finite and known, or until a modulus can be reduced to forms having invariants as factors. By transvection of the relatively complete system with the system of the modulus, in the first case one obtains the absolutely complete system, while in the second case the relatively complete and absolutely complete systems coincide. By Hilbert's general proof the finiteness of form systems, this procedure must necessarily come to an end.

In our case, the modulus (abc) of the first relatively complete system can be led back to the moduli

$$\Delta = (abc)^2 a_x^2 b_x^2 c_x^2 \quad \text{and} \quad \nu = (abu)^4;$$

from this the relatively complete system modulo ν is readily obtained. As the sequence of moduli we now choose the forms

$$\nu; \qquad \nu^{(\nu)} = (\nu\nu_1 x)^4 = s_x^4,$$
$$\nu^{(s)} = (ss'u)^4 \ldots,$$

and adjoin, as further moduli, two quadratic forms occurring in the formation of the relatively complete system modulo s, namely u_σ^2 and t_x^2. One can then show that the modulus following s, namely $(ss'u)^4$, is reducible to the modulus (ϱ, t). Since, however, the simultaneous system of two quadratic forms is finite

[1] P. Gordan, "Über the volle Formensystem of the ternären biquadratischen form" $f = x_1^3 x_2 + x_2^3 x_3 + x_3^3 x_1$ (Math. Annalen vol. XVII, pp. 217–233, 1880); G. Maisano, 1. "Sistemi completi dei primi cinque gradi della forma ternaria biquadratica e degl' invarianti, covarianti e contravarianti di sesto grado" (Giorn. di Battaglini XIX). 2. "Sui covarianti indipendenti di 6° grado nei coefficienti della forma biquadratica ternaria" (Rend. Circ. Mat. di Palermo I, 1887); E. Pascal, "Contributo alla teoria della forma ternaria biquadratica e delle sue varie decomposizioni in fattori" (Memoria premiata dalla R. Accademia delle scienze fisiche e matematiche di Napoli, 1905).

[2] By "order" the dimension in the coefficients is to be understood, and by "degree" the dimension in the variables.

[3] In his second short note Maisano attempts to prove a linear dependence among the three covariants of order 6 and degree 6. In contrast to this not quite complete proof, Pascal believes he has proved the linear independence of the three covariants of order 6, as well as that of the three invariants of order 9. That, however, a linear relation does in fact exist between the three covariants on the one hand and the three invariants on the other, emerged in the course of my computations; in Pascal's notation the explicit formulas are

$$0 = 20\Omega_1 + 6\Omega_2 - 3\Omega_3 + 4fC_1 - 12fC_2 - 4A \cdot \Delta,$$

$$0 = 4A^3 - 15AB + 30C - 90D + 9E.$$

[4] For the terminology, see Gordan–Kerschensteiner, *Vorlesungen über Invariantentheorie*, vol. II, p. 227.

and known, the termination described above has thereby been reached. As the relatively complete system modulo (ϱ, t) one obtains 331 formations. —

I add a few details concerning the method used.

The fundamental process for producing forms, the folding process, can be defined in the ternary domain as follows:

If in a symbolic product

$$s_x^m t_x^n u_\sigma^\mu u_\tau^\nu$$

one replaces the pairs of factors

	$s_x t_x$	$u_\sigma u_\tau$	$s_x u_\sigma$ or $s_x u_\tau$	$t_x u_\tau$ or $t_x u_\sigma$
respectively by	(stu)	$(\sigma\tau x)$	s_σ or s_τ	t_τ or t_σ
folding	I	II	III	IV,

then the forms so arising have been obtained from the original form by folding[5].

Here one may still always put $s_\sigma = 0;\ t_\tau = 0$. For the relation among the individual foldings, the following theorem holds:

The foldings I and II are fundamental foldings, from which, independently of the order of composition, the foldings III and IV can be composed. In other words: to form all forms arising from a given expression by folding, one need only apply foldings I and II[6].

By a "form sequence" we mean an initial form together with all forms arising from it by folding into itself. By the theorem, a form sequence $s_x^m t_x^n u_\sigma^\mu u_\tau^\nu$ can be arranged in a rectangular scheme. In proceeding, one obtains:

1. by moving one column to the right, all forms arising by folding I from the adjacent forms;

2. by moving one row downward, all forms arising by folding II from the forms standing above, and hence all forms arising by folding.

Under these assumptions, the theorems on reducers can be stated in their most general form, under the definition

"A reducer is a reducible form sequence,"

as follows:

If the initial form of a form sequence is reducible because one of its terms has arisen by folding with a reducer, and if the final form of the form sequence has arisen from this same term by folding, then the whole form sequence is reducible.

Further reduction methods to be mentioned are:

1. the so-called "double reduction," that is, the reduction of a form in two ways in order to obtain a relation between the higher forms;

2. "folding with decomposed forms," which partly has the character of reduction by reducers and partly that of "double reduction."

[5] Gordan, Math. Annalen, vol. XVII, p. 219.

[6] The theorem has an exception in the case where n and μ, respectively m and ν, vanish simultaneously; the "form sequence" then reduces to the diagonal term.

2. On the Formation of the form System of the Ternary Biquadratic form

Journal for the reine and angewandte Mathematik 134 (1908), pp. 23–90 and two tables

Introduction.

Work by Gordan, Maisano, and Pascal[7][8] deals with the form system of the ternary biquadratic form. Gordan sets up the complete form system, consisting of 54 formations, of the special automorphic form

$$f = x_1^3 x_2 + x_2^3 x_3 + x_3^3 x_1$$

on the basis of principles similar to those that he had given for form systems in the binary domain.

In Maisano's work, for the general biquadratic form, the forms up to and including the fifth order[9] are set up, together with some invariants, covariants, and contravariants of higher order, according to the method used by Gordan in volume I of the *Mathematische Annalen* for the ternary cubic form. Pascal, using Maisano's results, is chiefly concerned with the question of the decomposition of the biquadratic form into factors[10].

The aim of the following investigations is to set up the form system for the general ternary biquadratic form; in this work, namely, only the principal foundations are given, and a so-called "relatively complete system"[11] *is established.*

The work is closely connected with Gordan's work; however, the principles that were stated there only quite generally first had to be worked out in detail. With the aid of a theorem on the connection among the foldings and by introducing the "form sequence" (ğ 1), the reduction theorems are sharply formulated and completed (ğ 3), while the recursive establishment of special series expansions (ğ 2) gives the computational means for actually carrying out the reductions.

The basic idea for forming systems of ternary forms is the same as in the binary domain. Starting from a first relatively complete system – the system of forms taken over from the binary case – one passes, according to a definite law, to systems with ever higher modulus, until either the system of a modulus – the modulus taken as ground form – becomes finite and known, or until a modulus can be reduced to forms having invariants as factors. By transvection of the relatively complete system with the system of the modulus, in the first case the absolutely complete system arises, while in the second case the relatively complete and absolutely complete systems coincide. By Hilbert's general proof the finiteness of form systems, this procedure must necessarily come to an end.

In our case the modulus (abc) of the first relatively complete system (ğ 4) is reduced to the moduli

$$\Delta = (abc)^2 a_x^2 b_x^2 c_x^2 \quad \text{and} \quad \nu = (abu)^4$$

(ğ 5), and then the relatively complete system modulo ν is found (ğ 6). These results are already given in Gordan's work for the general biquadratic form; our manner of deriving them, however, is more easily transferred to forms of higher degree.

---

[7] A short extract from the Introduction and Chapter I appeared in the *Sitzungsberichte of the physikalisch-medizinischen Sozietät Erlangen 1907*, pp. 176–179.

[8] P. Gordan, on the complete form system of the ternary biquadratic form

$$f = x_1^3 x_2 + x_2^3 x_3 + x_3^3 x_1.$$

(*Math. Annalen*, vol. XVII (1880), pp. 217–233.) G. Maisano, 1) *Sistemi completi dei primi cinque gradi della forma ternaria biquadratica e degl' invarianti, covarianti e contravarianti di sesto grado.* (Giorn. di Battaglini XIX.) 2) *Sui covarianti indipendenti di 6° grado nei coefficienti della forma biquadratica ternaria.* (Rend. Circ. Mat. di Palermo I, 1887.) E. Pascal, *Contributo alla teoria della forma ternaria biquadratica e delle sue varie decomposizioni in fattori.* (Memoria premiata dalla R. Accademia delle scienze fisiche e matematiche di Napoli. 1905.)

[9] By "order" the dimension in the coefficients is to be understood, and by "degree" the dimension in the variables.

[10] In his second short note, Maisano attempts to prove a linear dependence of the three covariants of order 6 and degree 6. In contrast to this not quite complete proof, Pascal believes he has proved the linear independence of the three covariants of order 6, and likewise that of the three invariants of order 9. That, however, a linear relation does in fact exist between the three covariants on the one hand and the three invariants on the other is shown by formulas (13), ğ 11, and (22), ğ 17 note, of the present work, where these relations are given explicitly. According to a communication from Pascal, the contradiction is explained by a numerical error in the expression for his contravariant p (called ϱ here), p. 46 of his paper.

[11] For the terminology see ğ 3a.

As the sequence of moduli we now choose the forms (ğ 7)

$$\nu, \qquad \nu(\nu) = (\nu\nu_1 x)^4 = s_x^4, \qquad \nu(s) = (ss'u)^4, \ldots .$$

In forming the relatively complete system modulo s, two quadratic forms occurring in the system, u_ϱ^2 and t_x^2, are adjoined as moduli (ğğ 9 and 10), and accordingly the relatively complete system modulo (s, ϱ, t) is formed. It is then shown (ğ 17) that the modulus $(ss'u)^4$ is reducible to the moduli ϱ and t. The next higher system thereby passes over into a relatively complete system modulo (ϱ, t). Since, however, the simultaneous system of two quadratic forms is finite and known, and in the general case consists of 20 formations[12], the termination described above is reached with the establishment of the relatively complete system modulo (ϱ, t). The transvection of this system with the system of (ϱ, t) in order to form the absolutely complete system is reserved.

As the relatively complete system modulo (ϱ, t) one finds 331 formations, which in the appended table are ordered according to their degree in the variables x and u.

Finally we give an overview of the symbols introduced:

$$\begin{aligned}
f &= a_x^4, \\
\theta &= \theta_x^4 u_\vartheta^2 = (abu)^2 a_x^2 b_x^2, \\
K &= K_x^6 u_k^3 = (a\theta u) u_\vartheta^2 a_x^3 \theta_x^3, \\
j &= u_j^6 = (a\theta u)^4 u_\vartheta^2, \\
\Delta &= \Delta_x^6 = a_\vartheta^2 a_x^2 \theta_x^4 = (abc)^2 a_x^2 b_x^2 c_x^2, \\
N &= N_x^8 u_\eta = (a\Delta u) a_x^3 \Delta_x^5, \\
\nu &= u_\nu^4 = (abu)^4, \\
H &= H_x^2 u_\eta^4 = (\nu\nu_1 x)^2 u_\nu^2 u_{\nu_1}^2, \\
L &= L_x^3 u_l^6 = (\nu\eta x) H_x^2 u_\nu^3 u_\eta^3, \\
g &= g_x^6 = (\nu\eta x)^4 H_x^2, \\
\sigma &= u_\sigma^6 = H_\nu^2 u_\nu^2 u_\eta^4, \\
s &= s_x^4 = (\nu\nu_1 x)^4, \\
Z &= Z_x^4 u_\zeta^2 = (ss'u)^2 s_x^2 s_x'^2, \\
\varrho &= u_\varrho^2 = \theta_\nu^4 u_\vartheta^2, \\
t &= t_x^2 = a_\eta^4 H_x^2, \\
i &= a_\nu^4, \\
J &= s_\nu^4.
\end{aligned}$$

Chapter I. General Theorems on Ternary Forms.

ğ 1. The folding process. form sequences.

The fundamental process for producing forms is the folding process, which in the ternary domain can be defined as follows. Let there be given a symbolic product

$$s_x^m t_x^n u_\sigma^\mu u_\tau^\nu .$$

If one replaces the pairs of factors

$$s_x t_x \qquad u_\sigma u_\tau \qquad s_x u_\sigma \text{ or } s_x u_\tau \qquad t_x u_\tau \text{ or } t_x u_\sigma$$

respectively by

$$(stu) \qquad (\sigma\tau x) \qquad s_\sigma \text{ or } s_\tau \qquad t_\tau \text{ or } t_\sigma,$$

folding

$$\text{I} \qquad \text{II} \qquad \text{III} \qquad \text{IV},$$

[12] Cf. Clebsch–Lindemann, *Vorlesungen über Geometrie.* (Vol. I, p. 288 ff.) System of two cogredient forms. Gordan, "Über Büschel of Kegelschnitten." (*Math. Ann.* vol. XIX, p. 530.) System of two contragredient forms.

then the resulting forms have arisen from the original one by folding[13].

Here the expression $s_x^m t_x^n u_\sigma^\mu u_\tau^\nu$ can be regarded either as an actual product of two forms $S \cdot T$, or as a single form with several rows of symbols:

$$s_x^m t_x^n u_\sigma^\mu u_\tau^\nu = A_x^{m+n} u_x^{\mu+\nu}.$$

In the first case we speak of the folding of the form S with T, in the second case of the "folding of the form A in itself." For brevity we always assume in what follows, as indeed is the case for all forms later to be considered, that

$$s_\sigma^\lambda = 0, \qquad t_\tau^\lambda = 0 \tag{a}$$

for any λ and x distinct from 0, and in conjunction with any other foldings. This says that the form $s_x^m t_y^n u_\sigma^\mu u_\tau^\nu$ is a so-called "normal form," that is, it vanishes under application of the Ω-process, both with respect to the variables x and u and with respect to the variables y and v.

Thus condition (a) represents no restriction, but can always be achieved[14].

For the connection among the individual foldings the following theorem holds:

Theorem I. Foldings I and II are fundamental foldings from which, independently of the order of composition, foldings III and IV can be composed. In other words: in order to form all forms arising by folding from a given expression, one has to apply only foldings I and II.

Proof: By the identity theorem, respectively the product theorem for matrices, taking (a) into account, one obtains

$$\begin{aligned} (\widehat{st}\sigma x) &= -t_\sigma, \qquad (\widehat{\sigma\tau} su) = -s_\tau, \\ (\widehat{st}\tau x) &= s_\tau, \qquad (\widehat{\sigma\tau} tu) = t_\sigma, \\ (stu)(\sigma\tau x) &= s_\tau + t_\sigma - u_x\, s_\tau t_\sigma. \end{aligned}$$

Thus by composing foldings I and II one obtains foldings III and IV, and this holds both when applying folding II to folding I, i.e. to the factors $(stu)u_\sigma u_\tau$, and when applying folding I to folding II, to the factors $(\sigma\tau x)s_x t_x$.

By a *form sequence*[15] we mean an initial form together with all forms that have arisen from it by folding in itself, and we denote the form sequence by the initial form. A "higher form" is to mean here any form with more folding in itself, while among the equally entitled foldings s_τ and t_σ one has to be normalized as higher. According to the law of formation of the form sequence it follows that:

1) Each form of the form sequence is linear in the symbols of the initial form.

2) The form sequence is uniquely determined for initial forms with two rows each of contragredient symbols; for initial forms with more rows of symbols it is to be uniquely normalized by distinguishing special foldings among those connected by the identity theorem.

By Theorem I, a form sequence $s_x^m t_x^n u_\sigma^\mu u_\tau^\nu$ $(m > n;\ \mu > \nu)$ can be arranged according to the following rectangular scheme:

$s_x^m t_x^n u_\sigma^\mu u_\tau^\nu$	(stu)	$(stu)^2$	$\cdots$	✻
$(\sigma\tau x)$	$t_\sigma,\ s_\tau$	$t_\sigma(stu),\ s_\tau(stu)$	$\cdots$	$\vdots$
$(\sigma\tau x)^2$	$t_\sigma(\sigma\tau x),\ s_\tau(\sigma\tau x)$	$t_\sigma^2,\ t_\sigma s_\tau,\ s_\tau^2$	$\cdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(\sigma\tau x)^\nu$	$t_\sigma(\sigma\tau x)^{\nu-1},\ s_\tau(\sigma\tau x)^{\nu-1}$	$t_\sigma^2(\sigma\tau x)^{\nu-2},\ t_\sigma s_\tau(\sigma\tau x)^{\nu-2},\ s_\tau^2(\sigma\tau x)^{\nu-2}$	$\cdots$	$\vdots$
$\vdots$	$t_\sigma(\sigma\tau x)^\nu$	$t_\sigma^2(\sigma\tau x)^{\nu-1},\ t_\sigma s_\tau(\sigma\tau x)^{\nu-1}$	$\cdots$	$\vdots$
$\vdots$	$\vdots$	$t_\sigma^2(\sigma\tau x)^\nu$	$\cdots$	$\vdots$

and the correspondingly continued lower part

	$(stu)^n$	$\cdots$	$\cdots$
✻*)	$t_\sigma(stu)^{n-1},\ s_\tau(stu)^{n-1}$	$s_\tau(stu)^n$	$\cdots$
	$t_\sigma^2(stu)^{n-2},\ t_\sigma s_\tau(stu)^{n-2},\ s_\tau^2(stu)^{n-2}$	$t_\sigma s_\tau(stu)^{n-1},\ s_\tau^2(stu)^{n-1}$	$s_\tau^2(stu)^n.$

[13] Gordan, *Math. Annalen* vol. XVII, p. 219.

[14] Cf. Gordan, *Math. Annalen* vol. V, p. 104.

[15] Cf. Clebsch, "Über eine Fundamentalaufgabe of the Invariantentheorie" (Abh. of the Gött. Ges. d. Wiss. vol. XVII): ğ 17 and end of ğ 18. The "form sequence" differs from the "properly reduced equivalent system" introduced there by the principle of ordering according to higher forms.

Here one obtains, when one moves

1) one column to the right, all forms arising by folding I from the adjacent forms,

2) one row downward, all forms arising by folding II from the forms above,

and hence all forms arising by folding.

An arbitrary form of the total form sequence, $t_\sigma^\kappa s_\tau^\lambda (stu)^\mu$ or $t_\sigma^\kappa s_\tau^\lambda (\sigma\tau x)^\nu$, forms the beginning of a new form sequence, consisting of all those forms of the rectangular scheme with $t_\sigma^\kappa s_\tau^\lambda (stu)^\mu$ or $t_\sigma^\kappa s_\tau^\lambda (\sigma\tau x)^\nu$ as left upper corner, which have the factor $t_\sigma^\kappa s_\tau^\lambda$.

Supplementary remark. Theorem I has an exception in the case where the numbers n and μ (respectively m and ν) become equal to zero, so that foldings I, II, and IV no longer exist, while folding III (respectively IV) still does. In this case we designate as the form sequence the diagonal member of the scheme:

$$\begin{array}{ccccc} s_x^m u_\tau^\nu & & & & t_x^n u_\sigma^\mu \\ & s_\tau & & t_\sigma & \\ & s_\tau^2 & & t_\sigma^2 & \\ & & \ddots & & \\ & & s_\tau^\nu & & t_\sigma^\mu . \end{array}$$

In accordance with the absence of foldings I and II, the series expansion according to polars of the form sequence in this case always reduces to the initial member; however, the theorems on reducers remain valid.

ğ 2. Series expansions according to polars of the form sequence.

For forms with n variables two kinds of series expansions have been set up explicitly[16]:

1) for forms with one row each of contragredient variables, $s_x^m u_\tau^\nu$, a series progressing by powers of u_x, whose coefficients are "normal forms";

2) for forms with two rows of cogredient variables, $s_x^m t_x^n$, an expansion according to polars of the elementary covariants (polars of the form sequence $s_x^m t_x^n$), which in the ternary case reads as follows[17]:

$$s_x^m t_x^{n-\lambda} t_y^\lambda = \sum_\varrho \frac{\binom{m}{\varrho}\binom{\lambda}{\varrho}}{\binom{m+n-\varrho+1}{\varrho}} \left[(st\widehat{xy})^\varrho s_x^{m-\varrho} t_x^{n-\varrho} \right]_{y^{\lambda-\varrho}}. \tag{I}$$

We combine the two expansions by setting up, for forms with two rows each of contragredient variables,

$$s_x^m t_x^{n-\lambda} t_y^\lambda u_\sigma^\mu u_\tau^{\nu-\kappa} v_\tau^\kappa,$$

expansions according to powers of u_x, whose coefficients are composite polars of the form sequence $s_x^m t_x^n u_\sigma^\mu u_\tau^\nu$, taken with respect to the variables x and u.

It is enough to set up the series for two contragredient rows of symbols (respectively variables), since, by combining each two rows of symbols (variables) into a single new row, forms with more rows of symbols (variables) can be reduced to this case.

In order to ensure that all forms of the form sequence contain only two rows of symbols, respectively variables, we specialize:

$$\begin{array}{ll} \text{a) } \sigma = \widehat{st}, & \text{a') } y = \widehat{uv}, \\ \text{b) } s = \widehat{\sigma\tau}, & \text{b') } v = \widehat{xy}, \end{array}$$

and carry out the expansion for the specialization a), a').

By direct transfer of expansion I one obtains composite polars for forms $(stu)^\mu s_x^m t_x^{n-\lambda} t_y^\lambda$, whereas for forms $(stu)^\mu u_\tau^{\nu-\kappa} v_\tau^\kappa s_x^m t_x^{n-\lambda} t_y^\lambda$, instead of composite polars, terms of such a kind arise whose evaluation makes

---

*) Here, and similarly in what follows, the lower part marked with an asterisk is to be set at the correspondingly marked place at the upper right of the scheme.

[16] Cf. Gordan, "Über Kombinanten," ğğ 2 and 5 (*Math. Ann.* vol. V).

[17] Cf. Study, *Methoden to the Theorie of the ternären Formen* (Teubner 1889) II. ğ 7. In distinction to the derivation there, ours gives the method for the rapid computational determination of the numerical coefficients $C_{pr\varrho}$. The Clebsch–Study expansion, upon specialization a), a'), would read

$$(stu)^\mu u_\tau^{\nu-\kappa} v_\tau^\kappa s_x^m t_x^{n-\lambda} (tuv)^\lambda = \sum_{p,r,\varrho} C_{pr\varrho} \left[s_\tau^\varrho (stu)^{\mu+r-\varrho} \right]_{\widehat{uv}^{\lambda-r+\varrho}} {}_{v^{\nu-\varrho},\, u^p,\, (vw=\widehat{xw})},$$

and therefore does not permit the simplification that occurs already in the course of our calculation, once one knows that all terms with the factor u_x are to be omitted.

necessary the introduction of ever new auxiliary variables that are to be set equal only at the end, thereby complicating the calculation unnecessarily.

We therefore take an indirect route, by representing the composite polars of all forms of the form sequence, that is, expressions

$$\left[s_\tau^\varrho (stu)^{\mu-\varrho+r}\right]_{y^\lambda}^{v^\kappa},$$

by the initial members of these polars, and by inversion of the resulting recursive system of equations obtaining the desired expansion according to polars.

By the transfer principle, for the λ-th polar of a form $s_x^m t_x^n : [s_x^m t_x^n]_{y^\lambda}$ $(\lambda \leq n)$ the following expansion holds (the case $\lambda > n$ is reduced to the first by the expansion of $[s_y^m t_y^n]_{x^{m+n-\lambda}}$)[18]:

$$\left[s_x^m t_x^n\right]_{y^\lambda} = \sum_r (-1)^r \frac{\binom{m}{r}\binom{\lambda}{r}}{\binom{m+n}{r}} (st\widehat{xy})^r s_x^{m-r} t_x^{n-\lambda} t_y^{\lambda-r},$$

and correspondingly for the κ-th polar of $u_\sigma^\mu u_\tau^\nu : [u_\sigma^\mu u_\tau^\nu]_{v^\kappa}$

$$\left[u_\sigma^\mu u_\tau^\nu\right]_{v^\kappa} = \sum_\varrho (-1)^\varrho \frac{\binom{\mu}{\varrho}\binom{\kappa}{\varrho}}{\binom{\mu+\nu}{\varrho}} (\sigma\tau\widehat{uv})^\varrho u_\sigma^{\mu-\varrho} u_\tau^{\nu-\kappa} v_\tau^{\kappa-\varrho}.$$

By multiplication it follows, with introduction of the specialization a) and a'),

$$\left[s_x^m t_x^n (stu)^\mu u_\tau^\nu\right]_{\widehat{uv}^\lambda}^{v^\kappa} = \sum_{r,\varrho} c_{r\varrho} (st\widehat{uv})^r (st\widehat{uv})^\varrho s_x^{m-r} t_x^{n-\lambda} (tuv)^{\lambda-r} (stu)^{\mu-\varrho} u_\tau^{\nu-\kappa} v_\tau^{\kappa-\varrho},$$

and from this, by expansion according to powers of u_x with the first member distinguished ($\sum'_{r,\varrho}$ means that the member $r=0$, $\varrho=0$ is to be omitted) and taking account of (a) on p. 26,

$$\begin{aligned}
&s_x^m t_x^{n-\lambda} (tuv)^\lambda (stu)^\mu u_\tau^{\nu-\kappa} v_\tau^\kappa \\
&\quad = \left[s_x^m t_x^n (stu)^\mu u_\tau^\nu\right]_{\widehat{uv}^\lambda}^{v^\kappa} \\
&\qquad - \sum_{r,\varrho}{}' c_{r\varrho}\, s_\tau^\varrho (stu)^{\mu-\varrho+r} u_\tau^{\nu-\kappa} v_\tau^{\kappa-\varrho} s_x^{m-r} t_x^{n-\lambda} (tuv)^{\lambda-r+\varrho} v_x^r \\
&\qquad + u_x \sum_\varrho \sum_{r=1}^{\lambda} c_{r\varrho}\, s_\tau^\varrho (stu)^{\mu-\varrho+r-1} (stv) u_\tau^{\nu-\kappa} v_\tau^{\kappa-\varrho} s_x^{m-r} t_x^{n-\lambda} (tuv)^{\lambda-r+\varrho} v_x^{r-1} \\
&\qquad \vdots \\
&\qquad - (-1)^\lambda u_x^\lambda \sum_\varrho c_{\lambda\varrho}\, s_\tau^\varrho (stu)^{\mu-\varrho} (stv)^\lambda u_\tau^{\nu-\kappa} v_\tau^{\kappa-\varrho} s_x^{m-\lambda} t_x^{n-\lambda} (tuv)^\varrho,
\end{aligned} \tag{II}$$

where

$$c_{r\varrho} = (-1)^{r+\varrho} \cdot \frac{\binom{m}{r}\binom{\lambda}{r}}{\binom{m+n}{r}} \cdot \frac{\binom{\mu}{\varrho}\binom{\kappa}{\varrho}}{\binom{\mu+\nu}{\varrho}} \qquad \begin{array}{l}\text{for } \lambda \leq n, \\ \kappa \leq \nu.\end{array}$$

and correspondingly for the remaining combinations of the numbers $\lambda, n; \kappa, \nu$. Thus the expression $s_x^m t_x^{n-\lambda} (tuv)^\lambda (stu)^\mu u_\tau^{\nu-\kappa} v_\tau^\kappa$ is reduced to a composite polar, and, by applying the identity

$$(stv) u_\tau = (stu) v_\tau - s_\tau (tuv),$$

to a sum of analogously formed expressions corresponding to higher forms of the form sequence.

By iteration one arrives at the expansion

$$s_x^m t_x^{n-\lambda} (tuv)^\lambda (stu)^\mu u_\tau^{\nu-\kappa} v_\tau^\kappa = \sum_{p,r,\varrho} u_x^p\, C_{pr\varrho} \cdot \left[s_\tau^\varrho (stu)^{\mu-\varrho+r}\right]_{\widehat{uv}^{\lambda-r+\varrho}\, v^{\kappa-\varrho+p},\, v_x^{r-p}}. \tag{III}$$

The numerical coefficients $C_{pr\varrho}$ are computed uniquely and recursively from the coefficients $c_{r\varrho}$, $c'_{r\varrho}$ of the system of equations arising by iteration of (II) (cf. the example on p. 42). Analogous expansions arise for the other specializations.

[18] Gordan, *The Resultante binärer Formen* (Chap. I, ğ 5). Rend. Circ. Mat. di Palermo XXII. 1906.

ğ 3. Reduction theorems.

The known theorems on the reduction of forms and form systems shall now be brought into connection with ğğ 1 and 2, for which some definitions taken over from the theory of binary forms are necessary.

a) We call a system of forms a *relatively complete system* modulo a prescribed sequence of forms if it has the property that all formations arising by folding an arbitrary product of these forms can be expressed as integral rational functions of the forms of the system, up to an additive term consisting of expressions that have arisen by folding the system forms with the system of the modulus[19].

b) We call a form *reducible* when it can be expressed by forms having invariants as factors or by "higher forms," that is, by higher forms of the total form sequence to which the form belongs, or by forms containing the symbols of the modulus in higher order.

The theorems on reducers[20] can now be stated in their most general form as follows:

Definition: *A reducer is a reducible form sequence.*

Theorem II. If the initial form of a form sequence is reducible because one of its members has arisen by folding with a reducer (has a reducer as factor), and if the final form of the form sequence has arisen from exactly this member by folding, then the total form sequence is reducible[21].

Proof: The form sequence arises from the initial member by folding in itself, hence by higher folding with the reducer on the one hand, and by folding the reducer in itself on the other hand. In both cases, by ğ 2, all forms of the form sequence can be represented as polars (transvections) over the form sequence of the reducer.

The inference from the initial form to the total form sequence no longer holds for the remaining reduction methods. These are:

1) so-called "double reduction."

By this we mean the reduction, in two different ways, of an expression that has two mutually independent reducers as factors, whereby relations arise between the higher forms to which one has reduced.

By systematic application of "double reduction" one must, on the one hand, obtain all relations[22]; on the other hand, if "double reduction" applied to different expressions supplies no new relations, one has both a criterion for the independence of the higher forms and a check on the calculation.

2) *Folding with decomposable forms.*

By "decomposable forms" are to be understood – with a slight generalization of the usual concept – forms that can be expressed by products of forms of lower degree and by "higher" forms. Products of forms pass into products under one folding; likewise products of nonlinear forms under twofold folding in the specializations a') and b') (ğ 2), according to the product theorem:

$$a_y b_y a_x b_x = \frac{1}{2} a_y^2 b_x^2 + \frac{1}{2} b_y^2 a_x^2 - \frac{1}{2}(ab\widehat{yx})^2.$$

First polars (transvections) and certain second polars of decomposable forms are therefore again decomposable forms. It follows that:

A member of a onefold (respectively twofold) transvection over a decomposable form, arising by onefold (respectively twofold) folding with a decomposable form, itself becomes a decomposable form:

a) if the next-higher forms in the form sequence of the decomposable form decompose or become reducible, or also if, under onefold folding, the specializations $y = \widehat{uv}$ or $v = \widehat{xy}$ occur;

b) if the remaining onefold foldings lead to higher forms (cf. ğ 12, B. H_k and $H_k(k\eta x)$).

Such a member of a transvection can also decompose:

c) if the remaining onefold foldings lead to lower forms that decompose independently of the folding with the decomposable form, that is, that can be expressed by products and by the form to be reduced, although

---

[19] Gordan–Kerschensteiner, *Vorlesungen über Invariantentheorie.* Vol. II. p. 227.

[20] Gordan, *Math. Annalen* vol. XVII, p. 222.

[21] The simplification that results from Theorem II can be seen in the following example. For the special form $f = x_1^3 x_2 + x_2^3 x_3 + x_3^3 x_1$, $a_y^2 a_x^2 u_y^2$ is a reducer. It follows by Theorem II that the form sequence

$$\theta_\nu(\vartheta\nu x)\theta_x^3 u_\vartheta u_\nu^2 = a_\nu^2(abu) - a_\nu b_\nu(aba),$$

is reduced, since $\theta_\nu^4 = a_\nu^2 b_\nu^2 (abu)^2$ has arisen from the member $a_\nu^2(abu)$ by folding. In Gordan, loc. cit., p. 231, by contrast, the reduction of the forms

$$\theta_\nu(\vartheta\nu x), \quad \theta_\nu(\vartheta\nu x)^2, \quad \theta_\nu^2, \quad \theta_\nu^2(\vartheta\nu x), \quad \theta_\nu^2(\vartheta\nu x)^2$$

is carried out individually.

[22] Thus, for example, the following were foand by "double reduction": the reduction of the form a_η^4 (ğ 10), the only form included superfluously in Maisano's system; and also the relations mentioned in the note to the Introduction between the three covariants and the three invariants.

in each case one must first verify by calculation that the numerical coefficient of the member concerned does not vanish identically. This is nothing other than "double reduction" of the lower form (cf. ğ 23, C. $H_q(\theta Hu)(\theta su)$).

Decomposable forms arise by all onefold foldings with functional determinants[23], and moreover by certain higher foldings. One has

$$(st\widehat{yx})s_y = \frac{1}{2}\,t\,s_y^2 - \frac{1}{2}\,s\,t_y^2 + \frac{1}{2}(st\widehat{yx})^2,$$

$$(st\widehat{yx})^2 s_y^2 = \frac{1}{3}\,t\,s_y^3 - \frac{1}{3}\,s\,t_y^3 + s_y(st\widehat{yx})^2 - \frac{1}{3}(st\widehat{yx})^3.$$

Analogous formulas hold for the dualistic forms

$$(\sigma\tau\widehat{\nu u})v_\sigma \quad \text{and} \quad (\sigma\tau\widehat{\nu u})v_\sigma^2.$$

From the theorems of this section the following rule follows for setting up all irreducible forms that arise from the folding of S with T:

Beginning with the lowest foldings, proceed along any previously fixed path (for example row by row, or symmetrically with respect to the diagonal member) in the formation of the form sequence ST until one reaches a form that has a reducer as factor. The form sequence defined by this form is to be omitted as soon as the final form satisfies the condition stated in Theorem II. After all reducible form sequences have been eliminated, all remaining reducible forms, and likewise all decomposable forms, are to be removed by applying double reduction. Places in the total form sequence that are covered twice by independently reducible form sequences give rise to the reduction of higher forms (cf. ğ 11, D).

[23] cf. Gordan, loc. cit. ğ 3.

Theorem III. *The forms taken over from the binary domain, that is, those forms which arise from the system forms of the corresponding binary form by bordering according to Clebsch's transfer principle, form a relatively complete system modulo* (abc).

Proof. To a binary relation asserting that the forms $Q'_1, \ldots, Q'_n$ form a complete system of a binary ground form,

$$Q' - F(Q') = 0 = \sum_{\lambda} \{(ab)c_x + (bc)a_x + (ca)b_x\}\varphi^*_\lambda,$$

there corresponds, by bordering, the ternary relation

$$Q - F(Q_i) = \sum_{\lambda} u_x \cdot (abc)\varphi_\lambda.$$

This is precisely the defining equation for a relatively complete system modulo (abc). For the biquadratic form, the system of the forms taken over consists of the following forms:

$$f = a_x^4, \qquad \theta = \theta_x^4 u_\vartheta^2 = (abu)^2 a_x^2 b_x^2, \qquad K = K_x^6 u_k^3 = (a\theta u) u_\vartheta^2 a_x^3 \theta_x^3,$$
$$j = u_j^6 = (a\theta u)^4 u_\vartheta^2, \qquad \nu = u_\nu^4 = (abu)^4,$$

among which the first four form a relatively complete system modulo $((abc), \nu)$.

ğ 5. Reduction of the modulus (abc) to the moduli Δ and ν.

The modulus (abc), given only by a bracket factor, is to be reduced, in agreement with the definition (ğ 3, a), to forms of the system. In other words, the form sequence (abc) is to be normalized uniquely (cf. ğ 1).

$$a_s^2 a_x u_x = \frac{1}{3} a_s^3 u_x = \frac{1}{3} S \cdot u_x. \tag{2}$$

$$\left.\begin{aligned} (a\Delta u)^2 &= a_s - \frac{S}{6} u_x^2, \\ (a\Delta u)^3 &= 0. \end{aligned}\right\} \tag{3}$$

$$\left.\begin{aligned} \theta(s) = (ss, x)^2 &= 2a_t + \frac{1}{3} S \cdot \theta - \frac{1}{3} T u_x^2, \\ \theta(t) = (tt, x)^2 &= -\frac{1}{3} S \cdot a_t + \frac{2}{3} T \cdot a_s + \frac{1}{18} S^2 \cdot \theta - \frac{1}{18} u_x^2 \cdot S \cdot T. \end{aligned}\right\} \tag{4}$$

Sequence of moduli: (abc); Δ; s; t (the system of the modulus t consists of the single form t).[24]

It will be shown that the forms

$$\Delta = (abc)^2 a_x^2 b_x^2 c_x^2, \qquad \nu = (abu)^4$$

suffice as moduli, that is, that the forms

$$\Delta = (abc)^2 a_x^2 b_x^2 c_x^2, \qquad a_\nu = (abc)(bcu)^3 a_x^3,$$
$$a_\nu^2 = (abc)^2 (bcu)^2 u_x^2, \qquad i = a_\nu^4 = (abc)^4$$

define the form sequence (abc). In the form sequence a_ν, the form a_ν^3 is missing according to the identity

$$a_\nu^3 = (abc)^3 a_x (bcu) = \frac{1}{3} u_x \cdot (abc)^4 = \frac{1}{3} i \cdot u_x.$$

For reducing a modulus to a higher one, according to the definition, we have to reduce the most general foldings, or all special foldings coming into consideration, with the modulus to foldings with the higher modulus.

In the present case the most general foldings arise from the expressions

$$(abc) a_x^3 b_y^3 c_z^3, \qquad (abc) a_x^2 b_y^2 c_z^2 a_z b_x c_x$$

(taken over from the cubic forms),

$$(abc) a_x b_y c_z a_x^2 b_x^2 c_x^2$$

[24] Gordan–Kerschensteiner, loc. cit., p. 134.

(taken over from the quadratic forms), and from the polarisation of these expressions.

For the calculation of these expressions by the polars of Δ and of the form sequence a_ν, respectively of their initial terms, we take the indirect route, as in ğ 2. We expand the polar terms

$$(abc)^2 a_x^2 b_y^2 c_z^2, \qquad a_\nu(\nu xy)(\nu yz)(\nu zx)a_x a_y a_z = (abc)(bc\widehat{x}u)(bc\widehat{y}z)(bc\widehat{z}x)a_x a_y a_z \quad \text{etc.}$$

as linear aggregates of expressions with the symbolic factor (abc) and obtain, by inverting the system of equations, the desired relations, as well as a relation between the polars taken according to different combinations of the variables. The identity theorem and the product theorem for determinants are used in the evaluation.

The system of equations is, for $(abc)a_x^3 b_y^3 c_z^3$:

$$1) \quad \sum_3 a_\nu(\nu yz)^3 a_x^3 = 6(abc)a_x^3 b_y^3 c_z^3 - 6\sum_3 (abc)a_x^3 b_y^2 b_z c_z^2 c_y^*,$$

$$2) \quad 3(abc)^2 a_x^2 b_y^2 c_z^2 \cdot (xyz) - \frac{1}{2}\sum_3 a_\nu^2(\nu yz)^2 \nu_x^2 (xyz) = 2\sum_3 (abc)a_x^3 b_y^2 b_z c_z^2 c_y - 4\sum_3 (abc)a_x a_y a_z b_y^2 b_z c_z^2 c_x,$$

$$3) \quad a_\nu(\nu xy)(\nu yz)(\nu zx)a_x a_y a_z = 2\sum_3 (abc)a_x a_y a_z b_y^2 b_z c_z^2 c_x,$$

$$4) \quad \sum_3 a_\nu(\nu yz)^3 u_x^3 - \frac{3}{2}\sum_3 a_\nu^2(\nu yz)^2 \nu_x^2(xyz) + \frac{1}{6} i\cdot(xyz)^3 = 6\sum_3 (abc)a_x a_y a_z b_y^2 b_z c_z^2 c_x.$$

It follows for

$$(abc)a_x^3 b_y^3 c_z^3,$$

and by analogous calculation for

$$(abc)a_x^2 b_y^2 c_z^2 a_z b_x c_x, \qquad (abc)a_x b_y c_z a_z^2 b_x^2 c_x^2 :$$

$$(abc)a_x^3 b_y^3 c_z^3 = \frac{3}{2}(abc)^2 a_x^2 b_y^2 c_z^2 (xyz) + \frac{3}{2}a_\nu(\nu xy)(\nu yz)(\nu zx)a_x a_y a_z - \frac{1}{12} i\cdot(xyz)^3,$$

$$\text{(IV.)} \quad (abc)a_x^2 b_y^2 c_z^2 a_z b_x c_x = \frac{2}{3}(abc)^2 a_x^2 b_y^2 c_z^2 c_x \cdot (xyz) + \frac{1}{3}a_\nu(\nu xy)(\nu yz)(\nu zx)a_x^3 - \frac{1}{6}a_\nu^2(\nu xy)(\nu zx)a_x^2 \cdot (xyz),$$

$$(abc)a_x b_y c_z a_z^2 b_x^2 c_x^2 = \frac{1}{6}(abc)^2 a_x^2 b_z^2 c_z^2 \cdot (xyz).$$

We have therefore obtained a relatively complete system modulo (Δ, ν), consisting of the four forms f, θ, K, j. It follows from this that all transvections of f over θ not taken over from the binary domain, as well as the transvection $(a\theta u)^2$ reducible in the binary case to $(ab)^4$, can be expressed by the symbols Δ and ν.[25]

We obtain the reduction formulas fundamental for what follows by specializing expansion IV, or more shortly by direct calculation (interchanging the symbols), for $a_\vartheta(a\theta u)^2$, $a_\vartheta^2((a\theta u)^2$, $(a\theta u)^2$, according to the following ansatz:

$$a_\vartheta(a\theta u)^2 = (abc)(bcu)(abu)^2 - \frac{1}{3}(abc)(bcu)\{(bcu)a_x - u_x(abc)\}^2,$$

$$a_\vartheta^2(a\theta u)^2 = (abc)^2(abu)^2 - \frac{1}{3}(abc)^2\{(bcu)a_x - u_x(abc)\}^2,$$

for $((a\theta u)^2)^*$:

$$(abu)a_y^3 b_x^3 = \frac{3}{2}u_\vartheta(\vartheta yx)\theta_y^2 + \frac{1}{4}(\nu yx)^3,$$

$$((abu)(acu))b_x^3 = \frac{3}{2}u_\vartheta(\vartheta\widehat{a}ux)(\theta au)^2 + \frac{1}{4}(\nu\widehat{a}ux)^3.$$

[25] $\sum_3$ refers to the sum of three terms obtained from the initial term by cyclic interchange of the variables. The equations also hold individually for each term of the sum.

$$\left.\begin{aligned}
(a\theta u)^2 &= \frac{1}{6}\nu\cdot f - \frac{2}{3}u_x\cdot a_\nu + \frac{2}{3}u_x^2\cdot a_\nu^2 - \frac{i}{18}u_x^4,\\
a_\vartheta &= \frac{1}{3}u_x\cdot\Delta,\\
a_\vartheta(a\theta u) &= 0,\\
a_\vartheta^2 &= \Delta,\\
(a\theta u)^3 &= 0,\\
a_\vartheta(a\theta u)^2 &= -\frac{5}{6}a_\nu + \frac{7}{6}u_x\cdot a_\nu^2 - \frac{i}{9}u_x^3,\\
a_\vartheta^2(a\theta u) &= 0,\\
(a\theta u)^4 &= j,\\
a_\vartheta(a\theta u)^3 &= 0,\\
a_\vartheta^2(a\theta u)^2 &= \frac{2}{3}a_\nu^2 - \frac{i}{9}u_x^2.
\end{aligned}\right\} \tag{1}$$

We add the formula, likewise obtained from the reduction of the modulus (abc):

$$a_\nu^3 a_x u_\nu = \frac{1}{3}i\cdot u_x. \tag{2}$$

From formulas (1.) and (2.) and from the formulas formed analogously for the ground form ν, all later reduction formulas are derived by polarisation, except for the relations for the decomposed forms. From formulas (1.) we see:

The form sequence leads:

$$\begin{aligned}
a_\vartheta(a\theta u)^2 &\quad\text{to}\quad \text{symbols } \nu \text{ alone},\\
a_\vartheta &\quad\text{to}\quad \text{symbols } \Delta \text{ and } \nu,\\
(a\theta u)^2 &\quad\text{to}\quad \text{symbols } j, \Delta \text{ and } \nu,\\
(a\theta u)^2 \text{ under folding I} &\quad\text{to}\quad \text{symbols } j \text{ and } \nu,\\
(a\theta u)^2 \text{ under folding II} &\quad\text{to}\quad \text{symbols } \Delta \text{ and } \nu.
\end{aligned}$$

We can therefore replace:

1. modulo (Δ,ν): foldings with j are replaced by corresponding foldings with $(a\theta u)^2$ or $(a\theta u)^3$;
2. modulo (ν): foldings with Δ are replaced by corresponding foldings with a_ϑ or $a_\vartheta(a\theta u)$, or also by special foldings with $(a\theta u)^2$ (which lead only to a single folding I).

In particular:

$$\begin{aligned}
(a\theta u)^2\theta_y^2\theta_x^2 &= \frac{1}{3}(jyx)^2 \pmod\nu, & (a\theta u)^2 u_y\theta_y &= -\frac{1}{6}(jyx)^2 \pmod\nu,\\
(a\theta u)^2\nu_y^2 &= \frac{1}{3}(\Delta u\nu)^2 \pmod\nu, & (a\theta u)(a\theta\nu)u_\vartheta\nu_\vartheta &= -\frac{1}{6}(\Delta u\nu)^2 \pmod\nu,\\
(a\theta u)^2 u_\nu^2\vartheta_\nu^2 &= \frac{1}{3}(\Delta u\nu)^2\Delta_\nu \pmod\nu.
\end{aligned}$$

ğ 6. Reduction of the modulus (Δ,ν) to the modulus (ν).

The reduction formulas of the preceding paragraph give us the means to set up the relatively complete system modulo ν directly; we shall see that to the system of the transferred forms one has only to add the forms Δ and $(a\Delta u) = N$ (analogously as for the cubic form, and indeed valid in general).

For the reduction of the modulus Δ we consider all special foldings coming into consideration, that is, the foldings of the relatively complete system modulo (Δ,ν) with the system of Δ, and begin with the forms lowest in the coefficients, the foldings of f with Δ.

For the reduction of the forms $(a\Delta u)^2$, $(a\Delta u)^3$, $(a\Delta u)^4$, we replace the symbols Δ by lower forms of the form sequence according to ğ 5; that is, we develop the expressions

$$a_\vartheta b_\vartheta(b\theta u)^2, \qquad a_\vartheta(a\theta u)b_\vartheta(b\theta u)^2, \qquad a_\vartheta(a\theta u)b_\vartheta(b\theta u)^3$$

1) by polars of the form sequence a_ϑ (symbols Δ and ν),

2) by polars of the form sequence $b_\vartheta(b\theta u)^2$ (symbols ν),

and obtain the reduction formulas (calculation below):

$$\begin{aligned}
&\text{a)} \quad (a\Delta u)^2 = \frac{1}{2}(\vartheta\nu x)^2 - \frac{2}{5}f\cdot a_\nu^2 - \frac{4}{5}u_x\cdot\theta_\nu(\vartheta\nu x)^2 \\
&\qquad\qquad + u_x^2\left\{\frac{1}{6}i\cdot f - \frac{1}{40}S\right\}, \\
&\text{b)} \quad (a\Delta u)^3 = -\frac{3}{10}\theta_\nu(\vartheta\nu x), \\
&\text{c)} \quad (a\Delta u)^4 = \frac{21}{10}\theta_\nu^2 - \frac{3}{10}\Pi - \frac{6}{5}u_x\cdot\theta_\nu^3 + \frac{1}{10}u_x^2\cdot\theta.
\end{aligned} \tag{3}$$

(The same results are also reached by the double reduction of the expressions $a_\vartheta^2(b\theta u)^2$, $a_\vartheta^2(b\theta u)^3$, $a_\vartheta^2((a\theta u)^2(b\theta u)^2$ and $a_\vartheta^2((a\theta u)(b\theta u))^3$ after elimination of a_ϑ^2.)

From formulas (3.) it follows that $(a\Delta u)^2$ is a reducer with respect to the modulus ν. Hence:

1) The reduction of the system of Δ: the form sequence $(\Delta\Delta' u)^2 = a_\vartheta^2((a\Delta u)^2$ has the reducer $(a\Delta u)^2$ as a factor.

2) The reduction of the system arising by folding with the modulus Δ:

The form sequence $(\theta\Delta u)^2$ has the reducer $(a\Delta u)^2$ as a factor.

For the forms $(\theta\Delta u)$ and Δ_ϑ one obtains:

$$(a\Delta u)^2(abu) = (\theta\Delta u) - u_x\cdot\Delta_\vartheta(\theta\Delta u),$$

$$(a\Delta u)(a\Delta b) = -\frac{1}{2}\Delta_\vartheta + \frac{1}{2}u_x\cdot\Delta_\vartheta^2.$$

From the reducer $(\theta\Delta u)$, however, follows the reduction of the system arising by folding with the modulus Δ.

The relatively complete system modulo ν therefore consists of the six forms:

$$f,\ \theta,\ K,\ j,\ \Delta,\ N.$$

As an example of the sequence expansion in § 2 we give the derivation of formula (3.)a in full; in later calculations the final formula III will be set down directly. (Polars of vanishing forms have already been omitted during the calculation; the first line gives the values inserted according to Expansion II, and the second line gives the final values found recursively, beginning with the last equation of the system.) It follows, according to Expansion II:

$$\begin{aligned}
&1) \quad m=3, \quad n=4, \quad \lambda=2, \quad \mu=0, \quad \nu=\chi=1, \\
a_\vartheta b_\vartheta(b\theta u)^2 &= [a_\vartheta]_{b^2}b + \frac{6}{7}\{a_\vartheta b_\vartheta(a\theta u)(b\theta u) - u_x a_\vartheta b_\vartheta(a\theta b)(b\theta u)\} \\
&\quad - \frac{1}{7}\{a_\vartheta(a\theta u)^2 b_\vartheta - 2u_x a_\vartheta(a\theta u)(a\theta b)b_\vartheta + u_x^2 a_\vartheta(a\theta b)^2 b_\vartheta\} \\
&= \frac{2}{3}(a\Delta u)^2 + \frac{1}{5}[a_\vartheta(a\theta u)^2]b + \frac{1}{30}f[a_\vartheta^2(a\theta u)^2] - \frac{2}{5}u_x[a_\vartheta(a\theta u)^2]b^2 \\
&\quad - \frac{1}{15}u_x[a_\vartheta^2(a\theta u)^2]b + \frac{1}{5}u_x^2[a_\vartheta(a\theta u)^2]b^3 + \frac{1}{30}u_x^2[a_\vartheta^2(a\theta u)^2]b^2; \\
&2) \quad m=2, \quad n=3, \quad \lambda=1, \quad \mu=1, \quad \nu=\chi=1, \\
a_\vartheta(a\theta u)b_\vartheta(b\theta u) &= \frac{2}{5}\{a_\vartheta(a\theta u)^2 b_\vartheta - u_x a_\vartheta(a\theta u)(a\theta b)b_\vartheta\} + \frac{1}{2}a_\vartheta^2(b\theta u)^2 \\
&\quad - \frac{1}{5}\{a_\vartheta^2(b\theta u)(a\theta u) - u_x a_\vartheta^2(a\theta b)(b\theta u)\} \\
&= \frac{1}{2}(a\Delta u)^2 + \frac{2}{5}[a_\vartheta(a\theta u)^2]b + \frac{1}{15}[a_\vartheta^2(a\theta u)^2]f \\
&\quad - \frac{2}{5}u_x[a_\vartheta(a\theta u)^2]b^2 - \frac{1}{10}u_x[a_\vartheta^2(a\theta u)^2]b + \frac{1}{30}u_x^2[a_\vartheta^2(a\theta u)^2]b^2;
\end{aligned}$$

$$3)\quad m=2,\quad n=3,\quad \lambda=1,\quad \mu=1,\quad \nu=1,\quad \chi=2,$$

$$\begin{aligned}a_\vartheta(a\theta b)b_\vartheta(b\theta u) &= \frac{2}{5}\{a_\vartheta(a\theta b)(a\theta u)b_\vartheta - u_x a_\vartheta(a\theta b)^2 b_\vartheta\}\\ &= \frac{2}{5}[a_\vartheta(a\theta u)^2]b^2 + \frac{1}{30}[a_\vartheta^2(a\theta u)^2]b - \frac{2}{5}u_x[a_\vartheta(a\theta u)^2]b^3 - \frac{1}{30}u_x[a_\vartheta^2(a\theta u)^2]b^2;\end{aligned}$$

$$4)\quad m=1,\quad n=2,\quad \lambda=0,\quad \mu=2,\quad \nu=\chi=1,$$

$$\begin{aligned}a_\vartheta(a\theta u)^2 b_\vartheta &= [a_\vartheta(a\theta u)^2]b + \frac{2}{3}a_\vartheta^2(a\theta u)(b\theta u)\\ &= [a_\vartheta(a\theta u)^2]b + \frac{1}{6}[a_\vartheta^2(a\theta u)^2]f - \frac{1}{6}u_x[a_\vartheta^2(a\theta u)^2]b;\end{aligned}$$

$$5)\quad m=1,\quad n=2,\quad \lambda=0,\quad \mu=2,\quad \nu=1,\quad \chi=2,$$

$$\begin{aligned}a_\vartheta(a\theta u)(a\theta b)b_\vartheta &= [a_\vartheta(a\theta u)^2]b^2 + \frac{1}{3}a_\vartheta^2(a\theta b)(b\theta u)\\ &= [a_\vartheta(a\theta u)^2]b^2 + \frac{1}{12}[a_\vartheta^2(a\theta u)^2]b - \frac{1}{12}u_x[a_\vartheta^2(a\theta u)^2]b^2;\end{aligned}$$

$$6)\quad m=1,\quad n=2,\quad \lambda=0,\quad \mu=2,\quad \nu=1,\quad \chi=3,$$

$$a_\vartheta(a\theta b)^2 b_\vartheta = [a_\vartheta(a\theta u)^2]b^3;$$

$$7)\quad m=2,\quad n=4,\quad \lambda=2,\quad \mu=\nu=\chi=0,\quad \text{(according to Expansion I)},$$

$$a_\vartheta^2(b\theta u)^2 = [a_\vartheta^2]_{ub^2} + \frac{1}{10}\{[a_\vartheta^2(a\theta u)^2]f - 2u_x[a_\vartheta^2(a\theta u)^2]b + u_x^2[a_\vartheta^2(a\theta u)^2]b^2\};$$

$$8)\quad m=1,\quad n=3,\quad \lambda=1,\quad \mu=1,\quad \nu=\chi=0,\quad \text{(Expansion I)},$$

$$a_\vartheta^2(a\theta u)(b\theta u) = \frac{1}{4}[a_\vartheta^2(a\theta u)^2]f - \frac{1}{4}u_x[a_\vartheta^2(a\theta u)^2]b;$$

$$9)\quad m=1,\quad n=3,\quad \lambda=1,\quad \mu=\chi=1,\quad \nu=0,\quad \text{(Expansion I)},$$

$$a_\vartheta^2(a\theta b)(b\theta u) = \frac{1}{4}[a_\vartheta^2(a\theta u)^2]b - \frac{1}{4}u_x[a_\vartheta^2(a\theta u)^2]b^2.$$

From 1) and 4) it follows:

$$\begin{aligned}(a\Delta u)^2 &= \frac{6}{5}[a_\vartheta(a\theta u)^2]b + \frac{1}{5}f[a_\vartheta^2(a\theta u)^2] + \frac{3}{5}u_x[a_\vartheta(a\theta u)^2]b^2 - \frac{3}{20}u_x[a_\vartheta^2(a\theta u)^2]b\\ &\quad - \frac{3}{10}u_x^2[a_\vartheta(a\theta u)^2]b^3 - \frac{1}{20}u_x^2[a_\vartheta^2(a\theta u)^2]b^2,\\ (a\Delta u)^2 &= -a_\nu b_\nu + \frac{3}{5}fa_\nu^2 + \frac{4}{5}u_x a_\nu^2 b_\nu - \frac{3}{20}u_x^2 a_\nu^2 b_\nu^2 - \frac{1}{12}u_x^2 if.\end{aligned}$$

(For conversion into the symbols θ cf. § 8 and § 9.) Formula (3.)a can be computed still more briefly by direct transfer of Expansion I, introducing the auxiliary variable $w = x\widehat{u}b$ whereas already for formulas (3.)b and (3.)c the path taken here becomes the simpler one; for (3.)b one knows in advance, by § 9, that all terms with factor u_x are to be omitted. For the calculation of (3.)b and (3.)c one obtains:

$$(3.)\text{b})\quad 1)\quad a_\vartheta(a\theta u)b_\vartheta(b\theta u)^2 = \frac{1}{2}(a\Delta u)^3 + \frac{4}{5}[a_\vartheta(a\theta u)^2]_{ub}b + \frac{7}{360}[a_\vartheta^2(a\theta u)^2]_{ub^2},$$

$$2)\quad a_\vartheta(a\theta u)b_\vartheta(b\theta u)^2 = [a_\vartheta(a\theta u)^2]_{ub}b + \frac{13}{36}[a_\vartheta^2(a\theta u)^2]_{ub^2};$$

$$\begin{aligned}(3.)\text{c})\quad 1)\quad a_\vartheta(a\theta u)b_\vartheta(b\theta u)^3 &= \frac{1}{2}(a\Delta u)^4 + \frac{6}{5}[a_\vartheta(a\theta u)^2]_{ub^2}b + \frac{53}{120}[a_\vartheta^2(a\theta u)^2]_{ub^3}\\ &\quad - \frac{6}{5}u_x[a_\vartheta(a\theta u)^2]_{ub^3}b^2 - \frac{3}{5}u_x[a_\vartheta^2(a\theta u)^2]_{ub^2}b + \frac{19}{120}u_x^2[a_\vartheta^2(a\theta u)^2]_{ub^3}b^2,\end{aligned}$$

$$2)\quad a_\vartheta(a\theta u)b_\vartheta(b\theta u)^3 = \frac{3}{4}[a_\vartheta^2(a\theta u)^2]_{ub^2}.$$

Supplementary remark: the transvectants of f over j that are reducible according to § 5 are computed

analogously. One obtains

$$g_\nu = -\theta_\nu + u_x\left(\frac{9}{2}\theta_\nu^2 - \frac{1}{2}H\right) - 3u_x^2\theta_\nu^3 + \frac{1}{2}u_x^3\theta,$$
$$g_\nu^2 = \frac{21}{10}\theta_\nu^2 - \frac{3}{10}H - 2u_x\theta_\nu^3 + \frac{1}{2}u_x^2\theta, \tag{4}$$
$$g_\nu^3 = -\frac{7}{10}\theta_\nu^3 + \frac{1}{2}u_x^2\theta, \qquad g_\nu^4 = \frac{3}{5}\theta.$$

$$g_\nu^3 = -\frac{7}{10}\theta_\nu^3 + \frac{1}{2}u_x^2\theta, \qquad g_\nu^4 = \frac{3}{5}\theta. \tag{4}$$

From (3.) and (4.) it follows, by transfer from the binary domain, that

$$(\theta\theta' u)^2 = \frac{1}{3}\, j \cdot f \pmod{\nu}.^{26}$$

The remaining forms of the form sequence $(\theta\theta' u)^2$ and the form θ'_ν are reducible to symbols ν. We can therefore replace:

$$\text{mod } \nu: \quad \text{foldings with } f \cdot j \text{ by the corresponding foldings with } (\theta\theta' u)^2.$$

Furthermore,

$$(\vartheta\vartheta' x)^2 = \frac{4}{3} f \cdot \Delta, \qquad \theta_{g\nu}(\vartheta\vartheta' x) = -N.$$

Chapter III. The relatively complete system modulo (s, ϱ, t).

§ 7. Overview of the formation of the system.

In order to pass from the relatively complete system modulo ν to the relatively complete system with the next higher modulus, one has, by Definition § 3, to form the system of ν with respect to this higher modulus and to fold it with the forms of the relatively complete system modulo ν. But $\nu = u_\nu^4$, as a contravariant of the fourth degree, is dual to the form f. If therefore we regard ν as the ground form, we obtain a relatively complete system of six forms modulo $\nu(\nu) = (\nu\nu_1 x)^4 = s_x^4$.

Thus, for the formation of the relatively complete system modulo s (System III), we have to transvect

System I: $f,\ \theta,\ K,\ j,\ \Delta,\ N$ over
System II: $\nu,\ H = (\nu\nu_1 x)^2 u_\nu^2 u_{\nu_1}^2,\ L = (\nu\eta x) H_x^2 u_\nu^3 u_\eta^3,$
$g = (\nu\eta x)^4 H_x^2,\ \sigma = H_\eta^2 u_\nu^2 u_\eta^4,\ (\nu\sigma x).$

It will be shown (formula (13.)) that the form g is reducible, and hence that System II consists of only five forms.

In the course of the calculation the quadratic forms

$$\varrho = u_\varrho^2 = \theta_\nu^4 u_\vartheta^2, \qquad t = t_x^2 = a_\eta^4 H_x^2$$

are adjoined as moduli, so that one obtains a relatively complete system modulo (s, ϱ, t); and the modulus (ϱ, t) is to be regarded as a higher modulus than the modulus s.

The arrangement of the individual forms is to follow the order in the coefficients. We normalize the folding

$$\theta_\nu(K_\nu, \theta_\nu, \ldots)$$

as higher than the folding

$$H_y(H_y, L_y, \ldots).$$

Consequently, by § 1 and § 3b, the order of the individual forms of the same order is uniquely determined.

The formation of the forms of the same order is carried out in tabular form:

I. Indication of which forms of Systems I and II are to be folded with each other in order to obtain the prescribed order in the coefficients.

[26] Gordan–Kerschensteiner, loc. cit., p. 181.

II. Listing of the irreducible forms according to the scheme of the form sequence.

III. Reduction of the reducible or decomposable form sequences or forms, that is, of those places where the total form sequence breaks off, thereby proving that all irreducible constructions have been exhausted by those indicated.

IV. Consequences: 1) indication of newly arising reducers; 2) indication of those forms which do not enter, in products with forms of the same system, into folding with forms of the other system.

It will be shown that only the following occur:

1) foldings of one form of System I with one form of System II;

2) foldings of powers of θ, respectively H, or of two forms of one system with one form of the second system.

We shall obtain the following scheme for folding:

System I	folded with	System II
1. order f		2. order ν
2. ,, θ		4. ,, H
3. ,, K, j, Δ		6. ,, L, σ
4. ,, $N, \theta^2, f \cdot j$		8. ,, $(\nu\sigma x), H^2$
5. ,, $\theta \cdot K$		10. ,, $H \cdot L$
6. ,, $\theta^3, \Delta \cdot j$		12. ,, H^3.

For checking the calculation, besides the "double reduction", the two special forms serve:

$$\text{I.}\quad \begin{array}{llllll} f &= \sum x_1^3 x_2, & u_\nu^2 &= \frac{i}{6}u_x^2, & s &= \frac{i}{3}f, \\ a_\eta^2 &= -\frac{1}{3}i\theta, & H_\nu^2 &= \frac{i}{6}\theta, & \sigma &= -\frac{i}{6}j, \\ g &= -\frac{2}{3}i\Delta, & \varrho &= 0, & t &= 0, \end{array}$$

$$\text{II.}\quad \begin{array}{llllll} f &= \sum x_1^4, & s &= \frac{4}{3}if, & a_\eta^2 &= \frac{2}{9}i\theta, \\ \Delta_\nu^2 &= \frac{1}{15}i\theta, & \sigma &= \frac{4}{3}ij, & g &= \frac{4}{3}i\Delta, \\ \varrho &= 0, & t &= 0. \end{array}$$

Supplementary remark: for the ground form ν, formulas (1.), (2.), (3.), (4.) correspond to the following:

$$\begin{array}{c|c|c} (\nu\eta x)^2 = A & H_\nu(\nu\eta x) = 0 & H_\nu^2 = \sigma \\ (\nu\eta x)^3 = 0 & H_\nu(\nu\eta x)^2 = B & H_\nu^2(\nu\eta x) = 0 \\ (\nu\eta x)^4 = g & H_\nu(\nu\eta x)^3 = 0 & H_\nu^2(\nu\eta x)^2 = C, \end{array} \tag{5}$$

$$A = \frac{1}{6}s\nu - \frac{2}{3}u_x s_\nu + \frac{2}{3}u_x^2 s_\nu^2 - \frac{J}{18}u_x^4, \quad B = -\frac{5}{6}s_\nu + \frac{7}{6}u_x s_\nu^2 - \frac{J}{9}u_x^3, \quad C = \frac{2}{3}s_\nu^2 - \frac{J}{9}u_x^2.$$

$$s_\nu^3 u_x s_\nu = \frac{1}{3}u_x s_\nu^4 = \frac{1}{3}Ju_x. \tag{6}$$

$$\begin{aligned} &\text{a)}\quad (\nu\sigma x)^2 = \frac{1}{2}(Hsu)^2 - \frac{2}{5}\nu \cdot s_\nu^2 - \frac{4}{5}u_x\, s_\eta (Hsu)^2 + u_x^2 \left\{ \frac{1}{6}J \cdot \nu - \frac{1}{40}(ss'u)^4 \right\}, \\ &\text{b)}\quad (\nu\sigma x)^3 = -\frac{3}{10}s_\eta (Hsu), \\ &\text{c)}\quad (\nu\sigma x)^4 = \frac{21}{10}s_\eta^2 - \frac{3}{10}Z - \frac{6}{5}u_x s_\eta^3 + \frac{1}{10}u_x^2 s_\eta^4. \end{aligned} \tag{7}$$

$$\begin{aligned} &\text{a)}\quad g_\nu = -s_\eta + u_x\left(\frac{9}{2}s_\eta^2 - \frac{1}{2}Z\right) - 3u_x^2 s_\eta^3 + \frac{1}{2}u_x^3 s_\eta^4, \\ &\text{b)}\quad g_\nu^2 = \frac{21}{10}s_\eta^2 - \frac{3}{10}Z - 2u_x s_\eta^3 + \frac{1}{2}u_x^2 s_\eta^4, \\ &\text{c)}\quad g_\nu^3 = -\frac{7}{10}s_\eta^3 + \frac{1}{2}u_x s_\eta^4, \\ &\text{d)}\quad g_\nu^4 = \frac{3}{5}s_\eta^4. \end{aligned} \tag{8}$$

§ 8. Forms of the third order (System III).

Folding of f with ν.
Irreducible forms:

$$\begin{matrix} a_\nu & \cdot & \cdot & \cdot \\ \cdot & a_\nu^2 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & a_\nu^4 = i. \end{matrix}$$

Reduction:

$$a_\nu^3 = \frac{1}{3} i u_x \qquad \text{(formula (2.))}.$$

Consequences: 1) a_ν^3 is a reducer. 2) f enters into folding with ν only in products with contragredient forms (j). The same holds for ν with respect to f.

§ 9. Forms of the fourth order (System III).

Folding of θ with ν.
Irreducible forms:

$$\begin{matrix} (\theta\nu x) & \theta_\nu & \cdot & \cdot \\ (\theta\nu x)^2 & \theta_\nu(\theta\nu x) & \theta_\nu^2 & \cdot \\ \cdot & \theta_\nu(\theta\nu x)^2 & \cdot & \theta_\nu^3. \end{matrix}$$

reductions: From the reducer a_ν^3, by double reduction of the expressions $a_\nu^3(abu)$, $a_\nu^3 b_\nu$, $a_\nu^3 b_\nu(abu)$ according to the ansatz:

$$\begin{aligned} \theta_\nu^2(\vartheta\nu x) &= a_\nu^2(\widehat{a}b\nu x)(abu) - \frac{1}{3}(\nu\nu_1 x)^3 = a_\nu b_\nu(\widehat{a}b\nu x)(abu) + \frac{1}{6}(\nu\nu_1 x)^3 \\ &= a_\nu^3(abu) - a_\nu^2 b_\nu(abu) = 2a_\nu^2 b_\nu(abu) = \frac{2}{3}a_\nu^3(abu), \\ \theta_\nu^2(\vartheta\nu x)^2 &= a_\nu^2(\widehat{a}b\nu x)^2 - \frac{1}{3}(\nu\nu_1 x)^4 = a_\nu b_\nu(\widehat{a}b\nu x)^2 + \frac{1}{6}(\nu\nu_1 x)^4 \\ &= if - 2a_\nu^3 b_\nu + a_\nu^2 b_\nu^2 - \frac{1}{3}s = 2a_\nu^3 b_\nu - 2a_\nu^2 b_\nu^2 + \frac{1}{6}s = \frac{2}{3}if - \frac{2}{3}a_\nu^3 b_\nu - \frac{1}{6}s, \\ \theta_\nu^3(\vartheta\nu x) &= a_\nu^2 b_\nu(\widehat{a}b\nu x)(abu) = a_\nu^3 b_\nu(abu). \end{aligned}$$

The formulas obtained are:

$$\begin{array}{c|c|l} \theta_\nu^2(\theta\nu x) = 0 & \theta_\nu^3(\theta\nu x) = 0 & \theta_\nu^4 u_x^2 = u_\varrho^2 = \varrho \quad \text{(adjoined modulus, § 7)}, \\ \theta_\nu^2(\theta\nu x)^2 = \dfrac{4}{9}if - \dfrac{1}{6}s & & \end{array} \tag{9}$$

Consequences: 1) $\theta_\nu^2(\theta\nu x)^2$ is a reducer. 2) ν enters into folding with θ only in products with contragredient forms (g).

§ 10. Forms of the fifth order (System III).

$$\text{Folding of } \begin{cases} K, j, \Delta \text{ with } \nu, \\ f \text{ with } H. \end{cases}$$

Irreducible forms:

A)
$$\begin{matrix} \cdot & K_\nu & \cdot & \cdot \\ (k\nu x)^2 & \cdot & K_\nu^2 & \cdot \\ (k\nu x)^3 & K_\nu(k\nu x)^2 & \cdot & \cdot \\ \cdot & K_\nu(k\nu x)^3 & \cdot & \cdot \end{matrix}$$

B)
$$\begin{matrix} (j\nu x) \\ (j\nu x)^2 \\ (j\nu x)^3 \\ \cdot \end{matrix}$$

C)
$$\begin{matrix} \Delta_\nu \\ \cdot \\ \cdot \\ \cdot \end{matrix}$$

D)
$$\begin{matrix} (aHu) & (aHu)^2 & \cdot & \cdot \\ a_\eta & a_\eta(aHu) & a_\eta(aHu)^2 & \cdot \\ \cdot & a_\eta^2 & \cdot & \cdot \end{matrix}$$

reductions:

A) form sequence K_ν^3: reducer a_ν^3.
form $K_\nu^2(k\nu x)^2$: reducer $\theta_\nu^2(\vartheta\nu x)^2$.

$$(k\nu x), \quad K_\nu(k\nu x), \quad K_\nu^2(k\nu x)$$

are decomposable forms according to § 3.
B) form

$$\begin{aligned}(j\nu x)^4 = (\widehat{a}\theta\nu x)^4 &= a_\nu^4\theta + \theta_\nu^4 f - 4a_\nu^3\theta_\nu - 4a_\nu\{a_\nu\theta_x - (\widehat{a}\theta\nu x)\}^3 \\ &+ 6a_\nu^2\{a_\nu\theta_x - (\widehat{a}\theta\nu x)\}^2 = \varrho f + \frac{5}{3}i\theta - 6a_\nu^2(\widehat{a}\theta\nu x)^2 + 4a_\nu(\widehat{a}\theta\nu x)^3,\end{aligned}$$

and therefore

$$(j\nu x)^4 = \varrho f + \frac{5}{3}i\theta \ \mathrm{mod}(\Delta, \nu), \qquad \text{(cf. § 5 end)}.$$

C) form Δ_ν^4: reducer θ_ν^4.
forms Δ_ν^2 and Δ_ν^3: reducer a_ν^3 or θ_ν^4 by replacing the form Δ by lower forms of the form sequence (§ 5 end), i.e. by double reduction of the expressions

$$a_\vartheta a_\nu^3, \qquad a_\vartheta a_\nu^3\theta_\nu, \qquad a_\vartheta\theta_\nu^4.$$

The double calculation of Δ_ν^3 gives rise to the reduction of the higher form a_η^3.
Reduction formulas:

$$\begin{aligned}&\text{a)} \quad \Delta_\nu^2 = \frac{3}{5}a_\eta^2 - \frac{3}{10}(asu)^2 + \frac{1}{3}i\theta + \frac{1}{5}u_x^2(2a_\varrho^2 - t), \\ &\text{b)} \quad \Delta_\nu^3 = -\frac{3}{10}a_\varrho + \frac{3}{5}u_x\left(\frac{13}{10}a_\varrho^2 - \frac{2}{5}t\right), \\ &\text{c)} \quad \Delta_\nu^4 = a_\varrho^2 - \frac{2}{5}t.\end{aligned} \tag{10}$$

Derivation of the formulas:

$$\begin{aligned}\text{a)} \quad a_\vartheta a_\nu^3 = \frac{1}{3}i\theta &= [a_\vartheta]_{\nu^3} + \frac{6}{7}[a_\vartheta^2]_{\nu^2} + \frac{6}{5}[a_\vartheta(a\theta u)^2]_{\nu^2}\,\widehat{\nu}x^2 + \frac{11}{30}[a_\vartheta^2(a\theta u)^2]_\nu\,\widehat{\nu}x^2 \\ &- \frac{6}{7}u_x[a_\vartheta^2]_{\nu^3} - \frac{1}{6}u_x[a_\vartheta^2(a\theta u)^2]_{\nu^2}\,\widehat{\nu}x^2, \\ \frac{1}{3}i\theta = \Delta_\nu^2 &- \frac{2}{3}u_x\Delta_\nu^3 - a_\nu a_{\nu_1}(\nu\nu_1 x)^2 + \frac{2}{5}a_\nu^2(\nu\nu_1 x)^2 + \frac{1}{5}u_x^2 a_\nu^2 a_{\nu_1}(\nu\nu_1 x)^2;\end{aligned}$$

$$\begin{aligned}\text{b)} \quad a_\vartheta a_\nu^3\theta_\nu = 0 &= [a_\vartheta]_{\nu^4} + \frac{9}{14}[a_\vartheta^2]_{\nu^3} + \frac{3}{5}[a_\vartheta(a\theta u)^2]_{\nu^2}\,\widehat{\nu}x^2 + \frac{17}{120}[a_\vartheta^2(a\theta u)^2]_\nu\,\widehat{\nu}x^2 \\ &- \frac{9}{14}u_x[a_\vartheta^2]_{\nu^4} - \frac{1}{24}u_x[a_\vartheta^2(a\theta u)^2]_{\nu^2}\,\widehat{\nu}x^2, \\ 0 &= \frac{5}{6}\Delta_\nu^3 - \frac{1}{2}u_x\Delta_\nu^4 - \frac{1}{4}a_\eta^3 + \frac{1}{20}u_x a_\eta^4;\end{aligned}$$

$$\begin{aligned}\text{b')} \quad a_\vartheta\theta_\nu^4 = a_\varrho &= a_\vartheta\theta_\nu\{a_\nu - (a\theta\nu x)\}^3 \\ &= -\frac{3}{2}[a_\vartheta]_{\nu^3} + \frac{3}{5}[a_\vartheta(a\theta u)^2]_{\nu^2}\,\widehat{\nu}x^2 - \frac{37}{120}[a_\vartheta^2(a\theta u)^2]_\nu\,\widehat{\nu}x^2 \\ &+ \frac{3}{2}u_x[a_\vartheta^2]_{\nu^4} + \frac{49}{120}u_x[a_\vartheta^2(a\theta u)^2]_{\nu^2}\,\widehat{\nu}x^2, \\ a_\varrho &= -\frac{3}{2}\Delta_\nu^3 + \frac{3}{2}u_x\Delta_\nu^4 - \frac{11}{20}a_\eta^3 + \frac{7}{20}u_x a_\eta^4;\end{aligned}$$

$$\begin{aligned}\text{c)} \quad a_\vartheta^2\theta_\nu^4 = a_\varrho^2 &= [a_\vartheta^2]_{\nu^4} + \frac{3}{5}[a_\vartheta^2(a\theta u)^2]_{\nu^2}\,\widehat{\nu}x^2, \\ a_\varrho^2 &= \Delta_\nu^4 + \frac{2}{5}a_\eta^4.\end{aligned}$$

D) reduction of a_η^3 by double reduction of Δ_ν^3 (C).
The remaining reductions are obtained by a computation dualistically opposite to that of § 9.

Reduction formulas:

$$\begin{array}{rl|rl} a_\eta^2(aHu) & = -\frac{1}{6}(asu)^3, & a_\eta^2(aHu)^2 & = \frac{4}{9}i\nu - \frac{1}{6}(asu)^4, \\ a_\eta^3 & = -a_\varrho + \frac{3}{5}u_x a_\varrho^2 + \frac{1}{5}u_x t, & a_\eta^3(aHu) & = 0, \\ & & a_\eta^4 & = t \quad \text{(adjoined as a modulus).} \end{array} \tag{11}$$

Consequences:

1) $(j\nu x)^4$, Δ_ν^2, $a_\eta^2(aHu)$ are reducers.

2) ν enters only in products with contragredient forms in foldings with K, j, Δ; the same holds for f in relation to H, and for j in relation to ν, since $\theta_\nu(\theta \cdot j, \nu, x^3)$ becomes reducible according to § 11 B.

§ 11. Forms of the sixth order (System III).

$$\text{Folding of } \left\{ \begin{array}{l} \theta^2, f \cdot j, N \text{ with } \nu, \\ \theta \text{ with } H. \end{array} \right.$$

Irreducible forms:

A) $(\vartheta^2\nu x)^3$, $\quad \theta_\nu(\vartheta^2\nu x)^3$ $\quad$ B) $a_\nu(j\nu x)$, $\quad a_\nu^2(j\nu x)$ $\quad$ C) N_ν

D)

$(\vartheta\eta x)$	(θHu)	$(\theta Hu)^2$	$\cdot$
$(\vartheta\eta x)^2$	θ_η	$H_\vartheta(\theta Hu),\ \theta_\eta(\theta Hu)$	$\theta_\eta(\theta Hu)^2$
$\cdot$	$H_\vartheta(\vartheta\eta x),\ \theta_\eta(\vartheta\eta x)$	θ_η^2	$\theta_\eta^2(\theta Hu)$
	$\theta_\eta(\vartheta\eta x)^2$	$\cdot$	$\cdot$

reductions:

A) $(\vartheta^2\nu x)^4$ decomposes according to formula (3.)a:

$$(a\Delta\vartheta x)^4 = \frac{1}{2}(\vartheta^2\nu x)^4 - \frac{3}{5}f \cdot a_\nu^2(\nu\vartheta x)^2 = \frac{1}{3}\Delta^2 + f\Delta_\vartheta^2.$$

B) $a_\nu(j\nu x)^2$ decomposes according to formula (9.)a, indem wir according to § 6 end $f \cdot j$ by $(\theta\theta' u)^2$ ersetzen, and the reducibility of θ'_ϑ take account of:

$$\frac{1}{3}a_\nu(j\nu x)^2 = (\theta\theta'\nu x)^2\theta_\nu = \theta_\nu^3\theta - \theta_\nu^2\theta'_\nu = \theta_\nu^3\theta + \theta_\nu^2(\widehat{j}\nu\theta' u) = \theta_\nu^3\theta - \frac{2}{3}\theta_\nu^3\theta.$$

forms $a_\nu(j\nu x)^3$ and $a_\nu^2(j\nu x)^2$: reducer a_j and $(j\nu x)^4$:

$$a_\nu(j\nu x)^3 = a_j(j\nu x)^3 - (j\nu x)^3(j\nu\widehat{a}u),$$

$$a_\nu^2(j\nu x)^2 = a_j^2(j\nu x)^2 - 2a_j(j\nu x)^2(j\nu\widehat{a}u) + (j\nu x)^2(j\nu\widehat{a}u)^2.$$

C) form sequence N_ν^2; reducer Δ_ν^2. $(n\nu x)$ and $N_\nu(n\nu x)$ decompose as a transvection over functional determinants according to § 3.

D) *Overview of the reductions:*

a) form sequence $\theta_\eta^2 H_\vartheta$: reducer $a_\eta^2(aHu)$. (Leads to forms with higher symbols.)

b) form sequence $\theta_\eta H_\vartheta$: reducer $a_\eta^2(aHu)$ by double reduction. (Leads to forms with higher symbols and to higher forms of the total form sequence, i.e. to the form sequence θ_η^2.) Instead of $\theta_\eta H_\vartheta$ we consider the form sequence

$$\theta_\eta(\vartheta\eta x)(\theta Hu) = \theta_\eta H_\vartheta + \theta_\eta^2,$$

ersetzen in it the symbols θ by the lower form (abu), gelangen so to the double reduction of the form sequence

$$a_\eta^2(aHu)(abu) = \theta_\eta H_\vartheta + \frac{3}{2}\theta_\eta^2 \bmod s$$

up to the terminal form

$$a_\eta^3 b_\eta(bHu)(abu) = \theta_\eta^3 H_\vartheta + \frac{1}{2}\theta_\eta^4.$$

c) form sequence θ_η^3: By double reduction of those forms which simultaneously belong to the form sequences $\theta_\eta H_\vartheta$ and $\theta_\eta^2 H_\vartheta$ - i.e. the forms of the form sequence $\theta_\eta^2 H_\vartheta$ - to forms with higher symbols on the one hand, and to forms with higher symbols and to the higher form sequence θ_η^3 on the other hand.

d) forms $\theta_\eta^2(\vartheta\eta x)$, $\theta_\eta^2(\vartheta\eta x)^2$, $\theta_\eta^3(\vartheta\eta x)$: By double reduction by means of the reducers a analogous to the computation of § 9.

e) forms $\theta_\eta^2(\theta Hu)^2$ and $\theta_\eta^2(\vartheta\eta x)^2$: By double reduction of the expressions $\Delta_\nu^2(a\Delta u)^4$ and $(a\Delta\nu x)^4$ by means of the reducers Δ_ν^2 and $(a\Delta u)^4$.

f) forms H_ϑ and H_ϑ^2: Decomposition of forms. Is obtained for H_ϑ^2 by double reduction of the expression $\Delta_\nu^2(a\Delta u)^2$ or also by direct calculation of the products $(a_\nu^2)^2$, $a_\nu^2 b_{\nu_1}$ by forms of the system. (The analogous calculation of $(a_\nu)^2$ gives a relation between decomposable forms.)

g) Reduction of higher forms by the fact that forms of the form sequence $\theta \cdot H$ admit two reduction possibilities (belong to two reducible form sequences), namely:

g: by double reduction of $\theta_\eta^2(\vartheta\eta x)^2$; allows reduction d) and e) zu.

$s_\vartheta^2(\theta su)$: by double reduction of $\theta_\eta^3(\vartheta\eta x)$; allows reduction c) and d) zu.

$s_\vartheta^2(\theta su)^2$: by double reduction of $\theta_\eta^2 H_\vartheta^2$; allows reduction a) and has the reducers $\theta_\nu^2(\vartheta\nu x)^2$ as a factor.

s_ν^2: by double reduction of $\theta_\eta^3 H_\vartheta$; allows reduction a) and c) zu.

The proof of the independence of the remaining forms is obtained by double reduction of the form sequence $\Delta_\nu^2(a\Delta u)^2 = \theta_\eta^2$.

Execution of the reductions:

The existence of reductions a), b), c), d) is clear a priori, since according to the stated law of formation the relations arising from double reduction are independent of one another. For reductions e), f), g), it must be shown by computation that no identities arise.

Proceeding symmetrically with the diagonal term in the form sequence $\theta \cdot H$ up to the form θ_η, and partly indicating the calculation, we also give the formulas obtained by reductions a), b), c), d), since they are used partly in reductions e), f), g), and partly later.

1) H_ϑ and H_ϑ^2 according to f). According to the ansatz[27]

$$\begin{aligned} a_\nu b_{\nu_1}^2 &= \nu a_\nu b_\nu^2 - (aHu)(bHu)b_\eta \sim \nu a_\nu b_\nu^2 - f a_\eta (aHu)^2 - (abu)(aHu)b_\eta + (abu)^2 b_\eta, \\ a_\nu^2 b_{\nu_1}^2 &= b_\nu^2\{a_\nu u_\nu - (a\nu\nu_1 u)\}^2 \sim \nu\{a_\nu^2 b_\nu^2 - 2a_\nu b_\nu (aHu)(bHu) - \frac{1}{6}(asu)^2(bsu)^2\} \\ &\sim \nu a_\nu^2 b_\nu^2 - 2a^2(aHu)(abu) - \frac{1}{6}(asu)^2(bsu)^2 + (\vartheta\eta x)^2(\theta Hu)^2 \end{aligned}$$

after substitution of the value of $\theta_\eta H_\vartheta$, the formulas arise:

$$\begin{aligned} &\text{a)} \quad H_\vartheta \sim 2a_\nu a_\varrho^2 + 2\nu b_\nu(\vartheta\eta x)^2 + 2f a_\eta (aHu)^2 - 2\theta_\eta, \\ &\text{b)} \quad H_\vartheta^2 \sim (a^2)^2 + 2\theta_\eta^2 + \frac{2}{3}(\theta su)^2 + \frac{1}{12}s\nu - \frac{1}{9}if\nu - \frac{1}{6}f(asu)^4. \end{aligned} \tag{12}$$

2) $\theta_\eta H_\vartheta$ according to b):

$$\begin{aligned} a_\eta^2(aHu)(abu) &\sim [a_\eta^2(aHu)]_{bu} + \frac{1}{2}f[a_\eta^2(aHu)^2] = a_\eta b_\eta (aHu)(abu) \\ &\quad + a_\eta(\widehat{ab}\eta x)(abu)(aHu) \sim \theta_\eta(\vartheta\eta x)(\theta Hu) + \frac{1}{2}\theta_\eta^2 + \frac{1}{4}(\nu\eta x)^2. \end{aligned}$$

According to the formulas (5.) and (11.) follows:

$$\theta_\eta H_\vartheta \sim -\frac{3}{2}\theta_\eta^2 - \frac{1}{4}(\theta su)^2 - \frac{1}{12}s\nu + \frac{2}{9}if\nu.$$

3) $\theta_\eta H_\vartheta(\theta Hu)$ is computed according to b), analogously to $\theta_\eta H_\vartheta$:

$$\theta_\eta H_\vartheta(\theta Hu) \sim -\theta_\eta^2(\theta Hu) - \frac{1}{6}(\theta su)^3.$$

4) $\theta_\eta H_\vartheta(\vartheta\eta x)$ according to b); $\theta_\eta^2(\vartheta\eta x)$ according to d) (cf. § 9):

$$\theta_\eta H_\vartheta(\vartheta\eta x) \sim -\theta_\eta^2(\vartheta\eta x) - \frac{1}{6}s_\vartheta(\theta su) \sim -\frac{1}{3}(\vartheta\varrho x) - \frac{1}{6}s_\vartheta(\theta su),$$

[27] The sign $\sim$ in place of the equality sign means that products arising from u_x with higher forms, other than those arising by foldings III and IV, are omitted.

$$\theta_\eta^2(\vartheta\eta x) \sim \frac{2}{3}a_\eta^3(abu) \sim -\frac{1}{3}(\vartheta\varrho x).$$

5)

$\theta_\eta H_\vartheta^2$ according to b) from $a_\eta^2(aHb)(bHu)$ — $\theta_\eta^2 H_\vartheta$ according to a) from $a_\eta^3(Hab)(abu)$ — $\theta_\eta^2 H_\vartheta$ according to b) and thereby θ_η^3 according to c) from $a_\eta^3(bHu)(abu)$

$$\theta_\eta H_\vartheta^2 \sim -\frac{3}{2}\theta_\eta^2 H_\vartheta - \frac{1}{4}s_\vartheta(\theta su)^2 + \frac{1}{6}s_\nu - \frac{4}{9}ia_\nu \sim -\theta_\varrho - \frac{1}{6}s_\nu - \frac{1}{9}ia_\nu,$$

$$\theta_\eta^2 H_\vartheta \sim \frac{2}{3}\theta_\varrho - \frac{1}{6}s_\vartheta(\theta su)^2 + \frac{2}{9}s_\nu - \frac{2}{9}ia_\nu,$$

$$\theta_\eta^3 H_\vartheta \sim \frac{2}{3}\theta_\varrho - \frac{2}{3}\theta_\eta^3 + \frac{5}{36}s_\nu, \qquad \theta_\eta^3 \sim \frac{1}{4}s_\vartheta(\theta su)^2 - \frac{1}{8}s_\nu + \frac{1}{3}ia_\nu.$$

6) $\theta_\eta^2(\theta Hu)^2$ according to e):

$$\Delta_\nu^2(a\Delta u)^2 = [(a\Delta u)^4]_{\nu^2} = -\frac{12}{5}\theta_\eta^2(\theta Hu)^2 - \frac{3}{10}\sigma - \frac{1}{20}(\theta su)^4 + \nu\varrho \quad \text{(according to formula (3.)c)},$$

$$\Delta_\nu^2(a\Delta u)^4 = [\Delta_\nu^2]_{aa}^4 = -\frac{3}{5}\theta_\eta^2(\theta Hu)^2 + \frac{1}{5}\sigma - \frac{3}{10}(\theta su)^4 + \frac{1}{3}ij \quad \text{(according to formula (10.)a)},$$

$$\theta_\eta^2(\theta Hu)^2 = -\frac{1}{6}\sigma + \frac{1}{12}(\theta su)^4 - \frac{1}{9}ij + \frac{1}{3}\nu\varrho.$$

7) $\theta_\eta^2(\vartheta\eta x)^2$ according to d) and e). From this reduction of the higher form g.
By a computation analogous to that in § 9, it follows:

$$\begin{aligned}\theta_\eta^2(\vartheta\eta x)^2 &= \frac{1}{2}if - \frac{1}{2}a_\eta^2 b_\eta - \frac{1}{12}g = \frac{2}{3}tf - \frac{2}{3}a_\eta^3 b_\eta - \frac{1}{6}g \\ &= -\frac{1}{6}g - \frac{1}{3}(\vartheta\varrho x)^2 + \frac{4}{15}fa_\varrho^2 + \frac{8}{15}ft \quad \text{(according to formula (11.))}.\end{aligned}$$

By the corresponding computation as above follows:

$$((a\Delta\nu x)^4) = [(a\Delta u)^4]_{\nu x^4} = \frac{21}{10}\theta_\eta^2(\vartheta\eta x)^2 + \frac{7}{10}s_\vartheta^2 - \frac{3}{10}g \quad \text{(according to formula (3.)c)},$$

$$\begin{aligned}(a\Delta\nu x)^4 &= -\frac{1}{3}i\Delta + 6[\Delta_\nu^2]a^2 - 4[\Delta_\nu^3]a + \Delta_\nu^4 f \\ &= -\frac{36}{5}\theta_\eta^2(\vartheta\eta x)^2 - \frac{9}{5}s_\vartheta^2 - \frac{3}{5}g - \frac{3}{5}(\vartheta\varrho x)^2 \\ &\quad + \frac{5}{3}i\Delta + \frac{37}{25}fa_\varrho^2 + \frac{74}{25}ft \quad \text{(according to formula (10.))}.\end{aligned}$$

Thus

$$\begin{aligned}\frac{93}{10}\theta_\eta^2(\vartheta\eta x)^2 &= -\frac{3}{10}g - \frac{5}{2}s_\vartheta^2 - \frac{3}{5}(\vartheta\varrho x)^2 \\ &\quad + \frac{5}{3}i\Delta + \frac{37}{25}fa_\varrho^2 + \frac{74}{25}ft,\end{aligned}$$

and by comparing the two values of $\theta_\eta^2(\vartheta\eta x)^2$ according to g):

$$0 = g - 2s_\vartheta^2 + 2(\vartheta\varrho x)^2 + \frac{4}{3}i\Delta - \frac{4}{5}fa_\varrho^2 - \frac{8}{5}ft. \tag{13}$$

8) $\theta_\eta^2 H_\vartheta(\theta Hu)$ according to a) and b), from this $\theta_\eta^3(\theta Hu)$ according to c) (forms with the Faktor u_x vanish):

$$\theta_\eta^2 H_\vartheta(\theta Hu) = -\frac{1}{6}s_\vartheta(\theta su)^3 - \frac{1}{3}(\nu\varrho x),$$

$$\theta_\eta^2 H_\vartheta(\theta Hu) = -\frac{1}{3}\theta_\eta^3(\theta Hu) - \frac{1}{3}(\nu\varrho x),$$

$$\theta_\eta^3(\theta Hu) = \frac{1}{2}s_\vartheta(\theta su)^3.$$

9) $\theta_\eta^2 H_\vartheta(\vartheta\eta x)$ according to a) and b), from this $\theta_\eta^3(\vartheta\eta x)$ according to c). $\theta_\eta^3(\vartheta\eta x)$ according to d), from this reduction of the higher form $s_\vartheta^2(\theta su)$ according to g) (forms with the Faktor u_x vanish):

$$\theta_\eta^2 H_\vartheta(\vartheta\eta x) = \frac{1}{3}(atu),$$

$$\theta_\eta^2 H_\vartheta(\vartheta\eta x) = \frac{1}{3}(atu) + \frac{1}{3}\theta_\eta^3(\vartheta\eta x) - \frac{1}{6}s_\vartheta^2(\theta su),$$

$$\theta_\eta^3(\vartheta\eta x) = \frac{1}{2}s_\vartheta^2(\theta su),$$

$$\theta_\eta^3(\vartheta\eta x) = \frac{2}{5}\theta_\varrho(\vartheta\varrho x) + \frac{1}{5}(atu),$$

$$s_\vartheta^2(\theta su) = \frac{4}{5}\theta_\varrho(\vartheta\varrho x) + \frac{2}{5}(atu). \tag{14}$$

10) $\theta_\eta^2 H_\vartheta^2$ according to a) and by reducer $\theta_\nu^2(\vartheta\nu x)^2$, $\theta_\eta^3 H_\vartheta$ according to a) and c), θ_η^4 according to c), from this reduction of the higher forms $s_\vartheta^2(\theta su)^2$ and s_ν^2 according to g):

$$\text{According to a)}\quad \theta_\eta^2 H_\vartheta^2 = [a_\eta^2(aHu)^2]b^2 + \frac{1}{3}[a_\eta^4]_{bu^2} - \frac{1}{3}H_\nu^2(\nu\eta x)^2$$
$$= \frac{4}{9}ia_\nu^2 - \frac{1}{6}s_\vartheta^2(\theta su)^2 - \frac{5}{18}s_\nu^2 + \frac{1}{3}(atu)^2 + \frac{1}{54}Ju_x^2.$$

$$\text{By } \theta_\nu^2(\vartheta\nu x)^2:\quad \theta_\eta^2 H_\vartheta^2 = [\theta_\nu^2(\vartheta\nu x)^2]_{\nu_1} + \frac{1}{3}[\theta_\nu^4]_{\nu_1}\hat{\nu}_1 x^2 - \frac{1}{3}s_\vartheta^2(\theta su)^2$$
$$= \frac{4}{9}ia_\nu^2 - \frac{1}{6}s_\nu^2 - \frac{1}{3}s_\vartheta^2(\theta su)^2 + \frac{1}{3}(\nu\varrho x)^2.$$

$$\text{According to a)}\quad \theta_\eta^3 H_\vartheta = -[a_\eta^2(aHu)]_{bu}b^2 - \frac{1}{2}[a_\eta^2(aHu)^2]b^2 - \frac{1}{3}[a_\eta^3]b + \frac{1}{12}[a_\eta^4]_{bu^2}$$
$$+ \frac{1}{2}u_x[a_\eta^2(aHu)^2]b^3$$
$$= -\frac{2}{9}ia_\nu^2 + \frac{1}{12}s_\nu^2 + \frac{4}{15}\theta_\varrho^2 - \frac{7}{90}(\nu\varrho x)^2 + \frac{1}{30}(atu)^2 + \frac{2}{27}i^2u_x^2 - \frac{1}{36}Ju_x^2.$$

$$\text{According to c)}\quad \theta_\eta^3 H_\vartheta : a_\eta^3(Hab)(bHu) = \frac{1}{2}(atu)^2 = \theta_\eta^2 H_\vartheta(\theta Hu)(\vartheta\eta x) + \frac{1}{4}H_\nu^2(\nu\eta x)^2$$
$$+ \frac{1}{2}\theta_\eta^2 H_\vartheta^2 = \frac{3}{2}\theta_\eta^2 H_\vartheta^2 + \theta_\eta^3 H_\vartheta - u_x[a_\eta^2(aHu)^2]b^3$$
$$+ \frac{1}{4}H_\nu^2(\nu\eta x)^2,$$

and therefore

$$\theta_\eta^3 H_\vartheta = -\frac{2}{3}ia_\nu^2 + \frac{5}{12}s_\nu^2 + \frac{1}{2}(\nu\varrho x)^2 - \frac{1}{2}(atu)^2$$
$$+ \frac{4}{27}i^2u_x^2 - \frac{1}{12}Ju_x^2.$$

According to c)

$$\theta_\eta^4 = \frac{4}{9}ia_\nu^2 - \frac{1}{6}s_\nu^2 + \frac{16}{15}\theta_\varrho^2$$
$$- \frac{14}{45}(\nu\varrho x)^2 + \frac{2}{15}(atu)^2.$$

According to g), from the two values for $\theta_\eta^2 H_\vartheta^2$:

$$s_\vartheta^2(\theta su)^2 = \frac{2}{3}s_\nu^2 - 2(atu)^2 + 2(\nu\varrho x)^2 - \frac{1}{9}Ju_x^2$$
$$= \frac{8}{9}ia_\nu^2 + \frac{8}{15}\theta_\varrho^2 - \frac{14}{15}(atu)^2 + \frac{38}{45}(\nu\varrho x)^2 - \frac{4}{27}i^2u_x^2. \tag{15}$$

According to g), from the two values for $\theta_\eta^3 H_\vartheta$:

$$s_\nu^2 = \frac{4}{3}ia_\nu^2 + \frac{4}{5}\theta_\varrho^2 + \frac{8}{5}(atu)^2 - \frac{26}{15}(\nu\varrho x)^2 + \frac{1}{6}Ju_x^2 - \frac{2}{9}i^2u_x^2. \tag{16}$$

Formula (16.) gives the basis for the reduction of the modulus $(ss'u)^4$, and formula (13.) gives the basis for the reduction of the system of s. (§ 17.)

Consequences:

1) $a_\nu(j\nu x)^3$, $\theta_\eta H_\vartheta$, $\theta_\eta^2(\vartheta\eta x)$, $\theta_\eta^2(\theta Hu)^2$ are reducers, $a_\nu(j\nu x)^2$, H_ϑ and H_ϑ^2 decomposable forms.

2) The form of the system II: $j(\nu) = g = (\nu\eta x)^4 H_x^2$ is reducible.

3) Since the only contragredient form g becomes reducible, ν does not enter at all in powers or in products with forms of the same system in folding with System I.

θ enters into foldings only as a contravariant in products or powers; correspondingly, H enters only as a covariant (cf. § 13 B).

§ 12. Forms of the seventh order.

$$\text{Folding of } \begin{cases} \theta \cdot K \text{ with } \nu, \\ K, j, \Delta \text{ with } H, \\ f \text{ with } L, \sigma. \end{cases}$$

Irreducible forms:

$$\text{B)} \quad \begin{array}{c|c|c|c|c} \cdot & \cdot & (KHu)^2 & \cdot & \cdot \\ \cdot & K_\eta & \cdot & K_\eta(KHu)^2 & \cdot \\ (k\eta x)^2 & \cdot & K_\eta^2 & \cdot & \cdot \\ (k\eta x)^3 & H_k(k\eta x)^2,\ K_\eta(k\eta x)^2 & \cdot & \cdot & \cdot \\ \cdot & K_\eta(k\eta x)^3 & \cdot & \cdot & \cdot \end{array}$$

$$\text{C)} \quad \begin{array}{cc} (j\eta x) & H_j \\ \cdot & H_j(j\eta x) \\ \cdot & H_j^2 \end{array} \qquad \text{D)} \quad \begin{array}{c} (\Delta Hu) \\ \Delta_\eta \end{array}$$

$$\text{E)} \quad \begin{array}{cccc} a_i & (aLu)^2 & (aLu)^3 & \cdot \\ \cdot & \cdot & a_i(aLu)^2 & a_i(aLu)^3 \\ \cdot & a_i^2 & \cdot & \cdot \end{array}$$

reductions:

A) $(\vartheta \cdot k, \nu, x)^4$ decomposes as single Überschiebung over the decomposable form $(\vartheta^2\nu x)^4$.

B) form sequence $H_k K_\eta$: reducer $H_\vartheta\theta_\eta$.

form sequence $K_\eta^2(KHu)$: reducer $a_\eta^2(aHu)$.

form sequence $K_\eta^2(k\eta x)$: reducer $\theta_\eta^2(\vartheta\eta x)$.

The from this arising double reduction of the form sequence K_η^3 gives rise to the reduction of the higher form sequence $(j\eta x)^3$.

(KHu), $(k\eta x)$, $K_\eta(k\eta x)$ decomposable forms according to § 3.

$H_k(KHu)$, $K_\eta(KHu)$ decompose as arising by single folding with the decomposable form $K_\nu(k\nu x)$ and the functional determinant

$$K_\nu^2 = \theta_\nu^2(a\theta u) \equiv a_\nu^2(a\theta u) \mod \nu^2.$$

A relation between decomposable forms corresponds to the double representation of K_ν^2. One obtains:

$$H_k(KHu) = 2K_\nu(\nu\nu_1 k) = 2\theta_{\nu_1}(\nu\nu_1 a\theta) = 2\theta_\nu^2 a_\nu - a_\nu^2\theta_\nu + f\theta_\eta(\theta Hu)^2 - f\nu\theta_\vartheta^3 \mod \nu^3,$$

$$\begin{aligned} K_\eta(KHu) &= -K_\nu^2(\nu\nu_1 x) = -a_\nu^2(a\theta u)(\nu\nu_1 x) \\ &= a_\eta(aHu)^2\theta + a_\nu^2\theta_\nu = -\theta_\nu(\theta Hu)^2 f - \theta_\nu^2 a_\nu. \end{aligned}$$

Therefore

$$0 = a_\nu^2\theta_\nu + \theta_\nu^2 a_{\nu_1} + f\theta_\eta(\theta Hu)^2 + \theta a_\eta(aHu)^2 \mod \nu^3. \tag{17}$$

The forms H_k, $H_k(k\eta x)$, H_k^2, $H_k^2(k\eta x)$ decompose as arising by single folding with the decomposable forms H_ϑ and H_ϑ^2 (cf. § 3. 2), a) and b)).

Es is

$$H_k = H_\vartheta(a\theta u) \sim [H_\vartheta]_{ua} - fH_\vartheta(\theta Hu)$$

(specialization $y = uv$ of 2)a).

$$H_k(k\eta x) = H_\vartheta a_\eta - H_\vartheta\theta_\eta f, \qquad H_\vartheta a_\eta = \frac{5}{4}[H_\vartheta]a - \frac{1}{4}H_\vartheta a_\vartheta \quad (\S\ 3.2)b),$$

$$H^2_\vartheta(a\theta u) = [H^2_\vartheta]_{ua}, \qquad H^2_\vartheta a_\eta = [H^2_\vartheta]a = H^2_k(k\eta x) + H^2_\vartheta \theta_\eta f.$$

C) form sequence $(j\eta x)^3$: Reducible by double reduction of the form sequence K^3_η according to B); according to the ansatz:

$$0 = a^3_\eta(a\theta u) = \theta^3_\eta(a\theta u) = \theta_\eta + (a\theta\eta x)^3(a\theta u) - \theta^3_\eta(a\theta u) = \frac{1}{2}(j\eta x)^3 \ \mathrm{mod}(\nu^3, s, \varrho, t, i, J).$$

The analogous ansatz holds up to the terminal form of the form sequence:

$$0 = H^2_\vartheta(a\theta\eta x)a^3_\eta = H^2_\vartheta(a\theta\eta x)\theta^3_\eta - \frac{1}{2}H^2_\vartheta(j\eta x)^4 \ \mathrm{mod}(\nu^3, s, \varrho, t, i, J).$$

form $(j\eta x)^2$: decomposes 1) by twofold polarization of the relation for the decomposable form H^2_ϑ ((12.) b);

2) by direct calculation of the products $a_\nu\theta^3_\nu$; thereby Decomposition of the higher form $(\Delta Hu)^2$. One obtains:

$$\left.\begin{array}{ll} \text{a)} & \frac{1}{3}(\Delta Hu)^2 + \frac{1}{3}(j\eta x)^2 = \theta^2_\nu a^2_{\nu_1}, \\ \text{b)} & (j\eta x)^2 = \frac{4}{3}\theta^3_\nu a_{\nu_1}, \end{array}\right\} \ \mathrm{mod}(\nu^3, s, \varrho, t, i, J). \tag{18}$$

according to the ansatz:

$$H^2_\vartheta(a\theta u)^2 - \frac{1}{3}(\Delta Hu)^2 = 2\theta^2_\eta(a\theta u)(aHu) + \theta^2_\nu a^2_{\nu_1} = (a\theta u)(aHu)\{a_\eta - (a\theta\eta x)^2\} + \theta^2_\nu a^2_{\nu_1},$$

$$\begin{aligned} a_{\nu_1}\theta^3_\nu &= -(a\widehat{\nu}\nu_1 u)\theta^2_\nu(\theta\widehat{\nu}\nu_1 u) - \frac{1}{2}(u\nu\nu_1 u)\theta_\nu\theta_{\nu_1}(\vartheta\nu\nu_1 u) \\ &= -\frac{3}{2}\theta^2_\eta(\theta Hu)(aHu) = -\frac{3}{2}\theta^2_\eta(\theta Hu)(a\theta u) \\ &= -\frac{3}{2}\{a_\eta - (a\theta\eta x)^2\}\{(aHu) - (a\theta u)\}(a\theta u). \end{aligned}$$

D) form sequence $\Delta_\eta(\Delta Hu)$: reducer Δ^2_ν.

$(\Delta Hu)^2$ decomposable form according to C).

E) form sequence $a^2_i(aLu)$: reducer $a^2_\eta(aHu)$. forms (aLu) and $a_i(aLu)$: Decomposition as a transvectionen over functional determinants according to § 3.

F) form sequence a^3_σ: reducer a^3_ϱ.

forms a^2_σ and a^3_σ: reducer a^3_ν and a^3_η by double reduction of the corresponding expressions

$$H_\nu a^3_\nu \quad \text{and} \quad H_\nu a^3_\eta, \qquad H_\nu a^3_\nu a_\nu \quad \text{and} \quad H_\nu a^4_\eta$$

(cf. § 10. C) reduction of Δ^2_ν and Δ^3_ν).

From this reduction for the higher forms $a_\nu s_\nu(asu)^2$, $a^2_\nu s_\nu(asu)^2$ and for forms in symbolsn $\varrho, t(a_\nu, a^2_\eta)$ taking account of (16.):

$$\left.\begin{array}{rcl} a_\nu s_\nu(asu)^2 &=& \frac{1}{3}i\theta^2_\nu - \frac{1}{18}iH, \\ a^2_\nu s_\nu(asu)^2 &=& 0, \end{array}\right\} \ \mathrm{mod}(\varrho, t). \tag{19}$$

form a_σ: decomposes by polarization of (12.)b or, more briefly, by direct expansion of the products $a^2_\nu\theta^3_\nu$ according to the ansatz:

$$a^2_\nu\theta^3_{\nu_1} = (a^2_\nu\theta_{\nu_1})a_{\nu_1} - (a\theta\nu_1 x)^2 = -2a_\eta(aHu)(a\theta H)(a\theta\eta x) + (a\theta\nu_1 x)^2 a^2_\nu\theta_{\nu_1}$$

and taking account of the reduction of $H_j(j\eta x)^2$ (C):

$$a_\sigma = 2a^2_\nu\theta^3_{\nu_1} \ \mathrm{mod}(s, \varrho, t, i). \tag{20}$$

Consequences:

1) $(j\eta x)^3$, $\Delta_\eta(\Delta Hu)$, a^2_σ are reducers, $(j\eta x)^2$, $(\Delta Hu)^2$, a_σ decomposable forms.

2) f enters into folding with L only in products with contragredient forms; therefore f, and likewise K and N, do not enter at all into folding with σ and consequently with $(\nu\sigma x)$. The form j enters only in products with contragredient forms; Δ does not enter at all in products in folding with H and L (this follows from $\Delta_\eta(\Delta Hu)$ and $(\Delta Hu)^2$). Likewise σ, and consequently $(\nu\sigma x)$, do not enter in products in folding with any form of System I. Thus, among products in System II, taking account of the consequences of § 11, there remain only powers of H and products of H with L.

§ 13. Forms of the eighth order (System III).

$$\text{Folding of } \begin{cases} \Delta \cdot j \text{ with } \nu, \\ \theta^2, f \cdot j, N \text{ with } H, \\ \theta \text{ with } L, \sigma. \end{cases}$$

Irreducible forms:

A) $\Delta_\nu(j\nu x)$ B) $\begin{matrix}(\vartheta^2\eta x)^3 \\ (\vartheta^2\eta x)^4\end{matrix}$ $H_\vartheta(\vartheta^2\eta x)^3,\ \theta_\eta(\vartheta^2\eta x)^3,$

C) $(aHu)H_j,\quad a_\eta(aHu)H_j$ D) $H_n,\ N_\eta,$

E)
$$\left|\begin{matrix}\cdot \\ \theta_i \\ (\vartheta lx)^2 \\ \cdot\end{matrix}\right| \left|\begin{matrix}(\theta Lu)^2 \\ \cdot \\ \theta_i^2 \\ \theta_i(\vartheta lx)^2\end{matrix}\right| \left|\begin{matrix}(\theta Lu)^3 \\ L_\vartheta(\theta Lu)^2,\ \theta_i(\theta Lu)^2 \\ \cdot \\ \cdot\end{matrix}\right| \left|\begin{matrix}\cdot \\ \theta_i(\theta Lu)^3 \\ \cdot \\ \cdot\end{matrix}\right|$$

reductions:

A) $\Delta_\nu(j\nu x)^3$: reducer $a_\nu(j\nu x)^3$.

$\Delta_\nu(j\nu x)^2$ is reducible by the decomposable form $a_\nu(j\nu x)^2$ according to § 3. 2)b, taking account of the reducer $\theta_{\vartheta j}$. Indeed, according to § 11 B), one obtains:

$$\frac{3}{10}\Delta_\nu(j\nu x)^2 + \frac{3}{5}a_\nu(j\nu x)a_\vartheta(j\nu x) + \frac{1}{10}a_\nu(j\nu x)^2 = \frac{3}{5}\theta_\nu^3\theta_{\vartheta j} + \frac{2}{5}\theta_\nu^3\theta_{\vartheta j}\theta_{\vartheta j},$$

(reducer a_j and $\theta_{\vartheta j}$).

B) The forms $H_\vartheta(\vartheta'\eta x)^2$, $H_\vartheta^2(\vartheta'\eta x)$, $H_\vartheta^2(\vartheta'\eta x)^2$ decompose as arising by successive single folding with the decomposable forms H_ϑ and H_ϑ^2, respectively $H_\vartheta a_\eta$ and $H_\vartheta^2 a_\eta$ according to § 3. 2)b) and according to the relation:

$$H_\vartheta(\vartheta'\eta x)^2 = 2H_\vartheta a_\eta^2 f - 2H_\vartheta a_\eta b_\eta.$$

C) form sequence $a_\eta(j\eta x)^2$: reducers a_j and $(j\eta x)^3$.

form $a_\eta(j\eta x)$ decomposes: reducer a_j and single folding with the decomposable form $(j\eta x)^2$ according to § 3, 2)a (specialization $y = uv$).

form $a_\eta H_j$ decomposes: 1) by single folding with the decomposable form $a_\nu(j\nu x)^2$;

2) by a special twofold folding with the decomposable form $(j\eta x)^2$; from this one obtains a relation between decomposable forms.

From $a_\nu(j\nu x)^2$:

$$0 = \theta'_\nu\theta_\nu + 2a_\eta H_j \mod(s, \varrho, t, i, J).$$

From $(j\eta x)^2$:

$$0 = \theta'_\nu\theta_\nu - \frac{3}{2}a_\eta H_j \mod(s, \varrho, t, i, J)$$

(products with contravariants are omitted), according to the ansatz:

$$0 = \frac{1}{2}a_\nu(abu)^2\theta_\nu^3 + \frac{1}{2}u_x(ubu)\theta_{\nu_1}^3(\theta bu) - \frac{3}{4}(\widehat{j}\eta bu)^2 + \frac{3}{4}H_j(\widehat{j}\eta bu) - \frac{1}{8}fH_j^2$$

and by interchanging the symbols in $a_\nu(ubu)(\theta bu)\theta_{\nu_1}^3$.

D) form sequence $N_\eta(NHu)$: reducer Δ_ν^2.

(NHu), $(n\eta x)$, $N_\eta(n\eta x)$, $H_\eta(NHu)$ decomposable forms (cf. § 12 B), $(NHu)^2$ decomposes by single folding with the form $(\Delta Hu)^2$.

E) form sequences $\theta_i L_\vartheta$, $\theta_i^2(\theta Lu)^2$, $\theta_i^2(\vartheta lx)$:

reducers: $\theta_\eta H_\vartheta$, $\theta_\eta^2(\theta Hu)^2$, $\theta_\eta^2(\vartheta\eta x)$.

forms (θLu), (ϑlx), L_ϑ, $L_\vartheta(\theta Lu)$, $\theta_i(\theta Lu)$, $L_\vartheta(\vartheta lx)$, $\theta_i(\vartheta lx)$, L_ϑ^2, $L_\vartheta^2(\theta Lu)$, $\theta_i^2(\theta Lu)$ decompose. (Dualistically opposite to the decomposable forms of § 12 B).

F) form sequence $\theta_\sigma(\vartheta\sigma x)$: reducer a_σ^2.

forms $(\vartheta\sigma x)$ and $(\vartheta\sigma x)^2$ decompose, as arising by single folding with the decomposable form a_σ; θ_σ, by twofold folding arising, decomposes, since the form sequence

$$a_{\nu_2}^2(a\theta u)\theta_{\nu_1}^3 \equiv H_j^2(j\eta x) \equiv 0 \mod u_x(s, \varrho, t, i, J) :$$

$$\theta_\sigma = a_\sigma(abu)^2 = a_\nu^2(abu)^2\theta_\nu^3.$$

Consequences:

θ^3 or $\theta^2 K$ does not enter into folding with H; θ enters into folding with L only as a contravariant in powers or products, and not at all into folding with σ and $(\nu\sigma x)$.

N does not enter in products in folding with irgend einer form of System II enters, ebensowenig wie with powers or products of forms of System II. There remain an products in System I, taking account of the consequences of the last paragraphs, only products $f \cdot j$, $\Delta \cdot j$, powers of θ and products of $\theta \cdot K$.

§ 14. Forms of the ninth order (System III).

$$\text{Folding of } \begin{cases} \theta \cdot K \text{ with } H, \\ K, j, \Delta \text{ with } L, \\ j, \Delta \text{ with } \sigma, \\ f \text{ with } H^2. \end{cases}$$

Irreducible forms:

A) $(\vartheta \cdot k, \eta, x)^4,\ H_k(\vartheta \cdot k, \eta, x)^4$ B) $(KLu)^3,\ K_i(KLu)^3,\ K_i^2,\ (klx)^3,\ K_i(Klx)^3,$

C) $L_j,\ L_j^2$ D) $\Delta_i,$

E) $(j\sigma x)$ G) $(aH^2u)^3,\ (aH^2u)^4,\ a_\eta(aH^2u)^3.$

reductions:

A) the forms $H_\vartheta(k\eta x)^3,\ H_\vartheta^2(k\eta x)^2,\ H_\vartheta^2(k\eta x)^3$ decompose as arising by successive single folding with decomposable forms.

B) form sequences K_iL_k, $K_i^2(KLu)$, $K_i^2(klx)$:

reducers: $\theta_\eta H_\vartheta$, $a_\eta^2(aHu)$, $\theta_\eta^2(\vartheta\eta x)$.

forms L_i, $K_i(KLu)$, $K_i(klx)$, $(KLu)^2$, $(klx)^2$ decompose as a transvectionen over functional determinants (§ 3).

forms $L_k,\ L_k(KLu),\ L_k(KLu)^2,\ L_k(klx),\ L_k(klx)^2,\ L_k^2,\ L_k^2(KLu),\ L_k^2(klx),\ L_k^3,\ K_i(KLu)^2,\ K_i(klx)^2$ decompose as arising by single folding with the decomposable forms:

$$L_\vartheta,\ H_k(KHu),\ L_\vartheta(\vartheta lx),\ H_k^2,\ L_\vartheta^2,\ L_\vartheta^2(\theta Lu),\ K_\eta(KHu),\ \theta_i(\vartheta lx)$$

according to § 3. 2), a) and b).

C) form sequence $(jlx)^3$: reducer $(j\eta x)^3$.

forms $(jlx)^2$ and $L_j(jlx)$: arising by single folding with the decomposable form $(j\eta x)^2$.

D) form sequence $\Delta_i(\Delta Lu)$: reducer Δ_ν^2.

forms $(\Delta Lu)^2$, $(\Delta Lu)^3$: Single folding with the decomposable form $(\Delta Hu)^2$.

E) form sequence $(j\sigma x)^2$: reducer a_σ^2 by replacing j by lower forms of the form sequence (§ 5):

$$a_\sigma^2(a\theta u)^2 = \frac{1}{3}(j\sigma x)^2, \qquad a_\sigma^2(a\theta\sigma x)^2 = \frac{1}{3}(j\sigma x)^4.$$

F) form sequence Δ_σ^2: reducer a_σ^2.

form Δ_σ: reducer a_σ^2 by replacing Δ by lower forms of the form sequence:

$$a_\sigma a_\varrho^2 = \frac{2}{3}\Delta_\sigma \mod \nu.$$

Consequences: Only the form j enters in folding with σ and $(\nu\sigma x)$ enters.

N does not enter in folding with L enters, since the Δ_i correspondinglye form N_i decomposes.

§ 15. Forms of the tenth order (System III).

$$\text{Folding of } \begin{cases} \theta^2,\ f \cdot j \text{ with } L, \\ \theta \text{ with } H^2. \end{cases}$$

Irreducible forms:

A) $(\vartheta^2 lx)^4,\ \theta_i(\vartheta^2 lx)^4$ B) $(aLu)^2L_j,\ a_i(aLu)^2L_j,$

C) $(\theta H^2u)^3,\ (\theta H^2u)^4,\ H_\vartheta(\theta H^2u),\ \theta_\eta(\theta H^2u)^3.$

reductions:

A) and B): Decomposition of the remaining forms by single folding with decomposable forms.

C) Decomposition of the remaining forms according to § 13 B) by the dualistically opposite consideration.

Consequences:

$\theta^2 K$ does not enter into folding with L; correspondingly, $H^2 L$ does not enter into folding with K. The forms H^3 and $H^2 L$ do not enter into folding with θ. The folding scheme of § 7 is therefore proved.

§ 16. Forms of the 11th, 12th, 13th, and 15th orders (System III).

11th order.

$$\text{Folding of } \begin{cases} \theta \cdot K \text{ with } L, \\ K, j \text{ with } H^2, \\ j \text{ with } (\nu\sigma x), \\ f \text{ with } H \cdot L. \end{cases}$$

Irreducible forms:

A) $(\vartheta \cdot k, l, x)^5,\ \theta_i(\vartheta \cdot k, l, x)^5$ B) $(KH^2u)^4,\ K_\eta(KH^2u)^4,$

C) $(\nu\sigma j),$ D) $(a_\eta H \cdot L, u)^4.$

12th order.

$$\text{Folding of } \begin{cases} \theta^3 \text{ with } L, \\ \theta \text{ with } H \cdot L. \end{cases}$$

Irreducible forms:

E) $(\vartheta^3 lx)^6,$ F) $(\theta, H \cdot L, u)^4,$ $L_\vartheta(\theta, H \cdot L, u^4).$

13th order.

Folding of K with $H \cdot L$.

Irreducible forms:

G) $(K, H \cdot L, u)^5,$ $K_\eta(K, H \cdot L, u)^5.$

15th order.

Folding of K with H^3.

Irreducible form:

H) $(KH^3u)^6.$

reductions:

The forms H_j^2, H_j^2 have reducer L_j^3, from the relation:

$$(\nu lx)L_x^3 = -\frac{1}{2}H^2 \bmod(\sigma, s).$$

Decomposition or reducibility of the remaining forms follows from the considerations of the earlier paragraphs.

Consequences:

According to the folding scheme of § 7 and the consequences of §§ 8–15, the irreducible forms of System III (117 forms) are thereby exhausted.

Chapter IV. The relatively complete system mod (ϱ, t).

§ 17. Reduction of the modulus $(ss'u)^4$ and of the system of s.

For the formation of the next higher relatively complete system, one must, in analogy with § 7, form the system of s with respect to the next modulus

$$\nu(s) = (ss'u)^4$$

and fold it with the forms of the relatively complete system mod s. It will be shown that, after introduction of the modulus (ϱ, t) as the higher modulus,

A) the modulus $(ss'u)^4$ becomes reducible,

B) the system of s consists of the single form s.

A) The reduction of the modulus $(ss'u)^4$ follows at once from the reducer s_ν^2 found by formula (16.), § 11. From

$$s_\nu^2 = \frac{4}{3}ia_\nu^2 + \frac{4}{5}\theta_\varrho^2 + \frac{8}{5}(atu)^2 - \frac{26}{15}(\nu\varrho x)^2 + \frac{1}{6}J\cdot u_x^2 - \frac{2}{9}i^2\cdot u_x^2$$

there follows, by polarization from x to ν_1,

$$\begin{aligned}(ss'u)^4 &= -\frac{2}{3}J\cdot\nu + 6s_\nu^2 s_{\nu_1}^2 \\ &= \frac{24}{5}\theta_\nu^2\theta_\varrho^2 + \frac{48}{5}a_\nu^2(atu)^2 - \frac{52}{5}H_\varrho^2 + \frac{4}{3}i\cdot(asu)^4 + \frac{1}{3}J\cdot\nu - \frac{4}{9}i^2\cdot\nu,\end{aligned} \tag{21}$$

and with this the reduction of the modulus $(ss'u)^4$.

B) The reduction of

$$Z = (ss'u)^2 = \theta(s)$$

and hence the reduction of the system of s is obtained by replacing the form Z by the lower form g_ν^2, according to formula (8.)b, § 7, taking into account the relation

$$s_\eta^2 = s_\nu^2(\nu\nu_1 x)^2 - \frac{1}{3}Z.$$

The form g_ν^2 has, by formula (13.), § 11, the reducer s_ν^2 as a factor. By formula (8.) and (16.) one obtains

$$g_\nu^2 = -Z + \frac{14}{5}ia_\eta^2 + \frac{14}{15}i(asu)^2 \mod(\varrho, t),$$

and by formulas (13.), (14.), (15.), (16.),

$$\begin{aligned}g_\nu^2 &= 2[s_\vartheta^2]_{\nu^2} - \frac{4}{3}i\Delta_\nu^2 = 2s_\vartheta^2 s_\nu^2 - \frac{6}{5}[s_\vartheta^2(\theta su)^2]\widehat{\nu x}^{\,2} - \frac{4}{3}i\Delta_\nu^2 \\ &= \frac{4}{5}i\cdot a_\eta^2 - \frac{2}{5}i\cdot(asu)^2 + \frac{1}{3}J\cdot\theta \mod(\varrho, t).\end{aligned}$$

Thus

$$Z = 2i\cdot a_\eta^2 + \frac{4}{3}i\cdot(asu)^2 - \frac{1}{3}J\cdot\theta \mod(\varrho, t). \tag{23}$$

The relatively complete system mod $((ss'u)^4, \varrho, t)$ therefore passes into a relatively complete system mod (ϱ, t), and from this, by transvection over the known system of two quadratic forms, the absolutely complete system arises. In order to form the relatively complete system mod (ϱ, t), since by formula (23.) the system of s reduces to the form s, we must transvect the relatively complete system mod (s, ϱ, t) over s and over powers of s. It will be shown that powers of s enter into folding only with System I.

The announced relation is

$$\begin{aligned}(ass')^4 &= \frac{24}{5}\theta_\nu^2\theta_\varrho^2 a_\nu^2 a_\varrho^2 + \frac{48}{5}a_\nu^2 b_\nu^2(tab)^2 - \frac{52}{5}H_\varrho^2 a_\nu^4 + \frac{5}{3}J\cdot i - \frac{4}{9}i^3, \\ (ass')^4 &= \frac{24}{5}a_\varrho^2 a_{\varrho'}^2 - \frac{12}{5}t_\varrho^2 + \frac{5}{3}J\cdot i - \frac{4}{9}i^3.\end{aligned} \tag{22}$$

[27] From formula (21.) there follows the relation, mentioned in the note to the introduction, between the three invariants of order 9, with use of formula (10.)c.

Among forms of the same order and the same degree, we define as "higher forms" those which have arisen from higher forms of the relatively complete system mod (s, ϱ, t) by folding with s, regarding the folding with s merely as a polarization of the original forms. Thus the order of the individual forms is uniquely determined (cf. § 1, form sequences 2). For instance,

$$(\theta_\eta(\theta Hu), s, u)^2 \text{ is higher than } s_\eta((\theta Hu)^2, s, u),$$

$$(\theta_\eta(\theta Hu)^2, s, u) \text{ is higher than } (\theta_\eta(\theta Hu), s, u)^2.$$

We divide the resulting system into the four subsystems

System s_I : obtained by folding s and powers of s with System I;

System s_{II} : obtained by folding s with System II;

System s_{III} : obtained by folding s with the individual forms (without products) of System III and with products of one form each from Systems I and II;

System s_{IV} : obtained by folding s with products of one form each from Systems I and III, II and III, III and III.

It should also be noted that from now on all formulas are to be understood mod (ϱ, t); from formula (27.) on, they are to be understood mod $(\varrho, t, i, J,$ higher forms), without this being expressly stated each time.

For the reduction we collect the formulas obtained earlier:

$$\begin{aligned}
s_\nu^2 &= \frac{4}{3} i a_\nu^2 + \frac{1}{6} J \cdot u_x^2 - \frac{2}{9} i^2 \cdot u_x^2, \qquad & s_\nu^3 &= \frac{1}{3} J \cdot u_x, \quad s_\nu^4 = J, \\
g &= 2 s_\vartheta^2 - \frac{4}{3} i \Delta, & s_\vartheta^2(\theta su) &= 0, \\
s_\vartheta^2(\theta su)^2 &= \frac{8}{9} i \cdot a_\nu^3 - \frac{4}{27} i^2 \cdot u_x^2, & & \\
Z &= 2i \cdot a_\eta^2 + \frac{4}{3} i (asu)^2 - \frac{1}{3} J \cdot \theta, & & \\
g_\nu &= -s_\eta + u_x \left\{ 2 i a_\eta^2 - \frac{2}{3} i (asu)^2 + \frac{2}{3} J \cdot \theta \right\}, & & \\
g_\nu^2 &= \frac{4}{5} i a_\eta^2 - \frac{2}{5} i (asu)^2 + \frac{1}{3} J \cdot \theta, & g_\nu^3 &= 0, \qquad g_\nu^4 = 0.
\end{aligned} \tag{24}$$

Consequences:

$$s_\nu^3, \quad s_\vartheta^2(\theta su), \quad s_\vartheta^2 s_\nu, \quad s_\vartheta^2 \theta_\nu$$

are reducers.

§ 18. System s_I.

$$\text{Folding of } \begin{cases} s \text{ with } f;\ \theta;\ K, j, \Delta;\ f \cdot j, N;\ \Delta \cdot j, \\ s^3 \text{ with } \theta, K. \end{cases}$$

Irreducible forms.

Order 5:

$$(asu), \qquad (asu)^2, \qquad (asu)^3, \qquad (asu)^4.$$

Order 6:

(θsu)	$(\theta su)^2$	$(\theta su)^3$	$(\theta su)^4$
s_ϑ	$s_\vartheta(\theta su)$	$s_\vartheta(\theta su)^2$	$s_\vartheta(\theta su)^3$
.	s_ϑ^2	.	.

Order 7:

.	$(Ksu)^2$	$(Ksu)^3$	$(Ksu)^4$	B) s_j,
A) s_k	$s_k(Ksu)$	$s_k(Ksu)^2$	$s_k(Ksu)^3$	C) (Δsu), $(\Delta su)^2$.
.	s_k^2	.	.	

Order 8:

$$\text{A)}\quad s_j(asu),\ s_j(asu)^2,\ s_j(asu)^3,$$
$$\text{B)}\quad (Nsu)^2,\quad s_n,\quad s_n(Nsu).$$

Order 10:

$$\text{A) } s_j(\Delta su),\qquad \text{B) } s_\vartheta(\theta s'u)^4.$$

Order 11:

$$(Ks^2u)^6,\qquad s_k(Ks^2u)^5,\qquad s_k(Ks^2u)^6.$$

Reductions:

The form sequences

$$s_\vartheta^2(\theta su),\quad s_k^2(Ksu),\quad s_j^2,\quad (\Delta su)^3,\quad (Nsu)^3$$

have the reducer $s_\vartheta^2(\theta su)$ as a factor; s_j^2 and $(\Delta su)^3$ are obtained by going back from j and Δ to lower forms of the form sequence:

$$s_\vartheta^2(\theta su)(a\theta u)^3 = -\frac{1}{2}s_j^2,$$
$$s_\vartheta^2(\theta su)(a\theta u)^2 = \frac{1}{3}(\Delta su)^3,$$
$$s_\vartheta^2(\theta su)^2(a\theta u)^2 = \frac{1}{3}(\Delta su)^4 + \frac{1}{3}s_j^2.$$

Forms $s_\vartheta^2 s_{\vartheta'}$ and $s_\vartheta^2 s_{\vartheta'}^2$: reducers $s_\vartheta^2(\theta su)$ and $\theta_{\vartheta'}$:

$$s_\vartheta^2 s_{\vartheta'} = s_\vartheta^2\theta_{\vartheta'} - s_\vartheta^2(\theta s\widehat{\vartheta'}x),$$
$$s_\vartheta^2 s_{\vartheta'}^2 = s_\vartheta^2 s_{\vartheta'}\theta_{\vartheta'} - s_\vartheta^2 s_{\vartheta'}(\theta s\widehat{\vartheta'}x).$$

Form sequence $s_j(\Delta su)^2$: reducers Δ_j and $(\Delta su)^3$.

Consequences:

s does not enter into powers in folding with f, j, Δ, N. The forms f, j, Δ, N enter into folding only in products with contragredient forms; however, in products with f those forms may still be quadratic in x, and in products with Δ they may still be linear in x. Thus the following products of forms are to be considered:

$$f\cdot(0,\lambda),\quad f\cdot(1,\lambda),\quad f\cdot(2,\lambda),\quad j\cdot(\mu,0),\quad N,\quad \Delta\cdot(0,\lambda),\quad \Delta\cdot(1,\lambda)\quad(\lambda>0),$$

where (μ,λ) denotes a form of degree μ in x and of degree λ in u.

Neither θ nor K enters into powers or products with arbitrary forms in folding with s or s^2. For products with the functional determinant K, $K\cdot\varphi_x$ ($\varphi \neq f$ or θ), the relation between decomposing forms is

$$K\cdot\varphi_x = (a\theta u)\varphi_x = f\cdot(\varphi\theta u) - \theta\cdot(\varphi au).$$

The above scheme for folding System s_I is thereby proved.

§ 19. System s_{II}.

Folding of s with $\nu;\ H;\ L;\ H^2$.

Irreducible forms:

Order 6	Order 8	Order 10	Order 12
s_ν	$(Hsu),\ (Hsu)^2$	$(Lsu)^2,\ (Lsu)^3$	$(H^2su)^3$
·	s_η	s_l	·
·	$s_\nu^4 = J$	·	·

Reductions:

Form sequences $s_\eta(Hsu)$ and $s_l(Lsu)$: reducer s_ν^2.

Form sequence s_σ: reducer s_ν^2 from H, $s_\nu^2 = \frac{2}{3}s_\sigma$.

$(H^2su)^4$ decomposes by formula (7.)a (cf. § 11 A). Hence $(H\cdot L, s, u)^4$ also decomposes.

Consequences:

s^2 does not enter into folding with System II. The form ν enters only in products with contragredient forms. The form H, regarded as a covariant, enters into folding in products with forms $(1,\lambda)$, $(2,\lambda)$, $(3,\lambda)$,

with arbitrary λ. The forms σ and $(\nu\sigma x)$ do not enter at all, and L, as a functional determinant, does not enter into products in folding; the full transvections over covariants of System III become reducible. The products of Systems I and II that remain are

$$f \cdot \nu, \qquad \Delta \cdot \nu.$$

§ 20. Forms of order 7 (System s_{III}).

Folding of s with $f \cdot \nu$, a_ν, a_ν^2.
Irreducible forms:

$$\begin{gathered} s_\nu(asu), \quad a_\nu(asu), \quad s_\nu(asu)^2, \quad a_\nu(asu)^2, \quad s_\nu(asu)^3, \quad a_\nu(asu)^3, \\ a_\nu s_\nu, \quad a_\nu s_\nu(asu), \quad a_\nu^2(asu), \quad a_\nu^2(asu)^2. \end{gathered}$$

Reductions:

The evident reductions that arise by direct folding with the reducers s_ν^2 and $s_\eta(Hsu)$ will not be mentioned, nor will the decomposition of transvections with functional determinants.

For the forms $a_\nu s_\nu(asu)^2$ and $a_\nu^2 s_\nu(asu)^2$, see formula (19.), § 12; moreover,

$$a_\nu s_\nu(asu)^3 = a_\nu(a\widehat{\nu}_1\nu_2 u)^3(\nu_1\nu_2\nu) = 0.$$

Form sequence $a_\nu^2 s_\nu$: reducer $s_\vartheta^2(\theta su)$, obtained by going back from a_ν^2 to lower forms, i.e. by double reduction of the expressions

$$s_\vartheta^2(a\theta s)(a\theta u), \qquad s_\vartheta^2(a\theta s)(a\theta u)^2$$

according to the Ansatz

$$\begin{aligned} s_\vartheta^2(a\theta s)(a\theta u) &= [(a\theta u)^2]s^3 + \frac{1}{5}[a_\vartheta(a\theta u)^2]s^2 + \frac{1}{60}[a_\vartheta^2(a\theta u)^2]s \\ &= \frac{1}{2}a_\nu^2 s_\nu - \frac{2}{3}a_\nu^2 s_\nu^2, \\ s_\vartheta^2(a\theta s)(a\theta u)^2 &= \frac{4}{5}[a_\vartheta(a\theta u)^2]_{us}s^2 + \frac{23}{180}[a_\vartheta^2(a\theta u)^2]_{us}s \\ &= -\frac{1}{2}a_\nu^2 s_\nu(asu). \end{aligned}$$

Here $a_\nu^2 b_\nu(abu) = 0$.

The formulas obtained are

$$\begin{aligned} a_\nu^2 s_\nu &= \frac{4}{9}i\, a_\nu^2 b_\nu, & a_\nu s_\nu(asu)^2 &= \frac{1}{3}i\theta_\nu^2 - \frac{1}{18}iH, \\ a_\nu s_\nu(asu)^3 &= 0, & a_\nu^2 s_\nu(asu) &= 0, \\ a_\nu^2 s_\nu(asu)^2 &= 0. \end{aligned} \tag{25}$$

Consequences:

1) $a_\nu s_\nu(asu)^2$ and $a_\nu^2 s_\nu$ are reducers.

2) The values of the forms $(\Delta su)^3$, $(\Delta su)^4$, already recognized as reducible in § 19, are thereby obtained; likewise for the corresponding form sequence $(agu)^2$, which, when folded with ν, gives rise to double reduction through the reducer g_ν:

$$\begin{aligned} &\text{a)} \quad (\Delta su)^3 = -\frac{6}{5}a_\nu^2(asu) + 3a_\nu s_\nu(asu) + 2i\theta_\nu(\theta\nu x), \\ &\text{b)} \quad (\Delta su)^4 = -\frac{2}{5}a_\nu^2(asu)^2 + \frac{4}{3}i\theta_\nu^2 + \frac{1}{9}iH. \end{aligned} \tag{26}$$

From formula (24.) and (26.), mod (i, J) (cf. p. 71),

$$\begin{aligned} &\text{a)} \quad (agu)^2 = \frac{2}{3}(\Delta su)^2 - \frac{4}{3}a_\nu s_\nu + \frac{3}{5}s \cdot a_\nu^2, \\ &\text{b)} \quad (agu)^3 = 2a_\nu s_\nu(asu) - a_\nu^2(asu)^2, \\ &\text{c)} \quad (agu)^4 = -a_\nu^2(asu)^2. \end{aligned} \tag{27}$$

§ 21. Forms of 8th order (System s_{III}).

Folding of s with the forms of 4th order (System III). (§ 9.)

Irreducible forms:

$$\begin{array}{ll}(\vartheta\nu x)s_\nu, & ((\vartheta\nu x), s, u)^2,\\ ((\vartheta\nu x)^2, s, u), & ((\vartheta\nu x)^2, s, u)^2,\ \theta s_\nu,\\ (\vartheta\nu x)^2 s_\nu, & ((\vartheta\nu x)^2, s, u)s_\nu,\end{array}$$

$$\begin{array}{ll}((\vartheta\nu x), s, u)^3,\ (\theta_\nu su)^2, & ((\vartheta\nu x), s, u)^4,\ (\theta_\nu su)^3,\\ ((\vartheta\nu x)^2, s, u)^3,\ (\theta_\nu(\vartheta\nu x), s, u)^2,\ (\theta_\nu^2 su), & ((\vartheta\nu x), s, u)^3,\ (\theta_\nu^2 su)^2,\ (\theta_\nu(\vartheta\nu x), s, u)^4.\end{array}$$

Reductions:

$((\vartheta\nu x), s, u)s_\nu$ decomposes as a transvection over functional determinants, by § 3.

Form sequence $((\vartheta\nu x), s, u)^2 s_\nu$: reducers s_ν^2 and $s_\vartheta^2\theta_\nu$:

$$(\widehat{\vartheta}\nu su)s_\nu(\theta su) = s_\nu s_\vartheta(\theta su) = -\frac{1}{2}(\widehat{\vartheta}\nu su)^2(\theta su),$$

$$\theta_\nu(\widehat{\vartheta}\nu su)s_\nu = \theta_\nu s_\nu s_\vartheta = -\frac{1}{2}\theta_\nu(\widehat{\vartheta}\nu su)^2.$$

Form sequence $\theta_\nu s_\nu(\theta su)$: reducer $a_\nu s_\nu(asu)^2$ by double reduction of the expressions

$$a_\nu s_\nu(asu)^2(abu) \quad \text{and} \quad a_\nu s_\nu(asu)^2(abu)(sbu);$$

$\theta_\nu s_\nu(\theta su)^3$ by double reduction of $(agu)^3(abu)(bgu)^3$.

Form sequence $\theta_\nu(\vartheta\nu x)s_\nu$: reducer $a_\nu^2 s_\nu$ from $\theta_\nu(\vartheta\nu x)s_\nu = a_\nu^2(abu)s_\nu$.

Form sequence $(\theta_\nu(\vartheta\nu x)^2, s, u)$: double reduction of the forms of the sequence $\theta_\nu(\widehat{\vartheta}\nu su)s_\nu$, which at the same time belong to the form sequences $((\vartheta\nu x)su)^2 s_\nu$ and $\theta_\nu(\vartheta\nu x)s_\nu$.

The form $(\theta_\nu(\vartheta\nu x), s, u)$ decomposes as a single transvection over the functional determinant $\theta_\nu(\vartheta\nu x) = a_\nu^2(abu)$.

The form $((\vartheta\nu x)^2, s, u)^4$: double reduction of the expression $(a\Delta u)^2(\Delta su)^4$, or also of $(\theta gu)^4$, from formulas (27.) and analogously to the reduction of $(j\eta x)^4$ (§ 12 C)).

Double reduction gives the formulas:

$$\begin{aligned}
&0 = \theta_\nu s_\nu(\theta su) - \frac{1}{6}(\widehat{\vartheta}\nu su)^2(\theta su) - \frac{1}{12}(Hsu),\\
&0 = \theta_\nu s(\theta su)^2 - \frac{1}{4}(\widehat{\vartheta}\nu su)^2(\theta su)^2 - \frac{1}{24}(Hsu)^2,\\
&0 = (\widehat{\vartheta}\nu su)^2(\theta su)^2 + 2\theta_\nu(\widehat{\vartheta}\nu su)(\theta su)^2 + 3\theta_\nu^2(\theta su)^2 - \frac{1}{3}H(su)^2,\\
&0 = \theta_\nu s_\nu(\theta su)^3 + \frac{1}{2}\theta_\nu(\widehat{\vartheta}\nu su)(\theta su)^3,\\
&0 = \theta_\nu s_\nu s_\vartheta - \frac{1}{4}s_\eta, \quad 0 = \theta_\nu s_\nu s_\vartheta(\theta su), \quad 0 = \theta_\nu s_\nu s_\vartheta(\theta su)^2.
\end{aligned} \tag{28}$$

The last group corresponds to $((\theta_\nu(\vartheta\nu x)^2, s, u)^2, \ldots)$.

Consequences:

1) $\theta(\vartheta\nu x)s_\nu$, $(\widehat{\vartheta}\nu su)(\theta su)s_\nu$, $\theta_\nu(\widehat{\vartheta}\nu su)^2$, $(\widehat{\vartheta}\nu su)^2(\theta su)^2$ are reducers.

2) The forms of 4th order $(5, \lambda)$, $(6, \lambda)$ etc. do not enter into folding with s^2.

3) For the form sequence $(\theta gu)^2$, formulas (27.), with the reductions of this paragraph taken into account, give the following formulas:

$$\begin{aligned}
&\text{a)} \quad (\theta gu)^2 = \frac{4}{3}\theta_\nu s_\nu + \frac{2}{3}s_\nu s_\vartheta - \frac{1}{3}s\theta_\nu^2 - \frac{1}{9}sH - \frac{1}{3}f\,a_\nu^2(asu)^2 + \frac{1}{3}a_\nu^2(asu)^2,\\
&\text{b)} \quad (\theta gu)^3 = -\frac{1}{3}(\widehat{\vartheta}\nu su)^2(\theta su) - \theta_\nu(\widehat{\vartheta}\nu su)(\theta su) - \theta_\nu^2(\theta su),\\
&\text{c)} \quad (\theta gu)^4 = 2\theta_\nu^2(\theta su)^2 - \frac{1}{3}(Hsu)^2,\\
&g\vartheta(\theta gu) = (\widehat{\vartheta}\nu su)(\vartheta\nu x)s_\nu - \theta_\nu(\vartheta\nu x)(\widehat{\vartheta}\nu su),\\
&g\vartheta(\theta gu)^2 = \frac{2}{3}s\theta_\nu^3, \quad g\vartheta(\theta gu)^3 = \frac{1}{3}\theta_\nu^3(\theta su), \quad g\vartheta(\theta gu)^4 = 0.
\end{aligned} \tag{29}$$

§ 22. Forms of 9th order (System s_{III}).

Folding of s with the forms of 5th order (System III) and the product $\Delta \cdot \nu$ (§ 10).
Irreducible forms:

A) $(k\nu x)^2 s_\nu, ((k\nu x)^3, s, u), (k\nu x)^3 s_\nu, ((k\nu x)^2, s, u)^2, K_\nu s_\nu,$
$((k\nu x)^3, s, u)^2, ((k\nu x)^2, s, u) s_\nu, (K_\nu (k\nu x)^3, s, u),$
$(K_\nu su)^2,\ (K_\nu su)^3,\ (K_\nu su)^4, ((k\nu x)^2, s, u)^3, (K_\nu^2 su)^4,$

B) $(j\nu x) s_\nu, ((j\nu x)^2, s, u), (j\nu x)^3, s, u, ((j\nu x)^2, s, u)^2,$

C) $s_\nu(\Delta su), \quad (\Delta_\nu su),$

D) $(aHu) s_\eta, (a_\eta su), ((aHu), s, u)^2, ((aHu)^2, s, u),$
$(aHu)^2 s_\eta, (a_\eta su)^2, (a_\eta^2 su), ((aHu), s, u)^3, ((aHu)^2, s, u)^2,$
$((aHu), s, u)^4, (a_\eta su)^3, (a_\eta (aHu), s, u)^2, (a_\eta (aHu)^2, s, u), (a_\eta (aHu), s, u)^3.$

Reductions:

A) The reductions follow directly from the reductions of § 21 by single folding. The form sequence $K_\nu s_\nu (Ksu)^2$ has the reducers $a_\nu s_\nu (asu)^2$ and $\theta_\nu s_\nu (\theta su)^2$ as factors. Hence the higher forms $K_\nu^2 (Ksu)^2$, $K_\nu^2 (Ksu)^3$ decompose according to the Ansatz:

$$0 = a_\nu s_\nu (asu)^2 (a\theta u) = K_\nu s_\nu (Ksu)^2 - \theta_\nu s_\nu (\theta su)^2 (a\theta u).$$

B) Form sequence $(j\nu x)^2 s_\nu$: reducer $a_\nu^2 s_\nu$ from

$$(j\nu x)^2 s_\nu = 3 a_\nu^2 s_\nu (a\theta u)^2.$$

$((j\nu x)^3, s, u)^2$: reducer $a_\nu^2 s_\nu$ from

$$((j\nu x)^3, s, u)^2 = -6 a_\nu^2 s_\nu (a\theta u)^2 (\theta su).$$

C) Forms $\Delta_\nu (\Delta su)^2$ and $s_\nu (\Delta su)^2$: reducer g_ν from formula (27.)a.

Form $\Delta_\nu s_\nu$: 1) reducer $a_\nu^2 s_\nu$ from $a_g a_\nu^2 s_\nu = \frac{2}{3} \Delta_\nu s_\nu$; 2) decomposes by formula (27.)a through double reduction of the expression $(\Delta s \widehat{\nu} x)^2$.

Hence the higher form $a_\eta s_\eta$ decomposes.

D) Form sequence $(aHu)^2 s_\eta (asu)$: reducer $a_\nu s_\nu (asu)^2$ by double reduction of the form sequence $[a_\nu s_\nu (asu)^2]_{\nu_1 x^2}$; reduction of $(aHu)^2 s_\eta (asu)^2$ from $a_\nu s_\nu (asu)^2$ and $a_\nu s_\nu (asu)^3$. Hence the reduction of $(a_\eta, s, u)^4$.

Form sequence $a_\eta (aHu) s_\eta$: reducers $a_\nu^2 s_\nu$, $a_\eta^2 s_\eta$ by double reduction of the expression $(\Delta s \widehat{\nu} x)^3$, since $a_\eta^2 s_\eta$ does not arise by folding from the reducible term $a_\nu^2 s_\nu (\nu \nu_1 x)$ of the form $a_\eta (aHu) s_\eta$.

Form sequence $(a_\eta^2 su)^2$: reducer $a_\nu^2 s_\nu$ from

$$a_\nu^2 s_\nu s_{\nu_1} = -\frac{1}{2} (a_\eta^2 (Hsu))^2.$$

The form $(a_\eta (aHu), s, u)$ decomposes as a transvection over a functional determinant.

The reduction formulas obtained are:

$$\begin{aligned}
&\text{a)} \quad 0 = (aHu)^2 (asu) s_\eta - a_\eta (asu) (Hsu)^2 - a_\eta (aHu) (asu) (Hsu), \\
&\text{b)} \quad 0 = (aHu)^2 (asu)^2 s_\eta - a_\eta (aHu) (asu)^2 (Hsu), \\
&\text{c)} \quad 0 = a_\eta (asu)^2 (Hsu)^2, \\
&\qquad\quad 0 = a_\eta s_\eta + \frac{1}{4} a_\nu^2 g - \frac{1}{4} s \cdot a_\eta^2, \\
&\qquad\quad 0 = a_\eta (aHu) s_\eta - \frac{1}{2} a_\eta^2 (Hsu), \quad 0 = a_\eta^2 (Hsu)^2, \ldots, \quad 0 = a_\eta^2 s_\eta.
\end{aligned} \tag{30}$$

Consequences:

1) $(j\nu x)^2 s_\nu$, $\Delta_\nu s_\nu$, $\Delta_\nu (\Delta su)^2$, and consequently $N_\nu (Nsu)^2$, $(aHu)^2 (asu) s_\eta$, $a_\eta (aHu) s_\eta$, $a_\eta^2 (Hsu)^2$, are reducers; $a_\eta s_\eta$ is a decomposable form that passes into decomposable forms under all single and double foldings.

2) The forms of 5th order $(5, \lambda)$, $(6, \lambda)$ etc. do not enter into folding with s^2.

§ 23. Forms of the tenth order (System s_{III}).

Folding of s with the forms of the sixth order (System III) (§ 11).
Irreducible forms:

A) $(\vartheta^2\nu x)^3 s_\nu, ((\vartheta^2\nu x)^3, s, u), ((\vartheta^2\nu x)^3, s, u)^2, (\vartheta^2\nu x)^3 s_\nu s_\vartheta, \theta_\nu(\vartheta^2\nu x)^3 s_\vartheta,$

B) $a_\nu(j\nu x)s_\nu, (a_\nu(j\nu x), s, u)^2, (a_\nu(j\nu x), s, u)^3, (a_\nu(j\nu x), s, u)^4, (a_\nu^2(j\nu x), s, u)^2, (a_\nu^2(j\nu x), s, u)^3,$

C) $((\vartheta\eta x)^2, s, u), ((\vartheta\eta x), s, u)^2, (\theta Hu)s_\eta, (\theta_\eta su), ((\theta Hu), s, u)^2, ((\theta Hu)^2, s, u),$
$((\theta\eta x), s, u)^3, (\theta_\eta su)^2, (\theta_\eta^2 su), ((\theta Hu), s, u)^3, ((\theta Hu)^2, s, u)^2, (H_\vartheta(\theta Hu), s, u)^2,$
$(\theta_\eta(\theta Hu), s, u)^2, (\theta_\eta(\theta Hu)^2, s, u), ((\theta Hu), s, u)^4, (\theta_\eta su)^4, (\theta_\eta(\theta Hu), s, u)^3, (\theta_\eta^2(\theta Hu), s, u)^2.$

Reductions: A) The forms $((\vartheta^2\nu x)^3, s, u)^2$, $((\vartheta^2\nu x)^3, s, u)^3$ decompose:

$$(\vartheta\nu x)(\widehat{\vartheta\nu su})(\widehat{\vartheta\nu su}) = (\vartheta\nu x)s_\vartheta s_\nu - (\vartheta\nu x)s_\nu s_\vartheta = -2\theta(\vartheta\nu x)s_\nu s_\vartheta + (\vartheta\nu x)s_\vartheta^2.$$

The remaining forms either have reducers as factors or are single foldings with decomposed forms.

B) Reducer $a_\nu^2 s_\nu$ and $(\widehat{j\nu su})s_\nu$.

C) 1. The form sequence $(\theta Hu)^2 s_\eta$: a) reducer $(aHu)^2(asu)s_\eta$; b) double reduction of the form sequences $(\theta gu)^3 g_\nu$ and $g_\nu(agu)^3(bgu)^3(abu)$. Hence reduction of the higher forms $(\theta, s, u)^3$, $(H_\vartheta(\theta Hu), s, u)^3$ and $(a_\nu b_{\nu_1}^2, s, u)^4$ [the latter form replacing $(H_\vartheta su)^4$].

2. $(\vartheta\eta x, s, u)^4$: reducer $(a_\eta su)^4$.

3. $((\vartheta\eta x)^2, s, u)^3$: reducer $s_\vartheta^2 s_\nu$ from $(\widehat{\vartheta\eta su})^2(Hsu)$. The forms $(\vartheta\eta x)s_\eta$, $(\vartheta\eta x)^2 s_\eta$, $((\vartheta\eta x)^2, s, u)^2$, $\theta_\eta s_\eta$ decompose by folding with the decomposed form $a_\eta s_\eta$.

4. Form sequences $H_\vartheta(\theta Hu)s_\eta$, $\theta_\eta(\theta Hu)s_\eta$, $H_\vartheta(\vartheta\eta x)s_\eta$, $\theta_\eta(\vartheta\eta x)s_\eta$: reducers $a_\eta(aHu)s_\eta$ and $a_\eta^2 s_\eta$.

The form sequence $(\theta_\eta(\vartheta\eta x), s, u)^2$: reducer $a_\eta^2(Hsu)^2$ [except for $(\theta_\eta^2(\theta Hu), s, u)^2$, which arises from the term $a_\eta^2(\theta su)(Hsu)$ by folding].

5. $(H_\vartheta(\vartheta\eta x), s, u)$, $(H_\vartheta(\vartheta\eta x), s, u)^2$: double reduction of $a_\eta(aHu)s_\eta(abu)$ and $g_\vartheta(\theta gu)g_\nu$.

The form sequence $(H_\vartheta(\vartheta\eta x), s, u)^3$: reducer $((\vartheta\nu x)^2, s, u)^2 s_\nu$.

6. $(H_\vartheta(\theta Hu), s, u)$ decomposes by single folding with the decomposed form $(\theta_\nu(\vartheta\nu x), s, u)$ according to § 3. 2), c), that is, by double reduction of the lower decomposed form $(H_\vartheta su)^2$:[28]

$$\begin{aligned}
0 &= \theta_\nu(\vartheta\nu_1)(\theta su) + \frac{2}{3}\theta_\nu^2(\vartheta\nu_1 x)(\theta su) + \theta_\nu(\vartheta\nu x)(\theta su)s_{\nu_1} \\
&\equiv -\frac{1}{2}H_\vartheta(\theta Hu)(\theta su) + \theta_\eta(\theta su)(Hsu) + \frac{1}{2}H_\vartheta(\theta su)(Hsu) \\
&\equiv -\frac{1}{2}H_\vartheta(\theta Hu)(\theta su) + \theta_\eta(\theta su)(Hsu) + \frac{1}{2}[H_\vartheta]_{sx}^2 - \frac{1}{2}\frac{3}{5}H_\vartheta(\theta Hu)(\theta su) \\
&\equiv -\frac{3}{5}H_\vartheta(\theta Hu)(\theta su).
\end{aligned}$$

By double reduction, according to 1. and 5., the following formulae arise:

$$\begin{aligned}
0 &= \theta_\eta(\theta su)(Hsu)^2 + \frac{1}{4}H_\vartheta(\theta Hu)(\theta su)^2 \\
&\quad - \frac{3}{4}\theta_\eta(\theta Hu)(\theta su)(Hsu) - \frac{5}{4}\theta_\eta(\theta Hu)^2(\theta su)^3 \\
&\quad - (asu)^3 b_\eta(\theta Hu)^2 - a_\nu(asu)^3 b_\nu^2, \\
0 &= H_\vartheta(\theta Hu)(\theta su)^3 - 7\theta_\eta(\theta Hu)(\theta su)^2(Hsu), \\
0 &= a_\nu(asu)^2 b_{\nu_1}^2(bsu)^2 - \theta_\eta(\theta su)^2(Hsu)^2 \\
&\quad + 6\theta_\eta(\theta Hu)(\theta su)^2(Hsu), \\
0 &\equiv (H_\vartheta(\vartheta\eta x), s, u), \qquad\qquad 0 \equiv H_\vartheta(\widehat{\vartheta\eta su})(Hsu) - 4\theta_\eta^2(Hsu).
\end{aligned} \tag{31}$$

Consequences:

1. $(\theta Hu)^2 s_\eta$, $H_\vartheta(\theta Hu)s_\eta$, $\theta_\eta(\theta Hu)s_\eta$, $H_\vartheta(\vartheta\eta x)s_\eta$, $\theta_\eta(\vartheta\eta x)s_\eta$, $(H_\vartheta(\vartheta\eta x), s, u)$, $(\theta_\eta(\vartheta\eta x), s, u)^2$ are reducers.

[28] The sign $\equiv$ means that products of forms of lower degree have been omitted.

2. s^2 does not enter into folding with the forms $(5, \lambda)$, etc., of order 6.

§ 24. Forms of the 11th order (System s_{III}).

Folding of s with the forms of the 7th order (System III) (§ 12).
Irreducible forms:

A) $((k\eta x)^3, s, u)$, $(K_\eta(k\eta x)^3, s, u)$, $(K_\eta su)^2$, $((KHu)^2 su)^2$,
$((KHu)^2, s, u)^3$, $((KHu)^2, s, u)^4$, $(K_\eta(KHu)^2, s, u)^3$,

B) $((j\eta x), s, u)^2$, $(H_j su)$, $((j\eta x), s, u)^3$,

C) $(\Delta_\eta su)$,

D) $(aLu)^2 s_\eta$, $(a_\eta su)^2$, $((aLu)^2, s, u)^2$, $((aLu)^3, s, u)^2$, $((aLu)^3, s, u)^3$, $(a_l(aLu)^2, s, u)^2$.

Reductions:

A) Reduction or decomposition by single folding with the corresponding forms in the symbols $\theta - H$.

$(K_\eta(KHu)^2, s, u)$ and $(K_\eta(KHu)^2, s, u)^2$: decomposition according to § 3. 2), a), by folding with $K_\nu^2(Ksu)$, $K_\nu^2(Ksu)^2$.

$(K_\eta(KHu), s, u)^4 \equiv (a_\nu^2\theta_{\nu_1}, s, u)^4$: decomposition according to § 3. 2), b), from the decomposed form $K_\nu^2(Ksu)^3$.

B) Form sequence $(j\eta x)s_\eta$: reducer $(j\nu x)^2 s_\nu$.

Form $H_j(\widehat{j\eta su})(Hsu)$: reducer $(j\nu x)(\widehat{j\nu su})^2$.

Form $H_j(j\eta x)(Hsu)$: decomposes by reducing the decomposed form $((j\eta x)^2, s, u)^2$ by the reducer $(j\nu x)^2 s_\nu$ (formula (18.)a):

$$0 = -2(j\nu x)^2 s_\nu s_{\nu_1} = [(j\eta x)^2]_{su^2} + H_j(j\eta x)(Hsu).$$

C) Reducers $\Delta_\nu s_\nu$ and $\Delta_\nu(\Delta su)^2$.

D) Reduction and decomposition by single folding with the corresponding forms in the symbols $f - H$.

E) From (30.)c one obtains the reduction of the decomposed form sequence $(a_\sigma su)^2$:

$$0 = a_\eta(Hsu)^2(as\widehat{\nu x})^2 = a_\eta(Hsu)^2(a\widehat{\nu\eta}u)^2 + 2a_\eta(a\widehat{\nu\eta}u)(\widehat{\eta\sigma u})(Hsu)^2 = \frac{1}{3}a_\sigma(asu)^2,$$

$$0 = a_\eta a_\nu(Hsu)^2(as\widehat{\nu x})(asu) = a_\eta(a\widehat{\nu\eta}u)^2(Hsu)^2(asu) + a_\eta(a\widehat{\nu\eta}u)(\widehat{\eta\sigma u})(Hsu)^2(asu) = \frac{1}{3}a_\sigma(asu)^3.$$

Consequence: s^2 does not enter into folding with the forms of order 7.

§ 25. Forms of the 12th, 13th, 14th, and 15th orders (System s_{III}).

Folding of s with the forms of orders 8, 9, 10, 11 (System III) (§§ 13–16).
Irreducible forms:
12th order.

A) $((\vartheta^2\eta x)^4, s, u)$, $\theta_\eta(\vartheta^2\eta x)^3 s_\vartheta$,
B) $((aHu)H_j, s, u)^2$, $((aH \cdot u)H_j, s, u)^3$,
C) $(\theta_\nu su)^2$, $((\theta Lu)^2, s, u)^2$, $((\theta Lu)^3, s, u)$, $((\theta Lu)^2, s, u)^3$, $(\theta_l(\theta Lu)^2, s, u)^2$.

Reductions: The reductions arising by direct folding with reducers or decomposed forms are no longer to be mentioned.

B) Decomposition of $((aHu)H_j, s, u)$ and $(a_\eta(aHu)H_j, s, u)$ as transvections over functional determinants.

Decomposition of $(a_\eta(aHu)H_j, s, u)^2$: double reduction of the decomposed form $[\theta_\nu\theta_{\nu_1}^3]_{su^3}$ (§ 13. C):

$$0 \equiv [\theta_{\nu_1}^3\theta_\nu]_{su^3} \equiv -\frac{3}{4}\theta_\nu(\theta su)^2(\theta\theta' u)\theta_{\nu_1}^3$$
$$\equiv -\frac{9}{8}(\theta\theta'\eta su)(\theta\theta' u)(\theta Hu)(\theta' Hu)\theta'_\nu(\theta su) \equiv -\frac{3}{8}a_\eta(aHu)H_j(asu)^2.$$

C) From formulae (31.) follows the reduction of the decomposed forms

$$[L_\vartheta(\theta Lu)]_{su^3} \quad \text{and} \quad [\theta_l(\theta Lu)]_{s^2u^3},$$

that is, of the products $[\theta_\nu^2 H]_{su^3}$ and $[a_\nu^2(bHu)^2]_{su^3}$:

$$\begin{aligned}
&0 \equiv \theta_\nu^2(\theta su)^2(Hsu), 0 && \equiv [L_\vartheta(\theta Lu)]_{su^4} - 7[\theta_l(\theta Lu)]_{su^4},\\
&0 \equiv a_\nu^2(asu)^2(bHu)^2(bsu)\\
&\qquad + 6\theta_l(\theta Lu)^2(\theta su)(Lsu),\\
&0 \equiv \theta_\nu^3(\theta su)(Hsu)^2\\
&\qquad \text{from } 0 \equiv \theta_l^2(\theta Lu)(\theta su)(Lsu)^2\\
&\qquad \text{(reducer } a_\eta^2(Hsu)^2).
\end{aligned} \tag{32}$$

13th order.

$$\text{A) } ((KLu)^3, s, u)^2,\ ((KLu)^3, s, u)^3, \qquad \text{B) } (L_j su)^2, \qquad \text{C) } ((aH^2u)^3, s, u)^2.$$

14th order.

$$\text{A) } ((aLu)^2 L_j, s, u)^2, \qquad \text{B) } ((\theta H^2 u)^3, s, u)^2.$$

15th order.

$$((KH^2u)^4, s, u)^2.$$

Reductions: Decomposition of $(K_l(KLu)^3, s, u)^2$, $(H_\vartheta(\theta H^2u)^3, s, u)$, $((K, H\cdot L, u)^5, s, u)$ according to § 3. 2), c); that is, with simultaneous consideration of the decomposed forms $(K_l(KLu)^2, s, u)^3$, $(H_\vartheta(\theta H'u)^2, s, u)^2$, $((K, H\cdot L, u)^4, s, u)^2$.
Consequence: s^2 does not enter into folding with individual forms of System III.

§ 26. System s_{IV}.

1) *Folding of s with System I–III.*
Reductions: According to the reductions of the last paragraphs ($a_\nu^2 s_\nu(aHu)^2(asu)s_\eta$, etc.), the forms $(0, \lambda)$, $(1, \lambda)$, $(2, \lambda)$ do not permit foldings I and III simultaneously; hence, by § 18, the forms f, Δ, N do not enter in products in folding to form System s_{IV}.

The form j does not enter into folding, since, by the same reductions, the foldings contragredient to j,

$$(K_\nu(k\nu x)^3, s, u), \qquad ((\vartheta^2\eta x)^4, s, u) \quad \text{etc.},$$

correspond to the foldings cogredient to j:

$$K_\nu(k\nu x)^2 s_k, \qquad (\vartheta^2\eta x)^3 s_\vartheta \quad \text{etc.}$$

2) *Folding of s with System II–III*, that is, of s with $H\cdot(1, \lambda)$, $H\cdot(2, \lambda)$, $H\cdot(3, \lambda)$.
Irreducible forms:

A) $(a_\nu H, s, u)^4, ((aHu)^2 H, s, u)^3, ((aHu)^2 H, s, u)^4,$
$((aLu)^2 H, s, u)^4, ((aLu)^3 H, s, u)^3, ((aH^2u)^3 H, s, u)^4,$

B) $(a_\nu^2 H, s, u)^3, (a_\eta(aHu)^2 H, s, u)^3, (a_l(aLu)^2 H, s, u)^4,$

C) $(\theta_\nu H, s, u)^4, ((\theta Hu)^2 H, s, u)^3, ((\theta Hu)^2 H, s, u)^4,$
$((\theta Lu)^2 H, s, u)^4, ((\theta Lu)^3 H, s, u)^3, ((\theta H^2u)^3 H, s, u)^4,$

D) $(\theta_\eta(\theta Hu)^2 H, s, u)^3, (\theta_l(\theta Lu)^2 H, s, u)^4,$

E) $((KLu)^3 H, s, u)^4, ((KH^2u)^4 H, s, u)^4,$

F) $((j\nu x)^2 H, s, u)^3, ((j\nu x)^2 H, s, u)^4, ((j\eta x)H, s, u)^4,$
$(H_j H, s, u)^3, (L_j H, s, u)^4.$

Reductions: ν does not enter into folding, analogously to j.

B) and D). $(a_\nu^2 H, s, u)^4$ and $(\theta_\nu^2 H, s, u)^4$ decompose by formula (27.)c) and (29.)c), taking into account $(gHu)^2 = -\frac{1}{3}s\sigma$:

$$(a_\nu^2 H, s, u)^4 = \frac{1}{3}(asu)^4\sigma, \qquad (\theta_\nu^2 H, s, u)^4 = -\frac{1}{6}(\theta su)^4\sigma;$$

hence decomposition of $(a_\eta(aHu)H, s, u)^4$, $(\theta_\eta(\theta Hu)H, s, u)^4$.

$(\theta_\nu^2 H, s, u)^3$, $(\theta_\nu^3 H, s, u)^3$, and hence $(\theta_\eta^2(\theta Hu)H, s, u)^4$, decompose according to § 25, forms of order 12, C).

3) *Folding of s with System III–III*, that is, of s with forms of System III:

$$(3,\lambda)(3,\lambda),\quad (3,\lambda)(2,\lambda),\quad (3,\lambda)(1,\lambda),\quad (2,\lambda)(2,\lambda),\quad (2,\lambda)(1,\lambda),\quad (1,\lambda)(1,\lambda).$$

Irreducible forms:

A) $(a_\nu^2 a_\nu^2, s, u)^3, (a_\nu^2 a_\nu^2, s, u)^4, (a^2 a_\eta (aHu)^2, s, u)^3,$

B) $(a_\nu H_j, s, u)^4, ((aHu)^2 H_j, s, u)^3, ((aLu)^2 H_j, s, u)^4, ((aLu)^3 H_j, s, u)^2, ((aH^2u)^3 H_j, s, u)^3.$

Reductions:

Products II–III, for the same order in the symbols ν and f, are to be considered higher than products III–III.

The reductions arise partly from relations between products (syzygies), partly by replacing the products by the corresponding decomposed forms and reducing the folding of these forms with s. Products containing contravariants are always omitted, since they pass into products.

A) f quadratic, symbols ν of arbitrary order. By § 11, formulae (12.), and by analogous computation, one has:

$$1)\quad 0 = a_\nu b_{\nu_1} + \frac{1}{2} f(aHu)^2 - \frac{1}{4}\theta H + \frac{1}{2} u_x H_\vartheta - \frac{1}{4} u_x^2 H_\vartheta^2,$$

$$2)\quad 0 = a_\nu b_{\nu_1}^2 + f a_\eta (aHu)^2 - \theta_\eta - \frac{1}{2} H_\vartheta,$$

$$3)\quad 0 = a_\nu^2 b_{\nu_1}^2 - H_\vartheta^2 + 2\theta_\eta^2.$$

It follows that

$$4)\quad 0 = a_\nu^2 b_{\nu_1}^2 (j\nu_1 x),$$

$$5)\quad L_\vartheta(\theta Lu) = -a_\nu b_\eta (bHu)^2 + \frac{3}{4} a_\nu^2 (bHu)^2 + \frac{3}{4}\theta_\nu^2 H,$$

$$6)\quad L_\vartheta(\theta Lu) = -6 a_\nu b_\eta (bHu)^2 + 2 a_\nu^2 (bHu)^2 - \frac{1}{2}\theta_\nu^2 H,$$

$$7)\quad 0 = a_\nu (bHu)^2 + f(aLu)^3 + \theta_\nu H,$$

$$8)\quad 0 = a_\nu (bLu)^3 + \frac{3}{4}(\theta Hu)^2 H,$$

$$9)\quad 0 = (aHu)^2 (bHu)^2 + 2(\theta Hu)^2 H,$$

$$10)\quad 0 = a_\eta (aHu)^2 b_\eta (bHu)^2,$$

$$11)\quad 0 \equiv [a_\nu^2 b_\eta (bHu)]_{\widehat{su^4}}.$$

The reductions of

$$(H_\vartheta su)^4, \qquad (L_\vartheta(\theta Lu), s, u)^3, \qquad (L_\vartheta(\theta Lu), s, u)^4$$

(formulae (31.) and (32.)) together with formulae 1) to 11) give the reduction of all foldings of s with products that are quadratic in the symbols f and arbitrary in ν.

B) Products of two of the symbols f, θ, j; ν in arbitrary order. By formulae (17.), (18.), (20.), and by direct computation, the relations are:

$$1)\quad 0 = a_\nu \theta_{\nu_1} + \frac{1}{4}\theta(aHu)^2 + \frac{1}{4} f(\theta Hu)^2,$$

$$2)\quad 0 = \theta_\nu \theta_{\nu_1} + \frac{1}{2}\theta(\theta Hu)^2.$$

Therefore:

$$3)\quad 0 = 3a_\nu(\theta Hu)^2 + \theta(aLu)^3 + 2f(\theta Lu)^3,$$

$$4)\quad 0 = 3\theta_\nu(aHu)^2 + f(\theta Lu)^3 + 2\theta(aLu)^3,$$

$$5)\quad 0 = a_\nu(\theta Lu)^3, \qquad 0 = \theta_\nu(aLu)^3, \qquad 0 = (aHu)^2(\theta Hu)^2,$$

$$6)\quad 0 = a_\nu\theta_\nu^2 + \theta_\nu a_\nu^2 + f\theta_\eta(\theta Hu)^2 + \theta a_\eta (aHu)^2,$$

$$7)\quad 0 = \theta_\nu\theta_\nu^2 + \theta\theta_\eta(\theta Hu)^2 + \frac{1}{6} f H_j,$$

8) $0 = a_\nu (j\nu x)^2 + f H_j,$

9) $0 = (aHu)^2 (j\nu x)^2 - 2 a_\nu H_j,$

10) $0 = \theta_\nu (j\nu x)^2,$ $\qquad 0 = \theta H_j,$

11) $0 = a_\nu \theta_\nu^3 - \frac{3}{4}(j\eta x)^2,$

12) $0 = a_\nu^2 \theta_\nu^2 - \frac{1}{3}(j\eta x)^2 - \frac{1}{3}(\Delta Hu)^2,$

13) $0 = a_\nu^2 \theta_\nu^3 - \frac{1}{2} a_\sigma,$

14) $0 = \theta_\nu \theta_\nu^3,$ $\qquad 0 = a_\eta H_j.$

The formulae have been carried far enough for the products to become polarizable: that is, by folding only one new product arises, because a) the folding of the product into itself becomes reducible, and b) the remaining products arising by folding become reducible or lead to contravariants (cf. § 3. 2), a) and b)).

Formulae 1) to 5) give the reduction of all foldings of s with products arising from $a_\nu \theta_\nu$ by folding. Formulae 6) to 10) give the reduction of those products arising from $a_\nu \theta_\nu^2$ by folding. By § 24 A), taking formulae 6) to 10) into account, the foldings of s with products arising from $a_\nu^2 \theta_\nu$ decompose.

One has:

$$0 \equiv a_\nu^2 (asu)^2 \theta_{\nu_1} (\theta su)^2, \qquad 0 \equiv a_\nu^2 (asu) \theta_{\nu_1} (\theta su)^3 - K_\eta (KHu)^2 (Ksu)^3,$$
$$0 \equiv a_\nu^2 (asu)^2 \theta_{\nu_1} (\theta su), \qquad 0 \equiv a_\nu^2 (asu) \theta_{\nu_1} (\theta su)^2,$$
$$0 \equiv a_\nu^2 (asu) \theta_{\nu_1} (\theta su).$$

The reducers

$$((j\eta x)^2, s, u)^3 \text{ [from } (\widehat{\vartheta \eta s u})^2 (Hsu), \text{ § 23. } C3],$$
$$(H_j (j\eta x), s, u)^2 \text{ [§ 24, } B], \quad ((\Delta Hu)^2, s, u)^2 \text{ [§ 24, } C], \quad (a_\sigma su)^2 \text{ [§ 24, } E]$$

together with formulae 11) to 14) give the reduction of all products arising from $a_\nu \theta_{\nu_1}^3$, $a_\nu^2 \theta_{\nu_1}^2$, $a_\nu^2 \theta_{\nu_1}^3$.

Our preceding computations can be summarized in the following *conclusion*:

The relatively complete system modulo (ϱ, t) consists of the following 331 forms and subsystems, which are also reproduced below in tabular order.

Table I (cf. p. 90)

u \ x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0	i				f		Δ		$K_\nu(k\nu x)^3$		$K_\eta(k\eta x)^3$				$(\vartheta^3\eta x)^4$	$H_k(k\vartheta,\eta x)^4$		$\theta_l(\vartheta k,lx)^5$				$(\vartheta^2 lx)^6$
1		u_x				$\theta_\nu(\vartheta\nu x)^2$		$\theta_\eta(\vartheta\eta x)^2$	N	$(k\nu x)^3$	$\theta_\nu(\vartheta^2\nu x)^3$	$(k\eta x)^3$	$H_\vartheta(\vartheta^2\eta x)^3$ $\theta_\eta(\vartheta^2\eta x)^3$		$\theta_l(\vartheta^2 lx)^4$		$(\vartheta k,\eta,x)^4$					
2			a_ν^2		θ a_η^2		$(\vartheta\nu x)^2$	$K_\nu(k\nu x)^2$	$(\vartheta\eta x)^2$	$H_k(k\eta x)^2$ $K_\eta(k\eta x)^2$		$(\vartheta^2\nu x)^3$ $K_l(klx)^3$		$(\vartheta^2\eta x)^3$		$(\vartheta^2 lx)^4$						
3		θ_ν^3		a_ν	$\theta_\nu(\vartheta\nu x)$	Δ_ν a_η	K $H_\vartheta(\vartheta\eta x)$ $\theta_\eta(\vartheta\eta x)$	Δ_η	$(k\nu x)^2$ $\theta_l(\vartheta lx)^2$		$(k\eta x)^2$		$(klx)^3$									
4	ν		H θ_ν^2	$(j\nu x)^3$ $a_\eta(aHu)$	θ_η^2	$(\vartheta\nu x)$ a_l^2		N_ν $(\vartheta\eta x)$		H_η N_η $(\vartheta lx)^2$												
5		$a_\eta(aHu)^2$	$\theta_\eta^2(\theta Hu)$	θ_ν	$\frac{K_\nu^2}{(aHu)}$	θ_η	K_η^2 (ΔHu) a_l		Δ_l													
6	j σ		$(j\nu x)^2$ $(aHu)^2$	L $a_\nu^2(j\nu x)$ $H_\vartheta(\theta Hu)$ $\theta_\eta(\theta Hu)$	$\frac{K_\nu}{\theta_l^2}$			K_η														
7		$\theta_\eta(\theta Hu)^2$	$\frac{H_j(j\eta x)}{a_l(aLu)^2}$		$a_\nu(j\nu x)$ (θHu)		$\Delta_\nu(j\nu x)$ θ_l	K_l^2														
8	H_j^2 $a_l(aLu)^3$	$(\nu\sigma x)$ $(j\nu x)$	$(\theta Hu)^2$	$K_\eta(KHu)^2$ $(j\eta x)$ $(aLu)^2$																		
9		H_j $(aLu)^3$	$a_\eta(aHu)H_j$ $L_\vartheta(\theta Lu)^2$ $\theta_l(\theta Lu)^2$		(KHu)																	
10	$\theta_l(\theta Lu)^3$	L_j^2 $(j\sigma x)$ $a_\eta(aH^2u)^3$		$H_j(aHu)$ $(\theta Lu)^2$																		
11		$(\theta Lu)^3$	$K_l(KLu)^3$ L_j $(aH^3u)^3$																			
12	$(aH^2u)^4$	$a_\eta(aLu)^2L_j$ $H_\vartheta(\theta H^2u)^3$ $\theta_\eta(\theta H^2u)^3$		$(KLu)^3$																		
13	$(\nu\sigma j)$		$(aLu)^2L_j$ $(\theta H^3u)^3$																			
14	$(\theta H^2u)^4$	$K_\eta(KH^2u)^4$ $(a_\eta H\cdot L,u)^4$																				
15	$L_\vartheta(\theta,H\cdot L,u)^4$		$(KH^2u)^4$																			
16	$(\theta,H\cdot L,u)^5$																					
17	$K_\eta(K,H\cdot L,u)^5$																					
18		$(K,H\cdot L,u)^5$																				
19																						
20																						
21	$(KH^3u)^6$																					

(The numbers in the uppermost horizontal row denote the degree in the x; the numbers in the first vertical row denote the degree in the u.)

Table II (cf. p. 90)

u \ x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	J				s		s_j^3					s_ν	$(k\nu x)^3 s_\nu$	$(\vartheta^3\nu x)^2 s_\vartheta$ $(\vartheta^2\nu x)^2 s_\vartheta$		$\theta_\eta(\vartheta^2\eta x)^2 s_\eta$	
1							(asu)	s_η	s_i^2 (Δsu)	$s_\eta(Nsu)$ $(\vartheta\nu x)^2 s,u$	$((k\nu x)^3,s,u)_x$ $(K_\nu(k\nu x)^3,s,u)$		$K_\eta(k\eta x)^3,s,u$		$(\vartheta^2\nu x)^2 s_\nu$		$(\vartheta^2\eta x)^4,s,u$
2					$(asu)^2$	$s_\vartheta(\vartheta su)$	$(\Delta su)^2/a_\nu s_\nu$	$(\vartheta\nu x)^2,s,u$ $(\theta_l(\vartheta\nu x)^2,s,u)$		$\theta_\eta(\vartheta^2\eta x)^2,s,u$		$(k\eta x)^2 s_\nu$ $((k\nu x)^2,s,u)$		$(k\eta x)^3,s,u$			
3			$(asu)^3$	$s_\vartheta(\theta su)^2$ s_ν	$a_\nu s_\nu(asu)$ $a_l^2(asu)$	s_η	(θsu) $a_l^2 su$		$(Nsu)^2$ $(\vartheta\eta x)s_\nu$ $((\vartheta\nu x)^2,s,u)$	$((k\nu x)^2,s,u)^2$	$(\vartheta^2\eta x)^2,s,u$						
4	$(asu)^4$	$s_\vartheta(\theta su)^3$	$a_\nu^2(asu)^2$	$(\theta_\nu^2 su)$	$(\theta su)^2$	$s_k(Ksu)^3$ $a_\nu(asu)$ $s_\nu(asu)$	$((\vartheta\nu x)^2,s,u)^2$	$s_\nu(\Delta su)$ (Δsu) $(aHu)s_\eta$ $(a_\nu su)$		$(\Delta_\eta su)$							
5			$(\theta su)^3$	$s_k(Ksu)^3,s_j$ $s_\vartheta(\theta s'u)^4$ $s_\nu(asu)^2$ $a_\nu(asu)^2$	(Hsu) $((\vartheta\nu x)^2,s,u)$ $(\theta_\nu(\vartheta\nu x)^2,s,u)$ $(\theta_\nu^2 su)$	$((j\nu x)^2,s,u)$ $(aHu)^2 s_\nu$ $(a_\eta su)^2$	$(Ksu)^2$ s_η $(\theta_\eta^2 su)$		$((k\nu x)^2,s,u)^2$ $K_\nu s_\nu$								
6	$(\theta su)^4$	$s_\nu(asu)^3$ $a_\nu(asu)^3$	$(Hsu)^2$ $(\theta_\nu(\vartheta\nu x),s,u)^3$ $(\theta_\nu^2 su)^2$	$a_\eta s_\nu^2$ $(a_\eta(aHu),s,u)^2$ $(a_\eta(aH^2u),s,u)$	$(Ksu)^3$	$s_\eta(asu)$ $((\vartheta\nu x),s,u)^3$ $(\theta_\eta su)$	$((k\nu x)^2,s,u)^3$	$s_\nu(\Delta su)$ $a_\nu(j\nu x)s_\nu$ $(\theta Hu)s_\eta$ $(\theta_\eta su)$									
7	$\theta_\nu(\vartheta\nu x),s,u)^4$	$(a_\eta(aHu),s,u)^3$	$(Ksu)^4$ $(\theta_\eta^2(\theta Hu),s,u)^2$ $(a_\eta^2-a_l^2,s,u)^3$	$s_j(asu)^3$ $s_k(K^2u)^3$ $((j\nu x),s,u)^2$ $(\theta_\eta su)^2$	$((j\nu x),s,u)$ $((j\eta x),s,u)$ $(aHu),s,u)$ $(aH^2u),s,u)$	$((\vartheta\eta x),s,u)^3$	$(aLu)^3 s_l/(asu)^3$										
8	$(a^2-a_l^2,s,u)^4$	$s_j(asu)^3$ $s_k(K^2u)^3$ $((j\nu x),s,u)^4$ $(\theta_\eta su)^3$	$((j\nu x)^2,s,u)^2$ $(aHu),s,u)^3$ $((aHu)^2,s,u)^3$	$(Lsu)^2$ $(a_l^2(j\nu x),s,u)^3$ $H_\vartheta(\theta Hu),s,u)^3$ $\theta_l(\theta Hu),s,u)^3$	$(asu)^3$	$(K,su)^3$		$(K_\vartheta su)^2$									
9	$K_j^2 su^4$ $((aHu),s,u)^4$	$(Lsu)^4$ $(a_l^2(j\nu x),s,u)^4$ $(\theta_\nu(\theta Hu),s,u)^2$	$(K_\nu^2 u)^6$ $(a_\eta(aLu)^2,s,u)^3$ $(a_l^2 H,s,u)^3$	$(K,su)^3$	$(a_\nu(j\nu x),s,u)^3$ $(\theta Hu),s,u$ $(\theta Hu)^2,s,u$		$(\theta_l su)^3$										
10			$(K,su)^4$ $(a_l^2 a_\eta(aHu)^2,s,u)^3$	$((j\eta x),s,u)^3$ (H_j,su) $((aLu)^2,s,u)^2$ $((aLu)^3,s,u)$													
11	$(a_\nu(j\nu x),s,u)^4$ $((\theta Hu),s,u)^4$	$(K_l(KHu)^2,s,u)^3$ $((j\eta x),s,u)^3$ $((aLu)^2,s,u)^4$ $(a_\eta H,s,u)^3$	$(H^2su)^3$ $\theta_l(\theta Lu)^2,s,u)^3$		$((KHu)^2,s,u)^3$												
12		$(a_\eta(aHu)^2H,s,u)^3$	$((KHu)^3,s,u)^3$	$((aHu)H_j,s,u)^2$ $((\theta Lu)^2,s,u)^3$													
13	$((KHu)^3,s,u)^4$	$((aHu)H_j,s,u)^3$ $((\theta Lu)^2,s,u)^4$ $(\nu\cdot H,s,u)^3$	$(L_j su)^2$ $((aH^3u)^3,s,u)^3$ $((j\eta x)H,s,u)^3$ $((aHu)^2H,s,u)^3$														
14	$((j\nu x)^2H,s,u)^4$ $((aHu)^2H,s,u)^4$	$(\theta_\eta(\theta Hu)^2H,s,u)^3$		$((KLu)^3,s,u)^2$													
15	$(a_l(aLu)^3H,s,u)^4$	$((KLu)^3,s,u)^3$	$((aLu)^4L_j,s,u)^2$ $((\theta Hu)^3H,s,u)^3$ $((\theta Hu)^2H,s,u)^2$														
16	$((\theta Hu)^2H,s,u)^4$ $(\sigma\cdot H_j,s,u)^4$	$((j\eta x)H,s,u)^4$ $(H_jH,s,u)^3$ $((aLu)^2H,s,u)^4$ $((aLu)^3H,s,u)^3$															
17	$(\theta(\theta Lu)^2H,s,u)^4$		$((KH^3u)^3,s,u)^3$														
18		$((\theta Lu)^2H,s,u)^4$ $((\theta Lu)^3H,s,u)^3$ $(aHu)^2H,s,u)^4$															
19	$((aH^3u)^3H,s,u)^4$ $(L_jH,s,u)^5$																
20		$((KLu)^3H,s,u)^5$	$((aLu)^3H,s,u)^5$														
21	$((\theta H^3u)^3H,s,u)^4$ $((aLu)^2H_j,s,u)^4$																
22																	
23	$((KH^3u)^4H,s,u)^4$	$((aH^3u)^4H,s,u)^3$															

(The numbers in the uppermost horizontal row denote the degree in the x; the numbers in the first vertical row denote the degree in the u.)

3. On the Invariant Theory of Forms in n Variables[29]

Jahresbericht der DMV 19 (1910), pp. 101–104

In the projective invariant theory of forms in n variables the main problem has been solved: the finiteness of the system of forms has been proved. A series of further questions, however, have not been treated, namely those concerned with methods for investigating the connection among forms. I would like briefly to communicate the results that I have obtained with respect to such questions, but for the sake of clarity I shall first sketch the questions in the ternary domain, where they are known.

I have first in mind the two fundamental theorems of the symbolic method: the theorem that all invariant formations can be represented symbolically, and the second theorem that all relations existing among invariants are obtained by successive application of a small number of symbolic identities; thus the symbolic method gives all relations without leaving the domain of invariants.[30] Built upon this are the processes for generating the forms, the symbolic folding process and the nonsymbolic differentiation processes, the theory of series expansions, and the like. In this connection I should also mention a theorem proved in my dissertation,[31] namely that all foldings can be generated by successive application of the two possible "cogredient" foldings; by this, for a symbolic product $s_x t_x u_\sigma u_\tau$, I mean the two foldings (stu) and $(\sigma\tau x)$. On this theorem one can build the theory of reducers and of the reduction of systems of forms, in analogy with the binary domain, as I showed in my dissertation.

[29] Lecture delivered at the Salzburg meeting of natural scientists, 1909.

[30] Study: *Methoden zur Theorie der ternären Formen.* II. § 6. (Leipzig, Teubner, 1889.)

[31] *Über die Bildung des Formensystems der ternären biquadratischen Form.* § 1. (Crelle's Journal Bd. 134. 1908.)

When we now pass to the n-ary domain, even the first theorem of the symbolic method holds only in a conditional measure. It is well known that already for quaternary forms there occur, besides the point and plane coordinates x and u, line coordinates p_{ik}, the subdeterminants from two rows of point coordinates. Analogously, in the n-ary domain we have rows of variables p_ρ, whose individual elements are the subdeterminants from ρ rows x, and rows of symbols S^ρ, whose elements behave like subdeterminants from ρ rows s cogredient to the u. The symbolic representation by determinants is known to hold only when the symbol rows S^ρ are resolved into the rows s and these are distributed among different determinants; only such aggregates of determinants as depend on the S^ρ then have real meaning. But which aggregates of determinants accomplish this cannot be surveyed, and thereby all the other theorems mentioned in the ternary domain are lost.

I would now like to state a simple principle by which one obtains a symbolic representation explicit in the rows S^ρ, and thereby also recovers the remaining theorems. This is an application of the familiar theorem on corresponding matrices: "To each row of variables p_ρ there corresponds one-to-one another row $q_{n-\rho}$ whose individual elements are subdeterminants from $n-\rho$ rows u connected with the ρ rows x by equations $(u \mid x) = 0$." Correspondingly, to each symbol row S^ρ there is assigned another $S_{n-\rho}$, behaving as if it were composed from $n-\rho$ rows cogredient to the x.

The theorem also permits a second formulation, suited for applications: "To every matrix product $(v^{(1)} \cdots v^{(\rho)} \mid y^{(1)} \cdots y^{(\rho)})$,[32] where the rows of the second matrix are contragredient to those of the first, there is assigned a determinant; and conversely each determinant can be transformed into a matrix product with a prescribed number ρ of rows." Thus determinant and matrix product appear as fully equivalent, and the first theorem of the symbolic method assumes the form: "All invariant formations can be represented symbolically by matrix products." From two symbol rows S^σ, T^τ one can now, with the aid of rows of variables, very easily form a matrix product explicitly containing these symbol rows and hence representing an invariant formation of the form $(S^\sigma \mid p_\sigma)(T^\tau \mid p_\tau)$, namely the following:

$$(q_{n-\sigma-\lambda} S^\sigma \,|\, T_{n-\tau} p_{\tau-\lambda}), \qquad (\lambda = 1, 2, \ldots, \tau \text{ or } n-\sigma). \tag{1}$$

More important is the converse: that all invariant formations can be represented explicitly by matrix products, so that the above process is the extension of the binary and ternary folding process. To prove this converse it is necessary to transfer the second theorem of the symbolic method to the n-ary domain, namely to set up the totality of the independent indecomposable identities in which all rows S^ρ, p_ρ are regarded as indecomposable. These identities arise from the known ones containing only rows x and u,[33] by replacing the product theorem for determinants by a system of product theorems for matrices, and by contracting different matrix products into a single one by means of precisely these product theorems. One obtains in this way two dualistic formulas, of which only one is given:

$$\begin{gathered}(S_1^{\rho_1} S_2^{\rho_2} \cdots S_k^{\rho_k} \mid x p_{\rho-1}) = \sum_{i=1}^{k} \varepsilon\, (S_1^{\rho_1} \cdots S_{i-1}^{\rho_{i-1}} S_{i+1}^{\rho_{i+1}} \cdots S_k^{\rho_k} q_{n-\rho+1} \mid S_{n-\rho_i} x), \\ \rho = \sum_{i=1}^{k} \rho_i < n, \qquad \varepsilon = \pm 1.\end{gathered} \tag{2}$$

The only specialization contained in these formulas, namely that a row x enters, cannot be avoided; for completely general symbol and variable rows we arrive at a "decomposition identity," an identity in which a row p_ρ is decomposed into the individual rows x. The simplest special case of the decomposition identity was already used by Clebsch in his "fundamental problem of invariant theory" to derive the elementary covariants in the theory of series expansions. With the aid of these identities, which mediate the transition from the non-explicit determinant expressions to the matrix product, one can in fact show that the desired explicit symbolic representation is obtained with the matrix representation.

For the folding process, however, a theorem entirely analogous to that in the ternary domain holds, and the reduction theorems can likewise be built upon it analogously. If in (1) one denotes the number λ as the defect of the folding, and calls foldings for which $\sigma = \tau$ cogredient, then all foldings can be generated by successive application of the cogredient foldings of defect 1. The proof of this theorem rests essentially on the fact that the most general forms can be replaced by "normal forms," that is, by forms that vanish identically under the application of all invariant differential operations. In the quaternary domain this latter fact was proved by Mertens;[34] our knowledge of the most general differential operations–which, as is well

[32] That is, the sum over the products of corresponding determinants, formed from the matrix of the ρ rows v and that of the ρ rows y.

[33] E. Pascal in *Memorie d. R. Acc. d. Lincei.* (4) 5 (1888), p. 375.

[34] Über invariante Gebilde quaternärer Formen. Wiener Berichte. Bd. 98. 1889.

known, arise from the folding processes by replacing the symbol rows by differential symbols–allows us, using the decomposition identity, to transfer Mertens's proof almost verbatim to the n-ary domain.

4. On the Invariant Theory of Forms in n Variables

Journal für die reine und angewandte Mathematik 139 (1911), pp. 118–154

Introduction.

In the projective invariant theory of forms in n variables, the questions adjoining the main problem–the proof of finiteness of the system of forms–have scarcely been treated when one goes beyond the binary and ternary domains. These are the questions concerning the mutual dependence of the forms and the methods for controlling this connection among forms. These methods rest essentially–as has been completely proved in the binary and ternary domains–on two theorems designated by Study as the "fundamental theorems of the symbolic method," namely the theorem on the symbolic representability of the forms and the theorem on symbolic identities.[35] The latter theorem says that all relations existing among integral invariant formations are obtained by successive application of a small number of symbolic identities; thus the symbolic method, and only it, gives knowledge of the connection among forms without leaving the domain of invariants.

Gordan, in his Erlangen program,[36] already pointed to the reason for the difficulty in passing to n variables: it lies in the fact that the first theorem of the symbolic method is no longer valid in its general form. In the n-ary domain there occur, as is well known, variable rows of higher level p_ρ[37] and analogously symbol rows of higher level S^ρ; one arrives at these rows both when, as originally with Clebsch,[38] one starts from forms with arbitrarily many rows p_ρ, and when one starts, following F. Deruyts and A. Capelli,[39] from forms containing only arbitrarily many cogredient rows x. A symbolic representation that would contain the rows p_ρ, S^ρ explicitly[40] does not exist; it is necessary to resolve the p_ρ, S^ρ into the individual rows x and the s contragredient to them, and to distribute these among different determinants. It is indeed possible, by means of differential conditions (cf. formula (19.)), to verify that a given aggregate of determinants has the property of depending only on the rows p_ρ, S^ρ; but in this way one obtains no overview of the totality of invariant formations and of the processes for their generation.[41]

We shall now show in §§ 2 and 6 how, using the "theorem on corresponding matrices,"[42] the first fundamental theorem is recovered in its generality by replacing representation by determinants with representation by "matrix products." In § 2 it is shown that every matrix product explicitly containing the rows S^ρ, p_ρ is an invariant formation of the ground form; the converse given in § 6, that every invariant formation can be represented explicitly by matrix products, succeeds only through the transfer of the second fundamental theorem (§§ 3–5).

This theorem is known for forms that contain only variable rows x.[43] The general problem, to set up the totality of the indecomposable identities in which all rows S^ρ, p_ρ are regarded as indecomposable, was formulated by Study;[44] at the same time he sees in the number of identities that occur a measure of the difficulty of the methods in the n-ary domain. Since it is now possible to combine the totality of the identities in a single formula (36.), this difficulty is at least pressed down to a minimum. In applications, however, certain distinguished special cases of (36.) will often occur, such as (20.), (21.), characterized by the fact that they admit explicit representation without substitution of new rows; or formula (31.), designated as the "decomposition identity," since a row p_ρ appears to be decomposed into the rows y.

Upon the two fundamental theorems the further theory can now easily be built. The first theorem gives directly the processes for generating the forms, the symbolic folding process and the nonsymbolic differentiation processes,[45] while the decomposition identity eliminates, among these processes, all equivalent

[35] E. Study, *Methoden zur Theorie der ternären Formen* (Leipzig, Teubner, 1889). II. § 6. For the occurrence of these fundamental theorems also in the invariant theory of special transformation groups, cf. Study, *Das Apollonische Problem* (Math. Ann. Bd. 49 [1897]) and *Zur Differentialgeometrie der analytischen Kurven* (Transactions of the American Math. Society, Bd. 1 [1909]).

[36] P. Gordan, *Über das Formensystem binärer Formen.* S. 46. (Leipzig, Teubner, 1875).

[37] For the notation see § 1.

[38] A. Clebsch, über eine Fundamentalaufgabe der Invariantentheorie. (Abh. der Ges. d. Wiss. zu Göttingen, Bd. XVII, 1872).

[39] Cf. A. Capelli, *Lezioni sulla teoria delle forme algebriche* (Napoli 1902), § 22–24, and the literature cited there.

[40] More precise definition of "explicit representation" in § 2.

[41] A computationally very valuable development of the symbolism due to Study (communicated by F. Engel, Ber. d. K. Sächs. Ges. d. Wiss., math.-phys. Kl., 1900, p. 126, and for the quaternary domain by E. Study, *Geometrie der Dynamen*, p. 135) is also not an explicit representation in our sense. It would, for example, hardly lead to the nonsymbolic differentiation processes for generating the forms.

[42] Apart from Grassmann's *Ausdehnungslehre* of 1862, no. 112, first in A. Brill, über zwei Berührungsprobleme, § 2 (Math. Ann. Bd. 4. 1871).

[43] E. Pascal, Giorn. di mat. 26 (1888), pp. 33, 102; Rendic. d. Accad. d. Linc. (4) 4 (1888), p. 119; ib. Mem. (4) 5 (1888), p. 375.

[44] "Methoden . . . ", p. 204, note 17).

[45] In the paper "Invariante Gebilde von Nullsystemen" (Sitzungsber. d. Ak. d. Wiss. Wien, Bd. 97, Abt. IIa, 1888), Mertens arrived by another path, not directly generalizable, at the quaternary folding process. The alternating invariant of 6 rows S^2 occurring there differs from the one arising with us by a single application of substitution (11.) by an aggregate of even invariants. For a special case the quaternary folding process is also

ones (§ 6). Knowledge of the differentiation processes further yields the transfer of the concept of "normal form" to the n-ary domain and, by means of a proof procedure given by Mertens[46] in the quaternary domain, the theorem that a system of invariant formations can be replaced by an equivalent system of normal forms (§ 7). Under this latter assumption I showed in my dissertation[47] that the ternary folding process can be generated by successive application of two fundamental foldings. On the basis of this theorem and the theory of series expansions, I then developed, by introducing the concept of the "form row," the principal reduction theorems for systems of forms. Entirely analogously, in the n-ary domain the folding process can be generated from $n-1$ fundamental foldings (§ 8), and the reduction theorems can be set up (§ 9).

Afterword. On the occasion of the Salzburg communication, Prof. E. Müller of Vienna drew my attention to the fact that the calculation with matrix products underlying this paper is, in principle, identical with the calculus of Grassmann's theory of extension.[48] Indeed, Grassmann's "combinatorial product" $[S^{\rho_1} S^{\rho_2} \cdots S^{\rho_i}]$ can be regarded as a matrix given by these rows (cf. § 2), specifically the "progressive product" as the matrix of the rows themselves, the "regressive" as the matrix of the assigned rows $S_{n-\rho_1}, S_{n-\rho_2}, \ldots, S_{n-\rho_i}$, while the matrix corresponding to the "mixed product" arises when several rows S are combined by substitution (9.) into new rows P, Q. Our "assigned row" corresponds to Grassmann's "complement," our "matrix product" to a "mixed product of level number 0."

Under this correspondence, the development given in the *Ausdehnungslehre* of 1862, no. 113, becomes identical with a formula dualistic to our formula (32.). In the special case $\rho = 1$, (32.) goes over into (17.), the dualistic formula into (16.). From these special cases of Grassmann's development, Müller[49] has recently derived the identities (20.), (21.) mentioned above.

In contrast to the Grassmann–Müller derivation, our derivation at the same time gives the proof of completeness of the identities, which appears to be the essential point for the questions considered here, and it proceeds from (20.), (21.) further to the most general indecomposable identities (36.), which do not seem to have been noticed before now.

§ 1. Notations and definitions. Summary of known results.

We denote, as usual, by the variable row x the row of elements $x_1, x_2, \ldots, x_n$, and analogously by the variable row p_ρ $(\rho = 1, 2, \ldots, n-1)$ the row of the $\binom{n}{\rho}$ elements $p_{i_1 i_2 \ldots i_\rho}$, where $p_{i_1 i_2 \ldots i_\rho}$ denotes the $\binom{n}{\rho}$ determinants formed from the matrix of the ρ rows $x^{(1)}, x^{(2)}, \ldots, x^{(\rho)}$,

$$\begin{vmatrix} x_{i_1}^{(1)} & x_{i_2}^{(1)} & \cdots & x_{i_\rho}^{(1)} \\ x_{i_1}^{(2)} & x_{i_2}^{(2)} & \cdots & x_{i_\rho}^{(2)} \\ \vdots & \vdots & & \vdots \\ x_{i_1}^{(\rho)} & x_{i_2}^{(\rho)} & \cdots & x_{i_\rho}^{(\rho)} \end{vmatrix}, \qquad (i_1 < i_2 < \cdots < i_\rho = 1, 2, \ldots, n).$$

According to the theorem on corresponding matrices,[50] to every row p_ρ there is assigned one-to-one a second row $q_{n-\rho}$ by the relation, valid for each element of the row,

$$p_{i_1 i_2 \ldots i_\rho} = (-1)^{\frac{\rho(\rho+1)}{2} + i_1 + i_2 + \cdots + i_\rho} q_{j_1 j_2 \ldots j_{n-\rho}}, \tag{1}$$

where the i and j are each in good order and together form a complete permutation of the numbers 1 through n. The row $q_{n-\rho}$ consists of the $\binom{n}{\rho}$ determinants of degree $n-\rho$, $q_{j_1 j_2 \ldots j_{n-\rho}}$, formed from the matrix of $n-\rho$ rows $u^{(1)}, u^{(2)}, \ldots, u^{(n-\rho)}$ contragredient to the x. These rows satisfy the $\rho(n-\rho)$ condition equations

$$(u^{(k)} \mid x^{(l)}) = \sum_{\alpha=1}^{n} u_\alpha^{(k)} x_\alpha^{(l)} = 0; \qquad (k = 1, 2, \ldots, n-\rho;\ l = 1, 2, \ldots, \rho). \tag{2}$$

found in P. Gordan, *Das simultane System von zwei quadratischen quaternären Formen* (Math. Ann. Bd. 56. 1903).

[46] F. Mertens, Über invariante Gebilde quaternärer Formen. (Sitzber. d. Ak. d. Wiss. Wien. Bd. 98. Abt. IIa. 1889.)

[47] Über die Bildung des Formensystems der ternären biquadratischen Form. (Dieses Journal, Bd. 134. 1908.)

[48] Hermann GraSSmanns gesammelte mathematische und physikalische Werke. Ersten Bandes zweiter Teil: Die Ausdehnungslehre von 1862. In Gemeinschaft mit H. GraSSmann d. Jüngeren herausgegeben v. Fr. Engel (Leipzig, Teubner 1896).

[49] E. Müller, Beiträge zur GraSSmannschen Ausdehnungslehre. 1. Mitteilung: Einige allgemeine Sätze. (Sitzungsber. d. Ak. d. Wiss. Wien; Bd. 118. Abt. IIa. Juli 1909), Satz 16 und 18.

[50] Cf. for example Gordan–Kerschensteiner, *Vorlesungen über Invariantentheorie*, Bd. I, p. 99.

We shall assume them normalized (with Clebsch[51]) so that the proportionality factor otherwise entering in (1.) is set equal to one.

According to Clebsch[52] (and likewise according to the later investigations of F. Deruyts and A. Capelli, cf. the Introduction), the most general forms can be reduced to those that contain at most one of each of the $n-1$ rows p_ρ, and hence can be represented symbolically as follows:

$$(S^1 \mid p_1)^{m_1}(S^2 \mid p_2)^{m_2} \cdots (S^{n-1} \mid p_{n-1})^{m_{n-1}}, \tag{3}$$

where, in analogy with (2.), we have set

$$(S^\rho \mid p_\rho) = \sum S^{i_1 i_2 \ldots i_\rho} p_{i_1 i_2 \ldots i_\rho}.$$

In consequence of the nonlinear identical relations existing between the elements of a row p_ρ, the symbol rows S^ρ can be normalized so that they satisfy the very same identities, hence so that they behave like the determinants of a ρ-rowed matrix whose rows $s^{(1)}, s^{(2)}, \ldots, s^{(\rho)}$ are contragredient to the x.[53] Thus to each row S^ρ there can be assigned one-to-one another $S_{n-\rho}$ through the relation

$$S_{i_1 i_2 \ldots i_{n-\rho}} = (-1)^{\frac{(n-\rho)(n-\rho+1)}{2} + i_1 + i_2 + \cdots + i_{n-\rho}} S^{j_1 j_2 \ldots j_\rho}, \tag{4}$$

where again the i and j are each in good order and together exactly exhaust the numbers 1 through n. The elements $S_{i_1 i_2 \ldots i_{n-\rho}}$ of the row $S_{n-\rho}$ behave like the determinants formed from $(n-\rho)$ rows $\sigma^{(1)}, \sigma^{(2)}, \ldots, \sigma^{(n-\rho)}$ cogredient to the x, and the rows s and σ are linked by the $\rho(n-\rho)$ conditions

$$(s^{(k)} \mid \sigma^{(l)}) = 0, \qquad (k = 1, 2, \ldots, \rho;\ l = 1, 2, \ldots, n-\rho). \tag{5}$$

In consequence of the relations (1.) and (4.), each factor of (3.) is capable of the equivalent fourfold symbolic representation

$$(S^\rho \mid p_\rho) = (S^\rho q_{n-\rho}) = (S_{n-\rho} p_\rho) = (-1)^{\rho(n-\rho)} (q_{n-\rho} \mid S_{n-\rho}), \tag{6}$$

where, as always in what follows, $(S^\rho q_{n-\rho})$ and $(S_{n-\rho} p_\rho)$ are abbreviations for the determinants $(s^{(1)} \cdots s^{(\rho)} u^{(1)} \cdots u^{(n-\rho)})$ and $(\sigma^{(1)} \cdots \sigma^{(n-\rho)} x^{(1)} \cdots x^{(\rho)})$; by Laplace expansion these prove to depend only on the rows $S^\rho, q_{n-\rho}$ and respectively $S_{n-\rho}, p_\rho$, as the above notation is meant to indicate. The expressions $(S^\rho \mid p_\rho)$ and $(q_{n-\rho} \mid S_{n-\rho})$ mean, according to the preceding discussion, the products of the matrices of the rows s and x, respectively of the rows u and σ, where by matrix product is meant the sum over the products of corresponding determinants, that is, the value of the determinant of the product matrix.

The characteristic number $\rho(n-\rho)$ belonging to a symbol row (respectively variable row) will be called, following Clebsch, the weight of the row;[54] the number ρ, which gives the number of rows s, the upper weight index; the number $n-\rho$, which gives the number of rows σ, the lower weight index. It follows from the relations (4.) that a symbol row can occur in one and the same relation once with upper and once with lower weight index; the same holds for the occurrence of the corresponding rows p_ρ and $q_{n-\rho}$. It remains to note that we generally denote variable rows of higher level whose associated matrix consists of rows x by p, those whose matrix consists of rows u by q; symbol rows cogredient to the x by small Greek letters $\sigma, \tau, \alpha, \beta$; symbol rows cogredient to the u by small Latin letters s, t, a, b; all other symbol rows by capital Latin letters with weight index: S^ρ, T^τ, A^ρ or $S_{n-\sigma}$, $T_{n-\tau}$, $A_{n-\rho}$. Corresponding to an upper or lower weight index, we also write the individual elements of a row with upper or lower indices, as for instance in (4.).

§ 2. Representation by matrix products.

In what follows we always understand by "matrix product" the sum over the products of corresponding determinants of two matrices with the same number of rows, where the rows of the second matrix are contragredient to those of the first. The rows of each matrix may be: 1. individually given; 2. combined, as in (6.), into a row S^ρ; 3. united into different rows $S^\rho, S^\sigma \ldots$. The matrix product is to be denoted by the symbol (|) used in (6.). The representation (6.) is a special application of a second formulation of the theorem on corresponding matrices: "To every ρ-rowed matrix product $(v^{(1)} v^{(2)} \cdots v^{(\rho)} \mid y^{(1)} \cdots y^{(\rho)})$ there

[51] a. a. O. § 5.
[52] a. a. O. § 12.
[53] Clebsch, a. a. O. § 4.
[54] a. a. O. § 11.

is assigned a determinant; and conversely to every determinant there can be assigned a matrix product with prescribed number ρ of rows ($\rho = 1, 2, \ldots, n-1$)."[55] Indeed, one has only to combine the rows y into a row p_ρ (respectively the rows v into a row q_ρ) and to carry out the substitutions given by (1.) in order to pass from a given matrix product to the determinant and conversely. The value of the determinant is, however, not given by its individual elements, but first results from Laplace expansion. Since determinant and matrix product therefore prove to be equivalent, the theorem on the symbolic representability of the forms (the first fundamental theorem) is expressed also as follows:

Theorem I. "All invariant formations can be represented symbolically by matrix products, and conversely all matrix products are invariant formations."[56]

Representation by matrix products allows us to overcome the essential difficulty of the non-explicit representation caused by the determinant representation.[57] By "explicit representation" we mean a representation into which only the rows $S^\rho, T^\tau, \ldots$ themselves enter, or rows R^ρ uniquely derivable from these, but in which the individual component rows $s, t, \ldots$ no longer occur. We shall obtain in § 6, for all invariant formations that depend only on the symbol rows $S^\rho, T^\tau, \ldots$, a representation explicit in these symbol rows, and thereby the transfer to the n-ary domain of the generating processes, the folding process and the differentiation processes. The possibility of explicit representation is evident from the fact that only the simplest matrix products can be assigned precisely to the determinants occurring in the determinant representation, so that all other matrix products are combinations of different determinants into a single expression. For if one resolves the symbol and variable rows into the individual rows s, u, x, then, according to the first fundamental theorem in its usual form, an aggregate of determinants must necessarily arise. The proof that, conversely, all determinant aggregates that represent invariant formations of prescribed ground forms can be combined into explicit matrix products follows by using the second fundamental theorem (§ 6).

In order to obtain from two symbol rows S^σ, T^τ, with the help of variable rows, an invariant formation of the ground form $(S^\sigma \mid p_\sigma)(T^\tau \mid p_\tau)$ that explicitly contains all rows (the folding process), we need only form a matrix product of the third kind according to the definition given at the beginning of the paragraph:

$$(q_{n-\sigma-\lambda} S^\sigma \mid T_{n-\tau} p_{\tau-\lambda}), \qquad (\lambda = 1, 2, \ldots, \tau, n-\sigma). \tag{7}$$

Expanded, (7.) gives:

$$\begin{aligned}(v^{(1)} \ldots v^{(n-\sigma-\lambda)} s^{(1)} \ldots s^{(\sigma)} \mid \alpha^{(1)} \ldots \alpha^{(n-\tau)} y^{(1)} \ldots y^{(\tau-\lambda)}) \\ = \sum_{i,k,l} \varepsilon\, q_{k_1 \ldots k_{n-\sigma-\lambda}} S^{k_{n-\sigma-\lambda+1} \ldots k_{n-\lambda}} T_{l_1 \ldots l_{n-\tau}} p^{l_{n-\tau+1} \ldots l_{n-\lambda}},\end{aligned} \tag{8}$$

that is, an expression depending only on the rows S, T, q, p. Here $\varepsilon = \pm 1$[58] and the sum is to be understood in such a way that the indices of each row $S \ldots$ are in good order, and that for each combination $i_1, i_2, \ldots, i_{n-\lambda}$ the k as well as the l individually run through all then possible permutations of the numbers i. The number λ entering into (7.) will be called the defect of the folding in the case $\sigma > \tau$; the reason for this latter restriction appears in § 6.[59]

The determinants of the two matrices entering in (7.) can be regarded as elements of new rows $Q^{n-\lambda}, P_{n-\lambda}$ whose associated rows are Q_λ, P^λ. According to (8.), these rows Q, P can be expressed through the original S and q, respectively T and p. We indicate this by the equations

$$\begin{aligned} q_{n-\sigma-\lambda} S^\sigma = Q^{n-\lambda} \sim Q_\lambda, \qquad &\text{or also} \quad Q_\lambda = [q_{n-\sigma-\lambda} S^\sigma]_\lambda, \\ T_{n-\tau} p_{\tau-\lambda} = P_{n-\lambda} \sim P^\lambda, \qquad &\text{or also} \quad P^\lambda = [T_{n-\tau} p_{\tau-\lambda}]^\lambda. \end{aligned} \tag{9}$$

Taking (4.) into account, one then has, analogously to (6.), the equivalent fourfold symbolic representation for the matrix product (7.):

$$(q_{n-\sigma-\lambda} S^\sigma \mid T_{n-\tau} p_{\tau-\lambda}) = (q_{n-\sigma-\lambda} S^\sigma P^\lambda) = (Q_\lambda T_{n-\tau} p_{\tau-\lambda}) = (-1)^{\lambda(n-\lambda)} (P^\lambda \mid Q_\lambda). \tag{10}$$

A further substitution of new rows can be performed on (7.) by setting

$$(q_{n-\sigma-\lambda} S^\sigma \mid T_{n-\tau} p_{\tau-\lambda}) = (R^{\sigma+\lambda} \mid p_{\sigma+\lambda})(R^{\tau-\lambda} p_{\tau-\lambda}). \tag{11}$$

[55] For $\rho > n$ the matrix product is known to vanish; for $\rho = n$ it goes into the product of two determinants.

[56] Invariant formations of prescribed ground forms are, of course, only those aggregates of matrix products that depend on the symbol rows $S^\rho \ldots$.

[57] Cf. the Introduction.

[58] This notation is to be retained throughout.

[59] The number λ always runs up to the smaller of the two last indicated numbers.

Here too (8.) shows that the products of the elements of the rows R can be expressed uniquely through the rows S and T. The substitutions (9.) and (11.) will be used especially when a further folding with other rows is performed with (7.).

The matrix representation enables us to state invariantly the quadratic relations between the elements of a row p_ρ (from which, as is known, all the others follow), hence, according to § 1, the relations linear in the coefficients of the ground form that the rows S^ρ satisfy. These are the identities

$$(q_{n-\rho-\lambda}S^\rho \,|\, S_{n-\rho}p_{\rho-\lambda}) = 0, \qquad (\lambda = 1, 2, \ldots, \rho, n-\rho), \tag{12}$$

where the p and q are to be regarded as arbitrary quantities. We shall see in § 5 that the identities with odd defect number λ are consequences of those with higher defect. The relations (12.) are a direct consequence of the relations (5.); for one has

$$(q_{n-\rho-\lambda}S^\rho \,|\, S_{n-\rho}p_{\rho-\lambda}) = (v^{(1)} \cdots v^{(n-\rho-\lambda)}s^{(1)} \cdots s^{(\rho)} \mid \sigma^{(1)} \cdots \sigma^{(n-\rho)}y^{(1)} \cdots y^{(\rho-\lambda)}),$$

and the application of the product theorem gives, in consequence of (5.), a vanishing $(n-\lambda)$-rowed determinant. The identities (12.) say that in order to find all types of foldings it suffices to fold the product of forms linear in each variable row; or also, by § 6, that the normalized form $(S^\rho \mid p_\rho)^m$ possesses no invariant formation linear in the coefficients.[60]

The conditions (12.) are also sufficient to characterize the rows p_ρ. For the property that the individual elements of p_ρ are determinants of a matrix is an invariant property, and therefore it must be expressible invariantly; but by Theorem VI, the conditions (12.) give the greatest possible invariant restriction for the p_ρ, namely that the linear form formed from the row p_ρ as coefficients possesses no invariant formations at all.

§ 3. The symbolic identities.

We now have to transfer the second fundamental theorem of the symbolic method, namely to set up the totality of the irreducible indecomposable identities in which all rows S^ρ, p_ρ are regarded as indecomposable. We also stipulate the following. Corresponding to the meaning of symbol and variable rows, those identities are to be regarded as composite that arise when one specializes the variable row p_ρ to $p_{\rho-1}y$ and applies one of the identities of the system to the resulting expressions; while, on the other hand, identities containing k symbol rows are to count as indecomposable even if they arise from identities with fewer symbol rows by the above process. The rows S^ρ, p_ρ need not necessarily enter the identities explicitly; for their interpretation as indecomposable quantities it suffices to show that the matrix products that occur depend only on these rows. We shall show, however, that in this case, partly by applying substitution (11.), an explicit representation can always be obtained. The general identities are obtained, by means of the principle of matrix representation, from the special identities given by Pascal, which contain only rows x and u and constitute a direct transfer of those given by Study for the ternary domain:[61]

$$\sum_{i=1}^{n}(-1)^{i+1}(a^{(i)} \,|\, x)(a^{(1)} \cdots a^{(i-1)}a^{(i+1)} \cdots a^{(n)}u) = (-1)^{n+1}(u \,|\, x)(a^{(1)} \cdots a^{(n)}), \tag{13}$$

$$\sum \pm(a^{(1)} \,|\, x^{(1)})(a^{(2)} \,|\, x^{(2)}) \cdots (a^{(n)} \,|\, x^{(n)}) = (a^{(1)} \cdots a^{(n)})(x^{(1)} \cdots x^{(n)}), \tag{14}$$

$$\sum_{i=1}^{n}(-1)^{i+1}(u \,|\, a^{(i)})(a^{(1)} \cdots a^{(i-1)}a^{(i+1)} \cdots a^{(n)}x) = (-1)^{n+1}(u \,|\, x)(a^{(1)} \cdots a^{(n)}). \tag{15}$$

Two further identities arise from (13.) and (15.) through the substitutions $(a^{(i)} \mid x) = (a^{(i)}q_{n-1})$ and respectively $(u \mid a^{(i)}) = (p_{n-1}a^{(i)})$, and so by our interpretation they are not to be regarded as essentially different. (14.) represents the product theorem for determinants; we shall show how (13.) and (14.) (and, dualistically, (15.) and (14.)) can be replaced by the system of suitably formed product theorems for matrices. The product theorem, formed once for ρ-rowed matrices and once for $(\rho-1)$-rowed matrices, reads

$$(a^{(1)}a^{(2)} \cdots a^{(\rho)} \,|\, xp_{\rho-1}) = (a^{(1)}a^{(2)} \cdots a^{(\rho)} \mid xy^{(2)} \cdots y^{(\rho)}) = \sum \pm(a^{(1)} \,|\, x)(a^{(2)} \,|\, y^{(2)}) \cdots (a^{(\rho)} \,|\, y^{(\rho)}),$$

$$\sum \pm(a^{(2)} \,|\, y^{(2)}) \cdots (a^{(\rho)} \,|\, y^{(\rho)}) = (a^{(2)} \cdots a^{(\rho)} \mid y^{(2)} \cdots y^{(\rho)}) = (a^{(2)} \cdots a^{(\rho)}p_{\rho-1}) = (a^{(2)} \cdots a^{(\rho)}q_{n-\rho+1});$$

[60] Cf. an addendum by Study in Grassmann's works, first volume, second part, p. 510 (condition that a quantity S^ρ is simple).

[61] For formulation and literature of the problem, cf. the Introduction.

and from this follows the system of product theorems, where $\rho = 2, 3, \ldots, n$:

$$\begin{aligned}(a^{(1)}a^{(2)}\cdots a^{(\rho)} \,|\, xp_{\rho-1}) &= \sum_{i=1}^{\rho}(-1)^{i+1}(a^{(i)} \,|\, x)(a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(\rho)} \,|\, p_{\rho-1}) \\ &= \sum_{i=1}^{\rho}(-1)^{i+1}(a^{(i)} \,|\, x)(a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(\rho)}q_{n-\rho+1}).\end{aligned} \tag{16}$$

For $\rho = n$, (16.) goes over into (13.); if we further specialize $p_{n-1} = y^{(2)}p_{n-2}$, $p_{n-2} = y^{(3)}p_{n-3}$, etc., and apply the identities (16.) to the expressions $(a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(n)} \mid y^{(2)}p_{n-2})$, $(a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(h-1)}a^{(h+1)}\cdots a^{(n)} \mid y^{(3)}p_{n-3})$, etc., then we pass from (13.) to (14.). Thus the identity (14.) is, by our definition, composite from the identities (16.); equivalently, the system (16.) is equivalent to the identities (13.) and (14.). The system (16.) satisfies one of the conditions required for the general identities: it contains the row $p_{\rho-1}$ as an indecomposable quantity and at the same time in explicit form. It is the only system satisfying this condition and only this condition. For we can form no further determinants or matrix products from the rows a, x, p; and between these no relations independent of (16.) can exist, since otherwise, by eliminating $(a^{(1)}\cdots a^{(\rho)} \mid xp_{\rho-1})$, there would arise a relation between ρ ($\rho < n$) expressions $(a^{(i)} \mid x)(a^{(1)}\cdots a^{(i-1)}a^{(i+1)}a^{(\rho)}q_{n-\rho+1})$, whereas by (13.) at least $n+1$ such expressions must enter into a relation. From analogous considerations one obtains the system equivalent to (15.) and (14.):

$$\begin{aligned}(uq_{\rho-1} \,|\, a^{(1)}\cdots a^{(\rho)}) &= \sum_{i=1}^{\rho}(-1)^{i+1}(u \,|\, a^{(i)})(q_{\rho-1} \mid a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(\rho)}) \\ &= \sum_{i=1}^{\rho}(-1)^{i+1}(u \,|\, a^{(i)})(p_{n-\rho+1}a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(\rho)}).\end{aligned} \tag{17}$$

In order to pass from (16.) to identities between arbitrary rows $A^{\rho_1}, B^{\rho_2}, \ldots, x, p$, we observe that these identities must become identical with (16.) as soon as we resolve $A^{\rho_1} = a^{(1)}a^{(2)}\cdots a^{(\rho_1)}$, $B^{\rho_2} = b^{(1)}b^{(2)}\cdots b^{(\rho_2)}$, etc., and that they can also be combined into final expressions only by the operations determined by (16.) as soon as the individual expressions are of the type entering into (16.). Thus we obtain, if we also set

$$\rho = \rho_1 + \rho_2 + \cdots + \rho_k \leq n, \tag{18}$$

$$\begin{aligned}&(a^{(1)}\cdots a^{(\rho_1)}b^{(1)}\cdots b^{(\rho_2)}\cdots k^{(1)}\cdots k^{(\rho_k)} \,|\, xp_{\rho-1}) = (A^{\rho_1}B^{\rho_2}\cdots K^{\rho_k} \,|\, xp_{\rho-1}) \\ &= \sum_{i=1}^{\rho_1}(-1)^{i+1}(a^{(i)} \,|\, x)(a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(\rho_1)}B^{\rho_2}\cdots K^{\rho_k}q_{n-\rho+1}) \\ &\quad + (-1)^{\rho_1\rho_2}\sum_{i=1}^{\rho_2}(-1)^{i+1}(b^{(i)} \,|\, x)(b^{(1)}\cdots b^{(i-1)}b^{(i+1)}\cdots b^{(\rho_2)}A^{\rho_1}\cdots K^{\rho_k}q_{n-\rho+1}) \\ &\quad + \cdots \\ &\quad + (-1)^{(\rho_1+\cdots+\rho_{k-1})\rho_k}\sum_{i=1}^{\rho_k}(-1)^{i+1}(k^{(i)} \,|\, x)(k^{(1)}\cdots k^{(i-1)}k^{(i+1)}\cdots k^{(\rho_k)}A^{\rho_1}\cdots K^{\rho_{k-1}}q_{n-\rho+1}).\end{aligned}$$

Each individual sum (but not already a part of the sum) does in fact contain the rows $A^{\rho_1}, B^{\rho_2}, \ldots$ as indecomposable quantities; for it satisfies the necessary and sufficient conditions[62]

$$\left(a^{(i+1)}\middle|\frac{\partial}{\partial a^{(i)}}\right) = 0;\ \ldots\ ;\left(k^{(j+1)}\middle|\frac{\partial}{\partial k^{(j)}}\right) = 0. \quad (i = 1, 2, \ldots, \rho_1 - 1;\ j = 1, 2, \ldots, \rho_k - 1) \tag{19}$$

We show that it also contains all rows explicitly. For if we set $B^{\rho_2}\cdots K^{\rho_k}q_{n-\rho+1} = q_{n-\rho_1+1}$, then by (16.) and (10.) we obtain

$$\begin{aligned}\sum(-1)^{i+1}(a^{(i)} \,|\, x)(a^{(1)}\cdots a^{(i-1)}a^{(i+1)}\cdots a^{(\rho_1)}q_{n-\rho+1}) &= (A^{\rho_1} \,|\, xp_{\rho_1-1}) \\ &= (A_{n-\rho_1}xp_{\rho_1-1}) = (-1)^{(\rho_1+1)(n+1)}(q_{n-\rho_1+1} \,|\, A_{n-\rho_1}x)\end{aligned}$$

[62] Capelli, a. a. O. § 23, gives sufficient conditions: $\left(a^{(k)} \mid \frac{\partial}{\partial a^{(i)}}\right) = 0$, $(k > i,\ i = 1, 2, \ldots, \rho_1 - 1)$. These most simply imply the necessary and sufficient conditions by application of the Poisson bracket process after Wellstein, Von den Differentialgleichungen der projektiven Invarianten, Math. Ann. 67 (1909) § 3.

$$= (-1)^{(\rho_1+1)(n+1)}(B^{\rho_2}\cdots K^{\rho_k}q_{n-\rho+1}\,|\,A_{n-\rho_1}x).$$

If we compute the remaining sums analogously and subsequently set, since the rows are already characterized as distinct by the weight indices, $B^{\rho_2}=A^{\rho_2}$, $C^{\rho_3}=A^{\rho_3},\ldots$, then we obtain the desired identities:

$$\begin{aligned}(A^{\rho_1}A^{\rho_2}\cdots A^{\rho_k}\,|\,xp_{\rho-1}) &= \sum_{i=1}^{k}(-1)^{\delta_i}(A^{\rho_1}\cdots A^{\rho_{i-1}}A^{\rho_{i+1}}\cdots A^{\rho_k}q_{n-\rho+1}\,|\,A_{n-\rho_i}x),\\ \delta_i &= (\rho_1+\rho_2+\cdots+\rho_{i-1})\rho_i+(\rho_i+1)(n+1),\end{aligned}\tag{20}$$

and from (17.) the dualistic identities:

$$\begin{aligned}(uq_{\sigma-1}\,|\,A_{\sigma_1}A_{\sigma_2}\cdots A_{\sigma_k}) &= \sum_{i=1}^{k}(-1)^{\varepsilon_i}(uA^{n-\sigma_i}\,|\,p_{n-\sigma+1}A_{\sigma_1}\cdots A_{\sigma_{i-1}}A_{\sigma_{i+1}}\cdots A_{\sigma_k}),\\ \varepsilon_i &= (\sigma_1+\sigma_2+\cdots+\sigma_{i-1})\sigma_i+(\sigma_i+1)(n+\sigma).\end{aligned}\tag{21}$$

Theorem II. With (20.) and (21.) the totality of the indecomposable identities between the rows A^{ρ_i},x,p, respectively A_{σ_i},u,q, is exhausted, and at the same time the totality of those indecomposable identities that admit explicit representation without carrying out substitution (11.).

The first part of the theorem follows from the considerations leading to (20.) and (21.); the second part from the impossibility of an identity between two symbol rows:

$$(q_\rho A^\sigma\,|\,B_{\rho+\sigma-\tau}p_\tau) = \varepsilon_1(q_\rho B^{n-\rho-\sigma+\tau}\,|\,A_{n-\sigma}p_\tau)+\varepsilon_2(q_\rho q_{n-\tau}\,|\,B_{\rho+\sigma-\tau}A_{n-\sigma}),$$

where $\rho\le\tau\le\sigma$ and none of the rows has weight $1\cdot(n-1)$. (Other assumptions about ρ,τ,σ can be reduced to this one by interchanging the row designations.) This impossibility follows, for example, by expanding (8.) under the specialization $q_\rho=lM^{\rho-1}$, $q_{n-\tau}=lN^{n-\tau-1}$, if one sets $l_1=1$, $M^{2,3,\ldots,\rho}=1$, $A^{\rho+1,\ldots,\rho+\sigma}=1$, all other elements of the rows l,M,A equal to zero, while N and B are arbitrary. Since identities between arbitrary rows, by resolving a row p_τ into $y^{(1)}y^{(2)}\cdots y^{(\tau)}$, pass into identities composite from (20.), the second part of the assertion is proved as soon as (20.) can be generated from identities with only two symbol rows. In fact, from

$$(A^{\rho_1}A^{\rho_2}\,|\,xp_{\rho-1}) = \varepsilon(A^{\rho_1}q_{n-\rho+1}\,|\,A_{n-\rho_2}x)+(A^{\rho_1}\,|\,xp_{\rho_1-1}),\quad\text{where } p_{\rho_1-1}\sim A^{\rho_2}q_{n-\rho+1},\tag{20a}$$

by specializing $A^{\rho_1}=B^{\sigma_1}B^{\sigma_2}$, that is, by

$$(B^{\sigma_1}B^{\sigma_2}\,|\,xp_{\rho_1-1}) = \varepsilon(B^{\sigma_1}q_{n-\rho_1+1}\,|\,B_{n-\sigma_2}x)+(B^{\sigma_1}\,|\,xp_{\sigma_1-1}),\quad\text{where } p_{\sigma_1-1}\sim B^{\sigma_2}q_{n-\rho_1+1},$$

one obtains an identity (20.) in three symbol rows; and by further specializations of $B^{\sigma_1}=C^{\tau_1}C^{\tau_2}$, etc., the general identities (20.). The nonexistence of the explicit representation of an identity between two symbol rows and two arbitrary variable rows thus implies the nonexistence in the case of arbitrarily many symbol rows, provided that among the variable rows no row x or u is contained.

§ 4. The decomposition identities.

We now consider the most general case of identities among arbitrary symbol and variable rows in whose final expressions, without performing substitution (11.), a row p_τ occurs resolved into its individual rows $y^{(1)} \cdots y^{(\tau)}$; we call these identities "decomposition identities." Following the remark at the end of the preceding paragraph, we first determine them for the case of only two symbol rows, that is, we expand the expression $(q_\rho A^\sigma \,|\, B_{\rho+\sigma-\tau} p_\tau)$. We set:

$$q_{\rho-\alpha}^{(i_1 \dots i_\alpha)} \sim p_{n-\rho}\, y^{(i_1)} \cdots y^{(i_\alpha)}, \qquad p_{\tau-\alpha}^{(i_1 \dots i_\alpha)} = y^{(i_{\alpha+1})} \cdots y^{(i_\tau)}, \qquad p_\tau = y^{(1)} \cdots y^{(\tau)}. \tag{22}$$

With respect to the numbers ρ, σ, τ four cases must be distinguished:

$$\begin{aligned} &1) \quad \rho+\sigma \le n, \quad \tau \le \rho, \quad \tau \le \sigma; \\ &2) \quad \rho+\sigma \le n, \quad \tau \ge \rho, \quad \tau \le \sigma; \\ &3) \quad \rho+\sigma \le n, \quad \tau \le \rho, \quad \tau > \sigma; \\ &4) \quad \rho+\sigma \le n, \quad \tau \ge \rho, \quad \tau \ge \sigma. \end{aligned}$$

We shall single out the first case, and then briefly characterize the others from it. By (20.), (10.) and (9.) we obtain, when we decompose the row $y^{(1)} y^{(2)} \cdots y^{(\tau)} B_{\rho+\sigma-\tau}$ into $y^{(1)}$ and $y^{(2)} \cdots y^{(\tau)} B_{\rho+\sigma-\tau}$:

$$\begin{aligned} (q_\rho A^\sigma \,|\, y^{(1)} y^{(2)} \cdots y^{(\tau)} B_{\rho+\sigma-\tau}) &= (q_\rho^{(1)} A^\sigma \,|\, y^{(2)} \cdots y^{(\tau)} B_{\rho+\sigma-\tau}) \\ &\quad + (-1)^\rho (q_\rho [A_{n-\sigma} y^{(1)}]^{\sigma-1} \,|\, y^{(2)} \cdots y^{(\tau)} B_{\rho+\sigma-\tau}). \end{aligned} \tag{23}$$

The last term in (23.) now has exactly the form of the original expression–only σ is replaced by $\sigma-1$, and τ by $\tau-1$–and therefore again admits equation (23.). Thus, since $\tau \le \sigma$, we can apply operation (23.) τ times and, taking account of (10.), obtain the relation:

$$\begin{aligned} (q_\rho A^\sigma \,|\, p_\tau B_{\rho+\sigma-\tau}) &= (-1)^{\rho\sigma+(\sigma+\tau)(n+1)} (q_\rho B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} p_\tau) \\ &\quad + \sum_{i_1=1}^{\tau} (-1)^{\rho(i_1-1)} (q_{\rho-1}^{(i_1)} [A_{n-\sigma} y^{(1)} \cdots y^{(i_1-1)}]^{\sigma-i_1+1} \,|\, y^{(i_1+1)} \cdots y^{(\tau)} B_{\rho+\sigma-\tau}). \end{aligned} \tag{24}$$

Every term under the summation sign is again of the type of the original expression; ρ is replaced by $\rho-1$, σ by $\sigma-i_1+1$, and τ by $\tau-i_1$, so that condition 1) is even more strongly satisfied. Since $\tau \le \rho$, we can therefore apply operation (24.) τ times and obtain the desired decomposition identity:

$$\begin{aligned} (q_\rho A^\sigma \,|\, p_\tau B_{\rho+\sigma-\tau}) &= \varepsilon_{i_0} (q_\rho B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} p_\tau) \\ &\quad + \sum_{i_1=1}^{\tau} \varepsilon_{i_1} (q_{\rho-1}^{(i_1)} B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} p_{\tau-1}^{(i_1)}) \\ &\quad + \sum_{i_2=i_1+1}^{\tau} \varepsilon_{i_2} (q_{\rho-2}^{(i_1 i_2)} B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} p_{\tau-2}^{(i_1 i_2)}) + \cdots \\ &\quad + \varepsilon_{i_\tau} (q_{\rho-\tau}^{(i_1 \dots i_\tau)} B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma}) \\ &= \sum_{\alpha=0}^{\tau} \sum_{i_\alpha=i_{\alpha-1}+1}^{\tau} \varepsilon_{i_\alpha} (q_{\rho-\alpha}^{(i_1 \dots i_\alpha)} B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} p_{\tau-\alpha}^{(i_1 \dots i_\alpha)}). \end{aligned} \tag{25}$$

For the sign factor ε one obtains from (24.):

$$\begin{aligned} \varepsilon_{i_\alpha} = (-1)^{\delta_{i_\alpha}}, \qquad \delta_{i_\alpha} &= \sum_{\beta=1}^{\alpha} (\rho-\beta+1)(i_{\beta-1}+i_\beta+1) \\ &\quad + (\rho-\alpha)(\sigma+i_\alpha+\alpha) + (\sigma+\tau+\alpha)(n+1), \end{aligned} \tag{26}$$

where $i_0 = 0$ is to be put. The summation sign in (25.) is to be understood as follows: to each combination $i_1 i_2 \dots i_{\alpha-1}$, where $i_1 < i_2 < \cdots < i_{\alpha-1}$, all values i_α for which $i_{\alpha-1} < i_\alpha \le \tau$ are adjoined. Taking (26.) into account, one easily verifies that the individual sums in (25.) satisfy the differential equations analogous to (19.):

$$\left(\frac{\partial}{\partial y^{(i)}} \Big| y^{(i+1)} \right) = 0, \qquad (i = 1, 2, \dots, \tau-1), \tag{27}$$

and hence depend only on the row p_τ. Thus the decomposition identity is an indecomposable identity among the rows A, B, q, p; we shall return to its explicit representation in the next paragraph.

In case 2), operation (23.) can likewise be applied τ times, but operation (24.) stops after the ρ-th application. Thus in the final expression of (25.) the first summation sign must be replaced by $\sum_{\alpha=0}^{\rho}$. In cases 3) and 4), operation (23.) can be carried out only σ times; in place of (24.) one then has the relation:

$$\begin{aligned}(q_\rho A^\sigma \,|\, p_\tau B_{\rho+\sigma-\tau}) = (-1)^{\rho\sigma}(q_\rho^{(\sigma+1\ldots\tau)} B^{n-\rho+\tau-\sigma} \,|\, A_{n-\sigma} p_{\tau-\sigma}^{(\sigma+1\ldots\tau)}) \\ + \sum_{i_1=1}^{\sigma} (-1)^{\rho(i_1-1)} (q_{\rho-1}^{(i_1)} [A_{n-\sigma} y^{(1)} \cdots y^{(i_1-1)}]^{\sigma-i_1+1} \,|\, y^{(i_1+1)} \cdots y^{(\tau)} B_{\rho+\sigma-\tau});\end{aligned} \tag{28}$$

repeating (28.) $\tau-\sigma$ times, where the summation sign becomes $\sum_{i_\beta=i_{\beta-1}+1}^{\sigma+\beta-1}$–as the $(\sigma-i_1+1)$-fold application of (23.) to the terms under the summation sign in (28.) shows–gives all terms of the individual sum in (25.) corresponding to the index $\alpha = \tau - \sigma$, with the corresponding sign. Then cases 3) and 4) pass over into cases 1) and 2), for the numbers corresponding to σ, τ become $\sigma' = \sigma - i_{\tau-\sigma} + \tau - \sigma$, $\tau' = \tau - i_{\tau-\sigma} = \sigma'$; and as the procedure continues, $\tau' < \sigma'$. Thus in the final expression of (25.) the first summation sign must be replaced by $\sum_{\alpha=\tau-\sigma}^{\tau,\rho}$.

Analogously, from (21.) one obtains the dual decomposition identity, in which a row q_ρ is resolved into the individual rows $v^{(1)}, \ldots, v^{(\rho)}$. If we put

$$\dot{p}_{\tau-\beta}^{(i_1\ldots i_\beta)} \sim v^{(i_1)} \cdots v^{(i_\beta)} q_{n-\tau}; \qquad \dot{q}_{\rho-\beta}^{(i_1\ldots i_\beta)} = v^{(i_{\beta+1})} \cdots v^{(i_\rho)}; \qquad q_\rho = v^{(1)} \cdots v^{(\rho)}, \tag{29}$$

then

$$(q_\rho A^\sigma \,|\, p_\tau B_{\rho+\sigma-\tau}) = \sum_{\beta=\max(0,\tau-\sigma)}^{\min(\tau,\rho)} \sum_{i_\beta=i_{\beta-1}+1}^{\rho} \varepsilon(\dot{q}_{\rho-\beta}^{(i_1\ldots i_\beta)} B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} \dot{p}_{\tau-\beta}^{(i_1\ldots i_\beta)}), \tag{30}$$

where the summation index β runs from the larger of the lower values to the smaller of the upper values. All terms of an individual sum in (25.) and (30.) are polars of a single form, produced by the polar processes

$$\left(\frac{\partial}{\partial p_{\tau-\alpha}} \middle| p_{\tau-\alpha}^{(i_1\ldots i_\alpha)}\right), \qquad \left(q_{\rho-\alpha}^{(i_1\ldots i_\alpha)} \middle| \frac{\partial}{\partial q_{\rho-\alpha}}\right).$$

To express this, we denote by Π an aggregate of such polar operations, multiplied by constants, and obtain, in place of (25.) and (30.), the relation

$$(q_\rho A^\sigma \,|\, p_\tau B_{\rho+\sigma-\tau}) = \sum_{\alpha=\max(0,\tau-\sigma)}^{\min(\tau,\rho)} \Pi(q_{\rho-\alpha} B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} p_{\tau-\alpha}). \tag{31}$$

§ 5. The decomposition identities in explicit form.

If in (25), in case 4), we specialize τ to $\sigma + \rho$, we obtain

$$(q_\rho A^\sigma \,|\, y^{(1)} \cdots y^{(\rho+\sigma)}) = \sum_{1\le i_1<\cdots<i_\rho\le\rho+\sigma} \varepsilon_{i_\rho} (q_\rho \,|\, y^{(i_1)} \cdots y^{(i_\rho)}) (A^\sigma \,|\, y^{(i_{\rho+1})} \cdots y^{(i_{\rho+\sigma})}), \tag{32}$$

where $\varepsilon_{i_\rho} = (-1)^{\delta_{i_\rho}}$ and $\delta_{i_\rho} = \rho(\rho+1)/2 + i_1 + \cdots + i_\rho$. This is a more general form of the product theorem for matrices than (16.) and (17.), and follows by Laplace expansion of the determinant of the product matrix

$$\sum \pm (v^{(1)} y^{(1)}) \cdots (v^{(\rho)} y^{(\rho)}) (a^{(1)} y^{(\rho+1)}) \cdots (a^{(\sigma)} y^{(\rho+\sigma)}).$$

Thus the more general product theorem is composed out of the identities (20.) and (21.), respectively, and the selection of the special form (16.), (17.) is thereby explained.

Relation (32.) now gives the means for explicitly representing the decomposition identities. For this purpose we regard the forms occurring in (31.) as ground forms; that is, we perform substitution (11.), which changes nothing in the explicit representation in the rows A, B, since by (8.) the newly introduced rows R can be expressed through the rows A, B themselves and not through their component rows $a^{(1)} a^{(2)} \ldots$, $b^{(1)} b^{(2)} \ldots$. Thus let

$$(q_{\rho-\alpha} B^{n-\rho-\sigma+\tau} \,|\, A_{n-\sigma} p_{\tau-\alpha}) = (R_{\rho-\alpha} p_{n-\rho+\alpha} \,|\, R^{\tau-\alpha} p_{\tau-\alpha}). \tag{33}$$

Then, for the individual sum of (25.) corresponding to the index α, we get

$$\begin{aligned}&\sum \varepsilon_{i_\alpha}(R_{\rho-\alpha}p_{n-\rho}y^{(i_1)}\cdots y^{(i_\alpha)}\,|\,R^{\tau-\alpha}y^{(i_{\alpha+1})}\cdots y^{(i_\tau)})\\&\quad=\sum \varepsilon_{i_\alpha}([R_{\rho-\alpha}p_{n-\rho}]^\alpha y^{(i_1)}\cdots y^{(i_\alpha)}\,|\,R^{\tau-\alpha}y^{(i_{\alpha+1})}\cdots y^{(i_\tau)})\\&\quad=\varepsilon([R_{\rho-\alpha}p_{n-\rho}]^\alpha R^{\tau-\alpha}\,|\,p_\tau)=\varepsilon(R^{\tau-\alpha}q_{n-\tau}\,|\,R_{\rho-\alpha}p_{n-\rho}).\end{aligned}\tag{34}$$

Thus an explicit final expression is in fact obtained, and the symmetric form in which q_ρ and p_τ occur shows that (30.) leads to the same final expression, which is therefore independent of the original decomposition. There is a difference between (25.) and (30.) only as long as the rows y and v have independent meaning, so that the decomposition identity passes, by our definition, into a decomposable identity. To arrive at identities with more symbol rows, one need only, according to § 3 (end), resolve a row q_ρ into $q_{\rho_1}C^{\sigma_1}$, or p_τ into $p_{\tau_1}C_{\tau-\tau_1}$. The resulting expressions

$$(q_{\rho_1}C^{\sigma_1}\,|\,[R^{\tau-\alpha}q_{n-\tau}]_\lambda R_{\rho+\sigma_1-\alpha-\lambda}),\qquad([R_{\rho-\alpha}p_{n-\rho}]^\lambda R^{\tau-\alpha}\,|\,p_{\tau_1}C_{\tau-\tau_1})\tag{35}$$

are exactly of the type that occurs for two symbol rows, and therefore again admit explicit representation after a substitution corresponding to (33.). Repetition therefore gives explicit representation for arbitrarily many rows. It may also be noted that the first and last sums in (25.) and (30.), respectively, give the explicit representation without applying (33), solely by formula (32), or else reduce altogether to a single term containing all rows explicitly. The relation obtained from (32.) by resolving q_ρ into $q_{\rho_1}C^{\sigma_1}$ and so forth can be regarded as the product theorem in its most general form.

In summary we shall show:

Theorem III: With the identities

$$(q_\rho A^\sigma\,|\,p_\tau B_{\rho+\sigma-\tau})=\sum_{\alpha=\max(0,\tau-\sigma)}^{\min(\tau,\rho)}\varepsilon(R^{\tau-\alpha}q_{n-\tau}\,|\,R_{\rho-\alpha}p_{n-\rho}),\tag{36}$$

where the rows R are determined by (33), together with those obtained from them by resolving q_ρ, p_τ into $q_{\rho_1}C^{\sigma_1}$, etc., the totality of indecomposable identities is exhausted.

Indeed, the resulting identities are the most general of their kind, since the individual rows are no longer subject to any restriction as to weight or number, as was still the case in (20.) and (21.). Nor do any further identities among these rows exist; for when a row p_τ is resolved into $y^{(1)}\cdots y^{(\tau)}$, the most general identities are composed out of (20.), hence by § 3 (end) out of (20a.); and the composition discussed following (16.) is precisely the one carried out in § 4. The transition to arbitrarily many rows is supplied, as the discussion of (20a.) shows, by applying always the same operation to the expressions that arise from resolving q_ρ into $q_{\rho_1}C^{\sigma_1}$, and so on. It also follows that the direct transition from (20.) instead of from (20a.) gives nothing new. This is easily verified by calculation, by specializing once a row q_ρ in (25.), and another time carrying out the transition from (20.) by the method of § 4. In both cases the same sums arise, which pass by application of the general product theorem (see above) into the identities obtained from (36.). The identities (20.), (21.) correspond to the special cases $\tau=1$, $\rho=1$; only two individual sums then occur, and hence, in accordance with an earlier remark, explicit representation without the substitution (33.), agreeing with what was found before.

At the end let us briefly mention two special cases of the decomposition identity. Put in (31): $\tau=\sigma$, $\rho=n-\sigma$, and denote the row p_τ by $p'_\sigma\sim q'_{n-\sigma}$. Then

$$(A^\sigma\,|\,p_\sigma)(B^\sigma\,|\,p'_\sigma)-(A^\sigma\,|\,p'_\sigma)(B^\sigma\,|\,p_\sigma)=\sum_{\alpha=1}^{\min(\sigma,n-\sigma)}\Pi(q_{n-\sigma-\alpha}B^\sigma\,|\,A_{n-\sigma}p_{\sigma-\alpha}).\tag{37}$$

This is Clebsch's formula[63] for expanding a form with two cogredient rows p_σ, p'_σ into elementary covariants. The elementary covariants belonging to a form $(A^\sigma\,|\,p_\sigma)^m(B^\sigma\,|\,p'_\sigma)^n$ are then the following:

$$\left\{\sum_{\alpha=1}^{\min(\sigma,n-\sigma)}\varepsilon(q_{n-\sigma-\alpha}B^\sigma\,|\,A_{n-\sigma}p_{\sigma-\alpha})\right\}^\rho(A^\sigma\,|\,p_\sigma)^{m-\rho}(B^\sigma\,|\,p'_\sigma)^{n-\rho},\qquad(\rho=0,1,\ldots,m,n).\tag{38}$$

[63] Clebsch, loc. cit., pp. 25–32. Clebsch proves that the individual terms on the right-hand sides depend only on the rows A, B; the explicit representation would be obtained by applying (32.) to his expressions Φ_h.

They arise, as we shall briefly say, from the ground form by "cogredient folding of defect ρ" (cf. § 2).

Second, put $\tau = \sigma - \lambda$, $\rho = n - \sigma - \lambda$, $B^\sigma = A^\sigma$. Then

$$\begin{aligned}(q_{n-\sigma-\lambda}A^\sigma \,|\, A_{n-\sigma}p_{\sigma-\lambda}) &= (-1)^\lambda (q_{n-\sigma-\lambda}A^\sigma \,|\, A_{n-\sigma}p_{\sigma-\lambda}) \\ &\quad + (-1)^{(n-\sigma)(\sigma-\lambda)} \sum_{\alpha=1}^{\min(\sigma-\lambda,n-\sigma-\lambda)} \Pi(q_{n-\sigma-\lambda-\alpha}A^\sigma \,|\, A_{n-\sigma}p_{\sigma-\lambda}).\end{aligned} \tag{39}$$

Thus, as noted in § 2, the conditions (12.) characterizing the symbol rows for odd defect λ are consequences of the conditions of higher defect. For a linear form $(A^\sigma \,|\, p_\sigma) = (B^\sigma \,|\, p_\sigma)$, (39.) implies that its irreducible invariant formations that are quadratic in the coefficients reduce to ones of even defect; this agrees with the known fact that a linear form in the binary and ternary domains has no invariant formations.

It should be noted that the general identities were originally derived under the assumption that the individual rows satisfy conditions (12.). Since, however, these individual rows enter the identities only linearly, the latter also hold for the more general rows that do not satisfy conditions (12.).

§ 6. Explicit representation of the invariant formations. Folding and differentiation processes.

The results of the preceding paragraphs allow us to complete the theorem stated in § 2 on symbolic representability (the first fundamental theorem) by adding explicit representability; namely, we show:

Theorem IV: "All invariant formations of arbitrary ground forms can be represented explicitly by matrix products; that is, aside from variable rows p_ρ, only the rows $S^\sigma, \ldots, T^\tau$ of the original forms, or the rows P, Q, R derived from them by substitution (9.) or (11.), enter the final expressions."

For the proof, suppose that an invariant formation depends, besides variable rows, on the rows $S^\sigma, \ldots, T^\tau$; and suppose that these rows have been resolved sufficiently far into individual rows $S^\sigma = S^{\sigma_1} \cdots S^{\sigma_i}, \ldots, T^\tau = T^{\tau_1} \cdots T^{\tau_k}$ to make representation by determinants possible. Let the rows be ordered in a sequence $S^\sigma, \ldots, T^\tau$ that is arbitrary in itself but fixed once and for all. We pick out an aggregate of determinants that depends on the first total row $S^\sigma = S^{\sigma_1} \cdots S^{\sigma_i}$, not merely on individual component rows. This dependence, however, is by § 3–§ 5 a consequence of the general identities. If we now resolve a variable row p_ρ into the rows y, v, or one of the later rows T into the individual rows t, respectively τ, then the most general identities are composed out of (20.) and (21.). But these latter identities always lead to an expression containing the row $S^\sigma = S^{\sigma_1} \cdots S^{\sigma_i}$ explicitly, namely the left-hand side of (20.) and (21.); for by (19.) one verifies that only the complete sum on the right–not a part of it corresponding to a term of (20a.)–has the property of depending only on S^σ. As the procedure continues, all rows that have once entered explicitly remain explicit; application of the identities can at most require the combining of several rows into a single one, i.e. substitution (9.). If finally only a single row T^τ remains to be brought to explicit form, two cases are possible. There may still occur a free variable row, that is, one not connected with other rows by substitution (9.); resolving it into component rows y or v completes the procedure and gives, as in (31.), polars of one or more forms containing all rows explicitly. If no free variable row remains, then from the manner in which they arose we recognize, in the totality of the expressions that contain the individual rows t or τ but depend on the row T^τ, the terms of a decomposition identity; by § 5, however, these always admit explicit representation in all rows after applying substitution (11.). This proves the theorem in full generality. It should also be noted that when only two symbol rows occur, substitution (11.) never appears. For, since $\sigma, n-\sigma, \tau, n-\tau < n$, no variable rows can enter only when the two symbol rows are united in a single determinant and thus occur explicitly; but as soon as variable rows enter, (34.) and (33.) show that substitution (11.) becomes unnecessary.

It follows from what has just been said that, in order to generate all invariant formations, it suffices to unite the symbol rows, after adjoining variable rows, into all possible matrix products. The most general matrix product is now of the form

$$(P^{\mu_1} \cdots P^{\mu_i} \,|\, Q_{\nu_1} \cdots Q_{\nu_k}), \qquad \sum \mu = \sum \nu, \tag{40}$$

where the P and Q may be rows of the original forms, or may have arisen from the original rows by a sequence of substitutions (9.) or (11.), or finally may be variable rows. But the expressions (40.) can be generated by successively uniting two symbol rows at a time into a matrix product, with the help of variable rows; for from

$$(q_{n-\mu-\lambda}P^\mu \,|\, Q_{\nu_1}p_{n-\mu-\nu_1-\lambda}) = (R_\lambda Q_{\nu_1} \,|\, p_{n-\mu-\nu_1-\lambda})$$

one obtains, by uniting with the row Q_{ν_2}, an expression

$$([R_\lambda Q_{\nu_1}]^{n-\lambda-\nu_1} \,|\, Q_{\nu_2} p_{n-\mu-\nu_1-\nu_2-\lambda}) = (q_{n-\mu-\lambda} P^\mu \,|\, Q_{\nu_1} Q_{\nu_2} p_{n-\mu-\nu_1-\nu_2-\lambda}),$$

and hence, by continuing the procedure, an expression (40.). If P and Q are not rows of the original forms, then (9.) and (11.), in conjunction with what was just shown, imply that they too arose through a sequence of unions of two symbol rows at a time. Thus:

Theorem V: The process for generating all invariant formations, the folding process, consists in successively uniting two symbol rows at a time into a matrix product, with the help of variable rows.

From two symbol rows S^σ, T^τ, where $\sigma \geq \tau$, the following matrix products can be formed:

$$(q_{n-\sigma-\lambda} S^\sigma \,|\, T_{n-\tau} p_{\tau-\lambda}), \qquad (\lambda = 1, 2, \ldots, \min(\tau, n-\sigma)), \tag{41}$$

$$(q_{n-\tau-\mu} T^\tau \,|\, S_{n-\sigma} p_{\sigma-\mu}), \qquad (\mu = \sigma - \tau + \lambda), \tag{42}$$

$$(q_{n-\tau-\nu} T^\tau \,|\, S_{n-\sigma} p_{\sigma-\nu}), \qquad (\nu = 1, 2, \ldots, \sigma - \tau). \tag{43}$$

From (31.), however, the following values are obtained for (42.) and (43.):

$$(q_{n-\sigma-\lambda} S^\sigma \,|\, T_{n-\tau} p_{\tau-\lambda}) + \sum_\alpha \Pi(q_{n-\sigma-\lambda-\alpha} S^\sigma \,|\, T_{n-\tau} p_{\tau-\lambda-\alpha}), \tag{42a}$$

$$\Pi(q_{n-\sigma} S^\sigma)(T_{n-\tau} p_\tau) + \sum_\beta \Pi(q_{n-\sigma-\beta} S^\sigma \,|\, T_{n-\tau} p_{\tau-\beta}). \tag{43a}$$

Thus the forms (42.) can be expressed linearly by (41.) and polars of (41.), and the forms (43.) by polars of the ground form and of the forms (41.). Likewise (31.) gives the linear dependence of the forms (41.) on (42.) and polars of (42.). Hence, according to Clebsch's definition,[64] the forms (42.) are equivalent to the forms (41.), while (43.) leads back to the ground form. The generating process is therefore given with equal right by (41.) or (42.); we shall define the process (41.), which is simpler with respect to the number λ, as the folding process. The number λ, the defect of the folding (cf. § 2), gives the number of rows missing from the determinant product, namely in that matrix product which, for the given folding, contains the maximal number of rows. Since λ runs only up to the smaller of the two values $\tau, n-\sigma$, where $\sigma \geq \tau$, we have

$$\lambda \leq \frac{n}{2}, \ n \text{ even}; \qquad \lambda \leq \frac{n-1}{2}, \ n \text{ odd}. \tag{44}$$

The reduction of (42.) and (43.) to (41.) remains valid even when, through further folding, the rows p, q have passed into symbol rows; for by (36.) one has

$$(A^{n-\tau-\varkappa} T^\tau \,|\, S_{n-\sigma} B_{\sigma-\varkappa}) = \sum_{\alpha=\max(0,\varkappa-\sigma+\tau)}^{\min(\tau,n-\sigma)} \varepsilon(R^{\tau-\alpha} B^{n-\sigma+\varkappa} \,|\, A_{\tau+\varkappa} R_{n-\sigma-\alpha}),$$

where the rows R have arisen from S and T according to (33.). Thus these forms containing symbol rows only are obtained by folding $(q_\tau A^{n-\tau-\varkappa} \,|\, B_{\sigma-\varkappa} p_{n-\sigma})$ or $(q_{\tau-\alpha} B^{n-\sigma+\varkappa} \,|\, A_{\tau+\varkappa} p_{n-\sigma-\alpha})$–according as $\sigma - \tau \gtreqless 2\varkappa$– with the ground form and the forms (41.).

From the symbolic folding process one obtains, in the usual way, the invariant differentiation processes if one merely replaces the symbol rows $S^\sigma, T_{n-\tau}$ by the rows of differentiation symbols $\frac{\partial}{\partial p_\sigma}$, $\frac{\partial}{\partial q_{n-\tau}}$; as is well known, the product $\frac{\partial}{\partial p_{i_1 \ldots i_\sigma}} \frac{\partial}{\partial q_{j_1 \ldots j_{n-\tau}}}$ then has the real meaning $\frac{\partial^2}{\partial p_{i_1 \ldots i_\sigma} \partial q_{j_1 \ldots j_{n-\tau}}}$. Since the rows $\frac{\partial}{\partial p_\sigma}$ and $\frac{\partial}{\partial q_{n-\tau}}$ are cogredient with the rows $S^\sigma, T_{n-\tau}$, they satisfy the same identities as these, in particular also the ones existing between (42.) and (42a.), and between (43.) and (43a.). In summary we obtain:

Theorem VI: All invariant formations of arbitrary ground forms arise from these by repeated application of the symbolic folding process (41.), or also of the invariant differentiation processes

$$\left(q_{n-\sigma-\lambda} \frac{\partial}{\partial p_\sigma} \,\middle|\, \frac{\partial}{\partial q_{n-\tau}} p_{\tau-\lambda} \right), \qquad (\sigma \geq \tau, \ \lambda = 1, 2, \ldots, \min(\tau, n-\sigma)). \tag{45}$$

It remains to note that in every folding (41.) the total weight of the form, that is, the sum of the weights of the individual variable rows (cf. § 1), decreases by the positive number $2(\lambda^2 + \lambda(\sigma - \tau))$. This implies,

[64] Clebsch, loc. cit., § 7.

independently of the general finiteness proof, the finiteness of the form row, that is, of the totality of invariant formations of a given ground form that are linear in the coefficients.[65]

It should further be noted that Theorem VI still holds for forms that do not satisfy conditions (12.). For each factor in (3), $(S^\rho \,|\, p_\rho)^{m_\rho}$, can be replaced by a product of m_ρ linear factors $(A^\rho \,|\, p_\rho)(B^\rho \,|\, p_\rho)\cdots(M^\rho \,|\, p_\rho)$; the invariant formations thereby pass into those of a system of linear forms, which need only afterwards be set equal to one another. For every single linear form, however, conditions (12.)–which, when differential symbols are introduced, contain only second-order differential quotients–are always satisfied.

§ 7. Expansion of the general forms according to normal forms.

In what follows (§ 8) we shall derive a principal property of the folding process (41.), namely its composability from fundamental foldings. For this we need the transfer to the n-ary domain of an important theorem given by Mertens[66] in the quaternary domain. This theorem says that any finite system of forms can be replaced by an equivalent system of normal forms. By a "normal form" we mean–generalizing the binary and ternary definition[67]–a form all of whose invariant formations linear in the coefficients vanish identically, with the exception of the ground form itself. Thus by Theorem VI (§ 6) a normal form φ satisfies the system of differential equations

$$\left(q_{n-\sigma-\lambda}\frac{\partial}{\partial p_\sigma}\middle|\frac{\partial}{\partial q_{n-\tau}}p_{\tau-\lambda}\right)\varphi = 0, \qquad (\sigma \geq \tau,\ \lambda = 1, 2, \ldots, \min(\tau, n-\sigma)), \tag{46}$$

where the rows $q_{n-\sigma-\lambda}, p_{\tau-\lambda}$ are to be regarded as arbitrary quantities. In the quaternary domain–taking (39.) into account for $\sigma = \tau = 2$–these differential equations agree completely with the ten differential equations given by Mertens without introduction of the arbitrary rows p, q (loc. cit., formula 28). Their knowledge, together with Theorem VI, allows us to transfer his proof almost word for word to n variables. The only thing to add is the verification, obtained by the decomposition identity (30.), that the constructed forms are normal forms; in the quaternary domain this verification still follows without further transformation. It is therefore enough to give a short exposition of the proof, and for simplicity in the case relevant below, namely that of a single ground form f and its form row (cf. § 6, end); for invariant formations of arbitrary degree in the coefficients of arbitrarily many ground forms, the proof remains the same.

The basic idea of the proof is to replace, by introducing the transformed coefficients, a form with $n-1$ rows p_ρ by forms with n rows ξ cogredient to the x, namely the rows of the transformation quantities. From these forms the sought normal forms are obtained directly by invariant differentiation processes. The expansion of the general forms according to normal forms is mediated by a series expansion for forms with ρ ($\rho < n$) cogredient rows ξ; invariant differentiation processes lead back to the forms in the original rows p_ρ.

Let $\xi^{(1)}, \ldots, \xi^{(n)}$ be the rows of transformation quantities, so that

$$\begin{aligned} x_i &= \xi_i^{(1)}x_1' + \xi_i^{(2)}x_2' + \cdots + \xi_i^{(n)}x_n', \\ p_{i_1\ldots i_\rho} &= \sum_j (\xi_{i_1}^{(j_1)}\cdots\xi_{i_\rho}^{(j_\rho)})p'_{j_1\ldots j_\rho}. \end{aligned} \tag{47}$$

The transformed coefficients of the forms $f, \varphi, \ldots$ will be denoted by $(f), (\varphi), \ldots$, and let

$$f = (S^1 \,|\, p_1)^{m_1}(S^2 \,|\, p_2)^{m_2}\cdots(S^{n-1} \,|\, p_{n-1})^{m_{n-1}}.$$

Then

$$\begin{aligned} (f) = (S^1 \,|\, \xi^{(1)})^{m_{11}}\cdots(S^1 \,|\, \xi^{(n)})^{m_{1n}}(S^2 \,|\, \xi^{(1)}\xi^{(2)})^{m_{21}}\cdots(S^{n-1} \,|\, \xi^{(2)}\cdots\xi^{(n)})^{m_{n-1,n}} \\ \cdot (s^{(1)} \,|\, \xi^{(1)})^{k_1}(s^{(2)} \,|\, \xi^{(2)})^{k_2}\cdots(s^{(n)} \,|\, \xi^{(n)})^{k_n}, \end{aligned} \tag{48}$$

where $m_{11} + \cdots + m_{1n} = m_1$, and so on. From each coefficient (f) for which

$$k_1 \geq k_2 \geq k_3 \geq \cdots \geq k_n, \tag{49}$$

the differentiation process exhausting exactly the rows ξ,

$$\left(\frac{\partial}{\partial\xi^{(1)}}\middle|p_1\right)^{k_1-k_2}\left(\frac{\partial}{\partial\xi^{(1)}}\frac{\partial}{\partial\xi^{(2)}}\middle|p_2\right)^{k_2-k_3}\cdots\left(\frac{\partial}{\partial\xi^{(1)}}\cdots\frac{\partial}{\partial\xi^{(n-1)}}\middle|p_{n-1}\right)^{k_{n-1}-k_n}\left(\frac{\partial}{\partial\xi^{(1)}}\cdots\frac{\partial}{\partial\xi^{(n)}}\right)^{k_n} \tag{50}$$

[65] Cf. Clebsch, loc. cit., § 11 and 12: finiteness of the system of elementary covariants.

[66] F. Mertens, *Über invariante Gebilde quaternärer Formen* (see the Introduction), cited as "Mertens."

[67] Study, loc. cit., p. 54.

gives the form

$$\varphi = \left(s^{(1)} \mid p_1\right)^{k_1-k_2}\left(s^{(1)}s^{(2)} \mid p_2\right)^{k_2-k_3}\cdots\left(s^{(1)}\cdots s^{(n-1)} \mid p_{n-1}\right)^{k_{n-1}-k_n}\left(s^{(1)}s^{(2)}\cdots s^{(n)}\right)^{k_n}. \tag{51}$$

The forms φ are the sought normal forms. Indeed, they have the following properties defining normal forms.

1. They are invariant formations of the ground form f that are linear in the coefficients. This follows from the fact that they arise from f by the invariant differentiation processes $\left(\frac{\partial}{\partial p_\rho}\middle|\xi^{(i_1)}\xi^{(i_2)}\cdots\xi^{(i_\rho)}\right)$ and (50.). Thus (by § 6, end) they can be expressed linearly by polars of the finite form row of f. These polars are obtained by regarding the variables p_ρ entering φ as coefficients of a form decomposed into linear forms with the variable rows p_ρ:

$$H = (q_{n-1} \mid p_{n-1})^{k_1-k_2}(q_{n-2} \mid p_{n-2})^{k_2-k_3}\cdots(q_1 \mid p_1)^{k_{n-1}-k_n}. \tag{52}$$

The simultaneous invariants of the form rows f and H give all relevant polars, since the latter must be of the same dimension in the individual rows p_ρ as φ itself.

2. They satisfy the differential equations (46.). If the differential process (45.) is applied to φ, then

$$\varphi' = \left(q_{n-\sigma-\lambda}s^{(1)}\cdots s^{(\sigma)} \mid [s^{(1)}\cdots s^{(\tau)}]_{n-\tau}p_{\tau-\lambda}\right), \qquad (\sigma > \tau).$$

From the decomposition identity (30.) it follows, if the rows $q_\sigma = s^{(1)}\cdots s^{(\sigma)}$, $p_{n-\tau} = [s^{(1)}\cdots s^{(\tau)}]_{n-\tau}$ formed out of the rows s are identified with the q_ρ, p_τ occurring there, that

$$\varphi' = \sum_{\beta=\sigma-\tau+\lambda}^{n-\tau,\sigma}\sum_{i_\beta}\varepsilon\left(q_{\sigma-\beta}^{(i_1\ldots i_\beta)}q_{n-\tau+\lambda} \,|\, p_{\sigma+\lambda}p_{n-\tau-\beta}^{(i_1\ldots i_\beta)}\right).$$

Here

$$p_{n-\tau-\beta}^{(i_1\ldots i_\beta)} \sim s^{(1)}\ldots s^{(\tau)}s^{(i_1)}\ldots s^{(i_\beta)},$$

where $i_1, \ldots, i_\beta$ denote any β distinct numbers chosen from the numbers 1 to σ. Since $\beta > \sigma - \tau$, it follows that among these numbers $i_1, \ldots, i_\beta$ there must be some between 1 and τ; hence $p_{n-\tau-\beta}^{(i_1\ldots i_\beta)}$ vanishes identically, and therefore every individual matrix product, and with it φ', vanishes.

For the equivalence of the system of normal forms with the form row f, it remains only to show that all forms of the form row can be expanded in polars of the normal forms in the sense fixed under 1. Let Π be an aggregate of polar operations

$$\left(\frac{\partial}{\partial\xi^{(i)}}\middle|\xi^{(k)}\right), \qquad (i \neq k;\ i = 1, 2, \ldots, \rho;\ k = 1, 2, \ldots, \rho), \tag{53}$$

and let Π^σ be an aggregate of the special operations (53.) for which $i = \sigma$ and $k < \sigma$. For a form F of the ρ rows $\xi^{(1)}, \ldots, \xi^{(\rho)}$ that has degree k_ρ in the row $\xi^{(\rho)}$, the expansion[68] holds:

$$F = \sum_{\alpha=0}^{k_\rho}\Pi F_\alpha, \qquad (\rho \leq n), \tag{54}$$

where F_α has degree α in the last row $\xi^{(\rho)}$ and arises from F by the invariant differential operations

$$\left(\frac{\partial}{\partial\xi^{(1)}}\cdots\frac{\partial}{\partial\xi^{(\rho)}}\middle|\xi^{(1)}\ldots\xi^{(\rho)}\right)^\alpha \tag{55}$$

and Π^ρ. If, in constructing F_α, one replaces process (55.) by

$$\left(\frac{\partial}{\partial\xi^{(1)}}\cdots\frac{\partial}{\partial\xi^{(\rho)}}\middle|p_\rho\right)^\alpha, \tag{56}$$

then a form $F_\alpha(p_\rho)$ with only $\rho - 1$ rows $\xi^{(1)}, \ldots, \xi^{(\rho-1)}$ is obtained, to which (54.) can again be applied. Continuing the procedure leads to forms $G(p_\rho, p_{\rho-1}, \ldots, p_1)$. In order to obtain from these the expansion of F according to (54.), one replaces the individual rows p_ρ by $\xi^{(1)}, \ldots, \xi^{(\rho)}$ and applies to the resulting forms

[68] F. Mertens, *Über eine Formel der Determinantentheorie.* Sitzungsberichte der Akademie der Wissenschaften, Vienna, Math.-Naturw. Kl., vol. 91, 2nd section (1885), formula 20).

the polar process Π (53.); this gives (cf. (48.)) a sum of transformed coefficients (G). For $\rho = n$, the process (55.) remains at the first step. If c denotes numerical constants and we put, for brevity,

$$(\xi^{(1)}\xi^{(2)}\dots\xi^{(n)}) \sim \Delta; \qquad \left(\frac{\partial}{\partial\xi^{(1)}}\frac{\partial}{\partial\xi^{(2)}}\cdots\frac{\partial}{\partial\xi^{(n)}}\right) = \nabla, \tag{57}$$

then, in the case $\rho = n$,

$$F = \sum c\Delta^{\alpha}(G), \tag{58}$$

whereas for $\rho < n$ only $\alpha = 0$, and hence $\sum c(G)$, appears on the right.

Applying (58.) to a transformed coefficient (f) (48.), and using the commutativity of the polar processes Π^{σ} with all operations (56.) for which $\rho \geq \sigma$, as well as the fact that polars of transformed coefficients again give transformed coefficients, one obtains

$$G = \left(\frac{\partial}{\partial\xi^{(1)}}\middle|p_1\right)^{\beta_1}\left(\frac{\partial}{\partial\xi^{(1)}}\frac{\partial}{\partial\xi^{(2)}}\middle|p_2\right)^{\beta_2}\cdots\left(\frac{\partial}{\partial\xi^{(1)}}\cdots\frac{\partial}{\partial\xi^{(n-1)}}\middle|p_{n-1}\right)^{\beta_{n-1}}\nabla^{\beta_n}\Pi(f) = \sum c\varphi,$$

and from (58.) it follows that

$$(f) = \sum c\Delta^{\alpha}(\varphi) \qquad \text{(Mertens, formula 23))}. \tag{59}$$

To pass from (59.) to the expansion of f itself, we again regard the variables p_{ρ} as coefficients of a form H (52.) with the degrees $m_1, \dots, m_{n-1}$ corresponding to f, and put $m = m_1 + \dots + m_{n-1}$. Then, by the definition of invariants,

$$f \cdot \Delta^m = \sum(f)(H) = \sum c\Delta^{\alpha}(\varphi)(H),$$

and application of the process ∇^m that exactly exhausts the rows ξ gives

$$f = \sum c\Phi, \tag{60}$$

where the forms Φ are derived from φ and H by invariant differentiation processes with respect to the variables, and hence are simultaneous invariants of the form rows φ and H.[69] But since φ is a normal form, the form row φ reduces to the form φ itself; the form row H contains all possible invariant variable combinations. Thus the simultaneous invariants of φ and H are the polars of φ in the sense indicated under 1.; in other words, (60.) gives the expansion of f in polars of the normal forms. It remains to verify the same expansion for an arbitrary form θ of the form row f. Let Γ be the normal forms derived from (θ) by (50.), so that

$$(\theta) = \sum c\Delta^{\beta}(\Gamma). \tag{61}$$

The forms θ are characterized by the relation, valid for every transformed coefficient,

$$(\theta)\Delta^{\sigma} = \sum c(f) \qquad \text{(Mertens, formula 9))}.$$

But every form F of the n rows ξ which contains the factor Δ^{σ} also contains the second $\nabla^{\sigma}\Pi F$ (Mertens, formula 20)); hence

$$(\theta) = \sum c\nabla^{\sigma}(f), \qquad \text{therefore} \qquad \Gamma = \sum c\varphi,$$

and from (61.) we obtain the relation corresponding to (59.),

$$(\theta) = \sum c\Delta^{\beta}(\varphi),$$

which implies for θ the expansion (60.) in polars of the normal forms φ. Thus:

Theorem VII. Every form row f can be replaced by an equivalent system of normal forms.

[69] Instead of the direct conclusion, Mertens, § 7, introduces a series of further differential processes that essentially serve to form the form row H; this is done by our Theorem VI.

§ 8. Reduction of the folding process to fundamental foldings.

Following Theorem VII, we now carry out the reduction of the folding process to fundamental foldings mentioned at the beginning of § 7. We call (cf. § 5) every folding of two cogredient rows S^ρ, T^ρ a "cogredient folding", and specifically the cogredient folding of defect 1 of two rows S^ρ, T^ρ a "fundamental folding of type ρ". We then prove, completing Theorem VI:

Theorem VIII: The general folding process (41.) can be composed from the $(n-1)$ fundamental foldings of type ρ, where $\rho = 1, 2, \ldots, n-1$. In other words, to generate all invariant formations it suffices to apply successively the $n-1$ fundamental foldings.

In the binary domain the folding process (41.) coincides directly with the only possible fundamental folding; in the ternary domain I proved Theorem VIII in § 1 of my dissertation (cf. the Introduction). There, because of (44.), the general cogredient foldings are still identical with the fundamental foldings, and it is noteworthy that Theorem VIII for n variables gives the reduction to fundamental foldings, not merely the much weaker reduction to cogredient foldings. The proof is modeled in principle on the ternary proof: the most general foldings are constructed from the fundamental foldings, using the symbolic identities. We shall generate:

1. arbitrary foldings of defect 1 by cogredient foldings of defect 1, that is, by fundamental foldings (the analogue of the ternary case),
2. arbitrary foldings of defect λ by cogredient foldings of defect λ and arbitrary foldings of defect 1,
3. cogredient foldings of defect λ by cogredient foldings of defect $\lambda - 1$ and arbitrary foldings of defect 1.

As is essential, we assume by Theorem VII that the two forms S and T to be folded are normal forms. Thus, by (46.), the relations hold:

$$\begin{aligned}(q_{n-\sigma_1-\lambda}S^{\sigma_1} \,|\, S_{n-\sigma_2}p_{\sigma_2-\lambda}) = 0, \quad (\sigma_1 \geq \sigma_2,\ \lambda = 1, 2, \ldots, \sigma_2, n-\sigma_1),\\ (q_{n-\tau_1-\lambda}T^{\tau_1} \,|\, T_{n-\tau_2}p_{\tau_2-\lambda}) = 0, \quad (\tau_1 \geq \tau_2,\ \lambda = 1, 2, \ldots, \tau_2, n-\tau_1).\end{aligned} \tag{62}$$

It is further sufficient, by § 2 (end), to suppose that the forms S and T are linear in all variable rows; that is, the constructed forms belong to the form row

$$f = (S^1 \,|\, p_1)(S^2 \,|\, p_2)\cdots(S^{n-1} \,|\, p_{n-1})(T^1 \,|\, p_1)(T^2 \,|\, p_2)\cdots(T^{n-1} \,|\, p_{n-1}).$$

1) Generation of $(q_{n-\sigma-1}S^\sigma \,|\, T_{n-\tau}p_{\tau-1})$, where $\sigma > \tau$, from fundamental foldings of type $\tau + \alpha$, $\alpha = 0, 1, \ldots, \sigma - \tau$. From the fundamental folding of type τ

$$(q_{n-\tau-1}S^\tau \,|\, T_{n-\tau}p_{\tau-1})$$

we obtain, by the substitution $w \sim T_{n-\tau}p_{\tau-1}$, a form of the form row f with three rows of upper weight index (cf. § 1) $\tau + 1$:

$$(wS^\tau \,|\, p_{\tau+1})(S^{\tau+1} \,|\, p_{\tau+1})(T^{\tau+1} \,|\, p_{\tau+1}). \tag{63}$$

A fundamental folding of type $\tau + 1$ applied to (63.) gives

$$(q_{n-\tau-2}wS^\tau \,|\, S_{n-\tau-1}p_\tau);$$

from (31.), by the substitution $q_{n-\tau-2}w = q'_{n-\tau-1}$, this has the value

$$\varepsilon(q_{n-\tau-2}wS^{\tau+1} \,|\, S^\tau p_\tau) + \sum_{\alpha=1}^{\tau, n-\tau-1} \Pi(q'_{n-\tau-1-\alpha}S^{\tau+1} \,|\, S_{n-\tau}p_{\tau-\alpha}).$$

The expression under the summation sign vanishes identically by (62.); thus we have reached a form

$$(wS^{\tau+1} \,|\, p_{\tau+2})(S^{\tau+2} \,|\, p_{\tau+2})(T^{\tau+2} \,|\, p_{\tau+2}),$$

which is obtained from (63.) by changing τ into $\tau + 1$. Repeating the process $\sigma - \tau$ times therefore leads to the desired folding:

$$(wS^\sigma \,|\, p_{\sigma+1}) = \varepsilon(q_{n-\sigma-1}S^\sigma \,|\, T_{n-\tau}p_{\tau-1}).$$

We indicate the process just carried out by the formula

$$T^\tau S^\tau, \quad S^{\tau+1}, \quad S^{\tau+2}, \ldots, S^\sigma; \tag{64}$$

and see that only the normal-form property of S, not that of T, is used. A process dual to (64.) can be performed, using only the normal-form property of T, in the reverse order, namely:

$$S^\sigma T^\sigma, \quad T^{\sigma-1}, \quad T^{\sigma-2}, \ldots, T^\tau, \tag{65}$$

according to the relations:

$$\begin{aligned}
(q_{n-\sigma-1}S^\sigma \,|\, T_{1-\sigma}p_{\sigma-1}) &= \varepsilon(T_{n-\sigma}y \,|\, p_{\sigma-1}), \quad y \sim q_{n-\sigma-1}S^\sigma,\\
(q_{n-\sigma}T^{\sigma-1} \,|\, T_{n-\sigma}yp_{\sigma-2}) &= \varepsilon(T_{n-\sigma+1}y \,|\, p_{\sigma-2}),\\
&\vdots\\
(q_{n-\tau-1}T^\tau \,|\, T_{n-\tau-1}yp_{\tau-1}) &= \varepsilon(q_{n-\sigma-1}S^\sigma \,|\, T_{n-\tau}p_{\tau-1}).
\end{aligned}$$

We should also point out the connection with the decrease of total weight given in § 6 (end): for foldings of defect 1 this decrease has the value $2(1+(\sigma-\tau))$, and for fundamental foldings the value $2\cdot 1$. Therefore, if composition out of fundamental foldings is possible at all, exactly $\sigma-\tau+1$ such foldings are necessarily required, as was carried out above.

2) Generation of general foldings from cogredient and fundamental foldings. The weight decrease for a general folding (41) is $2(\lambda^2+\lambda(\sigma-\tau)) = 2[\lambda^2+(\sigma-\tau)(1+(\lambda-1))]$. This gives the possibility of decomposing it into a cogredient folding of defect λ (weight decrease $2\lambda^2$) and $\sigma-\tau$ foldings of defect 1 with difference of weight indices $\lambda-1$ (weight decrease $2\{1+(\lambda-1)\}$). In the case $\lambda=1$ this decomposition agrees with the one given under 1); we show that it can indeed be realized.

From the cogredient folding of defect λ

$$(q_{n-\tau-\lambda}S^\tau \,|\, T_{n-\tau}p_{\tau-\lambda})$$

we obtain, by the substitution $R^\lambda \sim T_{n-\tau}p_{\tau-\lambda}$, a form with the two rows of upper weight indices $\tau+\lambda$ and $\tau+1$:

$$(R^\lambda S^\tau \,|\, p_{\tau+\lambda})(S^{\tau+1} \,|\, p_{\tau+1}). \tag{66}$$

The row with the lower weight index $\tau+1$ belongs to a normal form; hence (66.) admits a folding of defect 1 composed out of λ fundamental foldings, in the order (65):

$$(R^\lambda S^\tau)S^{\tau+\lambda}, \quad S^{\tau+\lambda-1}, \quad S^{\tau+\lambda-2}, \ldots, S^{\tau+1}.$$

Taking account of (31.) and (62.), this gives

$$(q_{n-\tau-\lambda-1}R^\lambda S^\tau \,|\, S_{n-\tau-1}p_\tau) = \varepsilon(R^\lambda S^{\tau+1} \,|\, p_{\tau+\lambda+1}),$$

that is, a form obtained from (66.) by replacing τ by $\tau+1$, just as in 1) for (63.). Repeating the process $\sigma-\tau$ times leads to the desired folding:

$$(R^\lambda S^\sigma \,|\, p_{\sigma+\lambda}) = \varepsilon(q_{n-\sigma-\lambda}S^\sigma \,|\, T_{n-\tau}p_{\tau-\lambda}).$$

In the whole process only the normal-form property of S was used. Viewing T as a normal form gives the dual process, with complete reversal of the order, according to the formulas

$$\begin{aligned}
(q_{n-\sigma-\lambda}S^\sigma \,|\, T_{n-\sigma}p_{\sigma-\lambda}) &= \varepsilon(T_{n-\sigma}R_\lambda \,|\, p_{\sigma-\lambda}), \quad R_\lambda \sim q_{n-\sigma-\lambda}S^\sigma,\\
(q_{n-\sigma}T^{\sigma-1} \,|\, T_{n-\sigma}R_\lambda p_{\sigma-\lambda-1}) &= \varepsilon(T_{n-\sigma+1}R_\lambda \,|\, p_{\sigma-\lambda-1}),\\
&\vdots\\
(q_{n-\tau-1}T^\tau \,|\, T_{n-\tau-1}R_\lambda p_{\tau-\lambda}) &= \varepsilon(q_{n-\sigma-\lambda}S^\sigma \,|\, T_{n-\tau}p_{\tau-\lambda}).
\end{aligned}$$

3) Generation of cogredient foldings of defect λ from cogredient foldings of defect $\lambda-1$ and fundamental foldings. The weight decrease for cogredient foldings of defect λ is $2\lambda^2 = 2((\lambda-1)^2+2\lambda-1)$, giving the possibility of a decomposition into a cogredient folding of defect $\lambda-1$ and $2\lambda-1$ fundamental foldings.

This is most easily found by first putting $n = 2\lambda$. The only possible cogredient folding of defect λ is $(S^\lambda \,|\, T_\lambda) = (S^\lambda \,|\, T_{n/2})$; it contains one row u and one row x fewer than the folding of defect $\lambda - 1$ of the same rows, $(uS^\lambda \,|\, T_\lambda x)$. Conversely, we compose the folding of defect λ out of fundamental foldings which effect the disappearance of a row u and a row x (weight decrease $2(n-1) = 2(2\lambda - 1)$) and at the same time generate a new symbol row R^λ, together with a cogredient folding of defect $\lambda - 1$. The simplest folding that does this is the following one of defect 1:

$$(sT^\lambda \,|\, \sigma p_\lambda) = \varepsilon(S^{2\lambda-1} \,|\, R_{\lambda-1} p_\lambda) = \varepsilon(R^\lambda \,|\, p_\lambda),$$

where

$$R^{\lambda+1} = sT^\lambda, \quad s = S^1, \quad \sigma = S_1, \quad R^\lambda \sim \sigma R_{\lambda-1}.$$

By (65.) and (64.) it is composed out of the $2\lambda - 1$ fundamental foldings

$$T^\lambda S^\lambda, S^{\lambda-1}, \ldots, S^1; \qquad R^{\lambda+1} S^{\lambda+1}, S^{\lambda+2}, \ldots, S^{2\lambda-1}. \tag{67}$$

A folding of defect $\lambda - 1$, taking account of (21.) and (62.), gives

$$(uS^\lambda \,|\, \sigma R_{\lambda-1} x) = \varepsilon(R^{\lambda+1} \,|\, S_\lambda x) = \varepsilon(sT^\lambda \,|\, S^\lambda x) = \varepsilon(S^\lambda \,|\, T_\lambda).$$

The general case, for two rows S^ρ, T^ρ and arbitrary n, is obtained directly from the special one. In place of (67.) one has the following $2\lambda - 1$ fundamental foldings:

$$T^\rho S^\rho, S^{\rho-1}, \ldots, S^{\rho-\lambda+1}; \qquad R^{\rho+1} S^{\rho+1}, S^{\rho+2}, \ldots, S^{\rho+\lambda-1}. \tag{68}$$

The first half of the foldings gives the form

$$(q_{n-\rho-1} T^\rho \,|\, S_{n-\rho+\lambda-1} p_{\rho-\lambda}),$$

from which, by the substitutions

$$S_{n-\rho+\lambda-1} p_{\rho-\lambda} \sim w, \qquad T^\rho w = R^{\rho+1},$$

and application of the second half of the foldings, one obtains

$$(q_{n-\rho-\lambda} S^{\rho+\lambda-1} \,|\, R_{n-\rho-1} p_\rho).$$

Substituting

$$q_{n-\rho-\lambda} S^{\rho+\lambda-1} \sim y,$$

one obtains, by a cogredient folding of defect $\lambda - 1$,

$$(q_{n-\rho-\lambda+1} S^\rho \,|\, y R_{n-\rho-1} p_{\rho-\lambda+1}). \tag{69}$$

We show that this is the desired folding of defect λ. Substitute

$$R_{n-\rho-1} p_{\rho-\lambda+1} = R_{n-\lambda}$$

and observe that resolving y gives

$$(q_{n-\rho-\lambda+1} R^\lambda \,|\, S_{n-\rho} y) = \varepsilon(q_{n-\rho-\lambda} S^{\rho+\lambda-1} \,|\, S_{n-\rho} p'_{\rho-1}) = 0.$$

Thus by (20.) the value of (69.) is

$$\varepsilon(S^\rho R^\lambda \,|\, p_{\rho+\lambda-1} y) = \varepsilon(q_{n-\rho-\lambda} S^{\rho+\lambda-1} \,|\, [S^\rho R^\lambda]_{n-\rho-\lambda} p_{\rho+\lambda-1}).$$

This folding is of type (43.), hence equivalent to

$$(q_{n-\rho-\lambda} S^\rho \,|\, R_{n-\rho-1} p_{\rho-\lambda+1}) = \varepsilon(wT^\rho \,|\, R_\lambda p_{\rho-\lambda+1}), \qquad R_\lambda \sim q_{n-\rho-\lambda} S^\rho.$$

Here R_λ is already of the desired final form; the expression corresponds to the form $(sT^\lambda \,|\, S_\lambda x)$ in the special case. Now, observing that resolving w and R_λ gives

$$(wR^{n-\lambda} \,|\, T_{n-\rho} p_{\rho-\lambda+1}) = \varepsilon(q'_{n-1} R^{n-\lambda} \,|\, S_{n-\rho+\lambda-1} p_{\rho-\lambda}) = \varepsilon(q''_{n-\sigma-1} S^\rho \,|\, S_{n-\rho+\lambda-1} p_{\rho-\lambda}) = 0,$$

we get by (21.) the value

$$(wq_{n-\rho+\lambda-1}\,|\,T_{n-\rho}R_\lambda) = \varepsilon(q_{n-\rho+\lambda-1}[T_{n-\rho}R_\lambda]^{n-\lambda}\,|\,S_{n-\rho+\lambda-1}p_{\rho-\lambda}) \quad \text{equivalent to} \quad (q_{n-\rho-\lambda}S^\rho\,|\,T_{n-\rho}p_{\rho-\lambda}).$$

In the whole process only the normal-form property of S, not that of T, was used. Thus the cogredient folding of defect $\lambda-1$ used to generate (69.) can be replaced by $2\lambda-3$ fundamental foldings and a cogredient folding of defect $\lambda-2$, which in turn admits a decomposition into fundamental foldings, and so on. Analogously, the generation is obtained by using the normal-form property of T and applying the dualistic process, that is, the fundamental foldings

$$S^\rho T^\rho, \quad T^{\rho-1}, \ldots, T^{\rho-\lambda+1}; \qquad R^{\rho-1}T^{\rho-1}, \quad T^{\rho-2}, \ldots, T^{\rho-\lambda+1},$$

and a folding dual to (69.). The folding

$$(q_{n-\rho-\lambda}T^\rho\,|\,S_{n-\rho}p_{\rho-\lambda}),$$

equivalent to the preceding one, is then obtained.

Adding the decomposition obtained under 2), we have indeed obtained a generation of the most general foldings from fundamental foldings. It remains to show that this generation is unique, apart from permutation of the order, i.e. that to each folding there corresponds one and only one number α_ρ of fundamental foldings of type ρ, where $\rho = 1, 2, \ldots, n-1$.

Let m_ρ be the degrees in the variable rows p_ρ of the initial form f, and l_ρ the degrees of the form produced by folding. Each fundamental folding of type ρ transforms the degrees $m_{\rho-1}, m_\rho, m_{\rho+1}$ respectively into $m_{\rho-1}+1, m_\rho-2, m_{\rho+1}+1$. Thus the α satisfy the system of equations

$$m_\rho - l_\rho = -\alpha_{\rho-1} + 2\alpha_\rho - \alpha_{\rho+1}, \qquad (\rho = 1, 2, \ldots, n-1), \tag{70}$$

where α_0 and $\alpha_n = 0$ are to be put, and whose determinant has value n.[70] The α are thereby uniquely determined, and indeed, by Theorem VIII, as positive integers; this gives conditions for the differences $m_\rho - l_\rho$.

The results of this paragraph hold by virtue of relations (62.); however, if the relations (62.) do not hold, the final expressions are by no means equivalent to the initial expressions. The definition of equivalence given in § 6 also admits the formulation:[71] "Two forms are equivalent if and only if they differ by forms of higher folding, i.e. by forms that exhibit a greater weight decrease." This greater weight decrease always occurs when the two rows $q_{n-\sigma-i}, p_{\tau-\lambda}$ entering the folding are really variable rows, as happens in (41.), (42.), in the foldings appearing in this paragraph as equivalent, and also in the equivalent forms of Theorem VII. But it need not occur when these rows are derived from symbol rows by substitution, as was the case for the forms of this paragraph which could be expressed in terms of one another by virtue of (62.). One easily sees that the vanishing forms even have, in part, a higher total weight.

§ 9. Form rows. Reduction theorems.

We now define the form row introduced in § 6 (end) somewhat more sharply as "the totality of invariant formations of a given initial form that are linear in the coefficients, i.e. the totality of forms that arise from the initial form by folding in itself, arranged according to higher forms."

To explain the higher forms, suppose by Theorem VII that the initial form is given as a product of two normal forms $S \cdot T$. By a higher form we mean forms with higher folding in itself, and among forms with the same folding in itself, specially normalized ones. More precisely: suppose the form A has arisen by α_ρ fundamental foldings of type ρ, and the form B by β_ρ such foldings. Then B is higher than A:

1. if, in the system of inequalities $\beta_\rho \geq \alpha_\rho$, $\rho = 1, 2, \ldots, n-1$, the inequality sign holds for at least one value of ρ;[72]

2. if the equality sign holds for all values ρ, but fewer symbol rows have been combined into a single matrix product. This normalization proves necessary because of the reductions in § 8. Accordingly, for example, $(S^{n-1}\,|\,T_{n-1})$ is higher than $(S^{n-1}\,|\,[S^1T^\rho]_{n-\rho-1}p_\rho)$;

[70] If Δ_n denotes the n-rowed determinant, then the recurrence formula holds: $\Delta_n = 2\Delta_{n-1} - \Delta_{n-2}$; that is, $\Delta_n - \Delta_{n-1} = \Delta_{n-1} - \Delta_{n-2} = \cdots = \Delta_2 - \Delta_1 = 1$, since $\Delta_2 = 3$, $\Delta_1 = 2$.

[71] Cf. the consideration at the end of the next paragraph.

[72] If in the system of inequalities the sign $>$ holds in part and the sign $<$ in part, then the forms are not comparable, since a form arising from another by folding always has a positive value system of fundamental foldings, hence in our case positive or vanishing values $\beta_\rho - \alpha_\rho$.

3. if the equality sign holds for all values ρ and the number of symbol rows combined into one matrix product is the same, then B is made higher than A by a normalization arbitrary in itself but fixed once and for all. This normalization is always possible because of the finite number of forms belonging to a value system α; it can be achieved, for instance, by privileging the one form S (larger number of symbol rows S, larger sum of the upper weight indices of the rows S, and so on).

It is useful to think of the form row as arranged as an $(n-1)$-dimensional manifold of lattice points, where the $n-1$ directions correspond to the $n-1$ fundamental foldings. To every form there then corresponds one and only one value system α, i.e. a positive integral lattice point, while the different forms belonging to a value system α are uniquely determined in their order by the above normalization. An arbitrary form of the form row gives the initial form of a new form row, contained as a part of the total form row; indeed it is contained as the part consisting of the forms obtained from the new initial form by proceeding in the $n-1$ positive directions.

By virtue of Theorem VIII and the general theory of series expansions, exactly the reduction theorems of the binary and ternary domains (cf. dissertation, § 3) hold for form rows. We shall briefly derive the principal theorem. We first state the definition:

"In a given system of forms, suppose a certain finite number of forms has been combined into a module. We call a form reducible if it can be expressed by forms that have invariants as factors, or by 'higher forms'; that is, by higher forms of the total form row to which the form belongs, or by forms that contain the symbols of the module in higher order. A reducible form row is called a reducer." Then:

Theorem IX: If the initial form of a form row is reducible by having arisen through folding with a reducer, then the entire form row arising from this initial form is reducible.

For the proof, observe that a form h arising by folding a form f with a second form g can, because of (45.), be regarded as a form f containing several cogredient variable rows p_ρ, p'_ρ. Such forms can, by the general theory of series expansion, be represented as polars of the elementary covariants of f, by applying the series expansion successively to each pair of cogredient variable rows p_ρ, p'_ρ. By (38.), the elementary covariants that occur are the forms generated by cogredient folding. Since, however, the order in which the series expansion is applied is still arbitrary, we may in particular choose an order corresponding to the generation of the general foldings from fundamental foldings. The resulting system of elementary covariants is then identical with the form row f; the forms that arise by cogredient folding of higher defect are arranged among those that arise by fundamental foldings. But one also obtains polars of the form row f for any order of the series expansion, to which a second system of elementary covariants may correspond. Since the form row exhausts the totality of invariant formations, every form of the second system can be expressed linearly by polars of the form row, and indeed by polars of those forms that show the same or a greater weight decrease. The latter follows because (cf. § 7) the polars can be regarded as simultaneous invariants of a form row H (52.), with the degree numbers corresponding to the form h, and of the form row f. Every folding of H in itself corresponds to a weight decrease which, after substitution (11.) is performed, is transferred to the symbol rows and hence to the forms of f.[73]

An arbitrary form of the form row h has arisen by folding h in itself; that is, on the one hand by a higher folding of g with f, and on the other by folding f or g in itself. In both cases the series expansion leads to polars of the form row f, just as was shown above for the initial form h. If in particular f is a reducer, then an expansion in polars of the reducer results; hence the form row h becomes reducible.

Applications of the theorem to the reduction of complete systems of forms follow analogously to the binary and ternary domains.

[73] This consideration also underlies the second formulation of the equivalence concept (§ 8, end). Further explanations of the different systems of elementary covariants in the ternary domain are found in Study, loc. cit., II, § 7, Theorems 7) and 8). By our Theorem VII the same results also hold for n variables.

5. Rational Function Fields

Jahresbericht der DMV 22 (1913), pp. 316–319

The following questions originally go back to conversations with E. Fischer. Some of the questions, moreover, were already raised and settled by E. Steinitz for the special case of one indeterminate — and indeed under more general assumptions on the coefficient field.[74]

By a "rational function field" I understand a field whose elements are rational functions of n indeterminates, with coefficients from a prescribed number field, which in particular may also comprise all complex numbers. Examples of such fields are the field of symmetric functions of n quantities, or more generally the totality of rational functions of n indeterminates that allow the permutations of a certain group (Lagrange's *Gattungsbereiche*); furthermore, the invariant field.

Between the first two fields just mentioned and the latter there is a characteristic difference: the former contain n algebraically independent functions, the elementary symmetric functions; whereas the number of algebraically independent invariants is always smaller than the number of indeterminates. It is therefore important that, in general, one can associate such fields of the second kind one-to-one with fields of the first kind, by replacing some of the indeterminates by numbers. In what follows I shall therefore restrict myself to fields of the first kind, i.e. to fields with n algebraically independent functions; by virtue of the association, the results then hold in general.

The questions group themselves around three basis concepts: rational basis, minimal basis, and integrality basis.

1. By a "rational basis" I understand a finite number of functions of the field such that every function of the field can be represented as a rational combination of this finite number, with coefficients from the prescribed coefficient field. By simple considerations — which in the case of one indeterminate are also found in E. Steinitz, loc. cit. — one proves the existence of a rational basis for every rational function field. For example, by Lagrange's theorem, the elementary symmetric functions and one function belonging to the group form a rational basis for the Lagrange *Gattungsbereiche* mentioned earlier.

2. Every rational basis must contain (for fields of the first kind) at least n functions; if it contains exactly n functions, which then must be algebraically independent, I call it a "minimal basis." The question of the existence of a minimal basis can be answered in part by theorems of Lüroth, Castelnuovo, and Enriques.[75] According to these, for fields of one indeterminate there always exists a minimal basis: the Lüroth function of the field, uniquely determined up to fractional linear transformation (cf. Steinitz § 24). For fields of two indeterminates, a minimal basis exists always, and in general only, if one permits an algebraic extension of the coefficient field, whereas for three and more indeterminates a minimal basis in general does not exist at all. No attempt has yet been made to characterize the special fields with minimal basis.

I have pursued further the question of the minimal basis for Lagrange's *Gattungsbereiche*. Here it acquires the following meaning: "If the Lagrange *Gattungsbereich* belonging to the group G possesses a minimal basis, then one can construct rationally, by a parametric representation, the totality of equations with prescribed group G; and indeed for every number field that contains the coefficient field of the minimal basis — hence in particular for any arbitrary number field if this coefficient field is the field of rational numbers."

The simplest example is provided by the symmetric group; here the elementary symmetric functions form a minimal basis with rational numerical coefficients. From this one obtains as parametric representation simply the equation with indeterminate coefficients. Hilbert's irreducibility theorem shows how one passes from this to arbitrarily many affectless equations over every number field.

Now the existence of the minimal basis for all groups occurring in equations of degrees 3 and 4 follows directly from the theorems of Lüroth and Castelnuovo; at the same time it further appears that this minimal basis has rational numerical coefficients. Thus, for every arbitrary number field, one can rationally construct the totality of equations of degrees 3 and 4 with prescribed group. For the cyclic and dihedral groups there exists a minimal basis with the field of the nth roots of unity as coefficient field; the same holds for a few further metacyclic groups. The question whether the minimal basis is at all characteristic for certain groups must remain undecided.

3. To arrive at the last basis concept, I consider the totality of polynomials contained in the field. By

[74] E. Steinitz: Algebraische Theorie der Körper, especially § 24. Crelle's Journal 137. 1910.

[75] J. Lüroth: Beweis eines Satzes über rationale Kurven. Math. Ann. 9. 1875. — G. Castelnuovo: Sulla razionalità delle involuzioni piane. Math. Ann. 44. 1893. — F. Enriques: Sopra una involuzione non razionale dello spazio. Rend. Acc. Linc. vol. 21. 21 Jan. 1912.

an "integrality basis" I understand a finite number of these polynomials such that every polynomial of the field can be represented as an integral rational combination of this finite number, with coefficients from the prescribed coefficient field. The question of the existence of an integrality basis — which, for example, contains as a special case the finiteness of the invariant system — was posed by Hilbert in his "Mathematical Problems"[76] in a somewhat different formulation, as the problem of relatively integral functions.

For the moment I can indicate only one class of fields for which an integrality basis exists. Namely, if the field contains a system of n polynomials such that the homogeneous resultant of the terms of highest dimension of these polynomials is different from zero, then an integrality basis exists; it is given by the coefficients of all u in the equation, irreducible in the field, for the linear form:

$$u_0 = u_1x_1 + u_2x_2 + \cdots + u_nx_n.^{77}$$

If, in particular, the value of the resultant is equal to a unit of the coefficient field, then the integrality of the representation is also secured. An example of this class of fields is furnished by Lagrange's *Gattungsbereiche*, since the resultant of the elementary symmetric functions has the value ± 1. A further example (without integrality) is given by all fields that contain only one algebraically independent polynomial; here the integrality basis is identical with the Lüroth function of the smallest subfield containing all polynomials. Thus, as is well known, all integral rational projective invariants of a quadratic form in n variables are integral functions of the discriminant.

The condition just given is only sufficient, by no means necessary, for the existence of an integrality basis. One can easily construct fields in which the resultant of every n polynomials vanishes, and which nevertheless possess an integrality basis given by the coefficients of that irreducible equation. The question arises whether perhaps even in the most general case the coefficients of that equation furnish the integrality basis.

[76] D. Hilbert: Mathematische Probleme. Lecture, Paris 1900. Problem 14. Göttinger Nachr. 1900.

[77] This irreducible equation is found, in the case of one indeterminate, in E. Steinitz's proof of Lüroth's theorem.

6. Fields and Systems of Rational Functions

Math. Ann. 76 (1915), pp. 161–196

The present paper treats basis questions for arbitrary systems of rational and integral rational functions. The methods of field theory used here make the settlement of these questions for fields of rational functions — rational function fields[78] — appear as the essential matter, while the generalization of the results to arbitrary systems arises as a consequence.

Among basis questions for general systems, up to now only the existence of a module basis, guaranteed by Hilbert's theorem (Math. Ann. 36), has been known. In what follows, the question of rational representability is answered completely by the existence of a rational basis for every arbitrary system (§ 7); the rational basis of fields is already obtained in § 4. This existence of the rational basis permits us throughout to start from the abstractly defined field or system, and thereby to avoid difficulties that are caused only by the special choice of the rational basis and not by the system itself, such as the occurrence of special denominators or of fundamental points of the basis functions.

For fields the question of the minimal basis is also treated, i.e. of a rational basis consisting of algebraically independent functions (§ 6). The methods of field theory further lead to a distinguished rational basis, the involution basis[79] (§ 5), which becomes especially important for integrality domains consisting of polynomials (§ 8). In that setting it gives a representation with a fixed denominator (a power of a function determined by the integrality domain), as is known for example in the special case of the typical representation of invariants.

From rational representability we now draw, as far as possible, consequences for integral rational representability, i.e. for the question of finiteness in the narrower sense.

The finiteness theorems known up to now all rest on the fact that Hilbert's theorem on module bases guarantees finiteness for all systems in which a representation

$$F = A_1 f_1 + A_2 f_2 + \cdots + A_k f_k$$

entails a second representation

$$F = B_1 f_1 + B_2 f_2 + \cdots + B_k f_k,$$

where the B_i belong to the system and are of lower degree than F.

By contrast, the rational-basis theorem and the methods of field theory allow finiteness to be deduced under hypotheses of an entirely different kind.

Thus, as a partial answer to one of Hilbert's problems (*Mathematical Problems*, no. 14), one obtains a class of relatively integral functions (relatively integral domains of the first kind) that are finite integrality domains and whose integrality basis is furnished by the involution basis mentioned above (§ 10). By analogy with Hilbert's proof of Kronecker's theorem on a fundamental system of algebraic integers (*Complete Systems of Invariants*, § 2; Math. Ann. 42), one can further show that every regular system of polynomials — that is, every system that can be mapped onto a base-point-free system — possesses an integrality basis (§ 12), whereas it is easy to give nonregular systems having no integrality basis. As a simple example of this fact, we mention the theorem: "In any system whatsoever of infinitely many polynomials in one indeterminate, there is a finite number of these polynomials such that every polynomial of the system can be represented as an integral rational expression in these finitely many polynomials." Further examples occur in § 13.

Finally, the last sections (§§ 14 and 15) sharpen the basis theorems with respect to integrality.

An essential tool in the investigation is the transfer principle of § 3, according to which it is enough to consider all the basis questions raised here for systems in which the number of indeterminates equals the number of algebraically independent functions in the system.

The present paper was prompted by conversations with E. Fischer, especially by his question concerning the minimal basis of Lagrange genus domains. The investigations occasioned by it, which led to the construction of equations with prescribed group (cf. the cited communication on "Rational Function Fields," part 2), are reserved for a later publication.

The essential extension of the present paper beyond the original communication is that the basis theorems stated there only for fields or special integrality domains are transferred here to arbitrary systems. This

[78] Cf. a preliminary communication on the occasion of the Vienna meeting of natural scientists: Rationale Funktionenkörper, Jahresber. d. D. Math.-Ver. 22 (1913), where an overview is given of the questions and of the results concerning function fields.

[79] The name was chosen because, in its geometric interpretation, the rational function field represents the most general involution in a linear space.

transfer is achieved in a simple way by means of the concept of the smallest field containing an arbitrary system, as a generalization of the field of fractions of an integrality domain (§ 7). I was led to form this concept when K. Hentzelt, after becoming acquainted with the rational basis for fields, was able to prove the existence of a rational basis for arbitrary systems by way of Hilbert's module basis. I was likewise led to the theorem on the integrality basis of regular systems by K. Hentzelt's observation that the arguments I had applied to integrality domains remained valid for arbitrary systems satisfying the same hypotheses; I also owe Hentzelt several individual minor remarks.

Finally, it should be mentioned that, in the case of one indeterminate, the rational basis and minimal basis of fields are found in E. Steinitz's "Algebraische Theorie der Körper," § 24 (Crelle's Journal 137); there the coefficient domain is taken to be a field in the most general sense. The question of how far the theorems given here persist under these more general hypotheses is not addressed below; in any event the proofs require modification, since, for example, even the tools from the theory of functional determinants fail over fields of characteristic p.

§ 1. Fields $\mathfrak{K}_{n\rho}$ and systems $\mathfrak{S}_{n\rho}$.

In what follows we investigate systems of rational functions in n indeterminates, and in particular fields of rational functions.

By $f(x_1 \cdots x_n)$, $g(x_1 \cdots x_n)$, ..., or, in abbreviated form, $f(x)$, $g(x)$, ..., we shall therefore always mean rational functions of $x_1 \cdots x_n$; these are assumed to be in reduced form — that is, with numerator and denominator relatively prime. Integral rational functions (polynomials) will be denoted by capital letters, $F(x)$, $G(x)$, ... The coefficient domain Ω is assumed to be an arbitrary field of scalars and may in particular comprise all complex numbers; Ω may also contain a finite number of parameters.

The elements of Ω, hence all functions of degree zero, are always counted as belonging to the system.

With these conventions, a field consisting of rational functions — a rational function field — can be defined abstractly.

Definition I: A system of rational functions is called a field if it satisfies the following conditions:

1. *Together with $f(x)$, it also contains $c \cdot f(x)$ for every element c of Ω.*
2. *Together with $f(x)$ and $g(x)$, it always contains $f(x) + g(x)$, $f(x) \cdot g(x)$ and — for $g(x) \neq 0$ — the quotient $f(x) : g(x)$.*[80]

Special fields are those obtained by adjoining a finite number of rational functions

$$f_1(x),\ f_2(x), \ldots, f_k(x)$$

to Ω; they will be denoted by

$$\Omega\big(f_1(x) \cdots f_k(x)\big) \quad \text{or} \quad \Omega(f_1 \cdots f_k).$$

[81] Among these special fields, we also mention the field obtained by adjoining $x_1, \ldots, x_n$ to Ω,

$$\Omega(x_1 \cdots x_n),$$

which is identical with the totality of rational functions of $x_1 \cdots x_n$ with coefficients in Ω.

We also introduce (following E. Steinitz) the concept of an intermediate field:

"A field $\mathfrak{M}$ lies between Ω_1 and Ω_2 if it contains Ω_1 and is contained in Ω_2;"

Definition I may then also be formulated as follows:

A field of rational functions in n indeterminates is an intermediate field between Ω and $\Omega(x_1 \cdots x_n)$ and contains at least one function that genuinely involves all n indeterminates.

Besides the number of indeterminates, systems of rational functions have a further characteristic number: the number of algebraically independent functions, or the algebraic rank, defined as follows.

Definition II: A system of rational functions has algebraic rank ρ if one can specify ρ functions of the system that are algebraically independent, whereas every $(\rho + 1)$ functions of the system are algebraically dependent.[82]

[80] Here $f(x)$ and $g(x)$ may also be of degree zero, that is, elements of Ω.

[81] That these "special fields" already exhaust all fields follows in § 4.

[82] ρ functions $f_1(x) \cdots f_\rho(x)$ are called algebraically independent if every relation

$$F\big(f_1(x) \cdots f_\rho(x)\big) = 0 \quad \text{identically in } x_1 \cdots x_n$$

Systems of finitely or infinitely many rational functions in n indeterminates and of algebraic rank ρ will be denoted by the double index

$$\mathfrak{S}_{n\rho}.$$

In particular, by

$$\mathfrak{K}_{n\rho}$$

we shall mean a field in n indeterminates and of algebraic rank ρ. We have the inequality

$$1 \leq \rho \leq n.$$

We give a few examples of fields $\mathfrak{K}_{nn}$ and $\mathfrak{K}_{n\rho}$:

1. Fields $\mathfrak{K}_{nn}$ include the Lagrange genus domains, which may be defined as

> "the totality of rational (and integral rational) functions of $x_1 \cdots x_n$ that admit the permutations of a permutation group G on $x_1 \cdots x_n$."

They always contain the field of symmetric functions and hence also the n algebraically independent elementary symmetric functions.

2. Examples of fields $\mathfrak{K}_{n\rho}$ are the projective invariant fields, formed from the totality of the rational (and integral rational) invariants of one or more ground forms.[83] Here $\rho < n$, since the number of algebraically independent invariants is always smaller than the number of coefficients.

The corresponding statement holds for invariant fields with respect to subgroups of the projective group.

§ 2. Lemma on algebraically dependent functions.

The lemma of this section will show in § 3 that the algebraic rank is the true characteristic number of a system. More precisely, it shows that if some of the indeterminates are successively specialized to numerical values in such a way that ρ algebraically independent functions remain algebraically independent, then any function algebraically dependent on those ρ functions can neither vanish identically nor become indeterminate.

Let the system

$$(1) \quad g_1(x),\ g_2(x), \ldots, g_\rho(x)$$

have algebraic rank ρ, where $\rho < n$, and let $h(x)$ be a rational function algebraically dependent on the functions (1). By familiar theorems, the Jacobian matrix of (1) has rank ρ. We may therefore label the indeterminates so that

$$(2) \quad \frac{\partial(g_1\ g_2 \cdots g_\rho)}{\partial(x_1\ x_2 \cdots x_\rho)} = \frac{\Gamma(x)}{G(x)^{\rho+1}} \neq 0,$$

where $G(x)$ denotes, as usual, the common denominator of the functions (1).

Now choose the number a so that the product $G(x) \cdot \Gamma(x)$ is not divisible by $(x_i - a)$, where i is one of the numbers $\rho+1, \rho+2, \ldots, n$. After setting $x_i = a$, the common denominator of the functions (1) therefore cannot vanish identically, and the ρ functions

$$(3) \quad [g_1(x)]_{x_i=a}, \ldots, [g_\rho(x)]_{x_i=a}$$

are likewise algebraically independent. We shall say that the substitution $x_i = a$ preserves the algebraic rank of the system (1).

Let the irreducible equation satisfied by $h(x)$ over the functions (1) be

$$(4) \quad A_0(g_1 \cdots g_\rho) \cdot h(x)^\tau + A_1(g_1 \cdots g_\rho) \cdot h(x)^{\tau-1} + \cdots + A_\tau(g_1 \cdots g_\rho) = 0,$$

where $A_0(g_1 \cdots g_\rho)$ and $A_\tau(g_1 \cdots g_\rho)$ do not vanish identically. To obtain from this an identity between polynomials, set

$$(5) \quad g_i(x) = G_i(x) : G(x); \qquad h(x) = H_1(x) : H_2(x),$$

---

implies

$$F(\lambda_1 \cdots \lambda_\rho) = 0 \quad \text{identically in } \lambda_1 \cdots \lambda_\rho.$$

Otherwise they are called algebraically dependent.

[83] It is useful to consider only transformations of determinant 1; then every rational expression in arbitrarily many invariants again admits the transformation, and one indeed obtains a field. The homogeneous isobaric invariants taken by themselves do not form a field, but they do form a system $\mathfrak{S}_{n\rho}$.

and observe that $H_1(x)$ and $H_2(x)$ are relatively prime because $h(x)$ is assumed to be in reduced form. By (5), equation (4) becomes

$$(6)\quad \begin{aligned} &B_0(G\,G_1\cdots G_\rho)\cdot G(x)^{\sigma_0}\cdot H_1(x)^\tau + B_1(G\,G_1\cdots G_\rho)\cdot G(x)^{\sigma_1}\cdot H_1(x)^{\tau-1}H_2(x)\\ &\quad + \cdots + B_\tau(G\,G_1\cdots G_\rho)\cdot G(x)^{\sigma_\tau}\cdot H_2(x)^\tau = 0, \end{aligned}$$

where the B_k are homogeneous forms in G, G_i, and at least one of the nonnegative exponents σ_k must be zero.

Suppose now that $H_1(x)$ were divisible by $(x_i - a)$. By (6), the expression

$$B_\tau(G\,G_1\cdots G_\rho)\cdot G(x)^{\sigma_\tau}\cdot H_2(x)^\tau$$

would then also be divisible by $(x_i - a)$. Divisibility of $G(x)$ is excluded by hypothesis; divisibility of B_τ would in turn imply divisibility of

$$A_\tau = B_\tau : G^\lambda,$$

and hence the relation $A_\tau = 0$ among the functions (3), contrary to their assumed algebraic independence. Finally, since $H_2(x)$ is relatively prime to $H_1(x)$, it too cannot be divisible by $(x_i - a)$;[84] thus the assumption that $H_1(x)$ is divisible by $(x_i - a)$ leads to a contradiction. The same argument shows that $H_2(x)$ cannot be divisible by $(x_i - a)$ either. Consequently the function $[h(x)]_{x_i=a} = k(x)$ can neither vanish identically nor become indeterminate.

The preceding argument can be applied again to the system (3) and the function $k(x)$, again put into reduced form. Continuing in this way yields the following lemma.

Lemma: Let the two systems

$$\begin{gathered} g_1(x),\ g_2(x),\ldots,\ g_\rho(x),\\ g_1(x),\ g_2(x),\ldots,\ g_\rho(x),\ h(x) \end{gathered}$$

each have algebraic rank ρ, where $\rho < n$, and suppose, for instance, that

$$\frac{\partial(g_1\cdots g_\rho)}{\partial(x_1\cdots x_\rho)} = \frac{\Gamma(x)}{G(x)^{\rho+1}} \neq 0.$$

Choose the numbers

$$a_n,\ a_{n-1},\ldots,\ a_{\rho+1}$$

so that the substitution

$$x_n = a_n,\quad x_{n-1} = a_{n-1},\ldots,\quad x_{\rho+1} = a_{\rho+1}$$

does not make the product $G(x)\cdot\Gamma(x)$ vanish — that is, so that it preserves the algebraic rank of the system (1). In the successive substitutions

$$\begin{gathered} [h(x)]_{x_n=a_n} = h^{(n-1)}(x);\quad [h^{(n-1)}(x)]_{x_{n-1}=a_{n-1}} = h^{(n-2)}(x);\quad \cdots;\\ [h^{(\rho+1)}(x)]_{x_{\rho+1}=a_{\rho+1}} = h^*(x_1, x_2, \ldots, x_\rho) \end{gathered}$$

put each of the functions $h(x), h^{(n-1)}(x), \ldots, h^{(\rho+1)}(x)$ into reduced form. Under these hypotheses, neither the numerator nor the denominator of $h^*(x_1\cdots x_\rho)$ can vanish identically, and the function cannot become $\frac{0}{0}$.[85]

---

[84] This last conclusion, which rests on the reduced form, would no longer be possible for a substitution $x_i = a$, $x_k = b$ even if the remaining hypotheses were preserved. The functions $H_1(x)$ and $H_2(x)$ could then vanish simultaneously, and the quotient would become indeterminate under the substitution, equal to $\frac{0}{0}$; for example,

$$h(x) = \frac{x_3(\alpha x_1 + \beta x_2) + x_4(\gamma x_1 + \delta x_2)}{x_3(\alpha' x_1 + \beta' x_2) + x_4(\gamma' x_1 + \delta' x_2)}$$

under the substitution $x_3 = 0$, $x_4 = 0$.

[85] For example, for the function $h(x)$ in the preceding note, successive substitution gives

$$[h(x)]_{x_4=0} = h^{(3)}(x) = \frac{\alpha x_1 + \beta x_2}{\alpha' x_1 + \beta' x_2},\qquad h^*(x_1, x_2) = \frac{\alpha x_1 + \beta x_2}{\alpha' x_1 + \beta' x_2}.$$

§ 3. One-to-one mapping of systems $\mathfrak{S}_{n\rho}$ onto systems $\mathfrak{S}^*_{\rho\rho}$.

The lemma immediately gives a mapping of systems $\mathfrak{S}_{n\rho}$ onto systems $\mathfrak{S}^*_{\rho\rho}$ by replacing some of the indeterminates with numbers; the algebraic rank ρ thereby emerges as the true characteristic number.

Since $\mathfrak{S}_{n\rho}$ has algebraic rank ρ, it contains ρ algebraically independent functions,

$$g_1(x), \ldots, g_\rho(x), \tag{1}$$

If, further, $f(x)$ denotes an arbitrary function of $\mathfrak{S}_{n\rho}$, then the system

$$g_1(x), \ldots, g_\rho(x),\ f(x) \tag{2}$$

also has algebraic rank ρ; the systems (1) and (2) therefore satisfy the hypotheses of the lemma.[86]

Choose the numbers

$$a_n,\ a_{n-1}, \ldots, a_{\rho+1}$$

according to the lemma so that the substitution preserves the algebraic rank ρ of the system (1) — which can be done in arbitrarily many ways. Then, in the function defined by

$$\begin{aligned} [f(x)]_{x_n=a_n} &= f^{(n-1)}(x), \qquad [f^{(n-1)}(x)]_{x_{n-1}=a_{n-1}} = f^{(n-2)}(x); \ldots, \\ [f^{(\rho+1)}(x)]_{x_{\rho+1}=a_{\rho+1}} &= f^*(x_1, \ldots, x_\rho), \end{aligned}$$

namely

$$f^*(x_1, \ldots, x_\rho), \tag{3}$$

neither the numerator nor the denominator can vanish identically.

Now let $f(x)$ range over all the finitely or infinitely many functions of $\mathfrak{S}_{n\rho}$. Consider the system consisting of all functions (3). It has the following properties:

1. It has algebraic rank ρ, for it contains the functions arising from (1),

$$g_1^*(x_1, \ldots, x_\rho), \ldots, g_\rho^*(x_1, \ldots, x_\rho),$$

which are algebraically independent by the choice of $a_n, a_{n-1}, \ldots, a_{\rho+1}$. We shall therefore denote the system by

$$\mathfrak{S}^*_{\rho\rho}.$$

[87]

2. The correspondence $f(x) \longleftrightarrow f^*(x)$ is one-to-one without exception.

Indeed, if $f_1(x)$ and $f_2(x)$ belong to $\mathfrak{S}_{n\rho}$, then their difference

$$d(x) = f_1(x) - f_2(x)$$

is also algebraically dependent on the system (1), and

$$d^*(x) = f_1^*(x) - f_2^*(x).$$

Since $d(x)$ together with the system (1) satisfies the hypotheses of the lemma,

$$d(x) \neq 0$$

necessarily implies

$$d^*(x) \neq 0;$$

that is, distinct functions of $\mathfrak{S}_{n\rho}$ correspond to distinct functions of $\mathfrak{S}^*_{\rho\rho}$.

3. Every relation among functions of $\mathfrak{S}^*_{\rho\rho}$,

$$F(f_1^*(x), f_2^*(x), \ldots, f_k^*(x)) = 0 \quad \text{identically in } x_1 \cdots x_\rho,$$

implies, for the uniquely corresponding functions of $\mathfrak{S}_{n\rho}$,

$$F(f_1(x), f_2(x), \ldots, f_k(x)) = 0 \quad \text{identically in } x_1 \cdots x_n.$$

[86] If necessary, the indeterminates are to be renumbered.

[87] Correspondingly, $f^*(x)$, $g^*(x)$, ... will always denote image functions, that is, functions of $x_1 \cdots x_\rho$.

For every rational expression in $f_1(x), f_2(x), \ldots, f_k(x)$ is likewise algebraically dependent on the system (1).

Moreover, from

$$\begin{aligned} h(x) &= F\big(f_1(x), \ldots, f_k(x)\big) : \\ h^*(x) &= F\big(f_1^*(x), \ldots, f_k^*(x)\big). \end{aligned} \tag{4}$$

the lemma gives

$$h(x) \neq 0 \quad \text{implies} \quad h^*(x) \neq 0;$$

q.e.d.

In summary, we obtain

Theorem I: With every system $\mathfrak{S}_{n\rho}$ of (finitely or infinitely many) rational functions one may associate — in arbitrarily many ways — a system $\mathfrak{S}^*_{\rho\rho}$ in one-to-one correspondence with it, so that every relation among functions of $\mathfrak{S}^*_{\rho\rho}$ is preserved in $\mathfrak{S}_{n\rho}$, and conversely. In particular, by (4), a field $\mathfrak{K}_{n\rho}$ again corresponds to a field $\mathfrak{K}^*_{\rho\rho}$.

From Theorem I we also draw the consequence that simplifies all subsequent proofs: *properties of systems $\mathfrak{S}_{n\rho}$ that are characterized by finitely or infinitely many relations among functions of the system hold for the systems $\mathfrak{S}_{n\rho}$ as soon as they hold for an image system $\mathfrak{S}^*_{\rho\rho}$.*

We shall refer to this consequence briefly as the "transfer principle."

The simplest example of this mapping is furnished by the theory of algebraic invariants. Indeed, a linear transformation can always be used to assign numerical values to some coefficients of the ground form in such a way that every relation valid for the specialized form remains valid in general.

§ 4. Rational basis of the fields $\mathfrak{K}_{n\rho}$.

Throughout the investigations that follow, which center on concepts of a basis, we make use of the "transfer principle" of § 3. We first prove the existence of a basis for fields, but formulate the definitions in general:

Definition III: A finite set of functions of $\mathfrak{S}_{n\rho}$ is called a rational basis if every function of $\mathfrak{S}_{n\rho}$ can be expressed rationally in terms of this finite set, with coefficients in Ω.

The rational basis must contain ρ algebraically independent functions, since the algebraic rank of a system derived from a rational basis is equal to the algebraic rank of the rational basis.

We first show that the proof of existence of a rational basis admits the transfer principle. Indeed, Definition III may be recast as follows:

The functions of $\mathfrak{S}_{n\rho}$

$$g_1(x),\ g_2(x), \ldots, g_k(x)$$

form a rational basis if and only if the infinitely many relations

$$f(x) = \gamma(g_1(x), \ldots, g_k(x)) \tag{1}$$

hold, where $f(x)$ ranges over all functions of $\mathfrak{S}_{n\rho}$ and γ denotes a rational function of k arguments that varies with f.

Thus, if the image system $\mathfrak{S}^*_{\rho\rho}$ has the rational basis

$$g_1^*(x),\ g_2^*(x), \ldots, g_k^*(x),$$

and consequently satisfies the relations

$$f^*(x) = \gamma(g_1^*(x), \ldots, g_k^*(x)),$$

then, by Theorem I, the relations (1) hold for $\mathfrak{S}_{n\rho}$. Thus the *transfer principle for the rational basis* reads:

The existence of a rational basis for an image system $\mathfrak{S}^*_{\rho\rho}$ implies the existence of a rational basis for the original system $\mathfrak{S}_{n\rho}$.[88]

To prove the existence of a rational basis for all fields $\mathfrak{K}_{n\rho}$, we may therefore restrict ourselves to fields $\mathfrak{K}^*_{\rho\rho}$; here a direct generalization of an argument used by E. Steinitz yields the result.[89]

Let

$$g_1^*(x_1, \ldots, x_\rho), \ldots, g_\rho^*(x_1, \ldots, x_\rho) \tag{2}$$

be a system of ρ algebraically independent functions of $\mathfrak{K}^*_{\rho\rho}$. Eliminating $x_1, \ldots, x_\rho$ yields ρ relations:

$$\begin{aligned} F_1(g_1^*(x), \ldots, g_\rho^*(x), x_1) &= 0, \ldots, \\ F_\rho(g_1^*(x), \ldots, g_\rho^*(x), x_\rho) &= 0, \end{aligned} \tag{3}$$

where the indeterminate x_i genuinely occurs in each relation $F_i = 0$; otherwise, contrary to the assumption, there would be an algebraic dependence among the functions (2). The relations (3) state that

$$x_1, x_2, \ldots, x_\rho$$

are algebraic elements over

$$\Omega(g_1^*(x), \ldots, g_\rho^*(x)).$$

Thus the field obtained by adjoining $x_1, \ldots, x_\rho$,

$$\Omega(g_1^*, \ldots, g_\rho^*, x_1, \ldots, x_\rho) = \Omega(x_1, \ldots, x_\rho),$$

is a finite algebraic extension of $\Omega(g_1^*, \ldots, g_\rho^*)$. By a known theorem,[90] $\mathfrak{K}^*_{\rho\rho}$, as an intermediate field between $\Omega(g_1^*, \ldots, g_\rho^*)$ and $\Omega(x_1, \ldots, x_\rho)$, is itself algebraic over $\Omega(g_1^*, \ldots, g_\rho^*)$, while $\Omega(x_1, \ldots, x_\rho)$ is algebraic over

[88] The transfer principle is formulated correspondingly for every basis question treated here.

[89] E. Steinitz, Algebraische Theorie der Körper, § 24, Crelle's Journal 137 (1909).

[90] Compare, for example, Weber, Lehrbuch d. Algebra 1, § 144 (1st ed.) or § 55 (small edition).

$\mathfrak{K}^*_{\rho\rho}$. Thus $\mathfrak{K}^*_{\rho\rho}$ is obtained from $\Omega(g_1^*, \ldots, g_\rho^*)$ by adjoining a finite number of elements of $\mathfrak{K}^*_{\rho\rho}$, or indeed by adjoining one suitably chosen function; that is,

$$\mathfrak{K}^*_{\rho\rho} = \Omega(g_1^*, \ldots, g_\rho^*, g_{\rho+1}^*, \ldots, g_k^*) = \Omega(g_1^*, \ldots, g_\rho^*, g_0^*).$$

By the transfer principle, therefore,

Theorem II: Every field $\mathfrak{K}_{n\rho}$ possesses a rational basis of algebraic rank ρ; in particular, the rational basis may be chosen to contain at most $\rho + 1$ functions.

Let an arbitrary system of ρ algebraically independent functions of $\mathfrak{K}_{n\rho}$ be given by $h_1(x), \ldots, h_\rho(x)$. By the method above it can be extended to a rational basis

$$h_1(x), \ldots, h_\rho(x); h_{\rho+1}(x), \ldots, h_\sigma(x).$$

By the defining property there are relations

$$\begin{aligned} h_i(x) &= \chi_i(g_1(x), \ldots, g_k(x)) \quad (i = 1, 2, \ldots, \sigma), \\ g_j(x) &= \psi_j(h_1(x), \ldots, h_\sigma(x)) \quad (j = 1, 2, \ldots, k), \end{aligned}$$

where χ_i and ψ_j denote rational functions of their arguments; that is:

Every other rational basis is obtained from any given rational basis by a birational transformation; and:

If

$$h_1(x), \ldots, h_\rho(x)$$

is any system of ρ algebraically independent functions of $\mathfrak{K}_{n\rho}$, then $\mathfrak{K}_{n\rho}$ is a finite algebraic extension of

$$\Omega(h_1(x), \ldots, h_\rho(x)).$$

§ 5. Involution form and involution basis of the fields $\mathfrak{K}_{n\rho}$.

Whereas every rational basis constructed in § 4 had the disadvantage of depending on the arbitrarily chosen initial functions, we now prove the existence of a *rational basis uniquely determined by the field.*

By § 4, $\Omega(x_1, \ldots, x_\rho)$ is an algebraic extension — say of degree i — of $\mathfrak{K}^*_{\rho\rho}$ and, because

$$\mathfrak{K}^*_{\rho\rho}(x_1, \ldots, x_\rho) = \Omega(x_1, \ldots, x_\rho),$$

is obtained by adjoining the elements $x_1, \ldots, x_\rho$, which are algebraic over $\mathfrak{K}^*_{\rho\rho}$. We therefore consider the polynomial $\Phi^*(z, u)$ irreducible over $\mathfrak{K}^*_{\rho\rho}$ and having the root

$$z = u_1x_1 + u_2x_2 + \cdots + u_\rho x_\rho = u(x),$$

and which has degree i in z. Moreover, as the product of the factors conjugate to $[z - u(x)]$, $\Phi^*(z, u)$ is a homogeneous form of degree i in $z, u_1, \ldots, u_\rho$; its coefficient of z^i is therefore an element of $\mathfrak{K}^*_{\rho\rho}$ independent of u. Dividing by this leading coefficient to make it 1 uniquely determines the irreducible polynomial $\Phi^*(z, u)$. The homogeneous form so defined,

$$\begin{aligned} \Phi^*(z, u) = z^i + \sum{}' g^*_{\alpha\alpha_1\ldots\alpha_\rho}(x_1, \ldots, x_\rho) z^\alpha u_1^{\alpha_1} \cdots u_\rho^{\alpha_\rho}, \\ (\alpha + \alpha_1 + \cdots + \alpha_\rho = i), \end{aligned} \tag{1}$$

will be called the *involution form*[91] of $\mathfrak{K}^*_{\rho\rho}$; from (1) one obtains

$$\begin{aligned} \Phi(z, u) = z^i + \sum{}' g_{\alpha\alpha_1\ldots\alpha_\rho}(x) z^\alpha u_1^{\alpha_1} \cdots u_\rho^{\alpha_\rho}, \\ (\alpha + \alpha_1 + \cdots + \alpha_\rho = i), \end{aligned} \tag{2}$$

as an *involution form* of $\mathfrak{K}_{n\rho}$.

The coefficients of the involution form $\Phi^*(z, u)$ will prove to be a rational basis of $\mathfrak{K}^*_{\rho\rho}$; that is, the relation

$$\Omega(g^*_{\alpha\alpha_1\ldots\alpha_\rho}(x_1, \ldots, x_\rho)) = \mathfrak{K}^*_{\rho\rho} \quad (\alpha + \alpha_1 + \cdots + \alpha_\rho = i) \tag{3}$$

[91] The reason for this name emerges at the end of the section; $\sum'$ means that the summation extends over all terms except z^i.

holds. For the proof, observe that $\Phi^*(z,u)$ has coefficients in $\Omega(g^*_{\alpha\alpha_1\dots\alpha_\rho}(x))$ and, being irreducible over $\mathfrak{K}^*_{\rho\rho}$, is certainly irreducible over this subfield. Thus $\Phi^*(z,u)$ is the irreducible equation of $u(x)$ over $\Omega(g^*_{\alpha\alpha_1\dots\alpha_\rho}(x))$. It follows that $\Omega(x_1,\dots,x_\rho)$ is an algebraic extension — of degree i — of $\Omega(g^*_{\alpha\alpha_1\dots\alpha_\rho}(x))$. Since $\mathfrak{K}^*_{\rho\rho}$ lies between $\Omega(g^*_{\alpha\alpha_1\dots\alpha_\rho}(x))$ and $\Omega(x_1,\dots,x_\rho)$, equality of the degrees is known to imply equality of the fields, and hence relation (3). By the transfer principle, the coefficients of $\Phi(z,u)$ correspondingly give a rational basis of $\mathfrak{K}_{n\rho}$; thus we have

Theorem III: The coefficients of the involution form constitute a rational basis determined by the field, the involution basis; for fields $\mathfrak{K}^*_{\rho\rho}$ this basis is uniquely determined.[92]

We give also an irrational interpretation of this fact, which establishes the connection with the geometric theory of involutions.

Suppose the factorization of $\Phi^*(z,u)$ into linear factors in an extension field is

$$\begin{aligned}\Phi^*(z,u) = (z-u_1x_1-\cdots-u_\rho x_\rho)(z-u_1x_1^{(1)}-\cdots-u_\rho x_\rho^{(1)})\cdots\\ \cdot(z-u_1x_1^{(i-1)}-\cdots-u_\rho x_\rho^{(i-1)}).\end{aligned}\tag{4}$$

Comparison with (1) shows that the functions

$$g^*_{\alpha\alpha_1\dots\alpha_\rho}(x_1,\dots,x_\rho)\quad(\alpha+\alpha_1+\cdots+\alpha_\rho=i)$$

are precisely the elementary symmetric functions of the rows of quantities

$$\begin{array}{cccc} x_1 & x_2 & \cdots & x_\rho \\ x_1^{(1)} & x_2^{(1)} & \cdots & x_\rho^{(1)} \\ \vdots & \vdots & & \vdots \\ x_1^{(i-1)} & x_2^{(i-1)} & \cdots & x_\rho^{(i-1)}. \end{array}\tag{5}$$

Thus every function of $\mathfrak{K}^*_{\rho\rho}$ is a rational expression in these elementary functions and is symmetric in the rows (5); conversely, every symmetric function of the rows (5) belongs to $\mathfrak{K}^*_{\rho\rho}$.

Thus, as

$$f^*(x)=\frac{F^*(x)}{H^*(x)}$$

ranges over all functions of $\mathfrak{K}^*_{\rho\rho}$, the following infinite system of relations holds:

$$\frac{F^*(x)}{H^*(x)}=\frac{F^*(x^{(1)})}{H^*(x^{(1)})}=\cdots=\frac{F^*(x^{(i-1)})}{H^*(x^{(i-1)})},\tag{6}$$

or, collectively,

$$F^*(x^{(k)})H^*(x^{(l)})-F^*(x^{(l)})H^*(x^{(k)})=0\quad(k,l=0,1,\dots,i-1),$$

where neither $F^*(x^{(k)})$ nor $H^*(x^{(k)})$ vanishes identically, since these expressions are conjugate to $F^*(x)$ and $H^*(x)$ and are formally symmetric.

Conversely, every row of quantities ξ satisfying the infinitely many relations

$$F^*(x)H^*(\xi)-H^*(x)F^*(\xi)=0,\qquad H^*(\xi)\neq 0,\tag{7}$$

must belong to the rows of quantities (5).

Indeed, let $G^*(x)$ denote the common denominator of the coefficients of $\Phi^*(z,u)$. By assumption (7), the polynomial

$$G^*(\xi)\cdot\Phi^*(z,u;\xi),$$

which is also polynomial in ξ, does not vanish identically — that is, the coefficients of $\Phi^*(z,u;\xi)$ do not become indeterminate — and has the root

$$z=u_1\xi_1+u_2\xi_2+\cdots+u_\rho\xi_\rho.$$

By (7), $\Phi^*(z,u;x)$ therefore also has the root $z=u(\xi)$; thus ξ belongs to the rows of quantities (5). By (6), the corresponding assertion holds if ξ satisfies a system of equations with respect to a conjugate row of quantities:

$$F^*(x^{(k)})H^*(\xi)-H^*(x^{(k)})F^*(\xi)=0;\qquad H^*(\xi)\neq 0.$$

[92] For fields $\mathfrak{K}_{n\rho}$ the involution form may depend on the mapping; uniqueness can be obtained by using a mapping with indeterminate coefficients.

Thus the rows of quantities (5) are characterized as the solutions ξ of the system of equations

$$F^*(x)H^*(\xi) - H^*(x)F^*(\xi) = 0; \qquad H^*(\xi) \neq 0,$$

where $\frac{F^*(x)}{H^*(x)}$ ranges over all functions of $\mathfrak{K}^*_{\rho\rho}$; here the row x may also be replaced by any conjugate row.

Geometrically, interpreting each row x as a point, this says: in a ρ-dimensional linear space, the solutions of (7) form ∞^ρ groups of i points each, in such a way that any point of a group uniquely determines that group. Such a system of point groups is called an "*involution in a linear space.*"[93]

Correspondingly, a field $\mathfrak{K}_{n\rho}$ characterizes an involution in a linear space consisting of curves, surfaces, and so forth.

By the preceding, the degree i of $\Omega(x_1, \ldots, x_\rho)$ over $\mathfrak{K}^*_{\rho\rho}$ equals the number of solution systems of (7) satisfying the side condition $H^*(\xi) \neq 0$ — which we may call the solution systems of $\mathfrak{K}^*_{\rho\rho}$. Thus the argument used to prove the existence of the involution basis also admits the following irrational formulation:

"If $\mathfrak{L}^*$ is a subfield of $\mathfrak{K}^*_{\rho\rho}$ and every solution system of the field $\mathfrak{L}^*$ is also a solution system of $\mathfrak{K}^*_{\rho\rho}$, then $\mathfrak{L}^*$ and $\mathfrak{K}^*_{\rho\rho}$ are identical."

By the transfer principle, the corresponding statement holds for subfields $\mathfrak{L}$ of $\mathfrak{K}_{n\rho}$.

§ 6. Minimal basis of the fields $\mathfrak{K}_{n\rho}$.

This section surveys known theorems, but in an extended form made possible by the transfer principle and the existence of the rational basis.

Definition IV: A rational basis of $\mathfrak{K}_{n\rho}$ is called a minimal basis if it contains only the minimum number ρ of functions, which must then be algebraically independent.

Theorems of Lüroth, Castelnuovo, and Enriques[94] yield the following facts:

I. Every field $\mathfrak{K}_{n1}$ possesses a minimal basis: the Lüroth function of the field, uniquely determined up to a linear fractional transformation.

II. For fields $\mathfrak{K}_{n2}$, a minimal basis always exists — and in general exists only — if an algebraic extension of the coefficient field Ω is allowed.

III. For fields $\mathfrak{K}_{n\rho}$ ($\rho \geq 3$), no minimal basis exists in general. No characterization of the special fields $\mathfrak{K}_{n\rho}$ possessing a minimal basis has yet been attempted.

We briefly outline E. Steinitz's proof of Lüroth's theorem for fields $\mathfrak{K}^*_{11}$:[95]

Let $\Phi^*(z, u)$ be the involution form of $\mathfrak{K}^*_{11}$, and let $\psi^*(x)$ be any coefficient of $\Phi^*(z, u)$ in which the indeterminate x genuinely occurs. The degree of $\Omega(x)$ over $\Omega(\psi^*(x))$ proves to equal the degree of $\Omega(x)$ over $\mathfrak{K}^*_{11}$, from which equality of the fields follows. Moreover, if $\Omega(\chi^*(x)) = \Omega(\psi^*(x))$, then the mutual rational dependence of $\chi^*(x)$ and $\psi^*(x)$ implies that the two functions are related by a linear fractional transformation.

By the transfer principle, Lüroth's theorem therefore also admits the formulation:

The minimal basis of a field $\mathfrak{K}_{n1}$ consists of any function of the involution basis; any two functions of the involution basis of $\mathfrak{K}_{n1}$ are related by a linear fractional transformation.

G. Castelnuovo proves Fact II by means of the geometric theory of involutions for fields $\mathfrak{K}^*_{22}$ derived from a rational basis of three functions. Since the transfer principle remains valid under a finite algebraic extension of the coefficient field Ω, the existence of the rational basis makes this a proof for all fields $\mathfrak{K}_{n2}$.

Regarding III, it should be noted that Enriques constructs a nonrational involution in three-dimensional space; that is, a field $\mathfrak{K}_{33}$ possessing no minimal basis.

§ 7. Arbitrary system $\mathfrak{S}_{n\rho}$, linear family $\mathfrak{L}_{n\rho}$, and integrality domain $\mathfrak{J}_{n\rho}$ of rational functions. Existence of the rational basis.

From the existence of a rational basis for the fields $\mathfrak{K}_{n\rho}$ we shall now deduce the existence of a rational basis for arbitrary systems of rational functions and polynomials. We arrange these systems in the order in which

[93] The excluded solutions of (7), for which $F^*(\xi) = 0$ and $H^*(\xi) = 0$, as well as the excluded solutions of the system of equations corresponding to the involution basis, are called fundamental points of the involution; those "lying at infinity" that arise upon homogenization are to be counted as well.

[94] J. Lüroth: Beweis eines Satzes über rationale Kurven, Math. Ann. 9 (1875). — G. Castelnuovo: Sulla razionalità delle involuzioni piane, Math. Ann. 44 (1893). — F. Enriques: Sopra una involuzione non razionale dello spazio, Rend. Acc. Linc., Vol. 21, 21 Jan. 1912.

[95] Loc. cit., § 24.

they arise successively from one another through the elementary operations of addition, multiplication, and division.

I. As always, let $\mathfrak{S}_{n\rho}$ denote an arbitrary system of rational functions (or polynomials) in n indeterminates and of algebraic rank ρ. The elements of Ω are counted as belonging to the system.

II. The system $\mathfrak{L}_{n\rho}$ is called a *linear family* if it satisfies the conditions:

1. Together with $f(x)$, $\mathfrak{L}_{n\rho}$ always contains $c \cdot f(x)$, where c is an arbitrary element of Ω;

2. Together with $f(x)$ and $g(x)$, $\mathfrak{L}_{n\rho}$ always contains $f(x) + g(x)$.

III. The linear family $\mathfrak{J}_{n\rho}$ is called an *integrality domain* under the further condition:

3. Together with $f(x)$ and $g(x)$, $\mathfrak{J}_{n\rho}$ always contains $f(x) \cdot g(x)$.

IV. The integrality domain $\mathfrak{K}_{n\rho}$ is called a *field* under the further condition:

4. Together with $f(x)$ and $g(x)$ — where $g(x) \neq 0$ — $\mathfrak{K}_{n\rho}$ always contains the quotient $f(x) : g(x)$.

Conditions 1 through 4 are those stated for fields in § 1.[96]

These domains are now to be derived successively from one another.

a) An arbitrary system $\mathfrak{S}_{n\rho}$ is extended to a linear family $\mathfrak{L}_{n\rho}$ by requiring that:

$\mathfrak{L}_{n\rho}$ contains, in addition to $\mathfrak{S}_{n\rho}$, all and only those functions $h(x)$ that can be expressed linearly, with coefficients in Ω, in terms of finitely many functions of $\mathfrak{S}_{n\rho}$:

$$h(x) = c_1 f_1(x) + c_2 f_2(x) + \cdots + c_k f_k(x),$$

where $f_1(x), \ldots, f_k(x)$ range over all functions of $\mathfrak{S}_{n\rho}$, and $c_1, \ldots, c_k$ over all elements of Ω.

For adjoining rational expressions in functions of a system preserves its algebraic rank. The system $\mathfrak{L}_{n\rho}$ satisfies conditions 1 and 2 and is therefore a linear family. Moreover, by 1 and 2 every linear family containing $\mathfrak{S}_{n\rho}$ also contains $\mathfrak{L}_{n\rho}$; hence $\mathfrak{L}_{n\rho}$ is the smallest linear family containing $\mathfrak{S}_{n\rho}$.

b) Correspondingly, the smallest integrality domain $\mathfrak{J}_{n\rho}$ containing a linear family $\mathfrak{L}_{n\rho}$ is obtained by requiring that:

$\mathfrak{J}_{n\rho}$ contains, in addition to $\mathfrak{L}_{n\rho}$, all and only those functions $h(x)$ that can be expressed as a *polynomial expression* — with coefficients in Ω — in finitely many functions $f_1(x), \ldots, f_k(x)$ of $\mathfrak{L}_{n\rho}$, where $f_1(x), \ldots, f_k(x)$ range over all functions of $\mathfrak{L}_{n\rho}$.

c) Finally, the smallest field $\mathfrak{K}_{n\rho}$ containing an integrality domain $\mathfrak{J}_{n\rho}$ is obtained by requiring that $\mathfrak{K}_{n\rho}$ contain, in addition to $\mathfrak{J}_{n\rho}$, all and only those functions $h(x)$ that can be expressed as quotients of two functions of $\mathfrak{J}_{n\rho}$.

Combining the three extensions into a single step gives:

Every system $\mathfrak{S}_{n\rho}$ can be extended to a smallest field $\mathfrak{K}_{n\rho}$ containing it by requiring that:

$\mathfrak{K}_{n\rho}$ contains, in addition to $\mathfrak{S}_{n\rho}$, all and only those functions $h(x)$ that can be expressed as rational expressions — with coefficients in Ω — in finitely many functions $f_1(x), \ldots, f_k(x)$ of $\mathfrak{S}_{n\rho}$, where $f_1(x), \ldots, f_k(x)$ range over all functions of $\mathfrak{S}_{n\rho}$.

The existence of a rational basis for arbitrary domains follows immediately from this fact:

Let $\mathfrak{K}_{n\rho}$ be the smallest field containing $\mathfrak{S}_{n\rho}$, and let a rational basis of $\mathfrak{K}_{n\rho}$ be given by

$$h_1(x),\ h_2(x), \ldots, h_\sigma(x). \tag{1}$$

By the definition of $\mathfrak{K}_{n\rho}$, there are relations

$$\begin{aligned} h_1(x) &= r_1(g_1(x), \ldots, g_\lambda(x)); \ldots; \\ h_\sigma(x) &= r_\sigma(g_\mu(x), \ldots, g_\nu(x)), \end{aligned} \tag{2}$$

where $r_1, \ldots, r_\sigma$ are rational functions of their arguments, and

$$g_1(x), \ldots, g_\lambda(x), \ldots, g_\mu(x), \ldots, g_\nu(x) \tag{3}$$

all belong to $\mathfrak{S}_{n\rho}$. By the relations (2), the functions (3), as well as those in (1), form a rational basis of $\mathfrak{K}_{n\rho}$; because the functions (3) belong to $\mathfrak{S}_{n\rho}$, they are at the same time a rational basis of $\mathfrak{S}_{n\rho}$. We therefore have

Theorem IV: Every system $\mathfrak{S}_{n\rho}$ of rational functions (or polynomials) possesses a rational basis of algebraic rank ρ consisting of finitely many functions of the system.

Now suppose in particular that $\mathfrak{L}_{n\rho}$ is a linear family and that

$$g_1(x), \ldots, g_\rho(x),\ g_{\rho+1}(x), \ldots, g_\nu(x) \tag{4}$$

[96] $f(x)$ and $g(x)$ may also have degree zero, that is, they may be elements of Ω.

is a rational basis of $\mathfrak{L}_{n\rho}$. Suppose, for instance, that

$$g_1(x), \ldots, g_\rho(x)$$

are algebraically independent. If one then sets

$$g(x) = c_1 g_{\rho+1}(x) + c_2 g_{\rho+2}(x) + \cdots + c_{\nu-\rho} g_\nu(x),$$

then the c_i can be chosen as elements of Ω in such a way that

$$g_1(x), \ldots, g_\rho(x),\ g(x) \tag{5}$$

is a rational basis of the smallest field $\mathfrak{K}_{n\rho}$ containing $\mathfrak{L}_{n\rho}$. But because $\mathfrak{L}_{n\rho}$ is a linear family, $g(x)$ belongs to $\mathfrak{L}_{n\rho}$, and (5) is a rational basis of $\mathfrak{L}_{n\rho}$; that is,

Theorem V: A rational basis of every linear family $\mathfrak{L}_{n\rho}$ of rational functions (or polynomials) — and hence, in particular, a rational basis of every integrality domain $\mathfrak{J}_{n\rho}$ and every field $\mathfrak{K}_{n\rho}$ — may be chosen to contain at most $\rho + 1$ functions (and at least ρ).

The bound found in § 4 on the number of functions in a rational basis of a field therefore rests on the fact that a field is a linear family, whereas the restriction to ρ functions when a minimal basis exists uses all the defining conditions of a field.

It should also be noted that, by § 3 (4), all characteristic properties of the systems and of the smallest systems containing them are preserved under the mapping.

§ 8. Involution basis of the integrality domains $\mathfrak{J}_{n\rho}$ consisting of polynomials.

In the following sections we consider systems $\mathfrak{S}_{n\rho}$ whose elements are polynomials; first, integrality domains $\mathfrak{J}_{n\rho}$ consisting of polynomials. For these domains $\mathfrak{J}_{n\rho}$ we shall first establish the notions of divisibility.

Let $F(x), G(x)$ be two polynomials of $\mathfrak{J}_{n\rho}$, and let $L(x)$ be a common divisor of these polynomials, so that

$$F(x) = L(x) \cdot F_1(x), \qquad G(x) = L(x) \cdot G_1(x).$$

$L(x)$ is called a *common divisor in* $\mathfrak{J}_{n\rho}$ if and only if all three polynomials $L(x), F_1(x), G_1(x)$ belong to $\mathfrak{J}_{n\rho}$.

Two polynomials of $\mathfrak{J}_{n\rho}$ are called *relatively prime in* $\mathfrak{J}_{n\rho}$ if they have no common divisor in $\mathfrak{J}_{n\rho}$.

Let $\mathfrak{K}_{n\rho}$ be the smallest field containing $\mathfrak{J}_{n\rho}$. It follows from the definition that every function of $\mathfrak{K}_{n\rho}$ has a representation

$$f(x) = F_1(x) : F_2(x),$$

where $F_1(x), F_2(x)$ belong to $\mathfrak{J}_{n\rho}$ and are relatively prime in $\mathfrak{J}_{n\rho}$. Correspondingly, several functions of $\mathfrak{K}_{n\rho}$ can be brought to a common denominator in $\mathfrak{J}_{n\rho}$:

$$f_1(x) = \frac{F_1(x)}{F(x)}, \ldots, f_k(x) = \frac{F_k(x)}{F(x)}.$$

$F(x)$ is called *a least common denominator in* $\mathfrak{J}_{n\rho}$ if and only if the polynomials of $\mathfrak{J}_{n\rho}$

$$F(x), F_1(x), \ldots, F_k(x),$$

are relatively prime in $\mathfrak{J}_{n\rho}$.

Such a representation may be possible in different ways, since the laws of unique factorization into irreducible polynomials do not hold in $\mathfrak{J}_{n\rho}$ in general.

We now investigate the significance of the involution basis of $\mathfrak{K}_{n\rho}$ for $\mathfrak{J}_{n\rho}$ by extending the notions of involution form and involution basis to integrality domains. Let

$$\Phi(z,u) = z^i + \sum{}' g_{\alpha\alpha_1\ldots\alpha_\rho}(x) z^\alpha u_1^{\alpha_1} \cdots u_\rho^{\alpha_\rho}, \qquad (\alpha + \alpha_1 + \cdots + \alpha_\rho = i)$$

be an involution form of $\mathfrak{K}_{n\rho}$, and let $G(x)$ be a least common denominator in $\mathfrak{J}_{n\rho}$ of the coefficients of $\Phi(z,u)$. Multiplication by $G(x)$ transforms $\Phi(z,u)$ into a form $\Psi(z,u)$ whose coefficients are polynomials of $\mathfrak{J}_{n\rho}$ and are relatively prime in $\mathfrak{J}_{n\rho}$:

$$G(x) \cdot \Phi(z,u) = \Psi(z,u) = G(x) z^i + \sum{}' G_{\alpha\alpha_1\ldots\alpha_\rho}(x) z^\alpha u_1^{\alpha_1} \cdots u_\rho^{\alpha_\rho}, \qquad (\alpha + \alpha_1 + \cdots + \alpha_\rho = i).$$

Every form $\Psi(z,u)$ obtained from an involution form $\Phi(z,u)$ of $\mathfrak{K}_{n\rho}$ by multiplication by a polynomial of $\mathfrak{J}_{n\rho}$, in such a way that the coefficients of $\Psi(z,u)$ are polynomials of $\mathfrak{J}_{n\rho}$ and are relatively prime in $\mathfrak{J}_{n\rho}$, will be called an *involution form* of $\mathfrak{J}_{n\rho}$; the coefficients of $\Psi(z,u)$ will be called a corresponding *involution basis*.

It is immediately clear from the significance of the involution basis of $\mathfrak{K}_{n\rho}$ that every involution basis of $\mathfrak{J}_{n\rho}$ is also a rational basis. For the further investigation, consider an image domain $\mathfrak{J}^*_{\rho\rho}$ for whose smallest containing field $\mathfrak{K}^*_{\rho\rho}$ the irreducible equation having the root

$$z = u_1 x_1 + \cdots + u_\rho x_\rho$$

is $\Phi^*(z,u) = 0$.

By § 5, the coefficients of

$$\Phi^*(z,u) = z^i + \sum{}' g^*_{\alpha\alpha_1\ldots\alpha_\rho}(x) z^\alpha u_1^{\alpha_1} \cdots u_\rho^{\alpha_\rho}, \qquad (\alpha + \alpha_1 + \cdots + \alpha_\rho = i)$$

are the elementary symmetric functions of the rows of quantities conjugate over $\mathfrak{K}^*_{\rho\rho}$,

$$x, \quad x^{(1)}, \ldots, x^{(i-1)}.$$

Let $F^*(x)$ be any polynomial of $\mathfrak{K}^*_{\rho\rho}$. Since

$$F^*(x) = \frac{1}{i}\Big(F^*(x) + F^*(x^{(1)}) + \cdots + F^*(x^{(i-1)})\Big),$$

it follows that $F^*(x)$ is a polynomial symmetric function of these rows of quantities and can consequently be expressed as a polynomial in the elementary symmetric functions, that is, in the functions

$$g^*_{\alpha\alpha_1\ldots\alpha_\rho}(x).$$

If now

$$G^*(x)\cdot\Phi^*(z,u)=\Psi^*(z,u)=G^*(x)z^i+\sum{}'G^*_{\alpha\alpha_1\ldots\alpha_\rho}(x)z^\alpha u_1^{\alpha_1}\cdots u_\rho^{\alpha_\rho},\qquad(\alpha+\alpha_1+\cdots+\alpha_\rho=i)$$

is an involution form of $\mathfrak{J}^*_{\rho\rho}$, then every polynomial of $\mathfrak{K}^*_{\rho\rho}$, and in particular every polynomial of $\mathfrak{J}^*_{\rho\rho}$, is a polynomial expression in the quotients

$$G^*_{\alpha\alpha_1\ldots\alpha_\rho}(x):G^*(x).$$

Taking the transfer principle into account, we obtain

Theorem VI: Every integrality domain of polynomials $\mathfrak{J}_{n\rho}$ possesses at least one distinguished rational basis, the involution basis, such that in the rational representation of all polynomials of $\mathfrak{J}_{n\rho}$ in terms of the functions of the involution basis, only powers of one fixed function (the leading coefficient of the corresponding involution form) occur in the denominator.

§ 9. Relatively integral domains $\mathfrak{G}_{n\rho}$ consisting of polynomials.

In what follows we consider special integrality domains of polynomials that form an intermediate stage between integrality domains and fields.

An integrality domain of polynomials $\mathfrak{G}_{n\rho}$ is called a "relatively integral domain" if it satisfies the condition:

4a) Together with $F(x)$ and $G(x)$ — where $G(x)\neq 0$ — $\mathfrak{G}_{n\rho}$ contains the quotient $F(x):G(x)$ if and only if this quotient is polynomial in the indeterminates, that is, is a polynomial.

We first establish that relatively integral domains are precisely the totalities of polynomials in rational function fields $\mathfrak{K}_{n\sigma}$ $(\sigma\geq\rho)$.

Let $\mathfrak{K}_{n\rho}$ be the smallest field containing $\mathfrak{G}_{n\rho}$. Every function $f(x)$ of $\mathfrak{K}_{n\rho}$ can be represented as the quotient of two polynomials of $\mathfrak{G}_{n\rho}$:

$$f(x)=F_1(x):F_2(x),$$

where polynomials of degree zero are also allowed. Whenever $f(x)$ is a polynomial, it belongs to $\mathfrak{G}_{n\rho}$ by condition 4a); and since $\mathfrak{G}_{n\rho}$ cannot contain any other polynomials, *every relatively integral domain $\mathfrak{G}_{n\rho}$ is identical with the totality of the polynomials in the smallest field containing it.*

Conversely, let $\mathfrak{K}_{n\sigma}$ be any field of rational functions (thus not necessarily the smallest field containing a given system), and let $\mathfrak{J}$ be the totality of the polynomials contained in $\mathfrak{K}_{n\sigma}$. The system $\mathfrak{J}$ satisfies conditions 1, 2, and 3 for an integrality domain as well as condition 4a), and is therefore a relatively integral domain; that is, *the totality of the polynomials contained in a field $\mathfrak{K}_{n\sigma}$ forms a relatively integral domain $\mathfrak{G}_{n\rho}$ $(\rho\leq\sigma)$.*[97]

We further show that relatively integral domains are identical with Hilbert's "integrality domains of relatively integral functions."[98]

Let

$$G_1(x),\ldots,G_k(x)\tag{1}$$

be a rational basis of $\mathfrak{G}_{n\rho}$. By conditions 1, 2, 3, and 4a), every rational expression in the polynomials (1) that is polynomial in the indeterminates belongs to $\mathfrak{G}_{n\rho}$. Conversely, by the definition of a rational basis, every polynomial of $\mathfrak{G}_{n\rho}$ can be expressed rationally in terms of the polynomials (1); hence $\mathfrak{G}_{n\rho}$ is *identical with the totality of those rational expressions in the polynomials (1) that are polynomial in the indeterminates.* This is Hilbert's definition, which starts from a particular rational basis, whereas our definition uses only abstract properties of the domain.

For relatively integral domains, the definition of a common divisor given in § 8 for general integrality domains takes a simpler form:

Let $F(x),G(x)$ be two polynomials of $\mathfrak{G}_{n\rho}$ and let $L(x)$ be a common divisor of these polynomials. Then $L(x)$ is called a *common divisor in* $\mathfrak{G}_{n\rho}$ if and only if $L(x)$ belongs to $\mathfrak{G}_{n\rho}$.

[97] One may also have $\rho=0$; that is, the totality of the polynomials in $\mathfrak{K}_{n\sigma}$ may consist of elements of the coefficient field Ω.

[98] D. Hilbert: Mathematische Probleme. Lecture, Paris 1900. Problem 14 (Göttinger Nachrichten 1900).

For then the membership of the quotients $F(x) : L(x)$ and $G(x) : L(x)$ follows from condition 4a).

Another essential property of relatively integral domains is that the notion of being "algebraically integral over $\mathfrak{G}_{n\rho}$" can be defined by means of an arbitrary equation, just as is familiar for algebraic number fields or for the field $\Omega(x_1, \ldots, x_n)$.

Definition V: A quantity ξ is called algebraically integral over $\mathfrak{G}_{n\rho}$ — or relatively algebraically integral — if it satisfies an equation whose leading coefficient is 1 *and whose remaining coefficients are polynomials of $\mathfrak{G}_{n\rho}$.*

Suppose, for instance, that the relatively algebraically integral quantity ξ satisfies the equation

$$L(z) = z^\lambda + G_1(x)z^{\lambda-1} + \cdots + G_\lambda(x) = 0.$$

$L(z)$ is divisible by the polynomial irreducible over the smallest containing field $\mathfrak{K}_{n\rho}$,

$$M(z) = z^\mu + H_1(x)z^{\mu-1} + \cdots + H_\mu(x).$$

By the familiar extension of Gauss's theorem,[99] this divisibility implies that the rational functions $H_1(x), \ldots, H_\mu(x)$ are polynomials of $\mathfrak{K}_{n\rho}$ and therefore belong to $\mathfrak{G}_{n\rho}$. The relatively algebraically integral quantity ξ is thus characterized by its irreducible equation. In particular, every polynomial $F(x)$ of $\mathfrak{G}_{n\rho}$ is algebraically integral over $\mathfrak{G}_{n\rho}$, since it satisfies the equation $z - F(x) = 0$.

It should further be mentioned that, for an integrality domain $\mathfrak{J}_{n\rho}$ of polynomials, the smallest relatively integral domain $\mathfrak{G}_{n\rho}$ containing it is defined, in analogy with the smallest containing field, by the requirement:

$\mathfrak{G}_{n\rho}$ contains, in addition to $\mathfrak{J}_{n\rho}$, all and only those polynomials $H(x)$ that can be represented as quotients of two polynomials of $\mathfrak{J}_{n\rho}$.

This definition further implies that every involution form and involution basis of $\mathfrak{J}_{n\rho}$ gives rise to a corresponding one of $\mathfrak{G}_{n\rho}$ by removing, at most, a common divisor in $\mathfrak{G}_{n\rho}$ of all the polynomials in the basis.

For $\mathfrak{J}_{n\rho}$ and $\mathfrak{G}_{n\rho}$ possess the same smallest containing field $\mathfrak{K}_{n\rho}$; and every involution form of $\mathfrak{J}_{n\rho}$ is obtained from an involution form of $\mathfrak{K}_{n\rho}$ by multiplication by a polynomial of $\mathfrak{J}_{n\rho}$. Its coefficients therefore belong to $\mathfrak{G}_{n\rho}$, although they may have a common divisor in $\mathfrak{G}_{n\rho}$.[100]

Finally, it should be noted that the *image domain* of a relatively integral domain $\mathfrak{G}_{n\rho}$, which by § 7 is again an integrality domain $\mathfrak{J}^*_{\rho\rho}$ of polynomials, need not itself be relatively integral. Indeed, if $F(x)$ and $G(x)$ are two polynomials of $\mathfrak{G}_{n\rho}$ whose quotient is not a polynomial and consequently does not belong to $\mathfrak{G}_{n\rho}$, then the quotient $F^*(x) : G^*(x)$ likewise does not belong to $\mathfrak{J}^*_{\rho\rho}$. Yet this quotient, obtained by specializing some of the indeterminates, may very well be a polynomial; condition 4a) then fails for $\mathfrak{J}^*_{\rho\rho}$.[101]

§ 10. Relatively integral domains of the first kind and their integrality basis.

The notion of "relative algebraic integrality" introduced in § 9 (Definition V) makes it possible to specify a class of relatively integral domains that are finite integrality domains, and thus to answer affirmatively, at least for this class, a question raised by D. Hilbert (Mathematical Problems, Problem 14). We give

Definition VI: A finite set of polynomials of $\mathfrak{G}_{n\rho}$ is called an integrality basis if every polynomial of $\mathfrak{G}_{n\rho}$ can be expressed as a polynomial in this finite set, with coefficients in Ω. An integrality domain of polynomials that possesses an integrality basis is called a finite integrality domain.

We call the class of relatively integral domains under consideration, for which the involution basis will prove to be an integrality basis, relatively integral domains of the first kind, in accordance with

Definition VII: A relatively integral domain $\mathfrak{G}_{n\rho}$ is called of the first kind if it has an image domain $\mathfrak{G}^*_{\rho\rho}$ such that every polynomial in $x_1, \ldots, x_\rho$ (with coefficients from Ω) is algebraically integral over $\mathfrak{G}^*_{\rho\rho}$.

---

[99] Compare, for instance, J. König: Einleitung in die allgemeine Theorie der algebraischen GröSSen (Leipzig, B. G. Teubner, 1903), Kap. IX, § 2, or Weber (small edition), § 20.

[100] For example, for the integrality domain $\mathfrak{J}_{22}$ consisting of all polynomial expressions in x_1^2 and x_1x_2, one obtains the involution form

$$\Psi(z, u) = x_1^2z^2 - x_1^4u_1^2 - 2x_1^3x_2u_1u_2 - x_1^2x_2^2u_2^2.$$

Since x_1^2 belongs to $\mathfrak{J}_{22}$, and hence also to the smallest relatively integral domain $\mathfrak{G}_{22}$ containing it, it is a common divisor in $\mathfrak{G}_{22}$; the resulting involution form of $\mathfrak{G}_{22}$ is

$$\Psi(z, u) = z^2 - x_1^2u_1^2 - 2x_1x_2u_1u_2 - x_2^2u_2^2.$$

[101] For example, let $\mathfrak{J}_{32}$ consist of all polynomials that are rational expressions in $F = x_1^2x_2$ and $G = x_1^2(1 + x_3)$. The admissible specialization $x_3 = 0$ gives $F^* : G^* = x_2$, whereas $F : G$ is not a polynomial. Thus $\mathfrak{J}^*_{22}$ is not a relatively integral domain.

By this definition, the indeterminates $x_1, \ldots, x_\rho$, and consequently also the linear form $u(x) = u_1 x_1 + \cdots + u_\rho x_\rho$, are algebraically integral over $\mathfrak{G}^*_{\rho\rho}$. The irreducible polynomial having the root $z = u(x)$ — the involution form of the smallest containing field $\mathfrak{K}^*_{\rho\rho}$ — therefore has leading coefficient 1 and all its other coefficients are polynomials of $\mathfrak{G}^*_{\rho\rho}$. It is thus simultaneously an involution form of $\mathfrak{G}^*_{\rho\rho}$, and no other involution form can exist in $\mathfrak{G}^*_{\rho\rho}$. By the transfer principle, $\mathfrak{G}_{n\rho}$ likewise possesses an involution form whose leading coefficient is 1; and because, by Theorem VI, only this leading coefficient enters the denominator when all polynomials of $\mathfrak{G}_{n\rho}$ are rationally represented in terms of the corresponding involution basis, the involution basis is an integrality basis. Thus:

Theorem VII. Every relatively integral domain of the first kind is a finite integrality domain; its integrality basis is the involution basis obtained from the characterizing image domain. In particular, the integrality basis of a relatively integral domain of the first kind $\mathfrak{G}_{\rho\rho}$ is its uniquely determined involution basis.

We add a criterion for relatively integral domains of the first kind. Let $\mathfrak{G}_{n\rho}$ be of the first kind, with an integrality basis

$$F_1(x), F_2(x), \ldots, F_k(x). \tag{1}$$

Then, by a lemma of Hilbert,[102] there exist ρ algebraically independent polynomials of $\mathfrak{G}_{n\rho}$,

$$G_1(x), G_2(x), \ldots, G_\rho(x), \tag{2}$$

such that the polynomials (1), and hence every polynomial of $\mathfrak{G}_{n\rho}$, are algebraically integral over the polynomials (2). The same holds for every polynomial of the image domain $\mathfrak{G}^*_{\rho\rho}$ with respect to the corresponding polynomials

$$G^*_1(x), G^*_2(x), \ldots, G^*_\rho(x). \tag{3}$$

By Definition VII, therefore, every polynomial in $x_1, \ldots, x_\rho$ is also algebraically integral over the polynomials (3).

Conversely, suppose that an image domain $\mathfrak{J}^*_{\rho\rho}$ of an arbitrary relatively integral domain $\mathfrak{G}_{n\rho}$ contains ρ polynomials (3) over which every polynomial in $x_1, \ldots, x_\rho$ is algebraically integral. We shall show that $\mathfrak{J}^*_{\rho\rho}$ is then a relatively integral domain $\mathfrak{G}^*_{\rho\rho}$, and moreover that $\mathfrak{G}^*_{\rho\rho}$, and consequently $\mathfrak{G}_{n\rho}$, are of the first kind.

Indeed, let $F^*(x)$ be a polynomial of the smallest field $\mathfrak{K}^*_{\rho\rho}$ containing $\mathfrak{J}^*_{\rho\rho}$. By assumption, it is algebraically integral over the polynomials (3). The corresponding function of $\mathfrak{K}_{n\rho}$ is then algebraically integral over ρ polynomials of $\mathfrak{G}_{n\rho}$; it is therefore a polynomial $F(x)$ and belongs to $\mathfrak{G}_{n\rho}$, so $F^*(x)$ belongs to $\mathfrak{J}^*_{\rho\rho}$. Thus the image domain $\mathfrak{J}^*_{\rho\rho}$ contains every polynomial of $\mathfrak{K}^*_{\rho\rho}$ and is a relatively integral domain $\mathfrak{G}^*_{\rho\rho}$. Under the hypothesis, Definitions V and VII now imply immediately that $\mathfrak{G}^*_{\rho\rho}$, and hence also $\mathfrak{G}_{n\rho}$, are of the first kind; that is:

The relatively integral domains of the first kind $\mathfrak{G}_{n\rho}$ are characterized by the existence, in an image domain $\mathfrak{J}^*_{\rho\rho}$, of ρ polynomials over which every polynomial in $x_1, \ldots, x_\rho$ is algebraically integral. This hypothesis itself makes the image domain relatively integral.[103]

§ 11. Lemma on algebraically integral dependence.

We now give a criterion for every polynomial in $x_1, \ldots, x_\rho$ to be algebraically integral over ρ polynomials in $x_1, \ldots, x_\rho$,

$$G^*_1(x), \ldots, G^*_\rho(x). \tag{1}$$

If the polynomials (1) are homogeneous forms, then at every particular system of values for which (1) vanish, all forms algebraically integral over them vanish simultaneously; hence, in particular, so do $x_1, \ldots, x_\rho$.

The forms (1) can therefore vanish for no system of values other than

$$x_1 = 0, \ldots, x_\rho = 0;$$

their resultant must be nonzero.

Conversely, this condition is also sufficient and extends to inhomogeneous polynomials by the following

[102] D. Hilbert: Über die vollen Invariantensysteme, Math. Ann. 42 (1893), § 1. The lemma stated there only for homogeneous polynomials holds equally for inhomogeneous ones.

[103] For example, in the domain $\mathfrak{G}_{32}$ mentioned in the closing remark to § 9, the admissible specialization $x_1 = 1$ gives the two polynomials $F^* = x_2$, $G^* = 1 + x_3$, over which every polynomial in x_2, x_3 is algebraically integral. Thus $\mathfrak{G}_{32}$ is of the first kind, with $F(x)$ and $G(x)$ as an integrality basis.

Lemma: A sufficient condition for every polynomial in $x_1, \ldots, x_\rho$ to be algebraically integral over ρ polynomials in $x_1, \ldots, x_\rho$

$$G_1^*(x), \ldots, G_\rho^*(x)$$

is the nonvanishing of the resultant, taken with respect to $x_1, \ldots, x_\rho$, of the highest-degree homogeneous parts

$$H_1^*(x), \ldots, H_\rho^*(x)$$

of the polynomials (1):

$$R_0 = \begin{bmatrix} H_1^* & \cdots & H_\rho^* \\ x_1 & \cdots & x_\rho \end{bmatrix} \neq 0. \tag{2}$$

For homogeneous forms (1), condition (2) is necessary.[104]

For the proof, form the polynomials

$$\begin{gathered} \bar{G}_1^*(x) = G_1^*(x) - \lambda_1, \ldots, \bar{G}_\rho^*(x) = G_\rho^*(x) - \lambda_\rho, \\ \bar{\Phi}^*(x) = \Phi^*(x) - \mu, \end{gathered} \tag{3}$$

where $\lambda_1, \ldots, \lambda_\rho, \mu$ are indeterminates and $\Phi^*(x)$ is an arbitrary polynomial in $x_1, \ldots, x_\rho$. Let the resultant of the polynomials (3) with respect to $x_1, \ldots, x_\rho, 1$[105] be

$$R(\lambda, \mu) = \begin{bmatrix} \bar{G}_1^* & \cdots & \bar{G}_\rho^* & \bar{\Phi}^* \\ x_1 & \cdots & x_\rho & 1 \end{bmatrix}; \tag{4}$$

it is a polynomial in $\lambda_1, \ldots, \lambda_\rho, \mu$. According to F. Mertens, the leading coefficient in the expansion of (4) in powers of μ can be given explicitly;[106] one obtains

$$(-1)^\tau R(\lambda, \mu) = R_0^\sigma \mu^\tau + A_1(\lambda)\mu^{\tau-1} + \cdots + A_\tau(\lambda), \tag{5}$$

where $A_1(\lambda), \ldots, A_\tau(\lambda)$ are polynomials with integer coefficients in $\lambda_1, \ldots, \lambda_\rho$ and in the coefficients of the polynomials (3). This expansion first shows that, under assumption (2), $R_0 \neq 0$, the polynomial $R(\lambda, \mu)$ cannot vanish identically either. The identity in $x_1, \ldots, x_\rho, \lambda_1, \ldots, \lambda_\rho, \mu$,

$$R(\lambda, \mu) \equiv 0 \pmod{\bar{G}_1^*(x), \ldots, \bar{G}_\rho^*(x), \bar{\Phi}^*(x)},$$

becomes, under the substitution

$$\lambda_i = G_i^*(x), \qquad \mu = \Phi^*(x),$$

into

$$\begin{gathered} R(G_i^*(x), \Phi^*(x)) = R_0^\sigma \Phi^{*\tau}(x) + A_1(G_i^*(x))\Phi^{*\tau-1}(x) + \cdots \\ + A_\tau(G_i(x)) = 0, \end{gathered} \tag{6}$$

and this proves the lemma, since R_0 is, by assumption, an element of Ω.

§ 12. The integrality basis of regular systems $\mathfrak{S}_{n\rho}$ consisting of polynomials.

The lemma of § 11, together with the conclusion of § 10, immediately yields the following fact:

If an image domain $\mathfrak{J}_{\rho\rho}^*$ of $\mathfrak{S}_{n\rho}$ contains ρ polynomials such that the homogeneous resultant of their highest-degree homogeneous parts does not vanish identically — $R_0 \neq 0$ — then $\mathfrak{S}_{n\rho}$ is of the first kind and consequently is a finite integrality domain, with the involution basis as its integrality basis.

By means of the lemma, the condition $R_0 \neq 0$ now permits a second proof of the existence of an integrality basis, essentially due to D. Hilbert;[107] although this proof does not identify the involution basis as such, it applies uniformly to every system $\mathfrak{S}_{n\rho}$ having the stated property.

[104] For the theory of resultants, compare F. Mertens, Zur Theorie der Elimination (Parts I and II), Sitzungsber. d. k. Ak. d. Wiss. Wien, Math.-naturw. Kl. Abt. IIa, Bd. 108 (1899). Partly reproduced in J. König, Theorie d. algebr. GröSSen, Kap. VI.

[105] That is, the homogeneous resultant with respect to $x_1, \ldots, x_\rho, x_0$, after homogenizing the polynomials (3) by means of an additional indeterminate x_0 so that their degree in the x is preserved.

[106] Loc. cit., § 3 (proof of Theorem I), and explicitly § 6 (determination of the totality of all terms of the resultant R that contain a given power product $a_{\lambda\lambda}^{p_\lambda} a_{\mu\mu}^{p_\mu} \cdots a_{\sigma\sigma}^{p_\sigma}$ as a factor). In our case one sets $p_\lambda = 0$, $p_\mu = 0, \ldots, p_\sigma = \tau$, and $a_{\sigma\sigma} = (-\mu)$. Reproduced in König, Kap. VI, § 9.

[107] Über die vollen Invariantensysteme, § 2. Hilbert, assuming the existence of the integrality basis of the invariant field as established by other means, is concerned only with interpreting this basis through Kronecker's fundamental system of the algebraically integral quantities of a field.

Indeed, let the ρ polynomials of $\mathfrak{J}^*_{\rho\rho}$ for which $R_0 \neq 0$, and which are consequently algebraically independent, be

$$G_1^*(x), \ldots, G_\rho^*(x). \tag{1}$$

By the lemma, every polynomial in $x_1, \ldots, x_\rho$, and hence in particular every polynomial of the smallest field $\mathfrak{K}^*_{\rho\rho}$ containing $\mathfrak{J}^*_{\rho\rho}$, is algebraically integral over the polynomials (1). Let the corresponding polynomials in $\mathfrak{S}_{n\rho}$ be

$$G_1(x), \ldots, G_\rho(x), \tag{2}$$

Then, by the transfer principle, every polynomial of the smallest field $\mathfrak{K}_{n\rho}$ containing $\mathfrak{S}_{n\rho}$, and hence in particular every polynomial of $\mathfrak{S}_{n\rho}$, is algebraically integral over the polynomials (2). Conversely, every function of $\mathfrak{K}_{n\rho}$ that is algebraically integral over the polynomials (2) is a polynomial. Thus, regarding $\mathfrak{K}_{n\rho}$ by § 4 as an algebraic extension of $\Omega(G_1, \ldots, G_\rho)$, the totality of the polynomials in $\mathfrak{K}_{n\rho}$ — the relatively integral domain $\mathfrak{G}_{n\rho}$ — is identical with the algebraically integral elements of this field. Let $G(x)$ be a polynomial of $\mathfrak{K}_{n\rho}$ that completes (2) to a rational basis, and let $D(x)$ be the discriminant of the irreducible equation of degree k satisfied by $G(x)$ over $\Omega(G_1, \ldots, G_\rho)$. Then every polynomial in $\mathfrak{K}_{n\rho}$, and in particular every polynomial $F(x)$ of $\mathfrak{S}_{n\rho}$, admits, as an algebraically integral element, the representation

$$F(x) = \frac{\Gamma_1(G_i)G(x)^{k-1} + \Gamma_2(G_i)G(x)^{k-2} + \cdots + \Gamma_k(G_i)}{D(x)}. \tag{3}$$

Now let $F(x)$ range over all polynomials of $\mathfrak{S}_{n\rho}$. Applying Hilbert's Theorem I on the module basis (Math. Ann. 36) to the system formed from the corresponding functions

$$v_1\Gamma_1(G_i) + v_2\Gamma_2(G_i) + \cdots + v_k\Gamma_k(G_i)$$

shows that there are finitely many polynomials of $\mathfrak{S}_{n\rho}$,

$$F_1(x), F_2(x), \ldots, F_\lambda(x), \tag{4}$$

such that every polynomial of $\mathfrak{S}_{n\rho}$ admits a representation

$$F(x) = A_1(G_i)F_1(x) + A_2(G_i)F_2(x) + \cdots + A_\lambda(G_i)F_\lambda(x), \tag{5}$$

where $A_1, \ldots, A_\lambda$ are polynomials in the $G_i(x)$. Thus the polynomials (2) and (4) form an integrality basis of $\mathfrak{S}_{n\rho}$; that is:

Theorem VIII: If an image domain $\mathfrak{J}^*_{\rho\rho}$ of a system of polynomials $\mathfrak{S}_{n\rho}$ contains ρ polynomials such that the resultant of their highest-degree homogeneous parts does not vanish identically — $R_0 \neq 0$ — then $\mathfrak{S}_{n\rho}$ possesses an integrality basis.

This theorem admits a slight generalization. It is enough that the ρ polynomials (1) for which $R_0 \neq 0$ belong to the smallest integrality domain $\mathfrak{J}^*_{\rho\rho}$ containing $\mathfrak{S}^*_{\rho\rho}$. Indeed, the arguments leading to Theorem VIII show that representation (5) still holds. By definition, however, every polynomial $L(x)$ of the smallest integrality domain $\mathfrak{J}_{n\rho}$ containing $\mathfrak{S}_{n\rho}$ can be expressed as a polynomial in finitely many polynomials of $\mathfrak{S}_{n\rho}$ — which may vary with $L(x)$; hence there are σ polynomials of $\mathfrak{S}_{n\rho}$,

$$K_1(x), K_2(x), \ldots, K_\sigma(x), \tag{6}$$

such that the polynomials $G_i(x)$ are polynomial expressions in (6). Thus (6) and (4) give an integrality basis. We now introduce

Definition VIII: A system $\mathfrak{S}_{n\rho}$ of polynomials is called regular if an image domain $\mathfrak{J}^*_{\rho\rho}$ of the smallest integrality domain containing it contains ρ polynomials such that the resultant of their highest-degree homogeneous parts does not vanish identically — $R_0 \neq 0$.

we therefore have:

Theorem IX: Every regular system $\mathfrak{S}_{n\rho}$ of polynomials possesses an integrality basis.[108]

[108] Hilbert showed by an example that there are nonregular systems without an integrality basis (Gött. Nachr. 1891, p. 233). The following example is even simpler:

$$\mathfrak{S}_{22} = x_1, x_1x_2, x_1x_2^2, \ldots, x_1x_2^\nu, \ldots \quad \text{in inf.}$$

The existence of the integrality basis here would be equivalent to the existence of a positive integer ν such that the identities

$$x_1x_2^{\nu+\sigma} = \sum c \cdot x_1^{i_0}(x_1x_2)^{i_1}(x_1x_2^2)^{i_2}\cdots(x_1x_2^\nu)^{i_\nu} \quad (\sigma = 1, 2, \ldots)$$

We also give a geometric interpretation of regular systems, analogous to that given for the involution in § 5. For this purpose, consider, as in equation (7) there, the system of equations

$$L^*(x) - L^*(\xi) = 0, \tag{7}$$

where $L^*(x)$ ranges over all polynomials of $\mathfrak{J}^*_{\rho\rho}$. On homogenizing by means of x_0, ξ_0, let (7) become the following system of equations among homogeneous forms:

$$\xi_0^m M^*(x) - x_0^m M^*(\xi) = 0, \tag{8}$$

where, if $H^*(x)$ denotes the highest-degree homogeneous part of $L^*(x)$, the relation

$$H^*(x) \equiv M^*(x) \pmod{x_0} \tag{9}$$

holds.

We call the solutions of (8) that are independent of x — and hence distinct from the rows conjugate to x — the *fundamental points* of $\mathfrak{J}^*_{\rho\rho}$ (compare the note to § 5). Fundamental points are therefore the systems of values other than $\xi_1 = 0, \ldots, \xi_\rho = 0$ for which simultaneously

$$\xi_0^m = 0, \qquad M^*(\xi) = 0$$

hold simultaneously, or, by (9),

$$\xi_0 = 0, \qquad H^*(\xi) = 0.$$

If there are ρ forms $H^*(\xi)$ for which $R_0 \neq 0$, and which therefore have no common system of solutions, then $\mathfrak{J}^*_{\rho\rho}$ can have no fundamental point. If, in particular, $\mathfrak{S}^*_{\rho\rho}$ consists of homogeneous forms, then for $R_0 \neq 0$ the system $\mathfrak{S}^*_{\rho\rho}$ itself can have no fundamental point, since such a point would also be a fundamental point of $\mathfrak{J}^*_{\rho\rho}$. The converse holds as well. To see this, consider the system $\mathfrak{J}(H^*)$ formed by all the forms $H^*(x)$; this system is again an integrality domain.

Hilbert's Theorem I on the module basis and Hilbert's lemma (compare the citation in § 10) imply the existence of ρ forms of $\mathfrak{J}(H^*)$ whose vanishing forces every form of $\mathfrak{J}(H^*)$ to vanish. If $\mathfrak{J}^*_{\rho\rho}$ has no fundamental point, these ρ forms cannot vanish simultaneously, and their resultant satisfies $R_0 \neq 0$.

Thus:

Regular systems $\mathfrak{S}_{n\rho}$ of polynomials are characterized by the fact that an image domain $\mathfrak{J}^*_{\rho\rho}$ of the smallest integrality domain containing the system has no fundamental point. For regular systems $\mathfrak{S}^*_{\rho\rho}$ of homogeneous forms, the system itself has no fundamental point.[109]

§ 13. Examples of relatively integral domains of the first kind and of regular systems.

1. As a first example of a relatively integral domain of the first kind $\mathfrak{G}_{nn}$, consider the *totality of the polynomials in $x_1, \ldots, x_n$ that admit a given permutation group G* — thus the totality of the polynomials of a Lagrange genus domain. Since $x_1, \ldots, x_n$, by virtue of the identity

$$x_k^n - \sigma_1(x)x_k^{n-1} + \sigma_2(x)x_k^{n-2} + \cdots \pm \sigma_n(x) = 0 \qquad (k = 1, 2, \ldots, n), \tag{1}$$

are algebraically integral over the elementary symmetric functions belonging to $\mathfrak{G}_{nn}$, and hence, by Definition V, are algebraically integral over $\mathfrak{G}_{nn}$, the domain $\mathfrak{G}_{nn}$ is of the first kind. Moreover, because its elements are homogeneous forms and $n = \rho$, the domain $\mathfrak{G}_{nn}$, being of the first kind, forms a regular system (by the conclusion of § 10). Indeed, by (1), the resultant R_0 of the elementary symmetric functions cannot

hold. Comparing the degrees in x_1, x_2 already for $\sigma = 1$ gives the two equations for the exponents

$$1 = i_0 + i_1 + \cdots + i_\nu, \qquad \nu + 1 = i_1 + 2i_2 + \cdots + \nu i_\nu,$$

which plainly have no solution in non-negative integers. Thus $\mathfrak{S}_{22}$ possesses no integrality basis.

[109] The nonregular system $\mathfrak{S}_{22}$ given in the preceding note has the fundamental point

$$\xi_1 : \xi_2 : \xi_0 = 0 : 1 : 0.$$

vanish identically; the rules of resultant theory give $R_0 = \pm 1$. Since $\mathfrak{G}_{nn}$ is of the first kind and $n = \rho$, its *involution form* is uniquely determined as the involution form of the corresponding Lagrange genus domain. The quantities conjugate to $x_1, \ldots, x_n$ over this domain arise by applying the permutations of the group G; hence this involution form is

$$\begin{aligned} \Psi(z,u) &= \prod_i (z - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n}) \\ &= z^i + \sum{}' G_{\alpha\alpha_1\ldots\alpha_n}(x) z^\alpha u_1^{\alpha_1} \cdots u_n^{\alpha_n}, \end{aligned} \tag{2}$$

where the product extends over all permutations in G. Formula (2) is the "Galois form of the group G," and hence:

All polynomials in $x_1, \ldots, x_n$ that admit a permutation group G are polynomial expressions in the coefficients $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ of the Galois form of the group.

2. As examples of *regular systems*, consider systems $\mathfrak{S}_{n1}$ of polynomials, that is, systems containing only one algebraically independent polynomial.

Indeed, let $\mathfrak{S}_{11}^*$ be an image system of $\mathfrak{S}_{n1}$ and let

$$F^*(x) = a_0 x^k + a_1 x^{k-1} + \cdots + a_k \qquad (a_0 \neq 0)$$

be a polynomial of $\mathfrak{S}_{11}^*$. Then

$$R_0 = a_0 \neq 0. \tag{3}$$

[110] Thus $\mathfrak{S}_{n1}$ is regular by Definition VIII, and consequently:

Every system $\mathfrak{S}_{n1}$ of polynomials, in particular every system of infinitely many polynomials in one indeterminate, possesses an integrality basis.[111]

3. We now specialize the systems $\mathfrak{S}_{n1}$ to relatively integral domains $\mathfrak{G}_{n1}$, which, as regular systems, are relatively integral domains of the first kind by § 12. Their integrality basis is therefore an involution basis, which is also the involution basis of the smallest containing field $\mathfrak{K}_{n1}$. By § 6, however, any function of the involution basis of $\mathfrak{K}_{n1}$ is itself a minimal basis — we called it the Lüroth function of the field — and every function of the involution basis depends on this Lüroth function by a linear fractional transformation. In the present case the Lüroth function belongs to $\mathfrak{G}_{n1}$ and is therefore a polynomial. Every other polynomial of the involution basis thus depends linearly fractionally and, by (3), algebraically integrally on this Lüroth function $L(x)$; it is consequently affine-linear in $L(x)$, which therefore forms an integrality basis. On setting $u_1 = 1$, the involution form of $\mathfrak{G}_{11}^*$ becomes

$$\Psi^*(z) = L^*(z) - L^*(x),$$

which again exhibits $L(x)$ as an integrality basis. Thus:

The relatively integral domains $\mathfrak{G}_{n1}$ are of the first kind; their integrality basis consists of a single polynomial, the Lüroth function of the smallest containing field.

4. As a particular example of a relatively integral domain $\mathfrak{G}_{n1}$, consider the polynomial projective invariants of a quadratic form in s variables. In agreement with the preceding result, they are known to be polynomial expressions in the determinant $|a_{ik}|$ of the form; this determinant is also the Lüroth function of the corresponding invariant field.

§ 14. Systems of integer polynomials.

We now sharpen the basis theorems obtained above with respect to integer coefficients.

The coefficient field Ω will therefore be assumed below to be a finite algebraic number field; let $[\Omega]$ denote the totality of algebraic integers in Ω, which we shall call integers for short. An integer polynomial means a polynomial with coefficients in $[\Omega]$; from now on, $F(x), G(x), \ldots$ will denote only integer polynomials.

In analogy with § 7, we consider the various systems of integer polynomials:

An arbitrary system of integer polynomials will be called an integer system $\mathfrak{S}_{n\rho}$.

An integer linear family $\mathfrak{L}_{n\rho}$ is an integer system that, together with $F_1(x)$ and $F_2(x)$, always contains $c_1 F_1(x) + c_2 F_2(x)$, where c_1, c_2 are arbitrary integers in $[\Omega]$.

[110] Mertens, loc. cit., § 5.

[111] The simplest possible nonregular systems without an integrality basis are therefore systems $\mathfrak{S}_{22}$. Their existence is shown by Hilbert's example and by the example in the note to § 12.

An integer integrality domain $\mathfrak{J}_{n\rho}$ is an integer linear family that, together with $F(x)$ and $G(x)$, always contains $F(x) \cdot G(x)$.

An integer relatively integral domain $\mathfrak{G}_{n\rho}$ is an integrality domain that, together with $F(x)$ and $G(x)$ — where $G(x) \neq 0$ — contains the quotient $F(x) : G(x)$ if and only if that quotient is an integer polynomial.

As in § 7, the smallest integer integrality domain $\mathfrak{J}_{n\rho}$ containing an integer system $\mathfrak{S}_{n\rho}$ consists of all polynomials $H(x)$ that are polynomial expressions, with coefficients in $[\Omega]$, in finitely many polynomials of $\mathfrak{S}_{n\rho}$;

the smallest integer relatively integral domain $\mathfrak{G}_{n\rho}$ containing it consists of all integer polynomials $H(x)$ that are rational expressions in finitely many polynomials of $\mathfrak{S}_{n\rho}$.

We now turn to the transfer of the basis theorems. For the rational basis, observe that the notions of a field, the smallest containing field, and a rational basis, which rest only on "rationality," remain unchanged. Moreover, an image system $\mathfrak{S}^*_{\rho\rho}$ of an integer system $\mathfrak{S}_{n\rho}$ can again be chosen as an integer system in arbitrarily many ways. Since the arguments leading to the bound on the number of generators also remain valid for integer linear families, we obtain:

Theorem V′: Every integer system $\mathfrak{S}_{n\rho}$ possesses a rational basis; a rational basis of an integer linear family $\mathfrak{L}_{n\rho}$ may in particular be chosen to contain at most $\rho + 1$ polynomials.

We now investigate the analogue of the involution basis for integrality domains of polynomials (§ 8). For this purpose, the theorem on *symmetric functions of rows of quantities* must be extended to *integer coefficients* by the following

Lemma. The symmetric integer polynomials in n rows of quantities $(yz \cdots t)$:

$$\begin{array}{cccc} y_1 & z_1 & \cdots & t_1 \\ y_2 & z_2 & \cdots & t_2 \\ \vdots & \vdots & & \vdots \\ y_n & z_n & \cdots & t_n \end{array} \tag{1}$$

are integer-polynomial expressions in finitely many of them, namely the elementary symmetric functions

$$\begin{array}{c} \sigma_1(y), \sigma_2(y), \ldots, \sigma_n(y); \quad \sigma_1(z), \sigma_2(z), \ldots, \sigma_n(z); \quad \ldots; \\ \sigma_1(t), \ldots, \sigma_n(t); \end{array} \tag{2}$$

and the functions

$$\chi_1(y, z, \ldots, t), \ldots, \chi_k(y, z, \ldots, t), \tag{3}$$

that are integral over the ring generated by the functions (2) over $[\Omega]$.

Indeed, the n quantities $y_1, \ldots, y_n$ are integral over $[\Omega][\sigma_1(y), \ldots, \sigma_n(y)]$; the corresponding statement holds for $z_1, \ldots, z_n$ with respect to $\sigma_1(z), \ldots, \sigma_n(z)$, and so forth. The field of symmetric functions of the rows (1) is therefore algebraic over the field generated by the functions (2), and the elements of this field integral over the ring generated by (2) over $[\Omega]$ are precisely the symmetric integer polynomials in the rows (1). Choosing (3) as Kronecker's fundamental system proves the lemma.

Now let $\mathfrak{J}_{n\rho}$ be an integer integrality domain, let $\mathfrak{J}^*_{\rho\rho}$ be an integer image domain, and let

$$\Psi^*(z, u) = G^*(x) z^i + \sum{}' G^*_{\alpha\alpha_1 \ldots \alpha_\rho}(x) z^\alpha u_1^{\alpha_1} \cdots u_\rho^{\alpha_\rho}$$

be an involution form of $\mathfrak{J}^*_{\rho\rho}$; here $G^*(x)$ may also have degree zero, that is, it may be an element of $[\Omega]$. The elementary symmetric functions corresponding to the functions (2) are then certain quotients among

$$G^*_{\alpha\alpha_1 \ldots \alpha_\rho}(x) : G^*(x). \tag{4}$$

Since, by the lemma, the functions (3) are integral over the ring generated by (2) over $[\Omega]$, the corresponding functions of $\mathfrak{K}^*_{\rho\rho}$ are, by the extension of Gauss's theorem to polynomials with algebraic-integer coefficients, of the form

$$K^*_i(x) : (G^*(x))^\sigma, \tag{5}$$

where $K^*_i(x)$ are integer polynomials of $\mathfrak{J}^*_{\rho\rho}$. Thus the functions (5) belong to the domain when it is relatively integral; in general they are quotients of polynomials of $\mathfrak{J}^*_{\rho\rho}$.

If $F^*(x)$ is any integer polynomial of $\mathfrak{J}^*_{\rho\rho}$, then

$$F^*(x) = \frac{1}{i}\Big(F^*(x) + F^*(x^{(1)}) + \cdots + F^*(x^{(i-1)})\Big),$$

and therefore $i \cdot F^*(x)$ is a symmetric integer polynomial in the rows $x, x^{(1)}, \ldots, x^{(i-1)}$.

The lemma and the transfer principle therefore give:

Theorem VI′: For integer integrality domains $\mathfrak{J}_{n\rho}$, every involution form determines a distinguished rational basis such that every polynomial $F(x)$ of $\mathfrak{J}_{n\rho}$ admits a representation

$$F(x) = \frac{\Gamma(H(x), H_1(x), \ldots, H_\sigma(x))}{i \cdot H(x)^k},$$

where Γ is an integer polynomial. For integer relatively integral domains $\mathfrak{G}_{n\rho}$ having an integer relatively integral image domain $\mathfrak{G}^*_{\rho\rho}$, the denominator $H(x)$ is the leading coefficient of the corresponding involution form.

§ 15. Integer relatively integral domains of the first kind and regular systems.

For integer systems, the integrality basis is replaced by an integer integrality basis: a finite set of integer polynomials of the system such that every integer polynomial of the system can be expressed as an integer polynomial in this finite set.

The theorems on the integer integrality basis run essentially parallel to the earlier ones, and only the proofs require slight modifications.

First, Definition V (§ 9) carries over directly.

Definition V′: A quantity ξ is called algebraically integral with integer coefficients over the integer relatively integral domain $\mathfrak{G}_{n\rho}$ if it satisfies an equation whose leading coefficient is a unit of $[\Omega]$ and whose remaining coefficients are polynomials of $\mathfrak{G}_{n\rho}$.

As in § 9, the extension of Gauss's theorem to polynomials with algebraic-integer coefficients shows that this notion can equivalently be defined by the irreducible equation.

Definition V′ in turn gives the analogue of Definition VII.

Definition VII′: An integer relatively integral domain $\mathfrak{G}_{n\rho}$ is called of the first kind if it has a relatively integral image domain $\mathfrak{G}^*_{\rho\rho}$ such that every integer polynomial in $x_1, \ldots, x_\rho$ is algebraically integral with integer coefficients over $\mathfrak{G}^*_{\rho\rho}$.

To prove the finiteness of these domains of the first kind, first observe that, as in § 10, the definition implies that the leading coefficient of the involution form is a unit of $[\Omega]$.

By Theorem VI′ (§ 14), every polynomial $F(x)$ of $\mathfrak{G}_{n\rho}$ therefore admits a representation

$$F(x) = \frac{\Gamma(H_1(x), \ldots, H_\sigma(x))}{i}.$$

Applying to the system formed by the integer polynomials $\Gamma(H_1, \ldots, H_\sigma)$ Hilbert's Theorem II on the integer module basis (Math. Ann. 36), stated for ordinary integer coefficients, in its extension to polynomials with algebraic-integer coefficients,[112] proves the existence of an integer integrality basis; that is:

Theorem VII′: Every integer relatively integral domain of the first kind possesses an integer integrality basis.

We next carry over the definition of regular systems:

Definition VIII′: An integer system $\mathfrak{S}_{n\rho}$ is called integer-regular if an image domain $\mathfrak{J}^*_{\rho\rho}$ of the smallest integer integrality domain containing it contains ρ polynomials such that the resultant of their highest-degree homogeneous parts is a unit of $[\Omega]$ — $R_0 = \varepsilon$.

To carry over the proof of existence of an integrality basis, observe that the lemma of § 11 admits the following sharper form, which follows from equations (5) and (6) there and from the fact that $A_1(\lambda), \ldots, A_\tau(\lambda)$ are integer polynomials in $\lambda_1, \ldots, \lambda_\rho$:

A sufficient condition for every integer polynomial in $x_1, \ldots, x_\rho$ to be algebraically integral with integer coefficients over ρ integer polynomials is that the resultant of the highest-degree homogeneous parts of these polynomials be a unit of $[\Omega]$ — $R_0 = \varepsilon$.

[112] If $w_1, \ldots, w_k$ is a fundamental system of the algebraic integers in Ω, and one sets

$$\Gamma(H_1, \ldots, H_\sigma) = \Gamma_1(H)w_1 + \cdots + \Gamma_k(H)w_k,$$

then $\Gamma_1(H), \ldots, \Gamma_k(H)$ have ordinary integer coefficients. Applying Theorem II to the system formed by the forms $v_1\Gamma_1(H) + \cdots + v_k\Gamma_k(H)$ immediately proves the validity of the extension.

From this lemma, exactly as in § 12, representation (3) there follows for every polynomial $F(x)$ of an integer-regular system, where now $\Gamma_1(G_i), \ldots, \Gamma_k(G_i)$ are integer polynomials in the G_i. Furthermore, as in § 12, Hilbert's Theorem II (Math. Ann. 36), extended to polynomials with algebraic-integer coefficients, together with the definition of the smallest containing integer integrality domain, gives the existence of an integer integrality basis; that is:

Theorem IX′: Every integer-regular system possesses an integer integrality basis.

As an example of an integer relatively integral domain of the first kind, analogous to Example 1 in § 13, consider the totality $\mathfrak{G}_{nn}$ of the integer polynomials in a Lagrange genus domain. That $\mathfrak{G}_{nn}$ is of the first kind in the integer sense follows from the identity

$$x_k^n - \sigma_1(x)x_k^{n-1} + \cdots \pm \sigma_n(x) = 0 \qquad (k = 1, 2, \ldots, n);$$

since the resultant of the elementary symmetric functions has the value ± 1, $\mathfrak{G}_{nn}$ is also an integer-regular system.

By the lemma of § 14, a further example is the totality of the symmetric integer polynomials in n rows of quantities.

Erlangen, May 1914.

7. The finiteness theorem for the invariants of finite groups

Math. Ann. 77 (1916), pp. 89–92

In what follows, we give an entirely elementary finiteness proof for the invariants of finite groups — based only on the theory of symmetric functions — that also explicitly specifies a complete system; the usual proof, based on Hilbert's theorem on module bases (Ann. 36), proves only existence.[113]

Let the finite group $\mathfrak{H}$ consist of the h linear transformations (of nonzero determinant) $A_1, \ldots, A_h$, where A_k denotes the transformation

$$x_1^{(k)} = \sum_{\nu=1}^{n} a_{1\nu}^{(k)} x_\nu, \ldots, x_n^{(k)} = \sum_{\nu=1}^{n} a_{n\nu}^{(k)} x_\nu,$$

or, briefly, $(x^{(k)}) = A_k(x)$. Thus $\mathfrak{H}$ carries the row (x) with entries $x_1, \ldots, x_n$ into the rows $(x^{(k)})$ with entries $x_1^{(k)}, \ldots, x_n^{(k)}$. Since $A_1, \ldots, A_h$ must include the identity, the rows $(x^{(k)})$ also include (x). A polynomial (absolute) invariant of the group means a polynomial in $x_1, \ldots, x_n$ that remains identically unchanged under $A_1, \ldots, A_h$; hence every such invariant $f(x)$ satisfies

$$f(x) = f(x^{(1)}) = \cdots = f(x^{(h)}) = \frac{1}{h} \sum_{k=1}^{h} f(x^{(k)}). \tag{1}$$

1.

Formula (1) says that $f(x)$ is a symmetric polynomial in the rows $(x^{(1)}), \ldots, (x^{(h)})$. Since each summand $f(x^{(k)})$ contains only the single row $(x^{(k)})$, this is the simplest case, usually called the *one-row* case. By the familiar theorem on symmetric functions of rows of quantities,[114] $f(x)$ can therefore be expressed polynomially in the elementary symmetric functions of these rows, that is, in the coefficients $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ of the "Galois resolvent"

$$\begin{aligned} \Phi(z,u) &= \prod_{k=1}^{h} (z + u_1 x_1^{(k)} + \cdots + u_n x_n^{(k)}) \\ &= z^h + \sum G_{\alpha\alpha_1\ldots\alpha_n}(x) z^\alpha u_1^{\alpha_1} \cdots u_n^{\alpha_n}, \end{aligned} \qquad \left(\begin{array}{c} \alpha + \alpha_1 + \cdots + \alpha_n = h \\ \alpha \neq h \end{array} \right),$$

where the $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ are invariants of degree $\alpha_1 + \cdots + \alpha_n$ in the x's. We have thus proved:

The coefficients $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ of the Galois resolvent form a complete system of invariants of the group: every invariant is a polynomial expression in these finitely many invariants.

2.

Starting from (1), one may give the following still more elementary argument,[115] which also leads to a second complete system. Put

$$f(x) = a + b x_1^{\mu_1} \cdots x_n^{\mu_n} + \cdots + c x_1^{\nu_1} \cdots x_n^{\nu_n},$$

where $a, b, \ldots, c$ denote constants. Then by (1) one has

$$\begin{aligned} h \cdot f(x) &= h \cdot a + b \sum_{k=1}^{h} (x_1^{(k)})^{\mu_1} \cdots (x_n^{(k)})^{\mu_n} + \cdots + c \sum_{k=1}^{h} (x_1^{(k)})^{\nu_1} \cdots (x_n^{(k)})^{\nu_n} \\ &= h \cdot a + b \cdot J_{\mu_1\ldots\mu_n} + \cdots + c \cdot J_{\nu_1\ldots\nu_n}. \end{aligned}$$

Every invariant is therefore a linear combination of the special invariants

$$J_{\mu_1\ldots\mu_n} = \sum_{k=1}^{h} (x_1^{(k)})^{\mu_1} \cdots (x_n^{(k)})^{\mu_n},$$

[113] See, for example, Weber, *Lehrbuch der Algebra* (2nd ed.), vol. 2, § 57.

[114] See the note to 2.

[115] This amounts to a proof of the theorem on symmetric functions of rows of quantities in the one-row case just mentioned.

and it therefore suffices to prove the assertion for these special invariants. Apart from a numerical factor, however, $J_{\mu_1 \dots \mu_n}$ is the coefficient of $u_1^{\mu_1} \cdots u_n^{\mu_n}$ in the expression

$$S_\mu = \sum_{k=1}^{h} (u_1 x_1^{(k)} + \cdots + u_n x_n^{(k)})^\mu,$$

where $\mu = \mu_1 + \cdots + \mu_n$; this is the μth power sum of the h linear forms

$$\xi_1 = u_1 x_1^{(1)} + \cdots + u_n x_n^{(1)}, \dots, \xi_h = u_1 x_1^{(h)} + \cdots + u_n x_n^{(h)}.$$

It is well known that the infinitely many power sums S_μ are polynomial expressions in

$$S_1, S_2, \dots, S_h,$$

whose coefficients are the invariants

$$J_{\mu_1 \dots \mu_n} \qquad (\mu_1 + \cdots + \mu_n \leq h).$$

Thus we obtain a second complete system:

A complete system of invariants of the group is given by all invariants $J_{\mu_1 \dots \mu_n}$ for which $\mu_1 + \cdots + \mu_n \leq h$, where h is the order of the group.

The connection with 1 is obtained by observing that the power sums $S_1, \dots, S_h$ can be replaced by the elementary symmetric functions of $\xi_1, \dots, \xi_h$, which leads to the complete system of the $G_{\alpha\alpha_1 \dots \alpha_n}(x)$ given there. Both results show that every invariant is a polynomial expression in invariants whose degree in the x's does not exceed the order h of the group.

3.

The result just proved has consequences for rational representation. Every rational absolute invariant can be represented — as follows immediately by multiplying its numerator and denominator by the conjugates of the denominator under the group — as the quotient of two polynomial absolute invariants, which need not be relatively prime. Hence every rational absolute invariant can be expressed rationally in the coefficients $G_{\alpha\alpha_1 \dots \alpha_n}(x)$ of the Galois resolvent $\Phi(z, u)$. This theorem can also be proved easily in several ways without using the finiteness theorem; it is already stated in Weber II, § 58.[116]

4.

Finally, the results derived here are implicitly contained in my paper "Fields and Systems of Rational Functions":[117] the complete system given in 1 appears in Theorems VI and VII, while Theorem III gives a proof of rational representation independent of the present finiteness theorem.[118] In the present special case, however, both the argument and the result simplify considerably compared with the general theory. Conversations with E. Fischer led me to apply the general investigations to the invariants of finite groups; the substance of the proof in 2 — in the general case, the complete system occurring there cannot be defined rationally — and the note to 3 are also due to him.

Erlangen, May 1915.

---

[116] The proof given there, however, is not valid. It shows only that the function $\Psi(t)$ in formula (7) has invariants as coefficients, not that these invariants can be expressed rationally in the coefficients of $\Phi(t)$. This gap is avoided by using a familiar differentiation procedure, instead of Lagrange's interpolation formula, to express the $x_i^{(k)}$ in terms of ξ_k. Differentiating the identity $\Phi(-\xi_k, u) = 0$ with respect to all the u gives

$$\left[\frac{\partial \Phi}{\partial u_i} - x_i^{(k)} \frac{\partial \Phi}{\partial z} \right]_{z=-\xi_k} = 0.$$

Accordingly, for every rational function $\omega(x)$, the following formula must replace Weber's formulas (7) and (8):

$$\omega(x_1^{(k)}, \dots, x_n^{(k)}) = \omega\left(\frac{\partial \Phi/\partial u_1}{\partial \Phi/\partial z}, \dots, \frac{\partial \Phi/\partial u_n}{\partial \Phi/\partial z} \right)\Big|_{z=-\xi_k},$$

This contains only coefficients of $\Phi(z, u)$, and summing it over all k gives the desired representation when $\omega(x)$ is invariant.

[117] Math. Ann. 76, p. 161 (1915).

[118] For relative invariants, Theorems VIII and IX contain a finiteness proof that likewise rests on a different foundation from the usual proof, but again establishes only existence; this is because the relative invariants do not form a field.

8. On the polynomial representation of the invariants of a system of arbitrarily many ground forms

Math. Ann. 77 (1916), pp. 93–102

At the end of his contribution to the Schwarz Festschrift, "On the Invariants of a System of Arbitrarily Many Ground Forms," D. Hilbert conjectures that these invariants can be expressed polynomially in the finitely many invariants of the system (J, PJ), where J denotes a complete system of invariants of the linearly independent ground forms, and the invariants PJ arise from J by polar processes.

In I below, I show that this conjecture is indeed correct, as a simple consequence of the reduction theorem asserting that every form in arbitrarily many rows of n variables each can be represented as a sum of polars of forms that contain only n fixed rows and are themselves derived from the original form by polar processes. This reduction theorem, first formulated by F. Mertens, is a special case of the generalization by A. Capelli, F. Mertens, and J. Deruyts of the Clebsch–Gordan series expansion to forms in arbitrarily many rows of n variables each; that generalization was proved by formally transforming the differentiation processes.[119]

In II, I give a more conceptual proof of the reduction theorem by treating the question as a problem concerning the equivalence of linear families of forms. This viewpoint, and an essential part of the arguments used, are taken from a paper "On Algebraic Module Systems"[120] and from related unpublished theorems of E. Fischer, whose use he kindly permitted.

Finally, in III, I show how the corresponding considerations lead also to the most general series expansions.

I.

Let θ be a form homogeneous in each of the $N > n$ rows

$$A_1, A_2, \ldots, A_N,$$

where in general the row A_k consists of the n elements

$$A_k^{(1)}, A_k^{(2)}, \ldots, A_k^{(n)}.$$

The coefficients of θ may be indeterminates or elements of a given field of rationality. Let P further denote a polynomial — with rational-number coefficients — in the polar processes

$$P_{hk} = \left(A_h \frac{\partial}{\partial A_k}\right) = A_h^{(1)} \frac{\partial}{\partial A_k^{(1)}} + A_h^{(2)} \frac{\partial}{\partial A_k^{(2)}} + \cdots + A_h^{(n)} \frac{\partial}{\partial A_k^{(n)}},$$

where $P_{hk}P_{ij}\theta$ means that P_{hk} is applied to $P_{ij}\theta$.

The reduction theorem just mentioned is then expressed by the identity

$$\theta = \sum PZ, \tag{1}$$

where the forms Z contain only the rows

$$A_1, A_2, \ldots, A_n$$

and are derived from θ by polar processes P.

Now consider the system of ground forms (F'), consisting of the N forms of equal order and equal number of variables

$$F_1, F_2, \ldots, F_N,$$

whose coefficients are taken respectively as the N rows

$$A_1, A_2, \ldots, A_N.$$

Let (J) denote a complete system — consisting of finitely many invariants — for $F_1, \ldots, F_n$, such that every invariant of $F_1, \ldots, F_n$ is a polynomial expression in the invariants (J). Hilbert's conjecture then says that

[119] F. Mertens: "Über eine Formel der Determinantentheorie" (formula 5), Sitzb. d. Ak. d. Wiss. Wien, vol. 91, II. Abt. (1885), and, more fully and with applications, "Über ganze Funktionen von m Systemen von je n Unbestimmten," Monatsh. f. Math. u. Phys., vol. 4 (1893). For some of Capelli's proofs (beginning in 1882), see, for example, Math. Ann. 37 or the autographed "Lezioni sulla teoria delle forme algebriche" (1902). J. Deruyts: *Essai d'une théorie générale des formes algébriques*, Mém. d. la Soc. Roy. des Sciences de Liège (2) 17 (1892).

[120] E. Fischer: Über algebraische Modulsysteme und lineare homogene partielle Differentialgleichungen mit konstanten Koeffizienten, §§ 1–4, J. f. M. 140 (1911).

a complete system for the simultaneous invariants S of $F_1, \ldots, F_N$ is given by the finitely many invariants (J, PJ), where PJ denotes all invariants derivable from J by polar processes P.

Indeed, every simultaneous invariant S of (F') with rational-number coefficients is a form homogeneous in each of the N rows $A_1, \ldots, A_N$, so identity (1) applies to it. Since applying polar processes P to S is known to produce invariants again, the forms Z are likewise invariants; because they contain only the rows $A_1, \ldots, A_n$, they are simultaneous invariants of $F_1, \ldots, F_n$ and hence, by hypothesis, polynomial functions of the invariants (J). Thus identity (1) becomes

$$S = \sum PY,$$

where the Y are monomials in the invariants (J). By definition, carrying out the processes P on Y consists of successively applying the simple polar operations P_{hk} a finite number of times. The product rule for differentiation turns these into sums of products of invariants in (J) and (PJ). The same is true when P_{hk} is applied to a product of elements of (J) and (PJ); hence PY is likewise a polynomial expression in (J, PJ). *This proves the polynomial representability of all invariants S in terms of (J, PJ).*

II.

Before proving the reduction theorem, we recall some facts about linear families of forms. A *linear family of forms over K* means a system of forms of equal degree, complete in the sense that, together with θ_1 and θ_2, it always contains $c_1\theta_1 + c_2\theta_2$, where c_1, c_2 are elements of a prescribed field of rationality K, and K contains the coefficient field of the θ's. Among these forms there are always finitely many — say ρ — linearly independent over K, while every $\rho + 1$ forms satisfy a linear relation with coefficients in K; the family has *rank* ρ over K.[121] We shall use the immediate fact that if $\mathcal{L}$ and $\mathcal{T}$ are two linear families over K of the same rank ρ, and $\mathcal{T}$ is a subfamily of $\mathcal{L}$, then $\mathcal{L}$ and $\mathcal{T}$ are identical (equivalent).

With these preliminaries, we turn to the reduction theorem. The identity from I,

$$\theta = \sum PZ,$$

becomes an analogous identity for $P\theta$ when the same polar process P is applied to both sides. Thus the reduction theorem simultaneously represents every polar of θ as a sum of the special polars PZ. Conversely, these special polars certainly belong to the totality of all polars, so the reduction theorem asserts that the two linear families of forms are equivalent; in particular, the same holds for the subfamilies whose forms have the same degree as θ in each individual row. To prove this equivalence, we insert an intermediate family determined by the forms Z. For simplicity, we first give the proof for three binary rows $(N = 3, n = 2)$ and then briefly indicate the parallel general proof.

Thus let $\theta(x, y, z)$ have degrees α, β, p, respectively, in the rows

$$x_1x_2; \quad y_1y_2; \quad z_1z_2;$$

and initially let the coefficients of θ be indeterminates a (or rational numbers). We consider the following three linear families of forms.

1. The family $\mathcal{L}$, consisting of all forms $f(x, y, z)$ that arise from θ by polar processes P and have the same degree as θ in each of the rows x, y, z; in particular, $\mathcal{L}$ contains θ. Regarding $f(x, y, z)$ as a form in x, y, z and the indeterminates a, its coefficient field is the field R of rational numbers. One must also take $K = R$, since $c_1P_1 + c_2P_2$ is again a process P only when c_1, c_2 are rational numbers. Let $\mathcal{L}$ have rank ρ over R.

2. The family $\mathcal{S}$, consisting of all forms $g(\lambda; x, y)$ defined by

$$g(\lambda; x, y) = f(x, y, \lambda_1 x + \lambda_2 y),$$

or, in terms of polar processes,

$$\begin{aligned} g(\lambda; x, y) &= \frac{1}{p!}\left[(\lambda_1 x + \lambda_2 y)\frac{\partial}{\partial z}\right]^p f(x, y, z) \\ &= g_0(xy)\lambda_1^p + g_1(x, y)\lambda_1^{p-1}\lambda_2 + \cdots + g_p(xy)\lambda_2^p, \end{aligned}$$

[121] More general linear families of forms — whose rank need not be finite — are obtained by dropping either the restriction of equal degree or the requirement that K contain the coefficient field of the θ's.

where

$$i!(p-i)!\,g_i(xy) = \left(y\frac{\partial}{\partial z}\right)^i \left(x\frac{\partial}{\partial z}\right)^{p-i} f(xyz).$$

[122] Thus the $g_i(xy)$ provide the forms Z in identity (1). The g are forms with rational-number coefficients in x, y, λ and the indeterminates a; let $\mathcal{S}$ have rank σ over R.

3. The family $\mathcal{T}$, obtained from $\mathcal{S}$ by the inverse polar process, just as $\mathcal{S}$ is obtained from $\mathcal{L}$; the forms h of $\mathcal{T}$ are defined by

$$\begin{aligned} h(x,y,z) &= \frac{1}{p!}\left[z\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y}\right)\right]^p g(\lambda;xy) \\ &= h_0(xyz)+h_1(xyz)+\cdots+h_p(xyz), \end{aligned}$$

where, by 2,

$$h_i(xyz) = \left(z\frac{\partial}{\partial x}\right)^{p-i}\left(z\frac{\partial}{\partial y}\right)^i g_i(xy).$$

The individual h_i, and consequently also h, are thus forms PZ or sums of such forms; let $\mathcal{T}$ have rank τ over R.

The construction of the forms $h(x,y,z)$ of $\mathcal{T}$ shows that they arise from θ by polar processes P and have the same degree as θ in each of the rows x, y, z. Thus $\mathcal{T}$ is a subfamily of $\mathcal{L}$, and by the fact noted above it remains only to prove equality of their ranks. This proof makes no further use of the special structure of the $f(xyz)$ as polars of one and the same form θ.

a) To compare the ranks of $\mathcal{L}$ and $\mathcal{S}$, we use Lemma a): $f(x,y,\lambda_1 x+\lambda_2 y)=0$ necessarily implies $f(x,y,z)=0$. This follows immediately from the identity among three binary rows

$$(xy)z+(yz)x+(zx)y=0, \qquad (xy)=(x_1y_2-x_2y_1),\ldots,$$

which gives

$$f[x,y,(zy)x+(xz)y] = (xy)^p f(x,y,z).$$

Thus, substituting $\lambda_1=(zy)$ and $\lambda_2=(xz)$ into $f(x,y,\lambda_1x+\lambda_2y)=0$ (identically in λ), and using $(xy)\neq 0$, gives necessarily $f(x,y,z)=0$.

By this lemma, the forms of $\mathcal{S}$ and $\mathcal{L}$ correspond one-to-one. Indeed,

$$f_1(x,y,\lambda_1x+\lambda_2y)=g(\lambda;xy), \qquad f_2(x,y,\lambda_1x+\lambda_2y)=g(\lambda;xy)$$

necessarily implies

$$f_1(xyz)=f_2(xyz).$$

Moreover, every relation in $\mathcal{S}$ is preserved among the uniquely corresponding forms in $\mathcal{L}$, and conversely. For

$$c_1g^{(1)}(\lambda;xy)+c_2g^{(2)}(\lambda;xy)+\cdots+c_rg^{(r)}(\lambda;xy)=0$$

necessarily implies, by the lemma,

$$c_1f^{(1)}(x,y,z)+c_2f^{(2)}(x,y,z)+\cdots+c_rf^{(r)}(x,y,z)=0.$$

This proves that $\mathcal{L}$ and $\mathcal{S}$ have equal rank: $\rho=\sigma$.

b) To compare the ranks of $\mathcal{S}$ and $\mathcal{T}$, we use the corresponding Lemma b): $h(x,y,z)=0$ necessarily implies $g(\lambda;xy)=0$. By 3, the equation $h(x,y,z)=0$ is equivalent to the vanishing of the individual differential monomials

$$\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x_1}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y_1}\right)^{p_1}\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x_2}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y_2}\right)^{p_2} g(\lambda;x,y), \qquad p_1+p_2=p.$$

[122] As in I,

$$\left(t\frac{\partial}{\partial x}\right) = t_1\frac{\partial}{\partial x_1}+t_2\frac{\partial}{\partial x_2},$$

and hence in particular

$$\left[(\lambda_1x+\lambda_2y)\frac{\partial}{\partial z}\right] = (\lambda_1x_1+\lambda_2y_1)\frac{\partial}{\partial z_1}+(\lambda_1x_2+\lambda_2y_2)\frac{\partial}{\partial z_2},$$

$$\left[z\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y}\right)\right] = z_1\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x_1}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y_1}\right)+z_2\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x_2}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y_2}\right).$$

Further differentiation also yields the vanishing of the differential monomials

$$\left(\frac{\partial}{\partial x_1}\right)^{\alpha_1}\left(\frac{\partial}{\partial x_2}\right)^{\alpha_2}\left(\frac{\partial}{\partial y_1}\right)^{\beta_1}\left(\frac{\partial}{\partial y_2}\right)^{\beta_2}$$
$$\cdot\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x_1}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y_1}\right)^{p_1}\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x_2}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y_2}\right)^{p_2} g(\lambda;xy).$$

Consequently every linear combination of these differential monomials vanishes, and hence so does every form

$$f\left(\frac{\partial}{\partial x},\frac{\partial}{\partial y},\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial x}+\frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial y}\right)g(\lambda,xy).$$

Choose f in particular so that

$$f(x,y,\lambda_1x+\lambda_2y)=g(\lambda;xy),$$

Then one also obtains

$$g\left(\frac{\partial}{\partial\lambda};\frac{\partial}{\partial x},\frac{\partial}{\partial y}\right)g(\lambda,x,y)=0;$$

or, on writing

$$g(\lambda;xy)=\sum G_i\lambda_1^{\nu_1}\lambda_2^{\nu_2}x_1^{\alpha_1}x_2^{\alpha_2}y_1^{\beta_1}y_2^{\beta_2},$$

where the G_i are linear forms with rational-number coefficients in the indeterminates a, one has

$$\sum\nu_1!\nu_2!\alpha_1!\alpha_2!\beta_1!\beta_2!\,G_i^2=0,$$

and hence $g(\lambda;xy)=0$.

Exactly as in a), Lemma b) implies that *$\mathcal{S}$ and $\mathcal{T}$ have equal rank: $\sigma=\tau$.*

Thus a) and b) give $\rho=\tau$; since $\mathcal{T}$ is a subfamily of $\mathcal{L}$, this proves that the two linear families are equivalent. Hence every form of $\mathcal{L}$, and in particular θ, can be represented as a linear combination with rational-number coefficients of ρ linearly independent forms $h(x,y,z)$:

$$\theta=\sum c_ih^{(i)}(x,y,z)=\sum PZ.$$

This identity, derived for indeterminate coefficients a of θ, remains valid when the indeterminates a are replaced by elements of any field of rationality. Thus *the reduction theorem is proved in full generality for three binary rows.*

The general proof for N rows of n variables each is entirely parallel. Let $\theta(A)$ have degree α_i in the row A_i. We again consider three linear families of forms:

1. the family $\mathcal{L}$, consisting of all forms $f(A)$ that arise from $\theta(A)$ by polar processes P and have the same degree as $\theta(A)$ in each row A_i;

2. the family $\mathcal{S}$, consisting of all forms $g(\lambda;A_1\cdots A_n)$ obtained from $f(A)$ by the substitutions

$$A_{n+1}=\lambda_{n+1}^{(1)}A_1+\lambda_{n+1}^{(2)}A_2+\cdots+\lambda_{n+1}^{(n)}A_n,$$
$$\vdots$$
$$A_N=\lambda_N^{(1)}A_1+\lambda_N^{(2)}A_2+\cdots+\lambda_N^{(n)}A_n;$$

the coefficients of the individual monomials in the λ's in $g(\lambda;A_1\cdots A_n)$ give the forms Z in identity (1);

3. the family $\mathcal{T}$, consisting of all forms $h(A)$ defined by

$$h(A)=\left[A_{n+1}\left(\frac{\partial}{\partial\lambda_{n+1}^{(1)}}\frac{\partial}{\partial A_1}+\cdots+\frac{\partial}{\partial\lambda_{n+1}^{(n)}}\frac{\partial}{\partial A_n}\right)\right]^{\alpha_{n+1}}$$
$$\cdots\left[A_N\left(\frac{\partial}{\partial\lambda_N^{(1)}}\frac{\partial}{\partial A_1}+\cdots+\frac{\partial}{\partial\lambda_N^{(n)}}\frac{\partial}{\partial A_n}\right)\right]^{\alpha_N}g(\lambda;A_1\cdots A_n).$$

The form $h(A)$ is a sum of forms PZ.

The identity among every $n+1$ rows ensures that Lemma a) remains valid; Lemma b) remains valid as well, since the number of variables played no role in its proof. Thus $\mathcal{L}$ and $\mathcal{T}$ have the same rank and, since $\mathcal{T}$ is a subfamily of $\mathcal{L}$, are identical. Consequently,

$$\theta=\sum PZ$$

holds for indeterminate coefficients and therefore for coefficients in any field of rationality; *this proves the reduction theorem in general.*

III.

We briefly show how analogous arguments also yield the *general series expansion* (for $N \leq n$). Let Z be a form separately homogeneous in the n rows $A_1, \ldots, A_n$ of n quantities each, and let Δ be the determinant of these rows. We first prove the identity corresponding to (1):

$$Z = \sum PH \pmod{\Delta}, \tag{2}$$

where the forms H contain only the rows $A_1, \ldots, A_{n-1}$ and are derived from Z by processes P.

The proof converts the relations derived in II into congruences modulo Δ. For simplicity, take three ternary rows x, y, z and assume the coefficients to be indeterminates.

Define the three linear families $\mathcal{L}, \mathcal{S}, \mathcal{T}$ as in II for binary rows, and let their ranks be ρ, σ, τ. Let ρ^* and τ^* denote the ranks of $\mathcal{L}$ and $\mathcal{T}$ modulo Δ; that is, $\mathcal{L}$ contains ρ^*, but not $\rho^* + 1$, forms linearly independent modulo Δ. Then, as in II, we have

Lemma a): $f(x, y, \lambda_1 x + \lambda_2 y) = 0$ *necessarily implies* $f(xyz) \equiv 0 \pmod{\Delta}$*, and conversely.* Indeed, the identity among four ternary rows,

$$\Delta_1 x - \Delta_2 y + \Delta_3 z = \Delta t, \qquad \Delta_1 = (yzt), \ldots,$$

always gives a linear relation modulo Δ among three ternary rows:

$$\Delta_1 x - \Delta_2 y + \Delta_3 z \equiv 0 \pmod{\Delta},$$

and hence, as in II,

$$f(x, y, -\Delta_1 x + \Delta_2 y) \equiv \Delta_3^p f(x, y, z) \pmod{\Delta}.$$

Since Δ is irreducible and does not divide Δ_3, the identity $f(x, y, \lambda_1 x + \lambda_2 y) = 0$ (identically in λ) therefore necessarily implies $f(x, y, z) \equiv 0 \pmod{\Delta}$. The converse is clear from $\Delta(x, y, \lambda_1 x + \lambda_2 y) = 0$. Thus, as in II, $\rho^* = \sigma$.

Lemma b), with its proof, remains valid; hence $\sigma = \tau$.

To prove $\tau = \tau^*$, we use

Lemma c): $h(x, y, z) \equiv 0 \pmod{\Delta}$ *necessarily implies* $h(x, y, z) = 0$. As a polar, $h(x, y, z)$ is annihilated by the familiar Ω-process; this is expressed by the differential equation

$$\Delta\left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\right) h(x, y, z) - \left(\frac{\partial}{\partial x}\frac{\partial}{\partial y}\frac{\partial}{\partial z}\right) h(x, y, z) = 0.$$

[123] If $h(x, y, z) = \Delta(x, y, z) \cdot k(x, y, z)$, then further differentiation shows that

$$k\left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\right) \Delta\left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\right) = h\left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\right) h(x, y, z),$$

also vanishes, and hence so does $h(x, y, z)$. Thus $\rho^* = \sigma = \tau = \tau^*$; because $\mathcal{T}$ is a subfamily of $\mathcal{L}$, identity (2) is proved. The same argument proves the result for n variables.

Applying identity (2) to the multiplier of Δ gives an expansion

$$Z = \varphi_0 + \Delta\varphi_1 + \Delta^2\varphi_2 + \cdots + \Delta^\mu\varphi_\mu,$$

where each φ_i is annihilated by the Ω-process. Repeating the process i times gives — since, in general, $\Omega(\Delta \cdot \psi) = c_1\psi + c_2\Delta \cdot \Omega(\psi)$ —

$$c \cdot \Omega^i(Z) \equiv \varphi_i \pmod{\Delta};$$

while (2) gives

$$c \cdot \Omega^i(Z) \equiv \sum PH_i \pmod{\Delta},$$

where the H_i are derived from $\Omega^i(Z)$ in the same way as H is derived from Z. Lemma c), extended to n variables, therefore gives $\varphi_i = \sum PH_i$, and consequently

$$Z = \sum PH + \Delta \cdot \sum PH_1 + \Delta^2 \cdot \sum PH_2 + \cdots + \Delta^\mu \cdot \sum PH_\mu \tag{3}$$

[123] By 3 one has

$$-\left(\frac{\partial}{\partial\xi}\frac{\partial}{\partial\eta}\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial\xi} + \frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial\eta}\right)\right)\left(x\frac{\partial}{\partial\xi}\right)^{\alpha-1}\left(y\frac{\partial}{\partial\eta}\right)^{\beta-1}\left[z\left(\frac{\partial}{\partial\lambda_1}\frac{\partial}{\partial\xi} + \frac{\partial}{\partial\lambda_2}\frac{\partial}{\partial\eta}\right)\right]^{p-1} g(\lambda; \xi, \eta),$$

and $\Omega(h)$ therefore vanishes because the determinant factor vanishes.

as the most general expansion of a form in n rows of n variables each in terms of polars of forms in only $n-1$ *rows.*

The expansion for forms in N rows of n variables ($N < n$) is then obtained, as is well known, by a simple substitution. Put, for $N = 3$ and $n > 3$,

$$u = \xi_1 x + \xi_2 y + \xi_3 z, \quad v = \eta_1 x + \eta_2 y + \eta_3 z, \quad w = \zeta_1 x + \zeta_2 y + \zeta_3 z,$$

and expand $H(u, v, w) = Z(\xi, \eta, \zeta)$ by (3). Since ξ, η, ζ occur only in the combinations u, v, w, one then has

$$\left(\eta \frac{\partial}{\partial \xi}\right) = \left(v \frac{\partial}{\partial u}\right) \cdots, \qquad \Omega = \sum_{ikl} \left(\frac{\partial}{\partial u} \frac{\partial}{\partial v} \frac{\partial}{\partial w}\right)_{ikl} (xyz)_{ikl} = \nabla_{uvw}(xyz).$$

Under the specialization $\xi_1 = \eta_2 = \zeta_3 = 1$ and $\xi_2 = \xi_3 = \cdots = \zeta_2 = 0$, the form $H(u, v, w)$ becomes $H(x, y, z)$, while $\nabla_{uvw}(xyz)$ becomes, up to a numerical factor, $\nabla_{xyz}(xyz) = \nabla_{xyz}$, since applying $(y\partial/\partial x)$ and the analogous operators to the determinants $(xyz)_{ikl}$ makes them vanish. The corresponding statement holds for N rows, so (3) yields the expansion

$$H = \sum P\Phi + \sum P\Phi_1 + \cdots + \sum P\Phi_\mu, \tag{4}$$

where the Φ_i are obtained from $\nabla^i_{A_1 \ldots A_N} H$ by processes P and contain only the rows $A_1, \ldots, A_{N-1}$, apart from the determinant combinations occurring in ∇^i, which, as noted, play no role in polarization.

Replacing these determinants in ∇^i by indeterminates p, one can again expand the resulting forms by (4), finally obtaining

$$H = \Big[\sum P\psi(p)\Big]_{p=\text{determinants of } A_1 \cdots A_N}, \tag{5}$$

where the ψ are obtained from the original form by the processes P, $\nabla_{A_1 \ldots A_N}(p)$, $\nabla_{A_1 \ldots A_{N-1}}(p)$, and so forth. These expansions and their combinations — for example, applying (3), followed by (4) and (5), to the forms Z occurring in (1) — exhaust all known expansions for forms in arbitrarily many rows of n cogredient variables each.

Erlangen, 5 January 1915.

9. The Most General Domains from Integral Transcendental Numbers

Math. Ann. 77 (1916), pp. 103–128

Using the well-ordering theorem, E. Zermelo constructed a domain of "integral transcendental numbers," that is, a numerical domain $\mathfrak{G}$ with the following *abstract* properties:

I. The sum, difference, and product of two numbers of $\mathfrak{G}$ are again numbers of $\mathfrak{G}$.

II. Every real or complex number is the quotient of two numbers from $\mathfrak{G}$.

III. Every rational integer (respectively algebraic integer) is an element of $\mathfrak{G}$.

IV. No non-integral rational (respectively algebraic) number belongs to $\mathfrak{G}$.[124]

The construction rests on the fact that the well-ordering theorem establishes the existence of an *algebraic basis* of all numbers: a *system H of numbers η* among which there are no algebraic relations, but in terms of which every other number can be expressed algebraically. Because they are algebraically independent, the basis numbers η may be regarded as indeterminates; the desired domain thus becomes an integrality domain of rational and algebraic functions of the indeterminates η,[125] with coefficients in the field K of all algebraic numbers. The particular domain $\mathfrak{G}_\eta$ constructed by Zermelo is then characterized by the following *basis properties*:

$\mathfrak{G}_\eta$ contains:

1) all basis numbers η,

2) all polynomials in the η with integral[126] coefficients,

3) all algebraically integral functions of the η with integral coefficients.

$\mathfrak{G}_\eta$ excludes:

4) all fractional rational functions of the η with integral coefficients,

5) all nonintegral algebraic functions of the η with integral coefficients.[127]

It is easy to see (compare the examples in §§ 2 and 3) that there are domains $\mathfrak{G}$ essentially different from Zermelo's domain $\mathfrak{G}_\eta$: domains for which no well-ordering makes all basis properties 1)–5) hold and which therefore cannot be produced by Zermelo's construction under any well-ordering. In other words, there are domains $\mathfrak{G}$ that cannot be mapped one-to-one and isomorphically onto $\mathfrak{G}_\eta$. This raises the question of the *most general domains of integral transcendental numbers*, which will be answered completely below.

For this purpose, one must first determine which basis properties follow from the abstract defining properties and which depend on the particular construction. It is shown in § 1 that, for every prescribed domain $\mathfrak{G}$, there is a well-ordering for which basis properties 1) and 2) hold; hence *every domain $\mathfrak{G}$ can be constructed by means of an algebraic basis of all numbers.* None of the remaining basis properties need hold (§§ 2 and 3). In particular, another abstract property of Zermelo's domain fails for some domains $\mathfrak{G}$: *algebraic integral closedness.* It may be formulated as follows:

V. Every number integral, with algebraic-integer coefficients, over finitely many numbers of $\mathfrak{G}$ belongs to $\mathfrak{G}$.

The special domains satisfying V in addition to I–IV will be called domains $\mathfrak{H}$ of *algebraically integral transcendental numbers.* For the most general domains $\mathfrak{H}$, one obtains the simple results of § 4:

a) *The intersection of all domains $\mathfrak{H}$ constructible from the same basis H consists of all algebraically integral functions of the basis; it is therefore Zermelo's domain $\mathfrak{G}_\eta$, which is itself a domain $\mathfrak{H}$.* (This also gives an abstract characterization of Zermelo's domain.)

[124] E. Zermelo, Über ganze transzendente Zahlen, Math. Ann. 75, p. 434 (1914).

[125] For this reason, the arguments of the present paper partly parallel those of the author's earlier paper, Körper und Systeme rationaler Funktionen, Math. Ann. 76, p. 161 (1915).

[126] Throughout, "integral" means that the coefficients belong to the integrality domain $[K]$ of all algebraic integers. To define $\mathfrak{G}_\eta$, it would also suffice in 1)–5) to consider only ordinary integer coefficients; for more general domains, however, the basis properties would then be less simple.

[127] Zermelo, loc. cit., § 3.

b) *Every domain* $\mathfrak{H}$ *arises by algebraically integral adjunction*[128] *of an arbitrary system* $\mathfrak{S}(\eta)$ *to* $\mathfrak{G}_\eta$*, where* $\mathfrak{S}(\eta)$ *need satisfy only the condition that the adjunction introduce no nonintegral algebraic number into the domain.*

The results for the most general domains $\mathfrak{G}$ based on an algebraic basis are less simple. Here the intersection of all domains $\mathfrak{G}$ is not itself a domain $\mathfrak{G}$, and the construction of the most general domains is consequently harder to describe (ğ 5).

To obtain results analogous to those for the domains $\mathfrak{H}$, replace the algebraic basis by a *rational basis* Θ: a *system* Θ *of numbers* ϑ in terms of which every number can be expressed rationally, while under at least one well-ordering no basis number can be expressed rationally in terms of finitely many preceding basis numbers. The rational basis Θ must also satisfy the side condition that the integrality domain $[\Theta]$ consisting of all integer polynomials in the ϑ contain no nonintegral algebraic number. (The construction of such a basis with this side condition is given in ğ 7.) For the most general domains $\mathfrak{G}$ — which might also be called domains of *rationally integral transcendental numbers* — one again obtains the simple results of ğ 6:

a) *The intersection of all domains* $\mathfrak{G}$ *constructible from the same rational basis* Θ *consists of all polynomial functions of the basis; it is therefore the domain* $[\Theta]$*, which is itself a domain* $\mathfrak{G}$*.*

b) *Every domain* $\mathfrak{G}$ *arises by rationally integral adjunction of an arbitrary system* $\mathfrak{S}(\vartheta)$ *to* $[\Theta]$*, where* $\mathfrak{S}(\vartheta)$ *need satisfy only the condition that the adjunction introduce no nonintegral algebraic number into the domain.*

To obtain complete analogy with the domains $\mathfrak{H}$, one would have to omit the algebraic numbers from defining properties III and IV for the domains $\mathfrak{G}$. With this modification, the construction of integral elements by means of a rational basis extends to every arbitrary field (ğ 10), whereas Zermelo's construction presupposes that the field is algebraically closed.

As H *ranges over all algebraic bases, and* Θ *over all rational bases satisfying the side condition, results a) and b) yield the totality of all domains* $\mathfrak{H}$ *and* $\mathfrak{G}$*.* Grouping all isomorphic domains into a class, one can select from this totality a subset representing all the classes (ğ 8), of which there are, by ğ 9, at least countably infinitely many.

ğ 1. Proof of basis properties 1) and 2) for all domains $\mathfrak{G}$.

Let $\mathfrak{G}$ be any given domain of integral transcendental numbers, so that it possesses the abstract properties I–IV. Following the procedure that E. Zermelo applied to the field of all complex numbers, we select from $\mathfrak{G}$ an *algebraic basis* H *of all the numbers in* $\mathfrak{G}$. Since, by II, every real or complex number can be represented as the quotient of two numbers in $\mathfrak{G}$, H is at the same time an algebraic basis of *all* numbers. For every given domain $\mathfrak{G}$, the algebraic basis of all numbers can therefore be chosen to belong to $\mathfrak{G}$, so that *basis property 1) holds.* Moreover, by III, $\mathfrak{G}$ contains the integrality domain $[K]$ of all algebraic integers, and hence, by I, all polynomials in the basis elements η with coefficients in $[K]$; that is, all integral polynomials in the η, which form the integrality domain $[H]$. Thus *basis property 2) always holds*; in other words, *every domain* $\mathfrak{G}$ *can be constructed by means of an algebraic basis* H *of all numbers in such a way that* $\mathfrak{G}$ *contains the integrality domain* $[H]$ *as a subdomain.*

Remark. Starting from a basis H, one can of course nevertheless construct a domain $\mathfrak{G}$ for which basis properties 1) and 2) hold not with respect to H itself, but with respect to some other basis H'. For example, let $\mathfrak{G}'$ be obtained from the Zermelo domain $\mathfrak{G}_\eta$ by replacing some basis element η throughout the construction by a polynomial $f(\eta)$. Then $\mathfrak{G}'$ contains neither η nor $[H]$; but if the basis element η in H is replaced by $\xi = f(\eta)$ — whereupon H again becomes an algebraic basis H' — then basis properties 1) and 2) hold for $\mathfrak{G}'$ with respect to H'.

ğ 2. Exclusion of basis properties 4) and 5).

We now show that the domains $\mathfrak{G}$ need satisfy none of the remaining basis properties. First, properties 4) and 5) will be excluded by replacing the integrality domain $[H]$ in Zermelo's construction with a domain of integral rational "functionals."

[128] This expression is explained in ğ 4.

According to Weber,[129] a *rational functional* is any rational function with rational-number coefficients in the following uniquely determined representation:

$$A(\eta_1 \cdots \eta_t) = a \cdot \frac{E_1(\eta_1 \cdots \eta_t)}{E_2(\eta_1 \cdots \eta_t)},$$

where E_1 and E_2 are relatively prime primitive polynomials with rational-integer coefficients, and a is a positive rational number (the absolute value of A). If, in particular, a is a *rational integer*, then A is called an *integral rational functional*. The integral rational functionals thus include, as special cases, the rational integers and the polynomials with rational-integer coefficients, whereas nonintegral rational numbers and polynomials with nonintegral rational coefficients count as fractional rational functionals.

Let the domain $\mathfrak{G}$ now consist of the totality $\mathfrak{F}$ of all integral rational functionals of finitely many basis elements η at a time, together with all functions algebraically integral over $\mathfrak{F}$ — that is, functions satisfying some equation whose leading coefficient is unity and whose remaining coefficients are integral rational functionals.

The verification of properties I–IV for $\mathfrak{G}$ is exactly parallel to the corresponding argument for Zermelo's domain and will only be indicated briefly. First, II and III are immediate, since $\mathfrak{G}$ contains the Zermelo domain $\mathfrak{G}_\eta$ as a subdomain. By Gauss's theorem for polynomials with rational-integer coefficients, sums, differences, and products of integral rational functionals are again *integral* rational functionals; hence $\mathfrak{F}$ forms an integrality domain, and familiar arguments[130] then show that $\mathfrak{G}$ is likewise an integrality domain, establishing I. The extended Gauss theorem[131] further yields the two lemmas: "If z is algebraically integral over $\mathfrak{F}$ by virtue of *any* equation, then it is so also by virtue of the *irreducible* equation satisfied by z over the field of all rational functionals,"[132] and "the equation satisfied by an algebraic number and irreducible over the field of all rational numbers remains irreducible over the field of all rational functionals." Thus $\mathfrak{G}$ can contain no nonintegral algebraic number; this proves IV and hence all the abstract properties I–IV.

Under no well-ordering, however, can a basis be selected from $\mathfrak{G}$ in such a way that $\mathfrak{G}$ excludes all nonintegral rational and algebraic functions of the basis elements. For let $z(\eta)$ be any function of the domain chosen as a basis element, and hence defined by an equation

$$z^k + A_1(\eta)z^{k-1} + \cdots + A_k(\eta) = 0,$$

where

$$A_i(\eta) = a_i \cdot \frac{E_1(\eta)}{E_2(\eta)}$$

are integral rational functionals. Then $\frac{a_k}{z}$ belongs to $\mathfrak{G}$, as do $\frac{a_k}{\sqrt{z}}$, $\frac{a_k}{\sqrt[3]{z}}$, and so forth.[133] Thus *basis properties 4) and 5) are excluded for the totality of the domains $\mathfrak{G}$.*

Remark. An example in ğ 3 will show that, under every well-ordering, $\mathfrak{G}$ may also contain fractional rational functionals without containing a nonintegral rational or algebraic number.

ğ 3. Exclusion of basis property 3).

To exclude basis property 3), we use a generalized *module domain* in which the arguments of the polynomials belonging to the domain are no longer the indeterminates themselves, but all integral algebraic functions of those indeterminates,[134] while the indeterminates themselves serve as a module basis.

Let $\mathfrak{G}$ consist of *all elements*

$$z = \alpha + g_1(\eta)\eta_1 + g_2(\eta)\eta_2 + \cdots + g_t(\eta)\eta_t, \tag{1}$$

where α ranges over all algebraic integers, $\eta_1 \cdots \eta_t$ over all basis elements, and, for each fixed combination $\eta_1 \cdots \eta_t$, each of the functions $g_1(\eta) \cdots g_t(\eta)$ independently ranges over all integral algebraic functions of the η.[135]

[129] H. Weber, Lehrbuch der Algebra. Kleine Ausgabe, ğğ 96 and 97.

[130] Compare, for example, Weber, ğ 97, 8.

[131] Weber, ğ 20, 5.

[132] Compare Weber, ğ 97, 4.

[133] Quite analogously, every algebraic function of the η can be turned into an element of the functional domain $\mathfrak{G}$ by multiplication by a rational integer. Thus this domain has the property that *every complex number can be represented as the quotient of an element of $\mathfrak{G}$ by a rational integer* — in analogy with the algebraic numbers.

[134] By "integral algebraic functions" we shall always mean functions with *integral* coefficients; that is, functions satisfying some equation whose leading coefficient is unity and whose remaining coefficients are polynomials in the η with algebraic-integer coefficients — polynomials from $[H]$. In particular, all polynomials from $[H]$ are integral algebraic functions.

[135] The module property applies to the elements $z - \alpha$.

It is easy to verify properties I–IV for this module domain. First, I holds because the sum, difference, and product of two elements z again have the form (1). The domain $\mathfrak{G}$ also contains all basis elements η, as well as all elements $\eta \cdot g(\eta)$, where $g(\eta)$ ranges over all integral algebraic functions of the η. Hence all integral algebraic functions of the η, and therefore all algebraic functions of the η whatsoever, can be represented as quotients of two elements of $\mathfrak{G}$, which proves II. The representation (1) includes, in particular, all algebraic integers — take $g_1 = 0 \cdots g_t = 0$ — but z cannot equal a nonintegral algebraic number. For if z represents an algebraic number β, the identity

$$\beta = \alpha + g_1(\eta)\eta_1 + \cdots + g_t(\eta)\eta_t$$

in the η necessarily implies $\beta = \alpha$. This follows upon making the specialization

$$\eta_1 = 0 \cdots \eta_t = 0,$$

under which the multipliers $g_1(\eta) \cdots g_t(\eta)$ remain finite, since as integral algebraic functions they specialize to integral algebraic functions or numbers.[136] Thus conditions I–IV hold for $\mathfrak{G}$.

Under no well-ordering, however, can a basis be selected from $\mathfrak{G}$ *in such a way that all integral algebraic functions of the basis elements belong to* $\mathfrak{G}$. For let $z(\eta)$ be any function in the domain selected as a basis element — and thus one that genuinely involves the indeterminates η. We shall show that the functions

$$\xi = \sqrt[\nu]{z - \alpha}$$

cannot belong to $\mathfrak{G}$ once ν exceeds some finite bound depending on z.

Indeed, suppose that ξ belongs to $\mathfrak{G}$. By (1), it then has the form

$$\xi = \gamma + h_1(\eta)\eta_{i_1} + h_2(\eta)\eta_{i_2} + \cdots + h_\tau(\eta)\eta_{i_\tau},$$

where again $h_1(\eta) \cdots h_\tau(\eta)$ are integral algebraic functions of the η, while $\eta_{i_1} \cdots \eta_{i_\tau}$ are arbitrary basis elements and may, in particular, coincide with $\eta_1 \cdots \eta_t$. We must first show that the algebraic integer γ is zero. Since $h_1(\eta) \cdots h_\tau(\eta)$ are integral algebraic functions, setting $\eta_{i_1} = 0 \cdots \eta_{i_\tau} = 0$ makes ξ equal to γ, whatever the values of the remaining η. In particular, ξ equals γ under the specialization

$$\eta_{i_1} = 0 \cdots \eta_{i_\tau} = 0; \qquad \eta_1 = 0 \cdots \eta_t = 0.$$

Under this specialization, however, the function $(z - \alpha)$ vanishes by (1), and hence so does ξ. Consequently $\gamma = 0$, and

$$\xi = h_1(\eta)\eta_{i_1} + h_2(\eta)\eta_{i_2} + \cdots + h_\tau(\eta)\eta_{i_\tau}.$$

Raising this equation to the ν-th power gives

$$\xi^\nu = z - \alpha = F_\nu(\eta),$$

where $F_\nu(\eta)$ denotes a homogeneous, nonzero form of degree ν in $\eta_{i_1} \cdots \eta_{i_\tau}$ whose coefficients are integral algebraic functions of the η. Now $z - \alpha$, which by (1) is an *integral* algebraic function of the η, satisfies an equation irreducible over $[H]$:

$$(z - \alpha)^\chi + B(\eta)(z - \alpha)^{\chi - 1} + \cdots + C(\eta) = 0,$$

where the final coefficient $C(\eta)$ — the product of $(z - \alpha)$ and its conjugates — is a polynomial of some degree λ. On the other hand, multiplying $F_\nu(\eta)$ by the corresponding conjugates in $z - \alpha = F_\nu(\eta)$ gives

$$C(\eta) = G_{\nu\chi}(\eta),$$

where $G_{\nu\chi}(\eta)$ is a homogeneous form of degree $\nu\chi$ in $\eta_{i_1} \cdots \eta_{i_\tau}$ whose coefficients are polynomials in the η. Thus $G_{\nu\chi}$ has degree at least $\nu\chi$ in the η, so that $\lambda \geq \nu\chi$. In other words, *the functions* $\sqrt[\nu]{z - \alpha}$ *for which* $\nu > \lambda/\chi$ *do not belong to* $\mathfrak{G}$. *Basis property 3) is therefore excluded for the totality of the domains* $\mathfrak{G}$.

Remark. A slight generalization of the domain just constructed yields a domain $\mathfrak{G}$ that also contains *fractional functionals* under every well-ordering. Let $\mathfrak{G}$ consist of all elements

$$z = \alpha + \gamma_1(\eta)\eta_1 + \gamma_2(\eta)\eta_2 + \cdots + \gamma_t(\eta)\eta_t,$$

where $\gamma(\eta)$ now ranges over all algebraically integral, but *not necessarily integral*, functions of the η. The verification of properties I–IV remains the same as above. But along with every function z, $\mathfrak{G}$ also contains $a \cdot (z - \alpha)$, where a is an arbitrary rational or fractional algebraic number; hence fractional functionals occur under every well-ordering.

[136] This more detailed proof of IV is given because of the generalized example at the end of the section. Here it would suffice to observe that, by construction, z is an integral algebraic function.

ğ 4. The most general domains of algebraically integral transcendental numbers.

For convenience in formulating what follows, we introduce the expression "*an element z is algebraically integral over $\mathfrak{T}$*." This means that z satisfies *some* equation whose leading coefficient is unity and whose remaining coefficients are integral polynomials in elements of $\mathfrak{T}$, where $\mathfrak{T}$ is any given domain.[137]

A domain $\mathfrak{T}$ is called *closed under algebraic integrality* if it satisfies the following condition (compare the introduction):

V. Every element algebraically integral over $\mathfrak{T}$ belongs to $\mathfrak{T}$.

We first show that the *abstract property* V belongs to the Zermelo domain $\mathfrak{G}_\eta$. Suppose that an element z is algebraically integral over $\mathfrak{G}_\eta$ by virtue of an equation $f(z) = 0$. Multiplying $f(z)$ by its conjugates over $[H]$ shows that z is also algebraically integral over $[H]$ and hence belongs to $\mathfrak{G}_\eta$. The functional domain considered in ğ 2 is shown in the same way to be closed under algebraic integrality.

The module domain considered in ğ 3, which lacks basis property 3), shows that property V does not belong to every domain $\mathfrak{G}$. More precisely, ğ 3 showed that the module domain is not closed under algebraic integrality with respect to *any transcendental* element of the domain, whereas by III and IV it is, of course, so closed with respect to *every algebraic* element of the domain.

This leads us to single out from the totality of domains $\mathfrak{G}$ those that also possess abstract property V; they will be called "*domains $\mathfrak{H}$ of algebraically integral transcendental numbers*."

Let $\mathfrak{H}$ be such a domain, and let H be an algebraic basis of all the numbers in $\mathfrak{H}$; by II, H is at the same time an algebraic basis of *all* numbers. By III, I, and V, $\mathfrak{H}$ contains, besides H, all integral algebraic functions of the η — the Zermelo domain $\mathfrak{G}_\eta$. Thus, in analogy with ğ 1: *Every domain $\mathfrak{H}$ of algebraically integral transcendental numbers can be constructed by means of an algebraic basis of all numbers in such a way that $\mathfrak{H}$ contains the Zermelo domain $\mathfrak{G}_\eta$ as a subdomain.*

Now let H be any algebraic basis of all numbers, and let $\mathfrak{M}(\mathfrak{H})$ denote the totality of all domains $\mathfrak{H}$ that contain H. Every domain $\mathfrak{H}$ in $\mathfrak{M}(\mathfrak{H})$ contains, as just proved, the Zermelo domain $\mathfrak{G}_\eta$ as a subdomain; and since $\mathfrak{G}_\eta$ is itself a domain $\mathfrak{H}$, it is the *greatest common subdomain, or intersection, of all domains $\mathfrak{H}$ in* $\mathfrak{M}(\mathfrak{H})$. This defines $\mathfrak{G}_\eta$ abstractly. It also follows directly that $\mathfrak{M}(\mathfrak{H})$ is closed under intersections; that is, the intersection of all the domains $\mathfrak{H}$ in any subsystem of $\mathfrak{M}(\mathfrak{H})$ again belongs to $\mathfrak{M}(\mathfrak{H})$. Indeed, I and V hold for the intersection; II and III follow because $\mathfrak{G}_\eta$ is a subdomain, and IV because the intersection is a subdomain of each $\mathfrak{H}$.

As the functional-domain example in ğ 2 shows, domains $\mathfrak{H}$ generally contain functions in addition to those in $\mathfrak{G}_\eta$. Let $\psi(\eta)$ be one such rational or algebraic function of the η. By I, $\mathfrak{H}$ then also contains every integral rational combination of ψ and finitely many functions from $\mathfrak{G}_\eta$. The resulting integrality domain — consisting of all polynomials in ψ with coefficients in $\mathfrak{G}_\eta$ — will be denoted by $[\mathfrak{G}_\eta, \psi]$, and the process producing it will be called the "*rationally integral adjunction of ψ to $\mathfrak{G}_\eta$*." By V, $\mathfrak{H}$ also contains all functions algebraically integral over $[\mathfrak{G}_\eta, \psi]$. The resulting domain will be denoted by $\{\mathfrak{G}_\eta, \psi\}$, and the process producing it will be called the "*algebraically integral adjunction of ψ to $\mathfrak{G}_\eta$*." The domain $\{\mathfrak{G}_\eta, \psi\}$ consists of all integral algebraic functions of ψ with coefficients in $\mathfrak{G}_\eta$, and is therefore an integrality domain by familiar arguments.[138]

We show that $\{\mathfrak{G}_\eta, \psi\}$ is also closed under algebraic integrality, and hence satisfies condition V. Indeed, suppose z is algebraically integral over $\{\mathfrak{G}_\eta, \psi\}$ by virtue of an equation

$$f(z; a \cdots c) = z^\chi + az^{\chi-1} + \cdots + c = 0,$$

where $a \cdots c$, being elements of $\{\mathfrak{G}_\eta, \psi\}$, satisfy equations with coefficients in $[\mathfrak{G}_\eta, \psi]$:

$$a^\lambda + A_1 a^{\lambda-1} + \cdots + A_\lambda = 0,$$
$$\vdots$$
$$c^\mu + C_1 c^{\mu-1} + \cdots + C_\mu = 0.$$

Let the roots of these equations be $a, a' \cdots a^{(\lambda-1)} \cdots c, c' \cdots c^{(\mu-1)}$. Forming the product over all combinations of these roots gives

$$g(z) = f(z; a \cdots c) f(z; a' \cdots c') \cdots f(z; a^{(\lambda-1)} \cdots c^{(\mu-1)}),$$

[137] When $\mathfrak{T}$ is an integrality domain, the leading coefficient is unity and the remaining coefficients are elements of $\mathfrak{T}$.

[138] Compare, for example, Weber, ğ 97, 6 and 7.

The leading coefficient of $g(z)$ is unity, and its remaining coefficients are elements of $[\mathfrak{G}_\eta, \psi]$; consequently z belongs to $\{\mathfrak{G}_\eta, \psi\}$.[139]

Thus the domain $\{\mathfrak{G}_\eta, \psi\}$ has properties I and V and, because $\mathfrak{G}_\eta$ is a subdomain, also II and III. Whether IV holds depends on the choice of ψ. For example, IV fails for $\psi = \frac{1}{n \cdot \eta}$, since $\frac{1}{n}$ then belongs to the domain; but by ğ 2 it holds for $\psi = \frac{1}{\eta}$, and also for $\psi = \frac{\eta}{n}$. Indeed, in the latter case, if a function in $\{\mathfrak{G}_\eta, \psi\}$ represents an algebraic number, its value is unchanged upon setting $\eta = 0$; it thereby specializes to a function in $\mathfrak{G}_\eta$, and hence to an algebraic integer.

Thus $\{\mathfrak{G}_\eta, \psi\}$ becomes a domain $\mathfrak{H}$ as soon as ψ is required to ensure that no nonintegral algebraic number enters the domain through the algebraically integral adjunction.

In precisely the same way, one defines the rationally integral and, respectively, algebraically integral adjunction to $\mathfrak{G}_\eta$ of an arbitrary system $\mathfrak{S}$ of rational or algebraic functions of the η. The rationally integral adjunction produces the integrality domain $[\mathfrak{G}_\eta, \mathfrak{S}]$, consisting of all integral polynomials in finitely many elements of $\mathfrak{G}_\eta$ and $\mathfrak{S}$ at a time. The algebraically integral adjunction produces the domain $\{\mathfrak{G}_\eta, \mathfrak{S}\}$, consisting of all elements algebraically integral over $[\mathfrak{G}_\eta, \mathfrak{S}]$. Exactly as above, one shows that the integrality domain $\{\mathfrak{G}_\eta, \mathfrak{S}\}$ is closed under algebraic integrality and also satisfies II and III. Thus, as above:

$\{\mathfrak{G}_\eta, \mathfrak{S}\}$ becomes a domain $\mathfrak{H}$ as soon as $\mathfrak{S}$ is required to ensure that no nonintegral algebraic number enters the domain through the algebraically integral adjunction — that is, as soon as $\mathfrak{S}$ is an admissible system.[140]

It is important that the converse also holds: as $\mathfrak{S}$ ranges over all admissible systems, the domains $\{\mathfrak{G}_\eta, \mathfrak{S}\}$ actually exhaust all domains $\mathfrak{H}$ in $\mathfrak{M}(\mathfrak{H})$. Indeed, let $\mathfrak{H}$ be any domain in $\mathfrak{M}(\mathfrak{H})$, and let $\mathfrak{L} = \mathfrak{H} - \mathfrak{G}_\eta$ denote the system of all functions in $\mathfrak{H}$ that do not belong to $\mathfrak{G}_\eta$. By V, $\mathfrak{H}$ contains $\{\mathfrak{G}_\eta, \mathfrak{L}\}$ as a subdomain. Conversely, $\{\mathfrak{G}_\eta, \mathfrak{L}\}$ contains both $\mathfrak{G}_\eta$ and $\mathfrak{L}$ and, since these are disjoint and together comprise $\mathfrak{H}$, it contains $\mathfrak{H}$. Hence $\mathfrak{H} = \{\mathfrak{G}_\eta, \mathfrak{L}\}$; and since $\mathfrak{H}$ satisfies IV, $\mathfrak{L}$ is of course an admissible system.[141]

As H ranges over every possible algebraic basis, $\mathfrak{M}(\mathfrak{H})$ ranges, as proved at the outset, over the totality of all domains $\mathfrak{H}$. The results of this section therefore give a complete answer to the question of the most general domains $\mathfrak{H}$ of algebraically integral transcendental numbers:

a) *The intersection of all domains $\mathfrak{H}$ in $\mathfrak{M}(\mathfrak{H})$ is the Zermelo domain $\mathfrak{G}_\eta$, which is itself a domain $\mathfrak{H}$; $\mathfrak{M}(\mathfrak{H})$ is closed under intersections.*

b) *Every domain $\mathfrak{H}$ in $\mathfrak{M}(\mathfrak{H})$ is obtained by algebraically integral adjunction of an admissible system $\mathfrak{S}$ to $\mathfrak{G}_\eta$. As H ranges over every possible algebraic basis, $\mathfrak{M}(\mathfrak{H})$ ranges over the totality of all domains $\mathfrak{H}$.*[142]

ğ 5. The most general domains of integral transcendental numbers, based on an algebraic basis.

Let H be any algebraic basis of all numbers, and let $\mathfrak{M}(\mathfrak{G})$ denote the totality of all domains $\mathfrak{G}$ that contain H, and hence $[H]$. As H ranges over all possible bases, $\mathfrak{M}(\mathfrak{G})$ ranges over the totality of all domains $\mathfrak{G}$; as in ğ 4, we may therefore restrict attention to the domains $\mathfrak{G}$ in $\mathfrak{M}(\mathfrak{G})$.

All domains $\mathfrak{G}$ in $\mathfrak{M}(\mathfrak{G})$ contain $[H]$ as a subdomain; but since $[H]$ is not itself a domain $\mathfrak{G}$, one cannot conclude as in ğ 4 that $[H]$ is their greatest common subdomain. That it is so nevertheless is shown by a countable family of domains $\mathfrak{G}$ in $\mathfrak{M}(\mathfrak{G})$, obtained by a slight generalization of the module domain in ğ 3, which in fact have no common element outside $[H]$.

For each fixed ν, let the domains $\mathfrak{G}_\nu$ ($\nu = 1, 2, \ldots$) consist of all elements

$$z = f(\eta) + g_1(\eta)\eta_1^\nu + g_2(\eta)\eta_2^\nu + \cdots + g_t(\eta)\eta_t^\nu, \tag{1}$$

[139] Thus, defining algebraic integrality by *some* equation makes the notion of irreducibility over a base field unnecessary for the proofs of I and V. Compare ğ 2, where the lemma that passes from the definition by an arbitrary equation to the irreducible equation is needed only to prove IV. Since that lemma no longer holds in general here, IV must be imposed on the function ψ as a separate condition.

[140] More generally, the same argument shows that if $\mathfrak{T}$ is any domain and $\{\mathfrak{T}\}$ denotes the totality of elements algebraically integral over $\mathfrak{T}$, then $\{\mathfrak{T}\}$ is closed under algebraic integrality.

[141] It may already suffice to adjoin a subsystem of $\mathfrak{L}$. For example, the functional domain of ğ 2 is obtained by algebraically integral adjunction to $\mathfrak{G}_\eta$ of all integral rational functionals except the polynomials.

[142] The admissible systems $\mathfrak{S}$ can be found as follows. Place all nonintegral algebraic functions of the η under some well-ordering Ω, and admit to $\mathfrak{S}$ every function except those that, when algebraically integrally adjoined to $\mathfrak{G}_\eta$ and the previously admitted functions, produce a nonintegral algebraic number. The procedure may be stopped at any point. As Ω ranges over all well-orderings and, for each fixed Ω, the procedure is stopped at every possible point, all admissible systems $\mathfrak{S}$ are exhausted.

where $f(\eta)$ ranges over all integral polynomials in the η; $\eta_1, \ldots, \eta_t$ range over all basis elements; and, for each fixed combination $\eta_1^\nu, \ldots, \eta_t^\nu$, each of the functions $g_1(\eta), \ldots, g_t(\eta)$ independently ranges over all integral algebraic functions of the η.

As in ğ 3, one sees that the domains $\mathfrak{G}_\nu$ possess the abstract properties I–IV; $\mathfrak{G}_\nu$ contains only integral algebraic functions and, when $\nu = 1$, is identical with the domain of ğ 3. We now show that the domains $\mathfrak{G}_\nu$ have no common elements apart from the polynomials $f(\eta)$ in $[H]$. Let z be any integral algebraic, nonrational function of the η satisfying the following equation, irreducible over $[H]$:

$$z^\chi + a_1(\eta)z^{\chi-1} + a_2(\eta)z^{\chi-2} + \cdots + a_\chi(\eta) = 0, \tag{2}$$

where $\chi > 1$, and let λ be the largest of the degrees of the polynomials $a_1(\eta), \ldots, a_\chi(\eta)$. If z belongs to $\mathfrak{G}_\nu$, then $\zeta = z - f(\eta)$ satisfies the following equation, which is likewise irreducible over $[H]$:

$$\zeta^\chi + b_1(\eta)\zeta^{\chi-1} + b_2(\eta)\zeta^{\chi-2} + \cdots + b_\chi(\eta) = 0, \tag{3}$$

By (1), the symmetric functions $b_1(\eta), b_2(\eta), \ldots, b_\chi(\eta)$ of the ζ have lowest-degree terms of degrees at least $\nu, 2\nu, \ldots, \chi\nu$, respectively. Comparing (2) and (3) gives

$$b_1(\eta) = a_1(\eta) + \chi f(\eta).$$

Thus, if $\xi = z + \frac{a_1(\eta)}{\chi}$ satisfies

$$\xi^\chi + c_2(\eta)\xi^{\chi-2} + \cdots + c_\chi(\eta) = 0, \tag{4}$$

then

$$\xi - \zeta = \frac{b_1(\eta)}{\chi}; \qquad c_i(\eta) \equiv b_i(\eta) \pmod{\frac{b_1(\eta)}{\chi}}, \tag{5}$$

where $b_1(\eta)$ begins with terms of degree at least ν. Comparison of (2) and (4) shows that the $c_i(\eta)$ have degree χ in the coefficients $a_i(\eta)$ of (2), and hence degree at most $\chi\lambda$ in the η; on the other hand, all the $b_i(\eta)$ begin with terms of degree at least ν. Thus, choosing $\nu > \chi\lambda$, equation (5) gives

$$c_i(\eta) = 0; \qquad \xi^\chi = 0 \quad \text{or} \quad \left(z + \frac{a_1(\eta)}{\chi}\right)^\chi = 0.$$

that is, contrary to our assumption, z is rational in the η. It follows that:

If z is an integral algebraic, nonrational function of the η, then z cannot belong to any domain $\mathfrak{G}_\nu$ for which $\nu > \chi\lambda$, or:

The intersection of all domains $\mathfrak{G}$ in $\mathfrak{M}(\mathfrak{G})$ is the integrality domain $[H]$, which is not itself a domain $\mathfrak{G}$; consequently $\mathfrak{M}(\mathfrak{G})$ is not closed under intersections.

Consequently, the construction of the most general domains $\mathfrak{G}$ by means of an algebraic basis is less transparent than the construction of the domains $\mathfrak{H}$. The domain $[H]$ has properties I, III, and IV. If an arbitrary system $\mathfrak{S}$ is adjoined rationally integrally, properties I and III remain valid for the resulting integrality domain $[H, \mathfrak{S}]$, while IV becomes a separate condition on $\mathfrak{S}$. For a domain $\mathfrak{G}$ to result, II must also be imposed as a condition on $\mathfrak{S}$. Equivalently, for every field $\mathfrak{K}$ finite over (H)[143], there must exist a field $\mathfrak{L}$ finite over $\mathfrak{K}$ such that $[H, \mathfrak{S}]$ contains a primitive element of $\mathfrak{L}$.[144] Conversely, every domain $\mathfrak{G}$ in $\mathfrak{M}(\mathfrak{G})$ can be represented in the form $[H, \mathfrak{S}]$; hence all domains $\mathfrak{G}$ in $\mathfrak{M}(\mathfrak{G})$ are obtained as $\mathfrak{S}$ ranges over all systems subject to these restrictions. The next section will reveal the structure of the systems $\mathfrak{S}$ more simply by means of the "rational basis," while also giving a complete analogy with the theorems of ğ 4.

ğ 6. The most general domains of integral transcendental numbers, based on a rational basis.

In analogy with the algebraic basis, the rational basis is defined as follows: "A system Θ of numbers ϑ is called a rational basis of all numbers if every number can be expressed rationally in Θ — with coefficients

[143] (H) denotes the field of all rational functions of the η with algebraic-number coefficients.

[144] Compare ğ 7.

in K[145] — while, under at least one well-ordering, no basis number can be expressed rationally — with coefficients in K — in terms of finitely many preceding basis numbers."[146]

Let a domain $\mathfrak{G}$ of integral transcendental numbers be placed under a well-ordering Ω. An element z of $\mathfrak{G}$ may then be rationally expressible in terms of finitely many preceding elements of $\mathfrak{G}$; that is, it may satisfy an equation $z = \varphi(\xi)$, where $\varphi(\xi)$ is a rational function of $\xi_1, \ldots, \xi_t$ with coefficients in K. In particular, every algebraic number α in the domain satisfies the equation $z = \alpha$. The remaining elements ϑ of $\mathfrak{G}$ form a system Θ, which we shall show to be a rational basis of all elements of $\mathfrak{G}$. By construction, each ϑ is rationally independent of the preceding elements of Θ. The induction argument[147] further shows that every relation $z = \varphi(\xi)$ entails a relation $z = \psi(\vartheta)$. Otherwise there would be a first element $z_0 = \varphi_0(\xi_1, \ldots, \xi_t)$ that could not be expressed rationally in the ϑ, although the preceding $\xi_1, \ldots, \xi_t$ were rational functions of the ϑ — a contradiction. By II, Θ is at the same time a rational basis of all numbers. By III and I, $\mathfrak{G}$ contains, besides Θ, the integrality domain $[\Theta]$ of all integral polynomials in the ϑ as a subdomain, whereas by IV, $[\Theta]$ contains no nonintegral algebraic number. Thus the rational basis Θ of all numbers satisfies the side condition that the integrality domain $[\Theta]$ derived from it contain no nonintegral algebraic number;[148] Θ is a *rational basis with side condition* for all numbers. Thus, in analogy with ğ 2: *Every domain $\mathfrak{G}$ can be constructed by means of a rational basis with side condition in such a way that $\mathfrak{G}$ contains the integrality domain $[\Theta]$ as a subdomain.*

Let Θ be any rational basis with side condition for all numbers — its existence being assured by the existence of the domains $\mathfrak{G}$. Let $\mathfrak{N}(\mathfrak{G})$ denote the totality of all domains $\mathfrak{G}$ that contain Θ, and hence $[\Theta]$. As Θ ranges over all possible bases with side condition, $\mathfrak{N}(\mathfrak{G})$ ranges, by the preceding, over the totality of all domains $\mathfrak{G}$; we may therefore again restrict attention to the domains $\mathfrak{G}$ in $\mathfrak{N}(\mathfrak{G})$.

Now $[\Theta]$ is itself a domain $\mathfrak{G}$: every number can be expressed rationally in terms of Θ, and hence as the quotient of two polynomials in $[\Theta]$; by construction, $[\Theta]$ also satisfies the remaining conditions I, III, and IV. *Thus $[\Theta]$ is the greatest common subdomain, or intersection, of all domains $\mathfrak{G}$ in $\mathfrak{N}(\mathfrak{G})$. Moreover, $\mathfrak{N}(\mathfrak{G})$ is closed under intersections; that is, the intersection of all domains $\mathfrak{G}$ in any subsystem of $\mathfrak{N}(\mathfrak{G})$ also belongs to $\mathfrak{N}(\mathfrak{G})$.* Indeed, I holds for the intersection; II and III follow because $[\Theta]$ is a subdomain, and IV because the intersection is a subdomain of a domain $\mathfrak{G}$.

The rationally integral adjunction to $[\Theta]$ of an arbitrary system $\mathfrak{S}$ of rational functions of the ϑ — every algebraic function of the ϑ can, by the property of the rational basis, be expressed rationally in terms of certain other ϑ — produces an integrality domain $[\Theta, \mathfrak{S}]$ with properties I, II, and III. It is therefore a domain $\mathfrak{G}$ as soon as $\mathfrak{S}$ is an "admissible system," meaning that no nonintegral algebraic number enters the domain through the rationally integral adjunction. Conversely, every domain $\mathfrak{G}$ in $\mathfrak{N}(\mathfrak{G})$ admits a representation $[\Theta, \mathfrak{S}]$ if $\mathfrak{S}$ is taken to be the residual system $\mathfrak{G} - [\Theta]$. Thus, in complete analogy with ğ 4, the following results hold for the most general domains $\mathfrak{G}$:

a) *The intersection of all domains $\mathfrak{G}$ in $\mathfrak{N}(\mathfrak{G})$ is the integrality domain $[\Theta]$, which is itself a domain $\mathfrak{G}$; $\mathfrak{N}(\mathfrak{G})$ is closed under intersections.*

b) *Every domain $\mathfrak{G}$ in $\mathfrak{N}(\mathfrak{G})$ is obtained by rationally integral adjunction of an admissible system $\mathfrak{S}$ to $[\Theta]$. As Θ ranges over all possible rational bases with side condition, $\mathfrak{N}(\mathfrak{G})$ ranges over the totality of all domains $\mathfrak{G}$.*[149]

Remark. If an algebraic basis H of all elements of Θ is selected from Θ, then H is at the same time an algebraic basis of all numbers. Conversely, every algebraic basis can be extended to a rational basis by placing H first in the well-ordering. Accordingly, the construction in ğ 5 of the domains $\mathfrak{G}$ by means of an algebraic basis can be interpreted as follows: divide the system $\mathfrak{S}$ to be adjoined to $[H]$ into two subsystems, $\mathfrak{S}_1$ and $\mathfrak{S}_2$. Adjoining $\mathfrak{S}_1$ amounts to extending H to a rational basis with side condition, after which an admissible system $\mathfrak{S}_2$ is adjoined rationally integrally.

[145] Rational functions are always to be understood as having algebraic-number coefficients; these coefficients are included in the definition because of III and IV. It would be more appropriate to require rational-number coefficients both in III and IV and in the definition of the rational basis. The arguments of ğğ 6 and 7 remain literally unchanged if the field K of all algebraic numbers is simply replaced by the field of all rational numbers.

[146] In contrast to linear and algebraic bases, the ordering of the elements matters here. For example, in the ordering η, $\sqrt[4]{\eta}$ both elements must be admitted, whereas in the reverse ordering only $\sqrt[4]{\eta}$ need be admitted.

[147] Compare Zermelo, loc. cit., ğ 1.

[148] That this is a genuine condition follows, for example, because the two elements η, $\frac{1}{2\sqrt{\eta}}$ are not admissible as basis elements, whereas η, $\frac{1}{\sqrt{\eta}}$ are.

[149] For the most general admissible systems $\mathfrak{S}$, the statement in ğ 4 applies with "rational" in place of "algebraic."

ğ 7. Construction of the most general rational basis with side condition.

The results of the preceding section require a supplement. Although the *existence* of a rational basis with side condition for all numbers was proved there, no method was given for constructing one from a prescribed well-ordering. Because of the side condition, the construction is more involved when one starts with the field of all complex numbers rather than with a domain $\mathfrak{G}$.[150]

Place the field of all complex numbers under a well-ordering Ω. Elements of three kinds may then occur:

1. Elements y whose rationally integral adjunction to the preceding basis elements — recursively defined in 3. —[151] causes a nonintegral algebraic number to enter the resulting integrality domain. If no basis element precedes y, this domain consists of all integral polynomials in y. In particular, every nonintegral algebraic number is an element y, since the resulting integrality domain contains $y = \beta$.

2. Elements z that do not have property 1 but can be expressed rationally in terms of finitely many preceding numbers other than the y; thus they satisfy a relation $z = \varphi(\xi_1, \ldots, \xi_t)$, where φ is a rational function with coefficients in K and none of the ξ is a y. In particular, all algebraic integers α belong here, since they do not have property 1 and satisfy the relation $z = \alpha$.

3. Elements ϑ for which neither 1 nor 2 holds; these will be called basis elements. In particular, the first transcendental number ϑ_0 in the well-ordering is such a basis element: the integral polynomials in ϑ_0 cannot represent a nonintegral algebraic number, and ϑ_0 cannot depend rationally on the preceding algebraic numbers.

We shall now prove that the system Θ of all basis elements ϑ is a rational basis with side condition for all numbers.

Since no element y occurs among the ϑ, the integrality domain $[\Theta]$ cannot contain a nonintegral algebraic number; thus the side condition is satisfied. Since no element z occurs among the ϑ either, every ϑ is rationally independent of the preceding basis elements. Exactly as in ğ 6, the induction argument further shows that every relation $z = \varphi(\xi)$ in which none of the ξ is a y entails a relation $z = \psi(\vartheta)$. Hence all elements z can be expressed rationally in the ϑ.

It remains to prove the more difficult assertion that the y can likewise be expressed rationally in the ϑ. We first show that the y depend algebraically on the ϑ. By assumption, for each y there is at least one nonintegral algebraic number β admitting a representation

$$\beta = f_0(\vartheta) + f_1(\vartheta)y + \cdots + f_\chi(\vartheta)y^\chi, \tag{1}$$

where $f_0(\vartheta), \ldots, f_\chi(\vartheta)$ are polynomials in $[\Theta]$ and hence cannot represent nonintegral algebraic numbers. If y were algebraically independent of the ϑ, equation (1) would be an identity in y, giving $\beta = f_0(\vartheta)$ in contradiction to the properties of $[\Theta]$.

To deduce rational dependence from algebraic dependence, select from Θ an algebraic basis H of all elements of Θ. Since every y is an algebraic function of the ϑ, it is then also algebraically dependent on the η; thus $y = y(\eta)$ determines an algebraic extension field $(H, y(\eta))$ of (H). Because every η is also an element ϑ, the proof of rational dependence reduces to showing that every such field has a primitive element that is a rational function of the ϑ. More precisely, we shall show that multiplying $y(\eta)$ by a polynomial in the η makes it lose property 1, and hence turns it into such an element.

As is well known, only finitely many intermediate fields lie between (H) and (H, y). Let $\Omega_0 = (H), \Omega_1, \ldots, \Omega_\sigma$ be those among them that possess a primitive element expressible rationally in the ϑ, so that every element of the field is a rational function of the ϑ. This condition is always satisfied at least for $\Omega_0 = (H)$. Write the primitive function belonging to Ω_i as $\frac{g_i(\vartheta)}{h_i(\vartheta)}$, where g_i and h_i are polynomials in $[\Theta]$. Then, for a suitably chosen integer α_i, the polynomial in $[\Theta]$

$$\xi_i = g_i(\vartheta) + \alpha_i h_i(\vartheta)$$

[150] In ğ 6 b), it would suffice to let Θ range only over those special rational bases that consist of an algebraic basis together with algebraically integral functions of the basis elements; the side condition is then satisfied automatically. To see this, one need only use ğ 6 to extend an algebraic basis selected from $\mathfrak{G}$ to a rational basis, and then multiply each nonintegral algebraic function of the η in the resulting basis by a suitably chosen polynomial in the η; this preserves the basis property. The same construction transfers unchanged to the field of all complex numbers. The question arising from ğ 6 concerning the most general rational basis with side condition is, however, also of independent interest.

[151] The induction argument shows that such a recursive definition is possible.

is a primitive function of Ω_i, or of an algebraic field over Ω_i,[152] and every function $\psi(\eta)$ in Ω_i admits a representation

$$\psi(\eta) = \frac{a_1(\eta)\xi_i^{\kappa-1} + a_2(\eta)\xi_i^{\kappa-2} + \cdots + a_\kappa(\eta)}{a(\eta)} = \frac{A(\eta, \xi_i)}{a(\eta)}, \tag{2}$$

where $a(\eta), a_1(\eta), \ldots, a_\kappa(\eta)$ are integral polynomials in the η; consequently $A(\eta, \xi_i)$ and $a(\eta)$ are elements of $[\Theta]$.

By (2), the irreducible equation satisfied by y over Ω_i has the form

$$f^{(i)}(\eta)y^{\lambda_i} + f_1^{(i)}(\eta, \xi_i)y^{\lambda_i-1} + \cdots + f_{\lambda_i}^{(i)}(\eta, \xi_i) = 0,$$

and all its coefficients belong to $[\Theta]$. The function $y_i = f^{(i)}(\eta)\cdot y$ then satisfies the following equation, likewise irreducible over Ω_i:

$$y_i^{\lambda_i} + f_1^{(i)}(\eta, \xi_i)y_i^{\lambda_i-1} + \cdots + \left(f^{(i)}(\eta)\right)^{\lambda_i-1} f_{\lambda_i}^{(i)}(\eta, \xi_i) = 0,$$

It follows that y_i is algebraically integral over $[H, \xi_i]$; the same holds for the product of y_i with any polynomial in the η. In particular, the function

$$Y = f^{(0)}(\eta)f^{(1)}(\eta)\cdots f^{(\sigma)}(\eta)\cdot y \tag{3}$$

is algebraically integral over every domain $[H, \xi_i]$, by virtue in each case of the following equation, irreducible over Ω_i:

$$Y^{\lambda_i} + F_1^{(i)}(\eta, \xi_i)Y^{\lambda_i-1} + \cdots + F_{\lambda_i}^{(i)}(\eta, \xi_i) = 0 \qquad (i = 0, 1, \ldots, \sigma). \tag{4}$$

We now show that Y is the desired primitive element expressible rationally in the ϑ. Suppose that an algebraic number γ is represented by Y and $[\Theta]$:

$$\gamma = k_0(\vartheta) + k_1(\vartheta)Y + \cdots + k_\nu(\vartheta)Y^\nu, \tag{5}$$

where $k_0(\vartheta), \ldots, k_\nu(\vartheta)$ are polynomials in $[\Theta]$. Consider the irreducible equation satisfied by Y over the field generated by the coefficient domain in (5), $\mathfrak{K} = (H; k_0(\vartheta), \ldots, k_\nu(\vartheta))$. As is well known, this is the irreducible equation of Y over the intersection of $\mathfrak{K}$ and (H, Y), an intermediate field between (H) and (H, Y). By (3), (H, Y) is identical with (H, y). Moreover, every element of $\mathfrak{K}$, and hence every element of the intersection field, is expressible rationally in finitely many ϑ; the intersection field must therefore be one of $\Omega_0, \Omega_1, \ldots, \Omega_\sigma$, say Ω_τ. By (4), the desired irreducible equation consequently has degree λ_τ and is

$$Y^{\lambda_\tau} + F_1^{(\tau)}(\eta, \xi_\tau)Y^{\lambda_\tau-1} + \cdots + F_{\lambda_\tau}^{(\tau)}(\eta, \xi_\tau) = 0 \tag{6}$$

with coefficients that are polynomials from $[\Theta]$. By means of (6), equation (5) can be rewritten as

$$\gamma = K_0(\vartheta) + K_1(\vartheta)Y + \cdots + K_{\lambda_\tau-1}(\vartheta)Y^{\lambda_\tau-1}, \tag{7}$$

where $K_0(\vartheta), K_1(\vartheta), \ldots$ belong to $\mathfrak{K}$ and are at the same time polynomials in $[\Theta]$. Since γ is an algebraic number, (7) is a relation in Y of degree less than λ_τ and must therefore hold *identically* in Y. Hence

$$\gamma = K_0(\vartheta),$$

so γ belongs to $[\Theta]$ and is consequently an algebraic integer.

As γ ranges over all algebraic numbers representable by Y and $[\Theta]$, the intersection of (H, Y) with the corresponding field $\mathfrak{K}$ can range only over the fields $\Omega_0, \Omega_1, \ldots, \Omega_\sigma$, so all the preceding arguments remain valid. Thus *the rationally integral adjunction of* Y *to* $[\Theta]$ *cannot represent any nonintegral algebraic number.* Hence Y no longer has property 1; by 2 or 3, it is an element z or ϑ and is therefore expressible rationally in finitely many ϑ. By (3), the same holds for y: Θ *has been proved to be a rational basis of all numbers.* Conversely, placing Θ first in the well-ordering shows that every rational basis with side condition can be constructed according to 1, 2, and 3. We have therefore proved: *The construction given by 1, 2, and 3 yields the most general rational basis with side condition for all numbers.*

[152] Compare the end of ğ 5.

ğ 8. Classification of the domains $\mathfrak{G}$ and $\mathfrak{H}$ into classes.[153]

Alongside the question of the most general domains $\mathfrak{G}$ and $\mathfrak{H}$ arises the further question of the *essentially different* domains, which — in a sense to be made more precise below — cannot be generated by the same principle of construction. This leads to a classification of these domains into classes.

Two domains will be said to belong to the same class, or to be isomorphic, if their elements can be placed in one-to-one correspondence so that the sum and product of any two elements of one domain correspond to the sum and product of the corresponding elements of the other. It follows from this definition that under every isomorphism zero and unity correspond to themselves, and that every algebraic relation among finitely many elements is preserved for the corresponding elements, and conversely. Thus all rational numbers, as well as unity, correspond to themselves. The totality of the algebraic numbers — and likewise the totality of the algebraic integers — maps into itself, although an individual algebraic number may well correspond to one of its conjugates.

First observe that every domain in $\mathfrak{M}(\mathfrak{G})$, the totality of all domains $\mathfrak{G}$ containing a fixed algebraic basis H, is isomorphic to a domain in the totality $\mathfrak{M}^*(\mathfrak{G})$ associated with any other algebraic basis H^*. Indeed, the field of all complex numbers is obtained from every algebraic basis by algebraic extension and consequently has the same cardinality as the basis.[154] Thus H and H^* have the same cardinality, and the desired isomorphism is obtained by matching the basis elements η_i with η_i^*.[155] On the other hand, $\mathfrak{M}(\mathfrak{G})$ contains nonisomorphic, or essentially different, domains $\mathfrak{G}$, as the examples in ğğ 2, 3, and 5 show. Since an isomorphism preserves all algebraic relations, an algebraic basis must correspond to an algebraic basis; yet ğğ 2 and 3 showed that the functional and module domains possess no algebraic basis for which all the basis properties of the Zermelo domain hold. Since the functional domain of ğ 2 is closed under algebraic integrality, the subset $\mathfrak{M}(\mathfrak{H})$ likewise contains essentially different domains $\mathfrak{H}$.

We now show, in analogy with the basis construction, how to select from $\mathfrak{M}(\mathfrak{G})$ a subset $\mathfrak{L}(\mathfrak{G})$ whose domains $\mathfrak{G}$ are all essentially different, while every domain in $\mathfrak{M}(\mathfrak{G})$ — and hence every domain $\mathfrak{G}$ whatsoever — is isomorphic to a domain in $\mathfrak{L}(\mathfrak{G})$. Place $\mathfrak{M}(\mathfrak{G})$ under a well-ordering Ω. A domain $\mathfrak{G}$ in $\mathfrak{M}(\mathfrak{G})$ may then be isomorphic to a preceding domain, or it may not. The domains isomorphic to no preceding domain form a set $\mathfrak{L}(\mathfrak{G})$ which, by construction, contains only essentially different domains $\mathfrak{G}$. The induction argument further shows that every domain in $\mathfrak{M}(\mathfrak{G})$ is isomorphic to a domain in $\mathfrak{L}(\mathfrak{G})$. For if $\mathfrak{G}_1$ were the first domain for which this failed, then either $\mathfrak{G}_1$ would itself belong to $\mathfrak{L}(\mathfrak{G})$, or it would be isomorphic to a preceding domain $\mathfrak{G}_0$, which by hypothesis is isomorphic to a domain in $\mathfrak{L}(\mathfrak{G})$; the same would then hold for $\mathfrak{G}_1$. Since every domain $\mathfrak{G}$ belongs to some set $\mathfrak{M}^*(\mathfrak{G})$ and is therefore isomorphic to a domain in $\mathfrak{M}(\mathfrak{G})$, $\mathfrak{L}(\mathfrak{G})$ *represents the totality of the classes of domains* $\mathfrak{G}$.

Replacing the basis elements η in a domain $\mathfrak{G}$ in $\mathfrak{L}(\mathfrak{G})$ by the elements η^* of any other basis produces, as shown above, a domain isomorphic to $\mathfrak{G}$. Conversely, let $\mathfrak{G}^*$ be any domain isomorphic to some domain $\mathfrak{G}$ in $\mathfrak{L}(\mathfrak{G})$. If the basis elements η correspond to elements η^* of $\mathfrak{G}^*$, then the latter again form an algebraic basis, and $\mathfrak{G}^*$ contains the same algebraic functions of the η^* that $\mathfrak{G}$ contains of the η — or their conjugates. *Thus every domain isomorphic to* $\mathfrak{G}$ *is obtained by letting the algebraic basis* H *range over all possible algebraic bases in* $\mathfrak{G}$ *and in its conjugate domains over* (H)[156] *— whenever these conjugate domains differ from* $\mathfrak{G}$. From each fixed domain $\mathfrak{G}_i$ in $\mathfrak{L}(\mathfrak{G})$ one obtains in this way the class $\mathfrak{R}_i$, containing all and only the domains isomorphic to $\mathfrak{G}_i$, although each domain may occur more than once, or even infinitely often. By the procedure above, one can select from $\mathfrak{R}_i$ a subset $\mathfrak{R}_i^*$ that contains every domain isomorphic to $\mathfrak{G}_i$ exactly once. As $\mathfrak{R}_i^*$ ranges over all classes, one obtains the totality of all domains $\mathfrak{G}$, each exactly once. To characterize the class $\mathfrak{R}_i$, one may of course replace $\mathfrak{G}_i$ by any other member of the class from which all domains in $\mathfrak{R}_i$ can be derived as above. In summary:

A subset $\mathfrak{L}(\mathfrak{G})$ *can be selected from* $\mathfrak{M}(\mathfrak{G})$ *so that its domains* $\mathfrak{G}$ *correspond one-to-one, without repetition, to the totality of the classes. The class* $\mathfrak{R}_i$ *associated with* $\mathfrak{G}_i$ *is obtained by letting* H *range over every possible algebraic basis in* $\mathfrak{G}_i$ *and in its conjugates over* (H). *If* $\mathfrak{R}_i^*$ *denotes all mutually distinct domains in* $\mathfrak{R}_i$, *then, as* $\mathfrak{R}_i^*$ *ranges over all classes, the totality of all domains* $\mathfrak{G}$ *is obtained, each domain exactly once.*[157]

---

[153] Compare E. Steinitz, Algebraische Theorie der Körper, Crelle's Journal 137 (1910), especially ğğ 23 and 24. (Section 23 already proves the existence of an algebraic basis.)

[154] Steinitz, ğğ 23 and 24.

[155] This conclusion does not, of course, hold for the sets $\mathfrak{N}(\mathfrak{G})$ and $\mathfrak{N}^*(\mathfrak{G})$ associated with two rational bases Θ and Θ^*. Nor does the mutual rational expressibility of Θ and Θ^* imply that $\mathfrak{N}(\mathfrak{G})$ and $\mathfrak{N}^*(\mathfrak{G})$ are isomorphic; it does, however, establish an isomorphism between the fields (Θ) and (Θ^*).

[156] By II, the elements of these domains conjugate to $\mathfrak{G}$ can certainly be expressed rationally in the elements of $\mathfrak{G}$, but not necessarily as integral rational functions; the conjugate domains may therefore differ from $\mathfrak{G}$.

[157] Here $\mathfrak{M}(\mathfrak{G})$ is to be constructed according to ğğ 6 and 7: by ğ 7, extend an algebraic basis H to every rational basis Θ with side condition arising

The analogous statement holds for the domains $\mathfrak{H}$ of algebraically integral transcendental numbers.

ğ 9. An example of a countably infinite collection of classes of domains $\mathfrak{G}$.

The remarks on the constructions given in ğ 4 b) and ğ 6 b) show their cardinality to be that of all well-orderings, hence 2^c, where c is the cardinality of the continuum. This, however, gives no information about the cardinality of the totality of all domains $\mathfrak{G}$ when each domain is counted exactly once, and still less about the cardinality of all classes. To show at least that the number of classes is not finite, we give an example — analogous to those in ğ 5 — of countably infinitely many domains $\mathfrak{G}$ that will prove to be essentially different and therefore yield countably infinitely many classes.[158]

In analogy with ğ 5, (1), let the domain $\mathfrak{G}_\sigma$ consist of all elements

$$z \equiv a_0 + a_1(\eta) + \cdots + a_{\sigma-1}(\eta) \pmod{\mathfrak{M}_\sigma(\eta)}, \tag{1}$$

where the $a_i(\eta)$ are homogeneous forms of degree i in the η, and the module $\mathfrak{M}_\sigma$ has as a basis all power products of degree σ in the η[159]*, and as multipliers all integral algebraic functions of the η.* We show that under any isomorphism between two domains $\mathfrak{G}_\sigma$ and $\mathfrak{G}_\tau$ ($\sigma \neq \tau$), the modules $\mathfrak{M}_\sigma$ and $\mathfrak{M}_\tau$ must also correspond isomorphically; the impossibility will then follow readily.

Denote the indeterminates in $\mathfrak{G}_\tau$ by ξ, and let the elements $f(\eta)$ of $\mathfrak{G}_\sigma$ correspond to them under the isomorphism. Because the isomorphism is preserved under quotient formation, the domain $\mathfrak{G}_\xi$ of all integral algebraic functions of the ξ corresponds to a domain $\mathfrak{T}$ closed under algebraic integrality. This domain consists of all functions algebraically integral over the $f(\eta)$, and hence also integral algebraic in the η.

Suppose that the element (1) corresponds to an element of $\mathfrak{M}_\tau$. By the module property of $\mathfrak{M}_\tau$, the product of (1) with any element $\psi(\eta)$ of $\mathfrak{T}$ must then also belong to $\mathfrak{G}_\sigma$; in formulas:

$$(a_0 + a_1(\eta) + \cdots + a_{\sigma-1}(\eta))\psi(\eta) \equiv b_0 + b_1(\eta) + \cdots + b_{\sigma-1}(\eta) \pmod{\mathfrak{M}_\sigma}. \tag{2}$$

Setting all the η equal to zero gives $a_0\psi(0) = b_0$, so (2) can be rewritten as

$$(a_0 + a_1(\eta) + \cdots + a_{\sigma-1}(\eta))(\psi(\eta) - \psi(0)) \equiv c_1(\eta) + \cdots + c_{\sigma-1}(\eta) \pmod{\mathfrak{M}_\sigma}. \tag{3}$$

Along with $\psi(\eta)$, the functions

$$\chi_\nu(\eta) = \sqrt[\nu]{\psi(\eta) - \psi(0)}$$

belong to $\mathfrak{T}$ for every ν. Since $\chi_\nu(0) = 0$, the formulas analogous to (3) are

$$(a_0 + a_1(\eta) + \cdots + a_{\sigma-1}(\eta))\chi_\nu(\eta) \equiv c_1^{(\nu)}(\eta) + \cdots + c_{\sigma-1}^{(\nu)}(\eta) \pmod{\mathfrak{M}_\sigma} \quad (\nu = 1, 2, \ldots). \tag{4}$$

Let $A(\eta)$, of degree λ, be the product of $\chi_1 = \psi(\eta) - \psi(0)$ and its $\kappa - 1$ conjugates. Since $\chi_1(0) = 0$, $A(\eta)$ must begin with terms of degree at least one. Equation (4) gives

$$a_0\chi_\nu(\eta) \equiv 0 \pmod{\mathfrak{M}_1}; \qquad a_0^\nu\chi_1(\eta) \equiv 0 \pmod{\mathfrak{M}_\nu}; \qquad a_0^{\nu\kappa}A(\eta) \equiv 0 \pmod{\mathfrak{M}_{\nu\kappa}}, \tag{5}$$

and therefore, if $a_0 \neq 0$, the argument of ğ 3 gives $\lambda > \nu\kappa$. But the resulting inequality $\nu < \frac{\lambda}{\kappa}$ for arbitrarily large ν contradicts the closure of $\mathfrak{T}$ under algebraic integrality. Hence necessarily $a_0 = 0$. Equation (4) now gives

$$a_1(\eta)\chi_\nu(\eta) \equiv c_1^{(\nu)}(\eta) \pmod{\mathfrak{M}_2}; \qquad [a_1(\eta)]^{\nu\kappa}A(\eta) \equiv [c_1^{(\nu)}(\eta)]^{\nu\kappa} \pmod{\mathfrak{M}_{\nu\kappa+1}}, \tag{6}$$

Since $A(\eta)$ begins with terms of degree at least one, this implies $c_1^{(\nu)}(\eta) = 0$. Thus, in complete analogy with (5), for every ν,

$$a_1(\eta)\chi_\nu(\eta) \equiv 0 \pmod{\mathfrak{M}_2}; \qquad [a_1(\eta)]^{\nu\kappa}A(\eta) \equiv 0 \pmod{\mathfrak{M}_{2\nu\kappa}},$$

and hence $a_1(\eta) = 0$. Continuing in this way, alternating applications of (5) and (6) give

$$a_0 = 0, \qquad a_1(\eta) = 0, \quad \ldots, \quad a_{\sigma-1}(\eta) = 0.$$

from it, and for each Θ form, by ğ 6 b), the totality $\mathfrak{N}(\mathfrak{G})$ of all domains $\mathfrak{G}$ containing Θ.

[158] The domains $\mathfrak{G}$ of ğ 6 likewise yield countably infinitely many classes, but the proof is somewhat more complicated.

[159] Naturally, only finitely many power products of the η occur in the module for any individual z.

Since the analogous argument also applies to $\mathfrak{G}_\tau$, it follows that *under every isomorphism between* $\mathfrak{G}_\sigma$ *and* $\mathfrak{G}_\tau$ $(\sigma \neq \tau)$*, the modules* $\mathfrak{M}_\sigma$ *and* $\mathfrak{M}_\tau$ *correspond isomorphically.*

Suppose, for example, that $\sigma > \tau$. The elements $f(\eta)$ of $\mathfrak{G}_\sigma$ correspond to the indeterminates ξ. Since every element of $\mathfrak{G}_\tau$ can be represented by a polynomial in the ξ modulo $\mathfrak{M}_\tau$, the correspondence between $\mathfrak{M}_\tau$ and $\mathfrak{M}_\sigma$ implies that every element of $\mathfrak{G}_\sigma$ is a polynomial in the $f(\eta)$ modulo $\mathfrak{M}_\sigma$. Because $\sigma > \tau \geq 1$, the indeterminates η certainly do not belong to $\mathfrak{M}_\sigma$. They are therefore expressible as integral rational functions of the $f(\eta)$ modulo $\mathfrak{M}_\sigma$, so at least one $f(\eta)$ must have nonvanishing linear terms. Thus suppose

$$\xi : f(\eta) \equiv a_0 + a_1(\eta) \pmod{\mathfrak{M}_2} \quad [a_1(\eta) \neq 0],$$

$$\xi^\tau : [f(\eta)]^\tau \equiv a_0^\tau \pmod{\mathfrak{M}_1} \quad \text{for } a_0 \neq 0,$$

$$\equiv [a_1(\eta)]^\tau \pmod{\mathfrak{M}_{\tau+1}} \quad \text{for } a_0 = 0.$$

Now ξ^τ belongs to $\mathfrak{M}_\tau$, whereas $[f(\eta)]^\tau$ begins with nonvanishing terms of degree zero or τ and, since $\tau < \sigma$, cannot belong to $\mathfrak{M}_\sigma$. This contradicts the correspondence between $\mathfrak{M}_\sigma$ and $\mathfrak{M}_\tau$ derived above. The case $\tau > \sigma$ follows by interchanging η and ξ. We have therefore shown that $\mathfrak{G}_\sigma$ and $\mathfrak{G}_\tau$ are *nonisomorphic, or essentially different.* Thus *the domains* $\mathfrak{G}_i$ $(i = 1, 2, \ldots)$ *provide an example of countably infinitely many classes of domains* $\mathfrak{G}$*.*

Remark. Although every two domains $\mathfrak{G}_i$ are nonisomorphic, two such domains may nevertheless each be isomorphic to a subdomain of the other.[160] For example, let $\tau = 1$ and let σ be arbitrary:

$$\mathfrak{G}_1 : a_0 + \mathfrak{M}_1(\xi); \qquad \mathfrak{G}_\sigma : a_0 + a_1(\eta) + \cdots + a_{\sigma-1}(\eta) + \mathfrak{M}_\sigma(\eta).$$

The assignment $\xi = \eta$ makes $\mathfrak{G}_\sigma$ a proper subdomain of $\mathfrak{G}_1$. Conversely, the mutually one-to-one assignments $\xi = \eta^\sigma$ and $\eta = \sqrt[\sigma]{\xi}$ make $\mathfrak{G}_1$ a proper subdomain of $\mathfrak{G}_\sigma$. Thus every $\mathfrak{G}_i$ is also isomorphic to a proper subdomain of itself. In contrast to the notion of intersection, there is therefore no notion of an intersection class — that is, a class such that each of its domains is isomorphic to a proper subdomain of every domain in every other class — at least not a uniquely determined one.

ğ 10. The integral elements of an arbitrary field.

Provided that algebraic numbers are omitted from defining properties III and IV, the developments of the preceding sections have relied, for the domains $\mathfrak{G}$, only on the fact that the totality of the complex numbers forms a field.[161] For the domains $\mathfrak{H}$, they relied additionally on the algebraic closedness of this field. The results therefore admit a direct *generalization to the most general field*, abstractly defined, following Weber and E. Steinitz,[162] as "a system of elements with two operations, addition and multiplication, subject to the associative and commutative laws, connected by the distributive law, and admitting unrestricted and unique inverse operations."[163]

Every such field contains a unity element and hence the "prime field" generated from it by addition, multiplication, and their inverse operations. This prime field is either of the type of the rational numbers (characteristic 0) or of the type of the residue-class system modulo a prime p (characteristic p).[164] The *integral elements of the prime field* are then well defined as those obtained from unity by addition and subtraction. For a prime field of characteristic p, these integral elements already exhaust the prime field, so the prime field has no fractional elements. Every algebraically closed field contains an "absolutely algebraic field," obtained from the prime field by adjoining all elements algebraic over it; in characteristic 0, this is therefore of the type of the field of all algebraic numbers. The *algebraically integral elements of the absolutely algebraic field* are then well defined as all elements algebraically integral over the integral elements of the prime field, or equivalently over unity. Thus in characteristic p, the absolutely algebraic field likewise has no nonintegral algebraic elements. After these preliminary remarks, the definitions of "integral" and "algebraically integral" elements can be extended to arbitrary fields and, respectively, to algebraically closed fields: *The integral elements of a field* Ω *are defined as an integrality domain* $\mathfrak{G}$ *of elements of* Ω *whose quotient field*[165] *exhausts* Ω*, and which contains unity but no fractional element of the prime field.*

[160] This behavior can also occur for fields; compare Steinitz, loc. cit., conclusion.

[161] Only ğ 7 used the further assumption that the "prime field" of the rational numbers has infinitely many elements. When the prime field has only finitely many elements, however, that section simply drops out, as we shall see.

[162] Loc. cit., introduction.

[163] Only division by zero is excluded.

[164] Steinitz, ğ 4.

[165] That is, the field of all quotients of pairs of elements of $\mathfrak{G}$.

The algebraically integral elements of an algebraically closed field Ω are defined as an integrality domain $\mathfrak{H}$ of elements of Ω that is closed under algebraic integrality, whose quotient field exhausts Ω, and which contains unity but no nonintegral algebraic element of the absolutely algebraic field.

For fields of characteristic zero, the results obtained in the preceding sections apply verbatim, with the "algebraic numbers" replaced by the elements of the prime field or, respectively, of the absolutely algebraic field. In characteristic p, the results simplify considerably further: since the prime field has no fractional elements, the side condition on the rational basis and on the systems to be adjoined disappears entirely.[166] Thus: *The abstract definition admits as the integral elements of a field of characteristic p every integrality domain derived from an arbitrary rational basis, the field itself, and every integrality domain lying between such a domain and the field. Correspondingly, the algebraically integral elements of an algebraically closed field of prime characteristic may be any integrality domain closed under algebraic integrality that lies between the domain derived from an algebraic basis and the field itself — including both boundary domains.* Thus, for the most general fields of prime characteristic, as for their prime fields, the distinction between integral and fractional is blurred.

Erlangen, March 30, 1915.

[166] Compare the first note to this section.

10. The Functional Equations of the Isomorphic Mapping.

By

Emmy Noether in Göttingen.

Math. Ann. 77 (1916), pp. 536–545

Following Dedekind[*], by an *isomorphic mapping of the field* $\mathfrak{A}$ *onto a system* $\mathfrak{B}$—which subsequently also proves to be a field—one means *a single-valued correspondence such that to every element of* $\mathfrak{A}$ *there corresponds one and only one element of* $\mathfrak{B}$; *and such that to the sum, difference, product, and quotient of any two elements of* $\mathfrak{A}$ *there are always assigned the sum, difference, product, and quotient of the uniquely corresponding elements of* $\mathfrak{B}$.

Let such a mapping be effected by a function $f(z)$, which by the preceding is single-valued. If z then runs through all the elements $x, y, \ldots$ of the field $\mathfrak{A}$, the function $f(z)$ is characterized by the functional equations

$$(1)\quad f(x+y) = f(x) + f(y); \quad (2)\quad f(x-y) = f(x) - f(y);$$

$$(3)\quad f(x \cdot y) = f(x) \cdot f(y); \qquad (4)\quad f\left(\frac{x}{y}\right) = \frac{f(x)}{f(y)}.$$

In what follows, the most general single-valued solutions $f(z)$ *of these functional equations are to be given when* $x, y, \ldots$ *run through all real and complex numbers; that is, the most general function* $f(z)$ *that effects an isomorphic mapping of the field of all complex numbers.*[**] The solution for arbitrary fields follows in complete analogy.

G. Hamel[*] constructed the most general solutions of the functional equation (1) by means of a *linear* basis of all numbers. The construction given here for the solutions of (1) to (4)—and hence for the mapping function under which rational and algebraic operations are invariant—uses a *rational* and an *algebraic* basis of all numbers. After the isomorphic mapping is discussed more closely in 1, necessary conditions for $f(z)$ are given in 2; in 3 they are recognized as sufficient and lead to the actual construction.[**]—The solutions of (1) to (4), with the familiar exceptions $f(z) = z$ or $\overline{z}$, are discontinuous; in 4 it is further shown that they are "extremely discontinuous"—a fact that G. Hamel proved for the real solutions of (1), but that need not hold there in the complex domain.[***]

1. We first draw several consequences from the functional equations (1) to (4), directly for general fields $\mathfrak{A}$. By (1), single-valuedness implies $f(0) = 0$. If $f(y)$ does not vanish, then the original y cannot vanish either; the functional equations (1) to (4) therefore show that *the mapping system* $\mathfrak{B}$ *of all values* $f(z)$ *again forms a field.* Conversely, if the initial condition $f(0) = 0$ is prescribed, then (2) implies the single-valuedness of the function $f(z)$: *the requirement of single-valuedness and the initial condition* $f(0) = 0$ *are therefore equivalent.* From (4) it follows that $f(z)$ cannot vanish identically; from (3), further, that $f(z)$ vanishes only for $z = 0$. For from $f(y) = 0$ and $y \neq 0$, since z/y also belongs to $\mathfrak{A}$, it would follow that

$$f(z) = f\left(\frac{z}{y} \cdot y\right) = f\left(\frac{z}{y}\right) \cdot f(y) = 0,$$

and hence, in contradiction with (4), that $f(z)$ vanishes identically. Thus $f(x) = f(y)$ implies $x = y$; that is, to each value of $f(z)$ there also corresponds one and only one value of z: $f(z)$ *is a one-to-one function of* z.

---

[*] Cf., for example, Dirichlet–Dedekind, *Lectures on Number Theory* (4th ed.), Supplement XI, ğ 161. The term "isomorphic mapping" or "isomorphism", modeled on group theory, occurs only in the later literature; Dedekind speaks of the "permutations of a field".

[**] This question was raised to me on one occasion by Mr. Landau. As I subsequently noticed, part of the solutions already appears in H. Lebesgue, Sur les transformations ponctuelles, transformant les plans en plans, Atti Acad. Torino, 1906/07; and likewise implicitly in A. Ostrowski, Über einige Fragen der allgemeinen Körpertheorie, Crelle's Journal 143 (1913), ğ 2.

[*] G. Hamel: Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung: $f(x+y) = f(x)+f(y)$, Math. Ann. 60, p. 459 (1905).

[**] Cf. the parallel considerations in my paper: Die allgemeinsten Bereiche aus ganzen transzendenten Zahlen. Math. Ann. 77, p. 103 (1916), especially ğ 8 and ğ 10.

[***] Hamel's term "totally discontinuous" is used in a different sense in the rest of the literature.

As the functional equations show, the mapping effected by the inverse function is again isomorphic. Since every rational operation is composed of a finite number of additions, multiplications, and their inverses, one may also say: *The isomorphic mapping establishes a one-to-one correspondence between the elements of* $\mathfrak{A}$ *and those of* $\mathfrak{B}$, *such that all rational relations holding among any finite number of elements of* $\mathfrak{A}$,

$$F(x, y, \ldots, t) = 0,$$

are preserved in $\mathfrak{B}$, *and conversely.*

It should also be noted that for a field the function $f(z)$ is already characterized by the functional equations (1) and (3), the requirement that $f(z)$ not vanish identically, and the initial condition $f(0) = 0$. Indeed, (2) follows from (1) by replacing x by the element $(x - y)$ belonging to $\mathfrak{A}$; then (2) and $f(0) = 0$ give the single-valuedness of $f(z)$. As shown above, it follows further from (3), on replacing x by the element x/y belonging to $\mathfrak{A}$, that $f(y)$ cannot vanish for $y \neq 0$; this gives the validity of (4) and, at the same time, one-to-oneness. If instead of a field one starts from an integral domain $\mathfrak{J}$, then x/y need not belong to $\mathfrak{J}$, and one cannot infer one-to-oneness from (3). Here, however, the following most familiar formulation suffices: an isomorphic mapping is a *one-to-one* correspondence between the elements of $\mathfrak{J}$ and $\mathfrak{J}'$ such that sums always correspond to sums and products to products.[*)]

2. From now on, for simplicity, in place of $\mathfrak{A}$ let the underlying field be the field $\mathfrak{C}$ of all real and complex numbers. We must first discuss the systems of values assumed by $f(z)$. From (3) or (4) it follows that $f(1) = 1$, and thence, by the functional equations, for every *rational number* α, that $f(\alpha) = \alpha$; *thus every rational number corresponds to itself under the mapping.* Since an *algebraic number* β satisfies an irreducible equation with rational numerical coefficients $F(\beta, \alpha) = 0$, no. 1 and the preceding observation give $F(f(\beta), \alpha) = 0$; *every algebraic number therefore goes into itself or into one of its conjugates*, and by one-to-oneness the totality of algebraic numbers again corresponds to the field of all algebraic numbers. To determine the behavior of the *transcendental* numbers and at the same time separate the conjugate values, we take as basis a *rational basis of all numbers*[**)], that is, a system Θ of numbers ϑ that permits all numbers to be expressed rationally—with rational numerical coefficients[***)]—while under at least one well-ordering no basis number is rationally expressible in terms of finitely many preceding ones. The existence of this basis follows from the well-ordering theorem in exactly the same way as that of linear and algebraic bases.

Let $\mathfrak{C}$ be subjected to a well-ordering Ω. Then every number is either rationally expressible in terms of finitely many preceding ones, or is rationally independent of the preceding ones. The latter numbers form the basis Θ, and induction shows that every number is indeed rationally expressible in terms of finitely many ϑ's.

For every basis number ϑ, the "segment field $\mathfrak{K}(\vartheta)$" is defined as the set of all rational combinations of those basis numbers that precede ϑ in the well-ordering. The field $\mathfrak{R}$ of all rational numbers is to be regarded as the segment field of the first basis number. The number ϑ can behave in two ways with respect to $\mathfrak{K}(\vartheta)$: it can be algebraically dependent on $\mathfrak{K}(\vartheta)$, or algebraically independent of it. Since, by no. 1, all relations valid in $\mathfrak{C}$ are also valid in the mapping field, and conversely, the totality of values $f(\vartheta)$ corresponding to the ϑ's forms a basis of the mapping range, well-ordered by the well-ordering of Θ itself. In particular, the segment field $\mathfrak{K}(\vartheta)$ corresponds to the segment field $\mathfrak{K}(f(\vartheta))$; according as ϑ is algebraically dependent on, or independent of, $\mathfrak{K}(\vartheta)$, the same holds for $f(\vartheta)$ with respect to $\mathfrak{K}(f(\vartheta))$; and in the dependent case the irreducible equations for ϑ and $f(\vartheta)$ also correspond. The totality of those values ϑ that are in each case algebraically independent of $\mathfrak{K}(\vartheta)$ form—as induction again shows—an *algebraic basis of all numbers*[*)], that is, a system H of numbers η that permits all numbers to be expressed algebraically, while no algebraic relations hold among the η's themselves. To this algebraic basis H there corresponds in the mapping range another algebraic basis Z, which by one-to-oneness has the same cardinality as H—namely, the cardinality of the continuum, since algebraic extension is known not to increase cardinality.[**)] Once the values $f(\vartheta)$ are known, however, $f(z)$ is immediately obtained for every system of values, since $z = \psi(\vartheta)$ always implies $f(z) = \psi(f(\vartheta))$.

3. We now show that the necessary conditions found above actually provide the construction of $f(z)$. The basis Z, corresponding one-to-one to the algebraic basis H, is to be constructed and assigned to H as follows.

[*)] Cf., for no. 1, Dedekind, loc. cit., ğ 161.

[**)] Cf. my cited paper on "whole transcendental numbers", ğ 6.

[***)] By a "rational function" I shall always mean one whose coefficients are themselves rational numbers.

[*)] Cf. E. Zermelo: Über ganze transzendente Zahlen, ğ 1, Math. Ann. 75 (1914).

[**)] Cf. E. Steinitz: Algebraische Theorie der Körper. Crelle's Journal 137 (1910), ğ 24.

Choose a second well-ordering Ω', which supplies an algebraic basis Z' of all numbers; let Z, with elements ξ, be a subset of Z' having the same cardinality as Z', and hence as H. To each element η_i of H, assign one and only one correspondingly numbered ξ_i by stipulating that ξ_i be the *first*, in the well-ordering Ω', of all those elements of Z that have not been assigned to any element of H preceding η_i.

Now let $f(z)$ *be defined:*

(a) *for all rational numbers* α *by* $f(0) = 0$, $f(\alpha) = \alpha$;

(b) *for all quantities of the algebraic basis* H *by* $f(\eta_i) = \xi_i$;

(c) *for all remaining quantities* ϑ *of the rational basis* Θ*—those algebraically dependent on the segment field* $\mathfrak{K}(\vartheta)$*, and hence satisfying an equation* $F(\vartheta; \vartheta_{i_1} \cdots \vartheta_{i_\tau}) = 0$ *irreducible in* $\mathfrak{K}(\vartheta)$*—as a root of the equation* $F(f(\vartheta); f(\vartheta_{i_1}) \cdots f(\vartheta_{i_\tau})) = 0$;

(d) *for all remaining values* z*, which by the definition of* Θ *can be represented as* $z = \psi(\vartheta_{k_1} \cdots \vartheta_{k_\sigma})$*, by* $f(z) = \psi(f(\vartheta_{k_1}) \cdots f(\vartheta_{k_\sigma}))$.*)

To show that the function $f(z)$ so defined actually satisfies the functional equations (1) to (4), by no. 1 it suffices to prove this for (1) and (3), since $\mathfrak{C}$ is a field and $f(z)$, because of (a) and (b), cannot vanish identically and moreover satisfies the initial condition $f(0) = 0$. By means of the rational basis Θ, let $x, y, x + y$ be expressed as

$$x = \psi_1(\vartheta_1 \cdots \vartheta_t), \quad y = \psi_2(\vartheta_1 \cdots \vartheta_t), \quad (x + y) = \psi_3(\vartheta_1 \cdots \vartheta_t);$$

the proof that $f(z)$ satisfies the functional equation (1),

$$f(x) + f(y) - f(x + y) = 0,$$

is therefore, by (d), identical with showing that from

$$\psi_1(\vartheta) + \psi_2(\vartheta) - \psi_3(\vartheta) = \frac{H_1(\vartheta)}{H_2(\vartheta)} = 0$$

there always follows

$$\psi_1(f(\vartheta)) + \psi_2(f(\vartheta)) - \psi_3(f(\vartheta)) = \frac{H_1(f(\vartheta))}{H_2(f(\vartheta))} = 0,$$

where H_1, H_2 denote integral rational functions of their arguments. The functional equation (3) leads to exactly the same form of condition; hence the satisfaction of all the functional equations is identical with the following condition—which by nos. 1 and 2 is also necessary: for *every* integral rational function $H(\vartheta)$, from $H(\vartheta) = 0$ there always follows $H(f(\vartheta)) = 0$, and from $H(\vartheta) \neq 0$ there follows $H(f(\vartheta)) \neq 0$, the latter because a denominator occurs.

That this is indeed the case is shown by induction. Suppose that in $H(\vartheta_1 \cdots \vartheta_t)$, the basis quantity ϑ_t is the last in the well-ordering among $\vartheta_1 \cdots \vartheta_t$;**) then $H(\vartheta_1 \cdots \vartheta_t) = 0$ may be regarded as a relation satisfied by ϑ_t with respect to the segment field $\mathfrak{K}(\vartheta_t)$, and likewise $H(f(\vartheta_1) \cdots f(\vartheta_t)) = 0$ as a relation satisfied by $f(\vartheta_t)$ with respect to $\mathfrak{K}(f(\vartheta_t))$. If not all relations $H(\vartheta) = 0$ were also satisfied by $f(\vartheta)$, and conversely, then there would have to be a first basis quantity—say ϑ_0—for which at least one relation valid with respect to $\mathfrak{K}(\vartheta_0)$ failed to be preserved in the mapping field, or conversely, while the preceding segment fields $\mathfrak{K}(\vartheta_0)$ and $\mathfrak{K}(f(\vartheta_0))$ were isomorphic. In particular, by (a), the segment field of the first basis quantity of Θ, the field $\mathfrak{R}$ of all rational numbers, is isomorphic to its mapping field. Now suppose that $H(\vartheta_0)$ has the form

$$H(\vartheta_0) = a_0(\vartheta) \cdot \vartheta_0^\chi + a_1(\vartheta) \cdot \vartheta_0^{\chi-1} + \cdots + a_\chi(\vartheta),$$

where the $a_i(\vartheta)$ are quantities from $\mathfrak{K}(\vartheta_0)$. There are then two possibilities.

1) ϑ_0 is algebraically independent of $\mathfrak{K}(\vartheta_0)$. Then $H(\vartheta_0) = 0$ is satisfied identically in ϑ_0,*) so that $a_i(\vartheta) = 0$ for all coefficients and hence, by the isomorphism of $\mathfrak{K}(\vartheta_0)$ and $\mathfrak{K}(f(\vartheta_0))$, also $a_i(f(\vartheta)) = 0$. Thus $H(\vartheta_0) = 0$ always implies $H(f(\vartheta_0)) = 0$. Conversely, suppose that $H(f(\vartheta_0)) = 0$. Since ϑ_0, being algebraically independent of $\mathfrak{K}(\vartheta_0)$, belongs to the algebraic basis H, the number $f(\vartheta_0)$ belongs by (b) to

*) In (d), (a) is contained as a special case.

**) The expressions $H(\vartheta)$ that are of degree zero in the ϑ's go into themselves under the mapping and therefore need not be investigated further.

*) Because $x, y, \ldots$ can be expressed in terms of the ϑ's, this form of relation can very well occur.

the algebraic basis Z and is algebraically independent of $\mathfrak{K}(f(\vartheta_0))$. Thus all the $a_i(f(\vartheta))$ vanish, and by the isomorphism all the $a_i(\vartheta)$ vanish. It follows that $H(f(\vartheta_0)) = 0$ implies $H(\vartheta_0) = 0$, or that $H(\vartheta_0) \neq 0$ implies $H(f(\vartheta_0)) \neq 0$.

2) ϑ_0 is algebraically dependent on $\mathfrak{K}(\vartheta_0)$. Then $H(\vartheta_0)$ is divisible by the equation $F(\vartheta_0)$ irreducible with respect to $\mathfrak{K}(\vartheta_0)$; that is, identically in t,

$$H(t; a_i(\vartheta)) = F(t; \vartheta_i) \cdot G(t; \vartheta_i).$$

Since all the coefficients that occur belong to $\mathfrak{K}(\vartheta_0)$, the corresponding relation holds in the isomorphic field $\mathfrak{K}(f(\vartheta_0))$:

$$H(t; a_i(f(\vartheta))) = F(t; f(\vartheta)) \cdot G(t; f(\vartheta)).$$

But by (c), $f(\vartheta_0)$ was chosen to be a root of $F(t; f(\vartheta))$; hence $H(\vartheta_0) = 0$ implies $H(f(\vartheta_0)) = 0$.

Conversely, if $H(f(\vartheta_0)) = 0$, then the divisibility of $H(t; a_i(f(\vartheta)))$ by the function $F(t; f(\vartheta))$, irreducible with respect to $\mathfrak{K}(f(\vartheta_0))$, implies for the isomorphic field $\mathfrak{K}(\vartheta_0)$ the divisibility of $H(t; a_i(\vartheta))$ by $F(t; \vartheta)$. And since $F(t; f(\vartheta))$ arose from the irreducible equation for ϑ_0 by the isomorphic relation, and this relation is one-to-one, $F(t; \vartheta)$ necessarily represents the irreducible function whose root is ϑ_0. Thus $H(f(\vartheta_0)) = 0$ implies $H(\vartheta_0) = 0$, or $H(\vartheta_0) \neq 0$ implies $H(f(\vartheta_0)) \neq 0$.

Thus, from isomorphic segment fields $\mathfrak{K}(\vartheta_0)$ and $\mathfrak{K}(f(\vartheta_0))$, isomorphic fields again arise by adjoining ϑ_0 and $f(\vartheta_0)$, respectively; the assumption that this fails for some ϑ_0 leads to a contradiction. It is therefore proved that *the function $f(z)$ defined by (a) to (d) actually represents a solution of the functional equations (1) to (4), and, by 2, the most general one.*

All the arguments used in constructing $f(z)$ have used only the fact that the totality $\mathfrak{C}$ of all numbers forms a field; hence they hold for every abstractly defined field $\mathfrak{A}$. Here one should note that the field $\mathfrak{R}$ of rational numbers is replaced by the "prime field" of $\mathfrak{A}$, that is, by the field derived from the unit element of $\mathfrak{A}$ by the operations of addition and multiplication and their inverses. If, therefore, in (a) to (d) one replaces the rational numbers by the elements of the prime field, then *the function $f(z)$ so obtained effects the most general isomorphic mapping of an arbitrary abstractly defined field.*

4. It remains to show that the functions $f(z)$ defined for the field $\mathfrak{C}$ of all real and complex numbers—which, except for $f(z) = z$ or $\overline{z}$, are known to be discontinuous—are *extremely discontinuous*; that is, in every neighborhood of any real or complex number z_0 there are values z for which $f(z)$ comes arbitrarily close to any prescribed value Z_0. As G. Hamel proved loc. cit., this extreme discontinuity belongs to the *real* solutions $\varphi(x)$, defined for all *real* numbers, of the functional equation (1); but, as the examples below show, it need not belong to solutions defined on the complex numbers. Hamel argues as follows. If $\varphi(x)$ differs from $C \cdot x$, then there are at least two values of the linear basis[*)], say x_1 and x_2, such that $\varphi(x_1) : x_1 \neq \varphi(x_2) : x_2$; then the two equations

$$\alpha x_1 + \beta x_2 = a; \qquad \alpha\varphi(x_1) + \beta\varphi(x_2) = b$$

have a solution in real numbers α, β, and consequently a and b can be approximated arbitrarily closely by rational numbers α, β; because α, β are rational, however, $\alpha\varphi(x_1) + \beta\varphi(x_2)$ actually represents $\varphi(\alpha x_1 + \beta x_2)$. This argument fails for complex systems of values. In fact, one can also give solutions of (1) defined on the complex numbers that are discontinuous but not extremely discontinuous, for example

$$\varphi(z) = \varphi(x + iy) = \varphi(x) + i(y + \varphi(x)),$$

where $\varphi(x)$ denotes a real solution that is extremely discontinuous in the real domain; or, still more simply, $\varphi(z) = \varphi(x)$. In both cases the real part of $\varphi(z)$ is extremely discontinuous, while the imaginary part is determined by the real part.

This behavior, and at the same time the behavior of the function $f(z)$, becomes completely clear when one introduces the concept of rank. Put $z = x + iy$, $\varphi(z) = X + iY$, and call $\varphi(z)$ of rank four, three, two, or one, respectively, according as there exist no, one, two, or three linearly independent relations

$$c_1 x + c_2 y + c_3 X + c_4 Y = 0,$$

where, of course, the c's are real numbers.

[*)] The linear basis of all (real) numbers is given by a system of (real) numbers that permits all (real) numbers to be expressed linearly, with rational coefficients, while no linear relation with rational coefficients holds among any finite number of basis numbers.

1) Let $\varphi(z)$ have *rank four*. Then there exist at least four values of the linear basis, say z_1, z_2, z_3, z_4, such that the determinant

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ X_1 & X_2 & X_3 & X_4 \\ Y_1 & Y_2 & Y_3 & Y_4 \end{vmatrix}$$

does not vanish. The equations

$$\begin{aligned} \alpha x_1 + \beta x_2 + \gamma x_3 + \delta x_4 &= a, \\ \alpha y_1 + \cdot \ \cdot \ \cdot + \delta y_4 &= b, \\ \alpha X_1 + \cdot \ \cdot \ \cdot + \delta X_4 &= A, \\ \alpha Y_1 + \cdot \ \cdot \ \cdot + \delta Y_4 &= B \end{aligned}$$

therefore have a solution in real numbers $\alpha, \ldots, \delta$, and a, b, A, B can be approximated arbitrarily closely by rational numbers $\alpha, \beta, \gamma, \delta$. Moreover,

$$\alpha(X_1 + iY_1) + \beta(X_2 + iY_2) + \gamma(X_3 + iY_3) + \delta(X_4 + iY_4) = \varphi(\alpha z_1 + \beta z_2 + \gamma z_3 + \delta z_4).$$

Thus, "in general", the solutions $\varphi(z)$ are extremely discontinuous also in the complex domain; the *discontinuity values* of $\varphi(z)$ in the neighborhood of $z_0 = a + ib$ *form a two-dimensional linear manifold.*

2) Let $\varphi(z)$ have *rank three*. Then there are at least three systems of values of the linear basis, say z_1, z_2, z_3, such that the above determinant has rank three. The values a, b, A, B satisfying the relation

$$c_1 a + c_2 b + c_3 A + c_4 B = 0$$

and only these can be approximated arbitrarily closely; the *discontinuity values* form a *one-dimensional linear manifold* determined by $z_0 = a + ib$. As the examples given show, this case can actually occur.

3) Let $\varphi(z)$ have *rank two*. Since one can always choose two complex numbers z_1, z_2 such that

$$\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \neq 0,$$

the relations have the form

$$X = \lambda_1 x + \lambda_2 y; \qquad Y = \mu_1 x + \mu_2 y.$$

The resulting expression

$$\varphi(z) = (\lambda_1 x + \lambda_2 y) + i \cdot (\mu_1 x + \mu_2 y)$$

is precisely the most general *continuous* solution of the functional equation (1) in the domain of complex numbers.

4) Let $\varphi(z)$ have *rank one*. This case cannot occur in the domain of complex numbers; in the domain of *real* numbers it gives the *continuous* solution $\varphi(x) = C \cdot x$.

We now show that the *solutions $f(z)$ of the functional equations (1) to (4), defined for all real and complex numbers, can have only rank two or rank four.* Here rank two gives only the two *continuous* functions $f(z) = z$ or $\overline{z}$, as follows by combining 3) with the specializations $f(1) = 1$ and $f(i) = \pm i$. Since rank one has already been excluded, it remains to exclude rank three. We therefore assume that at least one relation exists,

$$c_1 x + c_2 y + c_3 X + c_4 Y = 0,$$

so that $f(z)$ has rank three, or possibly lower rank, and show that under this assumption the latter case always occurs. As again follows from the specializations $f(1) = 1$, $f(i) = \pm i$, the relation becomes

$$c_3(X - x) + c_4(Y \mp y) = 0,$$

where c_3 and c_4 do not both vanish. First suppose, say, that $c_4 = 0$. The relation $(X - x) = 0$ then means that to a purely imaginary z there also corresponds a purely imaginary $f(z)$. Thus for every real y, $f(iy) = i \cdot \mathfrak{Y}$, where $\mathfrak{Y}$ is again real. But since

$$f(iy) = \pm i f(y) \quad \text{also} \quad f(y) = \pm \mathfrak{Y},$$

it follows that to every real z there also corresponds a real $f(z)$; and because of $(X - x)$, all real values go into themselves. Thus one has only $f(z) = z$ or $\overline{z}$, and hence actually rank two. The conclusion is entirely analogous when $c_3 = 0$, $c_4 \neq 0$.

Now let c_3 and c_4 both be nonzero, so that the relation can be written in the form

$$(Y \mp y) = c \cdot (X - x)$$

with real, nonzero, finite c. This means that for $y = \pm cx$, one also has $Y = c \cdot X$. Hence, taking account of the functional equations, for every real x,

$$f(x \cdot (1 \pm ic)) = \mathfrak{X}(1 + ic) = f(x) \cdot (1 + if(c)),$$

where $\mathfrak{X}$ is again real. But by no. 1 the factor of $f(x)$ cannot vanish identically, and division gives

$$f(x) = \mathfrak{X}(\sigma + i\tau)$$

with real σ and τ, independent of x and $\mathfrak{X}$. In particular, to $x = 1$ there also belongs a real X_0, and the condition $1 = X_0(\sigma + i\tau)$ shows that necessarily $\tau = 0$, so that $f(x) = \sigma \cdot \mathfrak{X}$. Thus to every real z there also corresponds a real $f(z)$; equivalently, $y = 0$ necessarily implies $Y = 0$. Hence the linear relation for real z becomes $X - x = 0$;[*)] every real value corresponds to itself. One again has only $f(z) = z$ or $\overline{z}$, and hence actually rank two. Rank three is thereby excluded in all cases. Since, however—as the investigations of the first sections show—discontinuous solutions do in fact exist, and must therefore necessarily have rank four, the following theorem holds by 1): *"All solutions"* $f(z)$ of the functional equations (1) to (4)—with the exception of the continuous solutions $f(z) = z$ or $\overline{z}$—are extremely discontinuous in the real and in the complex domain.[**)]

Erlangen, 30 October 1915.

[*)] Here one uses the fact that $c \neq 0$, so that neither c_3 nor c_4 vanishes, whereas above only $c_4 \neq 0$ was used; therefore the case in which one of these two vanishes had to be dealt with first.

[**)] Lebesgue shows loc. cit. that the real and imaginary parts of $f(z)$ are both "non-measurable" functions of x and y; as the example at the beginning of no. 4, $\varphi(z) = \varphi(x) + i(y + \varphi(x))$, shows, this does not yet imply extreme discontinuity in the complex domain.

11. Equations with Prescribed Group.

By

Emmy Noether in Göttingen,

Math. Ann. 78 (1918), pp. 221–229

The problem of constructing equations with prescribed group can be attacked in two directions, which may briefly be called the „irrational“ direction, characterizing the roots, and the „rational“ direction, characterizing the coefficients.

In the „irrational“ direction, which proceeds by function-theoretic and arithmetic methods, lies Kronecker's theorem that all Abelian fields in the domain of the rational numbers are cyclotomic fields, together with the corresponding theorems for relatively Abelian fields over quadratic number fields. On the one hand, these theorems establish the realizability of all Abelian groups over these special domains of rationality; on the other hand, they supply the totality of the equations and at the same time give a deeper insight into the structure of the number fields thereby defined. Each individual theorem, however, is restricted to a special domain of rationality, and every new domain of rationality requires an entirely new treatment.

The „rational“, algebraic direction rests on Hilbert's irreducibility theorem, according to which, in representing the coefficients, one may restrict oneself to a parametric representation. To this direction belongs, for example, the existence of arbitrarily many equations with alternating group over any prescribed domain of rationality. Here the insight described above into the structure of the fields defined by the equations is naturally absent; but the advantage of this „rational“ direction lies in the fact that the realizability of the groups is proved for *all domains of rationality simultaneously*. Nevertheless, the parametric representations known up to now do not in general yield the totality of the equations.[*)]

What follows is a contribution to the „rational“ direction. *Sufficient conditions* are given for the *existence of parametric representations that, for an arbitrary domain of rationality, supply the totality of equations with prescribed group*. These conditions consist in the requirement that the invariant field belonging to the group—Lagrange's genus domain—be rationally representable by *independent* functions of the domain, that it possess a „minimal basis“; or, expressed otherwise, that it be isomorphic to the field of all rational functions in n indeterminates. As will be shown in ğ 2, this condition is satisfied, for example, by all the groups occurring in equations of degrees 3 and 4. The actual construction and more detailed discussion of these equations of degrees 3 and 4 are found in the dissertation of F. Seidelmann,[*)] an extract from which immediately follows this communication.

The question of the minimal basis of Lagrange's genus domains was raised to me by E. Fischer—as already mentioned in the paper „Körper und Systeme rationaler Funktionen“ (Math. Ann. 76)—independently of the connection just described, and provided the impetus for the present investigations.[**)]

ğ 1.

Sufficient Conditions for the Parametric Representation.

1. The possibility of reducing the construction of equations with prescribed group to a parametric representation follows from Hilbert's irreducibility theorem, which says the following. Suppose the equation

$$(1) \quad f(x) = x^n + F_1(\lambda_1 \cdots \lambda_r)x^{n-1} + \cdots + F_n(\lambda_1 \cdots \lambda_r) = 0$$

—where $F_i(\lambda_1 \cdots \lambda_r)$ denotes rational functions of the independent parameters $\lambda_1 \cdots \lambda_r$, with coefficients from a number field[***)] Ω—has, over the field $\Omega(\lambda_1 \cdots \lambda_r)$ of all rational functions of $\lambda_1 \cdots \lambda_r$ with coefficients

[*)] For solvable equations, the parametric representation of the coefficients can be replaced by one of the roots. Recently F. Mertens has given, for certain groups of degree 8, the most general root representations: „Gleichungen 8ten Grades mit Quaternionengruppen“, Sitzb. d. Ak. d. Wiss., Wien, Abt. IIa, vol. 125, p. 735. As I gather from this note, G. Bucht had already given the most general root expressions for always constructible normal forms of equations of degrees 3 and 4 and of equations of degree 8 with the groups mentioned: „Über einige algebraische Körper achten Grades“, Arkiv for Math., Astron. och Physik, vol. 6, no. 30. [Addition in proof.]

[*)] Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich. Erlangen 1916.

[**)] Cf. Part 2 of the preliminary communication on „Rationale Funktionenkörper“, Jahresb. d. d. Math. Vereinig., vol. 22, 1913.

[***)] In place of the number field, a general domain of rationality could also occur.

from Ω, the group Γ. Then the parameters λ can be replaced by arbitrarily many rational numbers in such a way that the resulting numerical equation

$$(2) \quad g(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

has, over Ω, precisely the group Γ. Such a $g(x)$ will be denoted more precisely by g_Γ.

The question now is whether *such a parametric representation* (1) *can be given that the resulting numerical equation* (2) *runs through the totality of all* g_Γ *when* $\lambda_1 \cdots \lambda_r$ *run through all quantities from* Ω—with the exclusion of those quantities from Ω that cause a reduction of the group.[*)] In other words, the nonlinear system of equations

$$(3) \quad F_1(\lambda_1 \cdots \lambda_r) = a_1; \quad \cdots; \quad F_n(\lambda_1 \cdots \lambda_r) = a_n$$

should have, for every system of values $a_1 \cdots a_n$ corresponding to a g_Γ, a solution in quantities $\lambda_1 \cdots \lambda_r$ from Ω. Since the system (3) is nonlinear, a restriction must be introduced from the outset when one requires the totality of the g_Γ to be obtained through a parametric representation. Indeed, in such nonlinear systems there can always occur singular systems of values $a_1 \cdots a_n$, satisfying an algebraic relation $H(a_1 \cdots a_n) = 0$, for which *no* solution exists;[**)] for them the parametric representation (1) fails and a supplementary representation becomes necessary. In the present case, however, these singular values of $a_1 \cdots a_n$ can, as will be shown, be characterized simply.

2. To obtain such a parametric representation, we impose the stronger requirement that the λ_i be *natural irrationalities belonging to the group, identically in the roots regarded as indeterminates.* By this we mean the following. If, in (1), the parameters $\lambda_1 \cdots \lambda_r$ are replaced by suitably chosen *rational* functions $\varphi_1(x) \cdots \varphi_r(x)$ of the indeterminates $x_1 \cdots x_n$—with coefficients from Ω—then (1) is to pass into

$$(4) \quad h(x) = x^n - \sigma_1(x) x^{n-1} + \sigma_2(x) x^{n-2} \cdots \pm \sigma_n(x)$$

—where $\sigma_1(x) \cdots \sigma_n(x)$ denote the elementary symmetric functions of $x_1 \cdots x_n$—and $h(x)$ is to have the group Γ over the domain of rationality $\Omega(\varphi_1(x) \cdots \varphi_r(x))$ thereby arising from $\Omega(\lambda_1 \cdots \lambda_r)$. Because of the independence of the parameters, $\varphi_1(x) \cdots \varphi_r(x)$ are also to be algebraically independent functions.

To make this requirement precise, the connection between $\Omega(\varphi_1(x) \cdots \varphi_r(x))$ and the group Γ must be clarified. For this purpose, we first determine the most general domain of rationality K over which $h(x)$ becomes h_Γ. Let Ω_Γ denote the field of all rational functions of $x_1 \cdots x_n$ with rational-number coefficients that admit Γ—also called the „Lagrange genus domain“ belonging to Γ, or the invariant field of Γ—and let $\Omega(\Omega_\Gamma)$ denote the corresponding field arising by adjoining Ω_Γ to Ω. Thus Ω_Γ is a subfield of the field $\mathfrak{R}(x_1 \cdots x_n)$ of all rational functions of $x_1 \cdots x_n$ with rational-number coefficients. According to the definition of the group, the most general domain K is then given by *any field that contains* Ω_Γ *as a subfield and whose intersection with* $\mathfrak{R}(x_1 \cdots x_n)$ *is exactly* Ω_Γ. Correspondingly, for every domain K containing Ω, its intersection with $\Omega(x_1 \cdots x_n)$ is $\Omega(\Omega_\Gamma)$. In particular, since by our requirement $\Omega(\varphi_1(x) \cdots \varphi_r(x))$ is a domain K, its intersection with $\Omega(x_1 \cdots x_n)$ is $\Omega(\Omega_\Gamma)$. On the other hand, since $\Omega(\varphi_1(x) \cdots \varphi_r(x))$ is a subfield of $\Omega(x_1 \cdots x_n)$, it is exactly equal to $\Omega(\Omega_\Gamma)$. The requirement therefore says that *Lagrange's genus domain* $\Omega(\Omega_\Gamma)$ *is to arise by adjoining the algebraically independent functions* $\varphi_1(x) \cdots \varphi_r(x)$ *to* Ω; here one must have $r = n$, since Ω_Γ contains the n algebraically independent elementary functions, while on the other hand no more than n functions can be algebraically independent. We shall say that $\varphi_1(x) \cdots \varphi_n(x)$ form a *minimal basis* of $\Omega(\Omega_\Gamma)$; or also that Ω_Γ possesses a minimal basis with coefficients from Ω.

3. It is now essential that this whole argument can be reversed, and thus actually leads to sufficient conditions[*)] for the desired parametric representation. We therefore assume that $\varphi_1(x) \cdots \varphi_n(x)$ is a minimal basis of $\Omega(\Omega_\Gamma)$; and let Ω be the smallest field containing the coefficients of $\varphi_1(x) \cdots \varphi_n(x)$. Then Ω is necessarily an algebraic number field and can in particular be the field $\mathfrak{R}$ of all rational numbers. Since $\sigma_1(x), \ldots, \sigma_n(x)$ belong to $\Omega(\Omega_\Gamma)$, there exist identities in $x_1 \cdots x_n$—where the F_i denote rational functions of their arguments:

$$(5) \quad \sigma_1(x) = F_1(\varphi_1(x) \cdots \varphi_n(x)); \quad \cdots; \quad \sigma_n(x) = F_n(\varphi_1(x) \cdots \varphi_n(x));$$

whereas conversely $\varphi_1(x) \cdots \varphi_n(x)$, and hence also $\varphi(x) = \mu_1 \varphi_1(x) + \cdots + \mu_n \varphi_n(x)$, depend algebraically on $\sigma_1(x) \cdots \sigma_n(x)$ by means of the equation irreducible over $\Omega(\sigma_1(x) \cdots \sigma_n(x))$,

$$(6) \quad G(\varphi(x); \sigma_1(x) \cdots \sigma_n(x)) = 0,$$

[*)] The occurrence of a double root of $g(x) = 0$ is also to be included here.

[**)] This will shortly be developed in general in a paper on the „alternative in nonlinear systems of equations.“

[*)] The requirement in 2 was strengthened relative to 1, so that the conditions need not be necessary.

which is again an identity in the x.

By virtue of (5), this identity (6) becomes

$$(7)\quad G(\varphi(x); F_1(\varphi_1 \cdots \varphi_n); \cdots ; F_n(\varphi_1 \cdots \varphi_n)) = H(\varphi_1(x) \cdots \varphi_n(x)) = 0;$$

and because of the algebraic independence of $\varphi_1(x) \cdots \varphi_n(x)$, (7) holds not only identically in x, but also identically in the φ_i; that is, identically in independent parameters λ,

$$(8)\quad H(\lambda_1 \cdots \lambda_n) = G(\mu_1\lambda_1 + \cdots + \mu_n\lambda_n; F_1(\lambda_1 \cdots \lambda_n); \cdots ; F_n(\lambda_1 \cdots \lambda_n)) = 0.$$

From the identity (8) it follows that the equation

$$(9)\quad f(x) = x^n - F_1(\lambda_1 \cdots \lambda_n)x^{n-1} + F_2(\lambda_1 \cdots \lambda_n)x^{n-2} \cdots \pm F_n(\lambda_1 \cdots \lambda_n) = 0$$

has the group Γ *over* $\Omega(\lambda_1 \cdots \lambda_n)$. For this identity shows that the rationally known $\lambda = \mu_1\lambda_1 + \cdots + \mu_n\lambda_n$ is a function of the roots belonging to Γ; but no further function belonging to a subgroup of Γ can be rationally known, as the substitution $\lambda_i = \varphi_i(x)$ shows, while under the same substitution λ is also distinct from all its conjugates. If, further, Ω^* is any number field containing Ω, then $f(x)$ *has the group* Γ *over* $\Omega^*(\lambda_1 \cdots \lambda_n)$; for by 2 the group is not reduced under the substitution $\lambda_i = \varphi_i(x)$ even after Ω^* is adjoined.

It remains to prove that, in the sense modified in 1, $f(x)$ actually runs through the totality of all g_Γ. For this, observe that by (5) the $F_i(\lambda)$ are algebraically independent functions of their arguments λ. The system of equations

$$(10)\quad F_1(\lambda_1 \cdots \lambda_n) = -a_1; \quad F_2(\lambda_1 \cdots \lambda_n) = a_2; \quad \cdots ; \quad F_n(\lambda_1 \cdots \lambda_n) = \pm a_n$$

therefore possesses solutions for every arbitrary system of values $a_1 \cdots a_n$—with the exception of the singular ones still to be specified. For every system of values $a_1 \cdots a_n$ corresponding to a g_Γ over Ω^*, the corresponding λ_i, as natural irrationalities belonging to the group,*) become quantities from Ω^*. Thus, as $\lambda_1 \cdots \lambda_n$ run through all systems of values, $g(x)$ runs through the totality of all equations (in the modified sense); and this totality contains the totality of the g_Γ to which values from Ω^* correspond. Conversely, since by Hilbert's irreducibility theorem values λ from Ω^* „in general“ also correspond to equations g_Γ, the parametric representation (9) actually yields, in the sense modified in 1, the totality of all g_Γ over Ω^*.

It remains to determine the singular systems of values for which the parametric representation fails. Split into numerator and denominator, let the functions of the minimal basis be given by

$$\varphi_i(x) = \frac{\psi_i(x)}{\chi_i(x)}.$$

On substituting this into the identities (5), suppose that these identities become, without cancellation,

$$(11)\quad \sigma_k(x) = \frac{G_k(x)}{H_k(x)} \quad \text{or} \quad H_k(x) \cdot \sigma_k(x) = G_k(x),$$

so that the product over all $H_k(x)$ is divisible by the product of all denominators $\chi_i(x)$. For all root systems $\alpha_1 \cdots \alpha_n$ for which the product

$$H_1(\alpha) \cdot H_2(\alpha) \cdots H_n(\alpha) \neq 0$$

and consequently no denominator $\chi_i(\alpha)$ vanishes either, one can divide (11) by $H_k(\alpha)$ and obtains

$$(12)\quad \sigma_k(\alpha) = \frac{G_k(\alpha)}{H_k(\alpha)} = F_k(\varphi_1(\alpha); \cdots ; \varphi_n(\alpha)),$$

where, because the denominators do not vanish, the $\varphi_i(\alpha)$ assume finite values—and for equations g_Γ become quantities from Ω^*. Equation (12) represents the solution system of (10) as soon as $\alpha_1 \cdots \alpha_n$ are chosen so that $a_k = (-1)^k\sigma_k(\alpha)$.*)

*) Cf. also below!

*) The solution of the equation is thereby reduced to the solution of the system consisting of independent functions:

$$\varphi_1(\alpha_1 \cdots \alpha_n) = \lambda_1; \quad \cdots ; \quad \varphi_n(\alpha_1 \cdots \alpha_n) = \lambda_n.$$

Thus only such coefficient systems $a_k = (-1)^k \sigma_k(\alpha)$ can become *singular* for which

$$H_1(\alpha) \cdot H_2(\alpha) \cdots H_n(\alpha) = 0;$$

for these, (11), instead of becoming a representation, passes into $0 = 0$. A special investigation is then needed to determine whether among the singular $a_1 \cdots a_n$ so defined there are also some that correspond to equations g_Γ, and for which number fields.[**)] In summary, we obtain the

Theorem: If the Lagrange genus domain belonging to the group Γ *possesses a minimal basis*[***)] *with coefficients from* Ω*, then for every number field* Ω^* *containing* Ω*, the totality of equations with prescribed group* Γ *over* Ω^* *can be constructed rationally by the parametric representation (2)—possibly with the exception of those singular with respect to the parametric representation, which can be given separately. The parameters are to run through all values from* Ω^* *that do not cause a reduction of the group. The construction is possible for every number field if the coefficient field* Ω *of the minimal basis is equal to the field* $\mathfrak{R}$ *of all rational numbers.*

Since, by Hilbert's irreducibility theorem, the parameter manifold is not lowered by excluding those values from Ω^* that cause a reduction of the group, it follows further: *From the existence of a minimal basis it follows that the manifold of equations with group* Γ *over* Ω^* *is equal to the manifold of the affect-free equations; the manifold is not lowered by the affect.*

§ 2.

Application to Special Equations.

We now prove the existence of the minimal basis for all groups occurring in equations of degrees 3 and 4; for this purpose we first show quite generally that, for equations of degree n, the problem can be reduced to one in $n-2$ indeterminates. The first reduction corresponds to the linear Tschirnhaus transformation for removing the second-highest term. We take as our first basis function $\varphi_1(x) = \sigma_1(x)$, and further observe that Ω_Γ can be obtained rationally from all *homogeneous* forms in $x_1 \cdots x_n$ that admit Γ. Let $p(x_1 \cdots x_n)$ be such a form. Then

$$q(x) = p\left(x_1 - \frac{\sigma_1(x)}{n}; \cdots; x_n - \frac{\sigma_1(x)}{n}\right) = p\left(x_i - \frac{\sigma_1(x)}{n}\right) = p(y_i)$$

also belongs to Ω_Γ, since it admits Γ, and moreover

$$p(x) \equiv p\left(x_i - \frac{\sigma_1(x)}{n}\right) \bmod \sigma_1(x),$$

or

$$p(x) = q(x) + \sigma_1(x) \cdot p_1(x),$$

with $p_1(x)$ belonging to Ω_Γ and moreover of smaller dimension than $p(x)$. Continuing this procedure shows that all homogeneous forms from Ω_Γ—and hence all rational functions from Ω_Γ whatsoever—can be rationally expressed in terms of $\varphi_1(x) = \sigma_1(x)$ and homogeneous forms

$$q(x) = p\left(x_i - \frac{\sigma_1(x)}{n}\right) = p(y_i).$$

The quantities y_i, however, satisfy the linear relation $\sum y_i = 0$; thus the $q(x)$ *depend on only* $(n-1)$ *arguments.*

The second reduction rests on the fact that the $q(x)$ are homogeneous forms in their arguments. We take as our second basis function

$$\varphi_2(x) = \frac{\tau_3(x)}{\tau_2(x)}, \quad \text{where} \quad \tau_3(x) = \sigma_3\left(x_i - \frac{\sigma_1(x)}{n}\right) = \sigma_3(y_i), \quad \tau_2(x) = \sigma_2\left(x_i - \frac{\sigma_1(x)}{n}\right) = \sigma_2(y_i);$$

[**)] For example, as F. Seidelmann has shown loc. cit., equations corresponding to such singular systems of values occur only for the alternating group of equations of degrees 3 and 4, and only for those number fields Ω^* that contain the field of the third roots of unity. In each case a simple supplementary representation can be given.

[***)] From the existence of one minimal basis there follows immediately the existence of arbitrarily many, derivable from the original one by reversible rational transformations.

thus $\varphi_2(x)$ is a homogeneous fractional function of first degree in $(n-1)$ arguments, namely the y_i with $\sum y_i = 0$. By means of $\varphi_2(x)$, however, all $q(x)$ can be rationally expressed in terms of the functions, likewise belonging to Ω_Γ,

$$r(x) = \frac{q(x)}{\varphi_2(x)^\lambda} = \frac{q(x)\cdot\tau_2(x)^\lambda}{\tau_3(x)^\lambda} = \frac{p(y_i)\cdot\sigma_2(y_i)^\lambda}{\sigma_3(y_i)^\lambda},$$

where λ denotes the degree of $q(x)$. Thus $r(x)$ is homogeneous of degree zero and therefore depends only on $(n-2)$ arguments, the ratios $y_1 : y_2 : \cdots : y_n$ with $\sum y_i = 0$. Hence Ω_Γ can be expressed rationally in terms of

$$\varphi_1(x) = \sigma_1(x); \quad \varphi_2(x) = \frac{\tau_3(x)}{\tau_2(x)}$$

and the *field of all functions $r(x)$ from Ω_Γ depending on these $(n-2)$ arguments*,[*)] whereby the desired reduction is accomplished.

For equations of degrees 3 and 4, this yields in particular a reduction to function fields in one and two arguments, respectively. But for these a minimal basis always exists by the theorems of Lüroth and Castelnuovo.[**)] In fact, in the case of one indeterminate, the minimal basis can be obtained by rational operations and therefore, specifically for Ω_Γ, contains only rational-number coefficients. In the case of two indeterminates, according to Castelnuovo, one might still have a basis with coefficients from an algebraic number field Ω; the actual investigation (cf. F. Seidelmann, loc. cit.) shows that here too, for every Ω_Γ, one obtains a basis with rational-number coefficients. This can be seen almost without calculation from the fact that for the four-group such a rational-number basis can be chosen, namely

$$\varphi_1(x) = \sigma_1(x); \quad \varphi_2(x) = \frac{vw}{u}; \quad \varphi_3(x) = \frac{w\cdot u}{v}; \quad \varphi_4(x) = \frac{u\cdot v}{w},$$

where

$$u = x_1 + x_2 - x_3 - x_4; \quad v = x_1 - x_2 + x_3 - x_4; \quad w = x_1 - x_2 - x_3 + x_4,$$

and from the fact that the alternating group passes into the cyclic group of the three basis functions $\varphi_2, \varphi_3, \varphi_4$, while each group of order eight passes into the symmetric group of two of these functions, thereby effecting a reduction to the groups of equations of degrees 3 and 2. For the cyclic group, however, a rational-number basis is already known from Abel, although not formulated as such.[*)] Thus it is proved: *The totality of equations of degrees 3 and 4 with prescribed group—possibly with the exception of those singular with respect to the parametric representation—can be constructed rationally by parametric representation over any prescribed domain of rationality; their manifold is equal to the manifold of the affect-free equations.*

The actual investigation shows (cf. F. Seidelmann, loc. cit.) that a supplementary representation is needed only for the alternating group and only over domains of rationality containing the field of third roots of unity, whereas in all other cases the parametric representation supplies the totality without qualification.

It should also be noted that the minimal basis is known for all *Abelian groups*.[**)] Here, however, the basis has coefficients from the cyclotomic field derived from the group characters. Thus, in this case, no new results can be obtained for the construction of equations with prescribed group.

Göttingen, July 1916.

[*)] For an equation of degree n without a second term,

$$f(x) = x^n + a_2x^{n-2} + a_3x^{n-3} + \cdots + a_n = 0,$$

this second reduction corresponds to the substitution $y = \frac{x\cdot a_2}{a_3}$, which is always possible when $a_2 \neq 0$, $a_3 \neq 0$ and by which $f(x)$, up to a factor, becomes

$$g(y) = y^n + \frac{a_2^3}{a_3^2}y^{n-2} + \frac{a_2^3}{a_3^2}y^{n-3} + \frac{a_4\cdot a_2^4}{a_3^4}y^{n-4} + \cdots + a_n\frac{a_2^n}{a_3^n} = 0;$$

that is, an equation containing only $n-2$ parameters:

$$g(y) = y^n + c\cdot y^{n-2} + c\cdot y^{n-3} + c_4y^{n-4} + \cdots + c_n = 0.$$

[**)] J. Lüroth: Beweis eines Satzes über rationale Kurven, Math. Ann. 9 (1875); G. Castelnuovo: Sulla razionalità delle involuzioni piane, Math. Ann. 44 (1893). That a minimal basis need not exist for fields in more than two indeterminates was shown by F. Enriques by a counterexample, Rend. Acc. Linc., vol. 21, 21 Jan. 1912.

[*)] Cf. Weber, Algebra (small edition), ğ 93, formula (12).

[**)] E. Fischer: Die Isomorphie der Invariantenkörper der endlichen Abelschen Gruppen linearer Transformationen. Gött. Nachr. 1915, and Zur Theorie der endlichen Abelschen Gruppen. Math. Ann. 77 (1915).

12. Invariants of Arbitrary Differential Expressions.

12. Invariants of Arbitrary Differential Expressions.

By

Emmy Noether in Göttingen.

Nachr. v. d. Ges. d. Wiss. zu Göttingen 1918, pp. 37–44

Presented in the session of 25 January 1918 by F. Klein.

By a differential expression I mean a function $f(x;dx) = f(x_1,\dots,x_n;\, dx_1,\dots,dx_n)$ of the n variables $x_1,\dots,x_n$ and their differentials $dx_1,\dots,dx_n$, which is assumed to be analytic in both systems of n arguments, but not necessarily real. I now take as underlying group the group of all analytic transformations of the variables, to which corresponds the group of all linear transformations of the differentials:

$$x_i = x_i(y_1,\dots,y_n); \qquad dx_i = \sum_k \frac{\partial x_i}{\partial y_k}\, dy_k; \qquad \delta x_i = \sum_k \frac{\partial x_i}{\partial y_k}\, \delta y_k, \tag{1}$$

under which $f(x,dx)$ is to pass into $g(y,dy)$. By an invariant of $f(x,dx)$ I mean an invariant with respect to this group and the group thereby induced for the higher differentials $d^2x, d\delta x, \dots$ and for the derivatives of $f(x,dx)$; that is, an (analytic) function J such that, for arbitrary f, and by virtue of (1), the following identity holds in the variables and in all the differentials that occur:

$$J\left(f, \frac{\partial f}{\partial dx} \cdots \frac{\partial^{\rho+\sigma} f}{\partial x^\rho \partial dx^\sigma} \cdots dx, \delta x, d^2x, \dots\right) = J\left(g, \frac{\partial g}{\partial dy} \cdots \frac{\partial^{\rho+\sigma} g}{\partial y^\rho \partial dy^\sigma} \cdots dy, \delta y, d^2y, \dots\right)^{1)}.$$

In precisely the same way one defines the invariant of a simultaneous system of differential expressions. If, in particular, such an invariant contains only first differentials $dx, \delta x$, and only derivatives with respect to these differentials, not with respect to the variables, then the occurrence of the variables in the functions and the linear transformation of the differentials do not enter into consideration; these special invariants are invariants with respect to the group of all linear transformations of the differentials $dx, \delta x$ with indeterminate coefficients, and will be called projective invariants of the simultaneous system.

For quadratic homogeneous differential forms, Christoffel (Crelle 70) and Ricci (Math. Annalen 54) have constructed a system of invariant formations such that all invariants become projective invariants of this simultaneous system. The questions concerning the totality of the invariants and concerning equivalence are thereby reduced to questions of linear invariant theory; this is what I shall call the "reduction theorem." The complete system consists of countably infinitely many forms; but for invariants of any finite order ρ (that is, those containing no derivatives with respect to the variables higher than the ρ-th), it consists only of finitely many forms.

In what follows I prove the validity of the "reduction theorem" for arbitrary differential expressions. Here again one has a complete system of countably infinitely many invariant formations, but only finitely many of them for each finite order. Whereas Christoffel and Ricci base the generation of the invariants and the proof of the reduction theorem on eliminations that are difficult to survey, I generate the invariants directly by invariant differentiation and variation processes (the latter can simply be regarded as differentiation processes with respect to other parameters). Following Lagrange (*Mécanique analytique*, part 2, section IV),

---

[1)] $\frac{\partial^{\rho+\sigma} f}{\partial x^\rho \partial dx^\sigma}$ will throughout be used as an abbreviation for

$$\frac{\partial^{\rho+\sigma} f}{\partial x_{i_1} \cdots \partial x_{i_\rho} \partial dx_{k_1} \cdots \partial dx_{k_\sigma}},$$

where the indices denote any of the numbers 1 to n.

Riemann (Works XXII) and Lipschitz (Crelle 70, 72) developed the algorithm of these invariant differentiation processes for quadratic differential forms, without, however, advancing as far as the reduction theorem. The auxiliary tool for proving the reduction theorem is furnished by the "normal coordinates" introduced by Riemann for quadratic forms (Works XIII), which transform the extremals of the associated variational problem emanating from a point into straight lines, but exist only for homogeneous differential expressions: — $f(x, \varkappa \cdot dx) = \Phi(\varkappa) \cdot f(x, dx)$[1] The inhomogeneous case, however, can be reduced to this one.

I. Generation of Invariants.

A generally nonterminating sequence of projective invariants of $f(x, dx)$ is furnished by the polars. Because the transformation of the differentials is linear, from $f(x, dx) = g(y, dy)$ it also follows that $f(x, dx + \lambda\delta x) = g(y, dy + \lambda\delta y)$; expansion in λ then gives the relations characteristic of invariance:

(2)
$$\begin{gathered} f(dx) = g(dy), \\ f_\delta = \sum \frac{\partial f(dx)}{\partial dx}\,\delta x = \sum \frac{\partial g(dy)}{\partial dy}\,\delta y, \\ \vdots \\ f_{\delta^\sigma} = \sum \frac{\partial^\sigma f(dx)}{\partial dx^\sigma}\,\delta x^\sigma = \sum \frac{\partial^\sigma g(dy)}{\partial dy^\sigma}\,\delta y^\sigma, \\ \vdots \end{gathered}$$

Each polar, by application of a variation process $\bar\delta$, gives rise to a nonterminating sequence of general invariants:

(3)
$$\begin{gathered} \bar\delta^\rho f(x, dx) = \bar\delta^\rho g(y, dy), \\ \vdots \\ \bar\delta^\rho f_{\delta^\sigma} = \bar\delta^\rho \sum \frac{\partial^\sigma f(dx)}{\partial dx^\sigma}\,\delta x^\sigma = \bar\delta^\rho \sum \frac{\partial^\sigma g(dy)}{\partial dy^\sigma}\,\delta y^\sigma, \\ \vdots \\ (\rho = 0, 1, 2, \ldots) \end{gathered}$$

By virtue of (1), the relations (2) and (3) allow one to read off the transformation laws for the derivatives of $f(x, dx)$, although these will not be needed below. From the invariants (3), by linear combination, one can now obtain the "normal form of the ρ-th variation," which is found for $\rho = 1$ in Lagrange and for $\rho = 2$ in Riemann. It is characterized by the elimination of the mixed differentials of order $\rho + 1$, namely $d^\rho\delta, d^{\rho-1}\delta^2, \ldots$. One obtains:

(4)
$$\begin{gathered} \Omega_1 = \delta f(dx) - df_\delta(dx), \\ \Omega_2 = \delta^2 f - \delta df_\delta + \frac{1}{2} d^2 f_{\delta^2}, \\ \vdots \\ \Omega_\rho = \delta^\rho f - \delta^{\rho-1} df_\delta + \frac{1}{2}\delta^{\rho-2} d^2 f_{\delta^2} + \cdots + \frac{(-1)^\rho}{\rho!}\, d^\rho f_{\delta^\rho}, \\ \vdots \end{gathered}$$

From the invariants (4), by generalizing an ansatz of Riemann, one can now obtain invariants that contain only first differentials; such invariants will be called "fundamental functions." Namely, if in Ω_1 the differentials are replaced by the differential quotients, then $\Omega_1 = 0$ (identically in $\bar\delta x$) gives exactly the Lagrange equations of the variational problem associated with

$$f\left(\frac{dx}{dt}\right).$$

I now impose the invariant condition that the direction $(d + \lambda\delta)$ satisfy these Lagrange equations:

[1] It is easy to see that $\Phi(\varkappa) = \varkappa^c$, where c denotes an arbitrary real or complex quantity.

(5) $$\Omega_1(d+\lambda\delta) = \bar\delta f(dx+\lambda\delta x) - (d+\lambda\delta) f_{\bar\delta}(dx+\lambda\delta x) = 0,$$
(identically in $\bar\delta x$),

from which, by the substitution $\bar\delta = d + \lambda\delta$, there also follows for homogeneous $f(dx)$:

(6) $$(d+\lambda\delta) f(dx+\lambda\delta x) = 0,$$

except in the case of homogeneity of first order. In the latter case, (6) is to be added as a new condition, since then the system of equations (5) represents only $(n-1)$ independent conditions. If in (5), or in (5) and (6), respectively, one sets the coefficients of the zeroth, first, and second powers of λ equal to zero, one obtains three invariant systems of equations $\varphi = 0$, $\psi = 0$, $\chi = 0$ (identically in $\bar\delta x$), by means of which $d^2x, d\delta x, \delta^2 x$ can be expressed in terms of first differentials. The further invariant systems of equations

(7) $$d^\sigma\varphi = 0, \qquad d^\sigma\psi = 0, \qquad d^\sigma\chi = 0, \qquad d^{\sigma-1}\delta\chi = 0,$$
$$d^{\sigma-2}\delta^2\chi = 0, \ldots, \delta^\sigma\chi = 0 \qquad (\sigma = 0, 1, 2, \ldots)$$

then suffice precisely to express all higher differentials in terms of first ones.[1)] Thus the functions (4), combined with the invariant system of equations (7), lead to fundamental functions $[\Omega_\rho]$ containing only first differentials; moreover, $[\Omega_1]$ vanishes identically.

Similarly, from the differential $\delta h(dx, \delta x)$ of a fundamental function h, one can by means of (7) again obtain a fundamental function, which will be called the "covariant derivative" $[h^{(1)}]$ of h; in general, let $[h^{(\nu)}]$ denote the covariant derivative of $[h^{(\nu-1)}]$. These two processes thus lead to a doubly infinite sequence of fundamental functions:

(8)
$$\begin{array}{cccccc} [\Omega_2], & [\Omega_2^{(1)}], & [\Omega_2^{(2)}] & \ldots & [\Omega_2^{(\nu)}] & \ldots \\ \vdots & & & & \vdots & \\ [\Omega_\rho], & [\Omega_\rho^{(1)}], & \ldots & \ldots & [\Omega_\rho^{(\nu)}] & \ldots \\ \vdots & \vdots & & & \vdots & \end{array}$$

It further turns out that the left-hand sides of the equations expressing the higher differentials in terms of first ones are cogredient to the first differentials (that is, they undergo the same linear transformations). Thus, if instead of the higher differentials one introduces these left-hand sides $p, q, r, \ldots$ as arguments of the invariant, then, apart from the derivatives, it depends only on quantities cogredient to one another. The formation of the functions (8) indicated above amounts simply to introducing these new quantities; every invariant thereby becomes a sum of invariants, from which one selects the one that contains precisely $dx, \delta x$, but not $p, q, r, \ldots$.

It will be shown below that, under the homogeneity assumption

— $f(\varkappa \cdot dx) = \Phi(\varkappa) \cdot f(dx)$ —

the fundamental functions (8) exhaust the complete system sought.

II. Normal Coordinates, Equivalence, and the Reduction Theorem.

I arrive at the normal coordinates by integrating the variational problem associated with $f\left(\frac{dx}{dt}\right)$:

(9) $$\Omega_1 = \delta f\left(\frac{dx}{dt}\right) - \frac{d}{dt} f_\delta\left(\frac{dx}{dt}\right) = 0 \quad \text{(identically in } \delta x\text{)},$$
$$\frac{d}{dt} f\left(\frac{dx}{dt}\right) = 0 \quad \text{(as a consequence or additional condition)}.$$

Because of the assumed homogeneity of $f(dx)$, this system of equations goes into itself under the parameter substitution $t = \varkappa\cdot\tau$. Thus, if by means of (9) one expresses $\frac{d^\rho x_i}{dt^\rho}$ as a function $\varphi_\rho^{(i)}\left(\frac{dx}{dt}\right)$ of the first derivatives, then $\varphi_\rho^{(i)}$ is homogeneous of order ρ:

(10) $$\varphi_\rho^{(i)}\left(\varkappa \cdot \frac{dx}{dt}\right) = \varkappa^\rho \varphi_\rho^{(i)}\left(\frac{dx}{dt}\right).$$

[1)] Only the linear form $\sum A_i\, dx_i$ requires special treatment, since here the system of equations (5) contains no second differentials.

If, in integrating (9), one now prescribes for $t = t_0$ the initial values

$$x = (x)_0, \qquad \frac{dx}{dt} = \left(\frac{dx}{dt}\right)_0$$

and sets

$$u_i = (t - t_0)\left(\frac{dx_i}{dt}\right)_0, \tag{11}$$

—where, by virtue of $f\left(\frac{dx}{dt}\right) = \text{const.}$, the parameter $(t - t_0)$ becomes proportional to the "length of the extremal"—then the expansion in powers of $(t - t_0)$, by (10), gives

$$x_i - (x_i)_0 = u_i + \frac{1}{2}\varphi_2^{(i)}(u) + \cdots + \frac{1}{\rho!}\varphi_\rho^{(i)}(u) + \cdots \tag{12}$$

This expansion can be regarded as a transformation of variables $x_i = x_i(u)$, where the quantities u are precisely the Riemann normal coordinates. Thus, by (11) and (12), these coordinates transform the extremals passing through $(x)_0$ into straight lines. Moreover, to an arbitrary transformation of variables $x = x(y)$ there corresponds, by (11), a linear transformation $u = u(v)$ of the associated normal coordinates, where the coefficients depend only on the arbitrary system of values $(x)_0$; hence the differentials $du, \delta u$ undergo the same transformation as the u themselves.

By means of (12), let $f(x, dx)$ pass into $F(u, du)$; or, expanded in powers of the u,

$$F(u, du) = F_0(u, du) + F_1(u, du) + \cdots + F_\rho(u, du) + \cdots \tag{13}$$

where $F_\rho(u, du)$ denotes a homogeneous form of dimension ρ in u. Because the transformation $u = u(v)$ is linear, the identity $F(u, du) = G(v, dv)$ also carries the individual homogeneous components into the corresponding ones:

$$F_\rho(u, du) = G_\rho(v, dv). \tag{14}$$

Thus, if one takes any fixed constant system of values for $(x)_0$, (13) and (14) show that the equivalence of $f(dx)$ with $g(dy)$ is equivalent to the equivalence of the associated systems of functions $F_\rho(u, du)$ under linear transformation. Furthermore, the $F_\rho(u, du)$, or the corresponding $F_\rho(\delta u, du)$, represent invariants of $f(dx)$, taken at the point $x = (x)_0$; indeed, they form a complete system of fundamental functions for this point $x = (x)_0$. Namely,

$$F_\rho(\delta u, du) = \frac{1}{\rho!}\sum \frac{\partial F_\rho}{\partial \delta u^\rho}\,\delta u^\rho; \qquad \frac{\partial F_\rho}{\partial \delta u^\rho} = \left(\frac{\partial F(du)}{\partial u^\rho}\right)_0,$$

and this latter derivative can, by means of (12), be expressed in just the same way through derivatives of $f(dx)$, taken for $x = (x)_0$, as the correspondingly formed derivative of $G(dv)$ can be expressed through derivatives of $g(dy)$. Because

$$\left(\frac{\partial^{\rho+\sigma} F(du)}{\partial u^\rho \partial du^\sigma}\right)_0 = \frac{\partial^{\rho+\sigma} F_\rho(\delta u, du)}{\partial \delta u^\rho \partial du^\sigma}$$

every invariant of $f(dx) = F(du)$, taken at the point $x = (x)_0$, becomes a projective invariant of the $F_\rho(\delta u, du)$, once the higher differentials have been replaced by the $p, q, r, \ldots$ cogredient to $dx, \delta x$. But $(x)_0$ can now be regarded as a parameter; to every invariant at the point $x = (x)_0$ there corresponds an invariant of $f(dx)$, if only $(x)_0$ is replaced again by x. Thus, if the $F_\rho(\delta u, du)$ become invariants $\Psi_\rho(\delta x, dx)$, taken for $x = (x)_0$—for $x = (x)_0$, $du, \delta u$ pass into $dx, \delta x$—then the Ψ_ρ themselves form the fundamental functions of a complete system. It remains to express this system of fundamental functions by explicit invariants of $f(dx)$, namely by the functions (8). Their generation by differentiation processes shows that this is possible. For the terms of highest order, these processes become simple polarization processes, and a transformation analogous to the Clebsch–Gordan series expansion, combined with induction on account of the neglected terms, proves the assertion. If one is dealing with invariants of a simultaneous system, then the covariant derivatives of the remaining differential expressions must be added to the fundamental functions (8), as is shown by introducing into these expressions the normal coordinates belonging to $f(dx)$.

The equivalence of $f(dx)$ with $g(dy)$, which had been reduced to (14), is therefore also equivalent to the equivalence of the Ψ_ρ, or equally of the functions (8), under linear transformation of the differentials, without any special integrability conditions being required, as follows from the possibility of reduction to (14). Thus

the reduction theorem is proved in all its parts. In particular, the identical vanishing of the sequence of functions $[\Omega_2], [\Omega_3], \ldots, [\Omega_\rho], \ldots$ is necessary and sufficient for $f(dx)$ to be transformable into an expression with constant coefficients.

Finally, if instead of the group of all analytic transformations one takes a subgroup as the basis, then the group of the corresponding linear transformations of the u also becomes a subgroup of the projective group; the invariants of $f(dx)$ again become invariants of the functions (8) under linear transformation, but now with respect to this subgroup. Thus, by homogenizing, the case of nonhomogeneous functions $f(dx)$ can be reduced to the affine group; the complete system can here be derived from the functions (8) formed for one additional variable.

From the reduction theorem one obtains the special case of quadratic forms, and more generally of forms of p-th dimension, from the fact that here the system of functions terminates with $[\Omega_2]$, more generally with $[\Omega_p]$ and its covariant derivatives, since all later fundamental functions become projective invariants of these. This explains the distinguished position of the Riemannian curvature form $[\Omega_2]$ for quadratic forms. The question of the equivalence of quadratic forms, or of forms of p-th dimension, comes down precisely to the equivalence of $[\Omega_2]$, or of $[\Omega_2] \ldots [\Omega_p]$, and of their covariant derivatives under linear transformation; and the identical vanishing of $[\Omega_2]$, or of $[\Omega_2] \ldots [\Omega_p]$, is necessary and sufficient for transformation into forms with constant coefficients, which, for quadratic forms, states one of the best-known results.

A more detailed presentation is to appear shortly in the *Mathematische Annalen*.

13. Invariant Variational Problems.

13. Invariant Variational Problems.

(For F. Klein on the fiftieth anniversary of his doctorate.)

By

Emmy Noether in Göttingen.

Nachr. v. d. Ges. d. Wiss. zu Göttingen 1918, pp. 235–257

Presented by F. Klein in the session of 26 July 1918[1)].

The subject is variational problems that admit a continuous group (in Lie's sense); the consequences which arise from this for the corresponding differential equations find their most general expression in the theorems formulated in §1 and proved in the following sections. For these differential equations arising from variational problems, much more precise assertions can be made than for arbitrary differential equations admitting a group, which form the subject of Lie's investigations. What follows therefore rests on a combination of the methods of the formal calculus of variations with those of Lie group theory. For special groups and variational problems this combination of methods is not new; I mention Hamel and Herglotz for special finite groups, Lorentz and his students (for example Fokker), Weyl and Klein for special infinite groups.[167] In particular, the second note of Klein and the present developments have mutually influenced one another; for this I may refer to the closing remarks of Klein's note.

§1. Preliminaries and formulation of the theorems

All functions occurring below are to be assumed analytic, or at least continuous and continuously differentiable a finite number of times, and single-valued in the domain under consideration.

By a "transformation group" one understands, as usual, a system of transformations such that for each transformation there exists an inverse transformation contained in the system, and such that the composition

[1)] The final version of the manuscript was submitted only at the end of September.

[167] Hamel: *Math. Ann.* vol. 59 and *Zeitschrift f. Math. u. Phys.* vol. 50. Herglotz: *Ann. d. Phys.* (4) vol. 36, especially §9, p. 511. Fokker, Verslag d. Amsterdamer Akad., 27 Jan. 1917. For the further literature compare the second note of Klein: Göttinger Nachrichten, 19 July 1918. In a paper by Kneser that has just appeared (*Math. Zeitschrift* vol. 2), the issue is the construction of invariants by a similar method.

of any two transformations of the system again belongs to the system. The group is called a finite continuous $\mathfrak{G}_\rho$ when its transformations are contained in a most general transformation depending analytically on ρ essential parameters ε (that is, the ρ parameters are not to be representable as ρ functions of fewer parameters). Correspondingly, by an infinite continuous $\mathfrak{G}_{\infty\rho}$ one understands a group whose most general transformations depend on ρ essential arbitrary functions $p(x)$ and their derivatives, analytically or at least continuously and with a finite number of continuous derivatives. An intermediate case between the two is the group depending on infinitely many parameters but not on arbitrary functions. Finally, a mixed group denotes one that depends both on arbitrary functions and on parameters.[168]

Let $x_1, \ldots, x_n$ be independent variables, and let $u_1(x), \ldots, u_\mu(x)$ be functions depending on them. If one subjects the x's and u's to the transformations of a group, then, because the transformations are assumed invertible, among the transformed quantities there must again be exactly n independent ones, denoted $y_1, \ldots, y_n$; the remaining quantities depending on these are denoted $v_1(y), \ldots, v_\mu(y)$. The transformations may also contain the derivatives of the u's with respect to the x's, thus $\partial u/\partial x$, $\partial^2 u/\partial x^2, \ldots$.[169] A function is called an invariant of the group if a relation holds:

$$P\left(x, u, \frac{\partial u}{\partial x}, \frac{\partial^2 u}{\partial x^2}, \ldots\right) = P\left(y, v, \frac{\partial v}{\partial y}, \frac{\partial^2 v}{\partial y^2}, \ldots\right).$$

In particular, an integral I is therefore an invariant of the group if a relation holds:

$$\begin{aligned} I &= \int\cdots\int f\left(x, u, \frac{\partial u}{\partial x}, \frac{\partial^2 u}{\partial x^2}, \ldots\right) \mathrm{d}x \\ &= \int\cdots\int f\left(y, v, \frac{\partial v}{\partial y}, \frac{\partial^2 v}{\partial y^2}, \ldots\right) \mathrm{d}y, \end{aligned} \tag{1}$$

where the integration is over an arbitrary real x-domain and the corresponding y-domain.[170]

On the other hand, for an arbitrary integral I, not necessarily invariant, I form the first variation δI, and transform it by partial integration according to the rules of the calculus of variations. As is well known, once δu, together with all its derivatives occurring at the boundary, is taken to vanish at the boundary, but is otherwise arbitrary, one obtains:

$$\delta I = \int\cdots\int \delta f \,\mathrm{d}x = \int\cdots\int \left(\sum_i \psi_i\left(x, u, \frac{\partial u}{\partial x}, \ldots\right) \delta u_i\right) \mathrm{d}x, \tag{2}$$

where the ψ's denote the Lagrange expressions, that is, the left-hand sides of the Lagrange equations of the corresponding variational problem $\delta I = 0$. This integral relation corresponds to an identity free of integrals in δu and its derivatives, which arises when one writes the boundary terms as well. As partial integration shows, these boundary terms are integrals over divergences, that is, over expressions

$$\operatorname{Div} A = \frac{\partial A_1}{\partial x_1} + \cdots + \frac{\partial A_n}{\partial x_n},$$

where A is linear in δu and its derivatives. Thus one obtains:

$$\sum_i \psi_i \,\delta u_i = \delta f + \operatorname{Div} A. \tag{3}$$

In particular, if f contains only first derivatives of the u's, then, in the case of the simple integral, the identity (3) is identical with Herr's so-called "Lagrangian central equation":

$$\sum_i \psi_i \,\delta u_i = \delta f - \frac{\mathrm{d}}{\mathrm{d}x}\left(\sum_i \frac{\partial f}{\partial u_i'} \,\delta u_i\right), \qquad \left(u_i' = \frac{\mathrm{d}u_i}{\mathrm{d}x}\right), \tag{4}$$

[168] Lie defines, in *Grundlagen für die Theorie der unendlichen kontinuierlichen Transformationsgruppen* (Reports of the Royal Saxon Society of Sciences, 1891), the infinite continuous group as a transformation group whose transformations are given by the most general solutions of a system of partial differential equations, once these solutions do not depend only on a finite number of parameters. This gives one of the types indicated above, different from the finite group; conversely, however, the limiting case of infinitely many parameters need not necessarily satisfy a system of differential equations.

[169] I suppress the indices, as far as possible also in summations; thus, for example, $\partial^2 u/\partial x^2$ denotes $\partial^2 u_\nu/\partial x_i \partial x_k$, and so on.

[170] I write $\mathrm{d}x, \mathrm{d}y$, for short, for $\mathrm{d}x_1 \cdots \mathrm{d}x_n, \mathrm{d}y_1 \cdots \mathrm{d}y_n$. All arguments $x, u, \varepsilon, p(x)$ occurring in the transformations are to be taken as real, whereas the coefficients may be complex. But since the final results are identities in the x, u, the parameters, and the arbitrary functions, they also hold for complex values as soon as all occurring functions are assumed analytic. Moreover, a large part of the results can be founded without integrals, so that the restriction to the real is not necessary even for the justification. By contrast, the considerations at the end of §2 and the beginning of §5 do not seem to be feasible without integrals.

whereas for the n-fold integral (3) becomes:

$$\sum_i \psi_i\,\delta u_i = \delta f - \frac{\partial}{\partial x_1}\left(\sum_i \frac{\partial f}{\partial\left(\frac{\partial u_i}{\partial x_1}\right)}\,\delta u_i\right) - \cdots - \frac{\partial}{\partial x_n}\left(\sum_i \frac{\partial f}{\partial\left(\frac{\partial u_i}{\partial x_n}\right)}\,\delta u_i\right). \tag{5}$$

For the simple integral and κ derivatives of the u's, (3) is given by:

$$\begin{aligned}\sum_i \psi_i\,\delta u_i = \delta f &- \frac{\mathrm{d}}{\mathrm{d}x}\left\{\sum_i\left[\binom{1}{1}\frac{\partial f}{\partial u_i^{(1)}}\delta u_i + \binom{2}{1}\frac{\partial f}{\partial u_i^{(2)}}\delta u_i^{(1)} + \cdots + \binom{\kappa}{1}\frac{\partial f}{\partial u_i^{(\kappa)}}\delta u_i^{(\kappa-1)}\right]\right\}\\ &+ \frac{\mathrm{d}^2}{\mathrm{d}x^2}\left\{\sum_i\left[\binom{2}{2}\frac{\partial f}{\partial u_i^{(2)}}\delta u_i + \binom{3}{2}\frac{\partial f}{\partial u_i^{(3)}}\delta u_i^{(1)} + \cdots + \binom{\kappa}{2}\frac{\partial f}{\partial u_i^{(\kappa)}}\delta u_i^{(\kappa-2)}\right]\right\}\\ &+ \cdots + (-1)^\kappa\frac{\mathrm{d}^\kappa}{\mathrm{d}x^\kappa}\left\{\sum_i\binom{\kappa}{\kappa}\frac{\partial f}{\partial u_i^{(\kappa)}}\delta u_i\right\}.\end{aligned} \tag{6}$$

A corresponding identity holds for the n-fold integral; in particular A contains δu up to the $(\kappa-1)$-st derivative. That (4), (5), and (6) do in fact define the Lagrange expressions ψ_i follows from the fact that, in the combinations on the right-hand sides, all higher derivatives of δu are eliminated, whereas the relation (2) is fulfilled, to which partial integration leads uniquely.

In what follows the issue is the two theorems:

I. If the integral I is invariant with respect to a $\mathfrak{G}_\rho$, then ρ linearly independent combinations of the Lagrange expressions become divergences; conversely, from this follows the invariance of I with respect to a $\mathfrak{G}_\rho$. The theorem also holds in the limiting case of infinitely many parameters.

II. If the integral I is invariant with respect to a $\mathfrak{G}_{\infty\rho}$ in which the arbitrary functions occur up to the σ-th derivative, then there exist ρ identical relations between the Lagrange expressions and their derivatives up to order σ; here too the converse holds.[171]

For mixed groups, the assertions of both theorems apply; hence there occur both dependencies and divergence relations independent of them.

Passing from these identities to the corresponding variational problem, and thus setting $\psi = 0$,[172] Theorem I says in the one-dimensional case — where the divergence becomes a total differential — that ρ first integrals exist, although nonlinear dependencies may occur among them;[173] in the multidimensional case one obtains the divergence equations that recently have often been called "conservation laws". Theorem II says that ρ of the Lagrange equations are consequences of the remaining ones.

The simplest example of Theorem II — without the converse — is the Weierstrass parameter representation; here, under homogeneity of first order, the integral is known to be invariant if one replaces the independent variable x by an arbitrary function of x, while leaving u unchanged ($y = p(x)$; $v_i(y) = u_i(x)$). Thus one arbitrary function occurs, but without derivatives; and to this corresponds the well-known linear relation between the Lagrange expressions themselves:

$$\sum_i \psi_i\,\frac{\mathrm{d}u_i}{\mathrm{d}x} = 0.$$

A further example is offered by the physicists' "general theory of relativity". Here one is dealing with the group of all transformations of the x's, $y_i = p_i(x)$, while the u's (denoted $g_{\mu\nu}$ and q) are subjected to the transformations thereby induced for the coefficients of a quadratic and a linear differential form, transformations that contain the first derivatives of the arbitrary functions $p(x)$. To this correspond the known n dependencies between the Lagrange expressions and their first derivatives.[174]

If, in particular, one specializes the group by admitting no derivatives of $u(x)$ in the transformations, and in addition by letting the transformed independent quantities depend only on the x's and not on the u's, then, as will be shown in §5, the invariance of I implies the relative invariance of $\sum_i \psi_i\delta u_i$,[175] and likewise of the divergences occurring in Theorem I, as soon as the parameters are subjected to suitable transformations. It follows further that the first integrals mentioned above also admit the group. For

[171] For certain trivial exceptional cases compare §2, second note.

[172] Somewhat more generally one may also set $\psi_i = T_i$; compare §3, first note.

[173] Compare the end of §3.

[174] Compare, for example, Klein's presentation.

[175] That is, $\sum_i \psi_i\delta u_i$ acquires a factor under transformations.

Theorem II one similarly obtains the relative invariance of the left-hand sides of the dependencies, combined by means of the arbitrary functions; and, as a consequence, also a function whose divergence vanishes identically and which admits the group — the function that in the physicists' theory of relativity mediates the connection between dependencies and energy theorem.[176] Finally, in group-theoretic form, Theorem II gives the proof of a related assertion of Hilbert concerning the failure of proper energy theorems in "general relativity". With these supplementary remarks Theorem I contains all the theorems on first integrals known in mechanics and so forth, whereas Theorem II can be described as the greatest possible group-theoretic generalization of the "general theory of relativity".

§2. Divergence relations and dependencies

Let $\mathfrak{G}$ be a continuous group, finite or infinite. It can always be arranged that the identical transformation corresponds to the value zero of the parameters ε, respectively of the arbitrary functions $p(x)$.[177] Thus the most general transformation will be of the form

$$y_i = A_i\left(x, u, \frac{\partial u}{\partial x}, \dots\right) = x_i + \Delta x_i + \cdots, \qquad v_i(y) = B_i\left(x, u, \frac{\partial u}{\partial x}, \dots\right) = u_i + \Delta u_i + \cdots,$$

where $\Delta x_i, \Delta u_i$ denote the terms of lowest dimension in ε, respectively in $p(x)$ and its derivatives; they are to be assumed linear in these quantities. As will be shown later, this is no restriction of generality.

Now let the integral I be an invariant with respect to $\mathfrak{G}$, so that relation (1) is fulfilled. In particular, I is then also invariant with respect to the infinitesimal transformation contained in $\mathfrak{G}$:

$$y_i = x_i + \Delta x_i, \qquad v_i(y) = u_i + \Delta u_i.$$

For this, relation (1) becomes:

$$\begin{aligned} 0 = \Delta I = \int\cdots\int f\left(y, v(y), \frac{\partial v}{\partial y}, \dots\right) \mathrm{d}y \\ - \int\cdots\int f\left(x, u(x), \frac{\partial u}{\partial x}, \dots\right) \mathrm{d}x. \end{aligned} \tag{7}$$

The first integral is to be extended over the $x + \Delta x$-domain corresponding to the x-domain. But this integration can also be transformed into an integration over the x-domain by means of the transformation valid for infinitesimal Δx:

$$\begin{aligned} \int\cdots\int f\left(y, v(y), \frac{\partial v}{\partial y}, \dots\right) \mathrm{d}y = \int\cdots\int f\left(x, v(x), \frac{\partial v}{\partial x}, \dots\right) \mathrm{d}x \\ + \int\cdots\int \mathrm{Div}(f \cdot \Delta x)\, \mathrm{d}x. \end{aligned} \tag{8}$$

If one therefore introduces, in place of the infinitesimal transformation Δu, the variation

$$\bar{\delta} u_i = v_i(x) - u_i(x) = \Delta u_i - \sum_\lambda \frac{\partial u_i}{\partial x_\lambda} \Delta x_\lambda, \tag{9}$$

then (7) and (8) become:

$$0 = \int\cdots\int \{\bar{\delta} f + \mathrm{Div}(f \cdot \Delta x)\} \mathrm{d}x. \tag{10}$$

Since the relation (10) is fulfilled when integrating over every arbitrary domain, the integrand must vanish identically. Thus the Lie differential equations for the invariance of I pass over into the relation

$$\bar{\delta} f + \mathrm{Div}(f \cdot \Delta x) = 0. \tag{11}$$

If one expresses $\bar{\delta} f$ here, by (3), in terms of the Lagrange expressions, one obtains

$$\sum_i \psi_i \bar{\delta} u_i = \mathrm{Div}\, B, \qquad (B = A - f \cdot \Delta x), \tag{12}$$

[176] Compare the second note of Klein.

[177] Compare, for example, Lie, *Grundlagen*, p. 331. If arbitrary functions are involved, then the special values a^σ of the parameters are to be replaced by fixed functions p^σ, $\partial p^\sigma/\partial x, \dots$; and correspondingly the values $a^\sigma + \varepsilon$ by $p^\sigma + p(x)$, $\partial p^\sigma/\partial x + \partial p/\partial x$, and so on.

and this relation therefore represents, for every invariant integral I, an identity in all occurring arguments; it is the desired form of the Lie differential equations for I.[178]

First assume $\mathfrak{G}$ to be a finite continuous group $\mathfrak{G}_\rho$. Since, by assumption, Δu and Δx are linear in the parameters $\varepsilon_1, \ldots, \varepsilon_\rho$, by (9) the same holds for $\bar\delta u$ and its derivatives; hence A and B are linear in the ε. I therefore put

$$B = B^{(1)}\varepsilon_1 + \cdots + B^{(\rho)}\varepsilon_\rho, \qquad \bar\delta u = \bar\delta u^{(1)}\varepsilon_1 + \cdots + \bar\delta u^{(\rho)}\varepsilon_\rho,$$

where $\bar\delta u^{(1)}, \ldots$ are functions of $x, u, \partial u/\partial x, \ldots$. From (12) follow the desired divergence relations:

$$\sum_i \psi_i \bar\delta u_i^{(1)} = \operatorname{Div} B^{(1)}, \ldots, \qquad \sum_i \psi_i \bar\delta u_i^{(\rho)} = \operatorname{Div} B^{(\rho)}. \tag{13}$$

Thus ρ linearly independent combinations of the Lagrange expressions become divergences. The linear independence follows from the fact that, by (9), $\bar\delta u = 0, \Delta x = 0$ would imply $\Delta u = 0, \Delta x = 0$, and hence a dependency between the infinitesimal transformations. But by hypothesis no such dependency holds for any parameter value; otherwise the $\mathfrak{G}_\rho$ arising again by integration from the infinitesimal transformations would depend on fewer than ρ essential parameters. The further possibility $\bar\delta u = 0,\ \operatorname{Div}(f\Delta x) = 0$ has been excluded. These conclusions remain valid in the limiting case of infinitely many parameters.

Now let $\mathfrak{G}$ be an infinite continuous group $\mathfrak{G}_{\infty\rho}$. Then again $\bar\delta u$ and its derivatives, hence also B, are linear in the arbitrary functions $p(x)$ and their derivatives.[179] Substitution of the values of $\bar\delta u$, still independently of (12), gives:

$$\sum_i \psi_i \bar\delta u_i = \sum_{\lambda,i} \psi_i \left\{ a_i^{(\lambda)}(x,u,\ldots)p^{(\lambda)}(x) + b_i^{(\lambda)}(x,u,\ldots)\frac{\partial p^{(\lambda)}}{\partial x} + \cdots + c_i^{(\lambda)}(x,u,\ldots)\frac{\partial^\sigma p^{(\lambda)}}{\partial x^\sigma} \right\}.$$

Now, analogously to the formula for partial integration, by means of the identity

$$\varphi(x,u,\ldots)\frac{\partial^\tau p(x)}{\partial x^\tau} = (-1)^\tau \frac{\partial^\tau \varphi}{\partial x^\tau}\, p(x) \quad \text{mod divergences},$$

the derivatives of p can be replaced by p itself and by divergences that are linear in p and its derivatives. Thus:

$$\sum_i \psi_i \bar\delta u_i = \sum_\lambda \left\{ a_i^{(\lambda)}\psi_i - \frac{\partial}{\partial x}(b_i^{(\lambda)}\psi_i) + \cdots + (-1)^\sigma \frac{\partial^\sigma}{\partial x^\sigma}(c_i^{(\lambda)}\psi_i) \right\} p^{(\lambda)} + \operatorname{Div}\Gamma, \tag{14}$$

with summation over i in the brace. In combination with (12) this gives:

$$\sum_\lambda \left\{ a_i^{(\lambda)}\psi_i - \frac{\partial}{\partial x}(b_i^{(\lambda)}\psi_i) + \cdots + (-1)^\sigma \frac{\partial^\sigma}{\partial x^\sigma}(c_i^{(\lambda)}\psi_i) \right\} p^{(\lambda)} = \operatorname{Div}(B - \Gamma). \tag{15}$$

I now form the n-fold integral over (15), extended over an arbitrary domain, and choose the $p(x)$'s so that they, together with all derivatives occurring in $B - \Gamma$, vanish at the boundary. Since the integral over a divergence reduces to a boundary integral, the integral over the left-hand side of (15) also vanishes for arbitrary $p(x)$'s that vanish at the boundary with sufficiently many derivatives. From the usual arguments it follows that the integrand vanishes for every $p(x)$, giving the ρ relations

$$\sum_i \left\{ a_i^{(\lambda)}\psi_i - \frac{\partial}{\partial x}(b_i^{(\lambda)}\psi_i) + \cdots + (-1)^\sigma \frac{\partial^\sigma}{\partial x^\sigma}(c_i^{(\lambda)}\psi_i) \right\} = 0, \qquad (\lambda = 1, 2, \ldots, \rho). \tag{16}$$

These are the desired dependencies between the Lagrange expressions and their derivatives when I is invariant with respect to $\mathfrak{G}_{\infty\rho}$. The linear independence follows as above, since the converse leads back to (12); and since one can again conclude from the infinitesimal transformations to the finite ones, as is carried out more fully in §4. Accordingly, for a $\mathfrak{G}_{\infty\rho}$, ρ arbitrary transformations already occur in the infinitesimal transformations. From (15) and (16) it follows further that $\operatorname{Div}(B - \Gamma) = 0$.

If, corresponding to a "mixed group", one takes Δx and Δu to be linear in the ε's and the $p(x)$'s, then by setting once the $p(x)$'s and once the ε's equal to zero, one sees that both the divergence relations (13) and the dependencies (16) exist.

[178](12) becomes $0 = 0$ for the trivial case — which can occur only if $\Delta x, \Delta u$ also depend on derivatives of u — when $\operatorname{Div}(f \cdot \Delta x) = 0,\ \bar\delta u = 0$. These infinitesimal transformations must therefore always be split off from the groups, and in the formulation of the theorems only the number of the remaining parameters or arbitrary functions is to be counted. Whether the remaining infinitesimal transformations still always form a group must be left open.

[179]That it is no restriction to assume the p's independent of $u, \partial u/\partial x, \ldots$ is shown by the converse.

§3. The converse in the case of the finite group

To prove the converse, the preceding considerations must first be run through, in essence, in reverse order. From the validity of (13), multiplying by the ε's and adding gives the validity of (12); and by means of the identity (3) one obtains a relation

$$\bar{\delta} f + \operatorname{Div}(A - B) = 0.$$

Thus, if one sets $\Delta x = \frac{1}{f}(A - B)$, one thereby arrives at (11); by integration this finally gives (7), $\Delta I = 0$, hence the invariance of I with respect to the infinitesimal transformation determined by $\Delta x, \Delta u$, where the Δu's are determined by (9) from Δx and $\bar{\delta} u$, and $\Delta x, \Delta u$ become linear in the parameters. But $\Delta I = 0$ implies, in the known way, the invariance of I with respect to the finite transformations arising by integration of the simultaneous system:

$$\frac{\mathrm{d}x_i}{\mathrm{d}t} = \Delta x_i, \qquad \frac{\mathrm{d}u_i}{\mathrm{d}t} = \Delta u_i, \qquad \left\{ \begin{array}{l} x_i = y_i, \\ u_i = v_i \end{array} \right\} \quad \text{for } t = 0. \tag{17}$$

These finite transformations contain ρ parameters $a_1, \ldots, a_\rho$, namely the combinations $t\varepsilon_1, \ldots, t\varepsilon_\rho$. From the assumption that there are to be ρ, and only ρ, linearly independent divergence relations (13), it follows further that the finite transformations, as soon as they do not contain the derivatives $\partial u / \partial x$, always form a group. In the contrary case, at least one infinitesimal transformation arising by Lie's bracket process would not be a linear combination of the remaining ρ; and since I also admits this transformation, there would be more than ρ linearly independent divergence relations. Or else this infinitesimal transformation would be of the special form $\bar{\delta} u = 0,\ \operatorname{Div}(f \Delta x) = 0$. But then Δx or Δu would depend on derivatives, contrary to the assumption. Whether this case can occur when derivatives appear in Δx or Δu must be left open; then all functions Δx for which $\operatorname{Div}(f \Delta x) = 0$ must still be added to the Δx determined above in order to obtain the group property again, but by agreement the parameters thereby added are not to be counted. This proves the converse.

It also follows from this converse that Δx and Δu may indeed be assumed linear in the parameters. If Δu and Δx were forms of higher degree in ε, then, because of the linear independence of the power products of the ε's, entirely corresponding relations (13), only in larger number, would follow; by the converse, these imply invariance of I with respect to a group whose infinitesimal transformations contain the parameters linearly. If this group is to contain exactly ρ parameters, then there must be linear dependencies among the divergence relations originally obtained from the terms of higher degree in ε.

It should also be noted that, in the case where Δx and Δu also contain derivatives of the u's, the finite transformations may depend on infinitely many derivatives of the u's; for in this case the integration of (17), when determining

$$\frac{\mathrm{d}^2 x_i}{\mathrm{d}t^2}, \quad \frac{\mathrm{d}^2 u_i}{\mathrm{d}t^2},$$

leads to

$$\Delta\left(\frac{\partial u}{\partial x_\lambda}\right) = \frac{\partial\, \Delta u}{\partial x_\lambda} - \sum_\nu \frac{\partial u}{\partial x_\nu} \frac{\partial\, \Delta x_\nu}{\partial x_\lambda},$$

so that in general the number of derivatives of u grows at every step. An example is:

$$f = \frac{1}{2} u'^2, \qquad \psi = -u'', \qquad \psi \cdot x = \frac{\mathrm{d}}{\mathrm{d}x}\{(u - u'x)\}, \qquad \bar{\delta} u = x\varepsilon,$$

$$\Delta x = -\frac{2u}{u'}\,\varepsilon, \qquad \Delta u = \left(x - \frac{2u}{u'}\right)\varepsilon.$$

Since the Lagrange expressions of a divergence vanish identically, the converse finally shows the following: if I admits a $\mathfrak{G}_\rho$, then every integral that differs from I only by a boundary integral, that is, by an integral over a divergence, also admits a $\mathfrak{G}_\rho$ with the same $\bar{\delta} u$'s, while its infinitesimal transformations will in general contain derivatives of the u's. Thus, corresponding to the preceding example,

$$f^* = \frac{1}{2}\left\{u'^2 - \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{u^2}{x}\right)\right\}$$

admits the infinitesimal transformation $\Delta u = x\varepsilon,\ \Delta x = 0$; whereas derivatives of u occur in the infinitesimal transformations corresponding to f.

If one passes to the variational problem, that is, if one sets $\psi_i = 0$,[180] then (13) becomes the equations

$$\operatorname{Div} B^{(1)} = 0, \ldots, \qquad \operatorname{Div} B^{(\rho)} = 0,$$

which are often called "conservation laws". In the one-dimensional case this gives:

$$B^{(1)} = \text{const.}, \ldots, \qquad B^{(\rho)} = \text{const.}.$$

Here the B's contain at most $(2\kappa-1)$-st derivatives of u (by (6)), as soon as Δu and Δx contain no derivatives higher than the κ-th derivatives occurring in f. Since ψ contains, in general, 2κ-th derivatives,[181] one thus has the existence of ρ first integrals. That nonlinear dependencies may exist among them is shown again by the above f. To the linearly independent $\Delta u = \varepsilon_1,\ \Delta x = \varepsilon_2$ correspond the linearly independent relations

$$u'' = \frac{\mathrm{d}}{\mathrm{d}x}u', \qquad u''u' = \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}x}(u')^2,$$

whereas among the first integrals $u' = \text{const.}$, $u'^2 = \text{const.}$ there is a nonlinear dependency. This is the elementary case in which $\Delta u, \Delta x$ contain no derivatives of u.[182]

§4. The converse in the case of the infinite group

First it is to be shown that the assumption of linearity of Δx and Δu is no restriction. Here this follows, even without the converse, from the fact that $\mathfrak{G}_{\infty\rho}$ depends formally on ρ, and only ρ, arbitrary functions. Namely, in the nonlinear case, when transformations are composed, the terms of lowest order add and the number of arbitrary functions would increase. Indeed, suppose for instance that

$$\begin{aligned} y &= A\left(x, u, \frac{\partial u}{\partial x}, \ldots; p\right) \\ &= x + \sum a(x, u, \ldots)p^\nu + b(x, u, \ldots)p^{\nu-1}\frac{\partial p}{\partial x} + c\,p^{\nu-2}\left(\frac{\partial p}{\partial x}\right)^2 + \cdots + d\left(\frac{\partial p}{\partial x}\right)^\nu + \cdots, \end{aligned}$$

where

$$p^\nu = (p^{(1)})^{\nu_1} \cdots (p^{(\rho)})^{\nu_\rho},$$

and correspondingly

$$v = B\left(x, u, \frac{\partial u}{\partial x}, \ldots; p\right).$$

Then, by composition with

$$z = A\left(y, v, \frac{\partial v}{\partial y}, \ldots; q\right),$$

the terms of lowest order give

$$z = x + \sum a(p^\nu + q^\nu) + b\left\{p^{\nu-1}\frac{\partial p}{\partial x} + q^{\nu-1}\frac{\partial q}{\partial x}\right\} + c\left\{p^{\nu-2}\left(\frac{\partial p}{\partial x}\right)^2 + q^{\nu-2}\left(\frac{\partial q}{\partial x}\right)^2\right\} + \cdots.$$

If here some coefficient other than a and b is different from zero, so that a term

$$p^{\nu-\sigma}\left(\frac{\partial p}{\partial x}\right)^\sigma + q^{\nu-\sigma}\left(\frac{\partial q}{\partial x}\right)^\sigma$$

actually occurs for $\sigma > 1$, then it cannot be written as the differential quotient of a single function, nor as a product of powers of such a quotient. Thus the number of arbitrary functions has increased against the hypothesis. If all coefficients other than a and b vanish, then, depending on the values of the exponents

[180] $\psi_i = 0$, or somewhat more generally $\psi_i = T_i$, where the T_i's are newly adjoined functions, are called "field equations" in physics. In the case $\psi_i = T_i$, the identities (13) pass into the equations $\operatorname{Div} B^{(\lambda)} = \sum_i T_i \bar{\delta} u_i^{(\lambda)}$, which in physics are also still called conservation laws.

[181] As soon as f is nonlinear in the κ-th derivatives.

[182] Otherwise one has additionally $u''u'^{\lambda-1} = \text{const.}$ for every λ, corresponding to

$$u''(u')^{\lambda-1} = \frac{1}{\lambda}\frac{\mathrm{d}}{\mathrm{d}x}(u')^\lambda.$$

$\nu_1, \ldots, \nu_\rho$, the second term is the differential quotient of the first (as, for example, always for a $\mathfrak{G}_{\infty 1}$), so that linearity actually occurs; or else the number of arbitrary functions increases here as well. Hence, because of linearity in $p(x)$, the infinitesimal transformations satisfy a system of linear partial differential equations; and, since the group property is fulfilled, they form an "infinite group of infinitesimal transformations" in Lie's sense (Grundlagen, §10).

The converse now results similarly to the case of the finite group. The existence of the dependencies (16), after multiplication by $p^{(\lambda)}(x)$ and addition, leads by means of the identical transformation (14) to

$$\sum_i \psi_i \bar{\delta} u_i = \operatorname{Div} \Gamma.$$

From this, as in §3, one obtains the determination of Δx and Δu, and the invariance of I with respect to these infinitesimal transformations, which in fact depend linearly on ρ arbitrary functions and their derivatives up to order σ. That these infinitesimal transformations, when they contain no derivatives $\partial u/\partial x, \ldots$, certainly form a group follows as in §3, since otherwise more arbitrary functions would occur by composition, whereas by assumption there are to be only ρ dependencies (16). Thus they form an "infinite group of infinitesimal transformations". But such a group consists (Grundlagen, Theorem VII, p. 391) of the most general infinitesimal transformations of a certain thereby defined "infinite group $\mathfrak{G}$ of finite transformations" in Lie's sense. Every finite transformation is thereby generated from infinitesimal ones (Grundlagen, §7),[183] and therefore arises by integration of the simultaneous system:

$$\frac{\mathrm{d}x_i}{\mathrm{d}t} = \Delta x_i, \qquad \frac{\mathrm{d}u_i}{\mathrm{d}t} = \Delta u_i, \qquad \left\{ \begin{array}{l} x_i = y_i, \\ u_i = v \end{array} \right\} \quad \text{for } t = 0.$$

It may be necessary, however, to let the arbitrary $p(x)$'s still depend on t. Thus $\mathfrak{G}$ in fact depends on ρ arbitrary functions. In particular, if it is sufficient to take $p(x)$ free of t, then this dependency is analytic in the arbitrary functions $q(x) = t\,p(x)$.[184] If derivatives $\partial u/\partial x, \ldots$ occur, it may be necessary to adjoin infinitesimal transformations $\bar{\delta} u = 0$, $\operatorname{Div}(f \Delta x) = 0$ before drawing the same conclusions.

Following an example of Lie (Grundlagen, §7), I now indicate a rather general case in which one can get as far as explicit formulae, which also show that the derivatives of the arbitrary functions occur up to order σ; in this case the converse is therefore complete. These are groups of infinitesimal transformations to which there corresponds the group of all transformations of the x's and the transformations of the u's thereby "induced"; that is, transformations of the u's in which Δu, and hence u, depends only on the arbitrary functions occurring in Δx. It is still assumed that the derivatives $\partial u/\partial x, \ldots$ do not occur in Δu. Thus:

$$\Delta x_i = p^{(i)}(x), \qquad \Delta u_i = \sum_{\lambda=1}^{n} \left\{ a_i^{(\lambda)}(x,u) p^{(\lambda)} + b_i^{(\lambda)} \frac{\partial p^{(\lambda)}}{\partial x} + \cdots + c_i^{(\lambda)} \frac{\partial^\sigma p^{(\lambda)}}{\partial x^\sigma} \right\}.$$

Since the infinitesimal transformation $\Delta x = p(x)$ generates every transformation $x = y + g(y)$ with arbitrary $g(y)$, one can in particular determine $p(x)$ as a function of t so that the one-parameter group is generated:

$$x_i = y_i + t\, g_i(y), \tag{18}$$

which for $t = 0$ becomes the identity and for $t = 1$ becomes the desired $x = y + g(y)$. Differentiation of (18) gives

$$\frac{\mathrm{d}x_i}{\mathrm{d}t} = g_i(y) = p^{(i)}(x,t), \tag{19}$$

where $p(x,t)$ is determined from $g(y)$ by inversion of (18); conversely, (18) arises from (19) by means of the side condition $x_i = y_i$ for $t = 0$, by which the integral is uniquely fixed. By means of (18), the x's in Δu can be replaced by the integration constants y and by t; the $g(y)$'s then occur exactly up to their σ-th derivatives, since in

$$\frac{\partial p}{\partial x} = \sum_k \frac{\partial g}{\partial y_k} \frac{\partial y_k}{\partial x}$$

[183] From this it follows in particular that the group $\mathfrak{G}$ generated from the infinitesimal transformations $\Delta x, \Delta u$ of a $\mathfrak{G}_{\infty\rho}$ leads back again to $\mathfrak{G}_{\infty\rho}$. For $\mathfrak{G}_{\infty\rho}$ contains no infinitesimal transformations depending on arbitrary functions and different from $\Delta x, \Delta u$, and cannot contain independent transformations depending on parameters either, since otherwise it would be a mixed group. But by the preceding argument the finite transformations are determined by the infinitesimal ones.

[184] The question whether this latter case perhaps always occurs was raised by Lie in another formulation (Grundlagen, §7 and §13, end).

the $\partial y/\partial x$ are expressed by $\partial x/\partial y$, and in general $\partial^\sigma p/\partial x^\sigma$ is replaced by its value in

$$\frac{\partial g}{\partial y}, \ldots, \frac{\partial^\sigma g}{\partial y^\sigma}, \ldots, \frac{\partial^\sigma x}{\partial y^\sigma}.$$

For the determination of the u's one therefore obtains the system of equations

$$\frac{\mathrm{d}u_i}{\mathrm{d}t} = F_i\left(g(y), \frac{\partial g}{\partial y}, \ldots, \frac{\partial^\sigma g}{\partial y^\sigma}, u, t\right), \qquad (u_i = v_i \text{ for } t = 0),$$

in which only t and u are variables, while $g(y), \ldots$ belong to the coefficient domain; hence integration gives

$$u_i = v_i + B_i\left(v, g(y), \frac{\partial g}{\partial y}, \ldots, \frac{\partial^\sigma g}{\partial y^\sigma}, t\right)_{t=1}.$$

Thus one obtains transformations that depend exactly on σ derivatives of the arbitrary functions. The identity is contained in this for $g(y) = 0$, by (18); and the group property follows from the fact that the procedure just described yields every transformation $x = y + g(y)$, whereby the induced transformation of the u's is uniquely determined, so that the group $\mathfrak{G}$ is exhausted.

It also follows incidentally from the converse that it is no restriction to assume that the arbitrary functions depend only on the x's, and not on $u, \partial u/\partial x, \ldots$. In the latter case, in the identical transformation (14), and hence also in (15), besides the $p^{(\lambda)}$'s there would occur the derivatives $\partial p^{(\lambda)}/\partial u$, $\partial p^{(\lambda)}/\partial(\partial u/\partial x), \ldots$. If one now successively takes the $p^{(\lambda)}$'s to be of zeroth, first, and higher degrees in $u, \partial u/\partial x, \ldots$, with arbitrary functions of x as coefficients, then dependencies (16) again arise, only in greater number. But by the preceding converse they can be brought back to the earlier case by being combined with arbitrary functions depending only on x. Similarly one shows that mixed groups correspond to the simultaneous occurrence of dependencies and independent divergence relations.[185]

§5. Invariance of the individual components of the relations

If the group $\mathfrak{G}$ is specialized to the simplest case, the one ordinarily considered, by admitting no derivatives of the u's in the transformations and by letting the transformed independent variables depend only on the x's and not on the u's, then one can infer the invariance of the individual components in the formulae. First, by familiar arguments, one obtains the invariance of

$$\int \cdots \int \left(\sum_i \psi_i \delta u_i\right) \mathrm{d}x,$$

hence the relative invariance of $\sum_i \psi_i \delta u_i$, where δ denotes any variation. Namely, on the one hand,

$$\delta I = \int \cdots \int \delta f\left(x, u, \frac{\partial u}{\partial x}, \ldots\right) \mathrm{d}x = \int \cdots \int \delta f\left(y, v, \frac{\partial v}{\partial y}, \ldots\right) \mathrm{d}y.$$

[185] As in §3, it follows here too from the converse that besides I, every integral I^* differing from it by an integral over a divergence also admits an infinite group with the same $\bar{\delta}u$'s; here, however, Δx and Δu will in general contain derivatives of the u's. Einstein introduced such an integral I^* into general relativity in order to obtain a simpler formulation of the energy theorems. I give the infinitesimal transformations admitted by this I^*, using exactly the notation of Klein's second note. The integral $I = \int \cdots \int K \,\mathrm{d}\omega = \int \cdots \int \mathfrak{R} \,\mathrm{d}S$ admits the group of all transformations of the w's and the group thereby induced for the $g_{\mu\nu}$'s. To this correspond the dependencies ((30) in Klein):

$$\sum \mathfrak{R}_{\mu\nu} g^{\alpha\beta}_{\mu\nu} + 2 \sum \frac{\partial g^{\alpha\beta}_{\mu\nu} \mathfrak{R}_{\mu\nu}}{\partial w^\sigma} = 0.$$

Now $I^* = \int \cdots \int \mathfrak{R}^* \,\mathrm{d}S$, where $\mathfrak{R}^* = \mathfrak{R} + \mathrm{Div}$, and consequently $\mathfrak{R}^*_{\mu\nu} = \mathfrak{R}_{\mu\nu}$, where $\mathfrak{R}^*_{\mu\nu}, \mathfrak{R}_{\mu\nu}$ denote the Lagrange expressions respectively. The given dependencies are therefore also dependencies for $\mathfrak{R}^*_{\mu\nu}$; and after multiplication by p^τ and addition, by reversing the transformations of product differentiation, one obtains

$$\sum \mathfrak{R}_{\mu\nu} p^{\mu\nu} + 2\,\mathrm{Div}\left(\sum g^{\mu\sigma} \mathfrak{R}_{\mu\tau} p^\tau\right) = 0,$$

$$\delta\mathfrak{R}^* + \mathrm{Div}\left(\sum 2 g^{\mu\sigma} \mathfrak{R}_{\mu\tau} p^\tau - \frac{\partial \mathfrak{R}^*}{\partial g^\sigma_{\mu\nu}} p^{\mu\nu}\right) = 0.$$

Comparison with the Lie differential equation $\delta\mathfrak{R}^* + \mathrm{Div}(\mathfrak{R}^* \Delta w) = 0$ gives

$$\Delta w^\sigma = \frac{1}{\mathfrak{R}^*}\left(\sum 2 g^{\mu\sigma} \mathfrak{R}_{\mu\tau} p^\tau - \frac{\partial \mathfrak{R}^*}{\partial g^\sigma_{\mu\nu}} p^{\mu\nu}\right), \qquad \Delta g^{\mu\nu} = p^{\mu\nu} + \sum g^{\mu\nu}_\sigma \Delta w^\sigma,$$

as infinitesimal transformations admitted by I^*. These infinitesimal transformations therefore depend on the first and second derivatives of the $g^{\mu\nu}$'s, and contain the arbitrary p's up to the first derivative.

On the other hand, for $\delta u, \delta(\partial u/\partial x), \ldots$ vanishing at the boundary, to which, because of the linear homogeneous transformation of $\delta u, \delta(\partial u/\partial x), \ldots$, there corresponds $\delta v, \delta(\partial v/\partial y), \ldots$ also vanishing at the boundary, one has

$$\int\cdots\int \delta f\left(x, u, \frac{\partial u}{\partial x}, \ldots\right) \mathrm{d}x = \int\cdots\int \left(\sum_i \psi_i(u, \ldots)\delta u_i\right) \mathrm{d}x,$$

$$\int\cdots\int \delta f\left(y, v, \frac{\partial v}{\partial y}, \ldots\right) \mathrm{d}y = \int\cdots\int \left(\sum_i \psi_i(v, \ldots)\delta v_i\right) \mathrm{d}y.$$

Thus, for $\delta u, \delta(\partial u/\partial x), \ldots$ vanishing at the boundary,

$$\int\cdots\int \left(\sum_i \psi_i(u, \ldots)\delta u_i\right) \mathrm{d}x = \int\cdots\int \left(\sum_i \psi_i(v, \ldots)\delta v_i\right) \mathrm{d}y$$

$$= \int\cdots\int \left(\sum_i \psi_i(v, \ldots)\delta v_i\right) \left|\frac{\partial y_i}{\partial x_k}\right| \mathrm{d}x.$$

If one expresses $y, v, \delta v$ in the third integral by $x, u, \delta u$, and sets it equal to the first, then one obtains a relation

$$\int\cdots\int \left(\sum_i \chi_i(u, \ldots)\delta u_i\right) \mathrm{d}x = 0$$

for δu vanishing at the boundary but otherwise arbitrary. From this it follows, as is known, that the integrand vanishes for arbitrary δu; hence the relation

$$\sum_i \psi_i(u, \ldots)\delta u_i = \left|\frac{\partial y_i}{\partial x_k}\right| \left(\sum_i \psi_i(v, \ldots)\delta v_i\right)$$

holds identically in δu. This expresses the relative invariance of $\sum_i \psi_i \delta u_i$, and consequently the invariance of

$$\int\cdots\int \left(\sum_i \psi_i \delta u_i\right) \mathrm{d}x.$$

186

To apply this to the derived divergence relations and dependencies, one must first show that the $\bar{\delta}u$ derived from $\Delta u, \Delta x$ actually satisfies the transformation laws for the variation δu, provided only that the parameters, respectively arbitrary functions, in $\bar{\delta}v$ are determined as they correspond to the similar group of infinitesimal transformations in y, v. Let T_q denote the transformation that carries x, u into y, v; and let T_p be an infinitesimal transformation in x, u. Then the similar one in y, v is given by $T_r = T_q T_p T_q^{-1}$, where the parameters, respectively arbitrary functions, r are determined by p and q. In formulae this is expressed as follows:

$$T_p: \ \xi = x + \Delta x(x, p), \qquad u^* = u + \Delta u(x, u, p);$$

$$T_q: \ y = A(x, q), \qquad v = B(x, u, q);$$

$$T_q T_p: \ \eta = A(x + \Delta x(x, p), q), \quad v^* = B(x + \Delta x(p),\, u + \Delta u(p), q).$$

But from this arises $T_r = T_q T_p T_q^{-1}$, hence

$$\eta = y + \Delta y(r), \qquad v^* = v + \Delta v(r),$$

where, by means of the inverse of T_q, one regards the x's as functions of the y's and retains only the infinitesimal terms. Thus one has the identity

$$\eta = y + \Delta y(r) = y + \sum \frac{\partial A(x, q)}{\partial x} \Delta x(p), \tag{20a}$$

[186]These arguments fail if y also depends on the u's, because then $\delta f(y, v, \partial v/\partial y, \ldots)$ also contains terms $\sum(\partial f/\partial y)\delta y$, so that the divergence transformation does not lead to the Lagrange expressions. They likewise fail if derivatives of the u's are admitted; then the δv's become linear combinations of $\delta u, \delta(\partial u/\partial x), \ldots$, and hence only after a further divergence transformation lead to an identity $\int\cdots\int(\sum \chi_i(u, \ldots)\delta u_i)\mathrm{d}x = 0$, so that on the right the Lagrange expressions again do not occur. The question whether the invariance of $\int\cdots\int(\sum \psi_i \delta u_i)\mathrm{d}x$ already allows one to conclude the existence of divergence relations is, by the converse, equivalent to the question whether it implies invariance of I with respect to a group that need not lead to the same $\Delta u, \Delta x$, but does lead to the same $\bar{\delta}u$. In the special case of the simple integral and only first derivatives in f, for the finite group one can infer the existence of first integrals from the invariance of the Lagrange expressions (compare, for example, Engel, Gött. Nachr. 1916, p. 270).

$$v^* = v + \Delta v(r) = v + \sum \frac{\partial B(x,u,q)}{\partial x}\Delta x(p) + \sum \frac{\partial B(x,u,q)}{\partial u}\Delta u(p). \tag{20b}$$

If, in this, one replaces $\xi = x + \Delta x$ by $\xi - \Delta\xi$, so that ξ goes back into x and hence Δx vanishes, then by the first formula (20) η also goes back into $y = \eta - \Delta\eta$. If under this substitution $\Delta u(p)$ goes over into $\bar\delta u(p)$, then $\Delta v(r)$ also goes over into $\bar\delta v(r)$, and the second formula (20) gives

$$v + \bar\delta v(y, v, \ldots, r) = v + \sum \frac{\partial B(x,u,q)}{\partial u}\,\bar\delta u(p),$$

$$\bar\delta v(y, v, \ldots, r) = \sum \frac{\partial B}{\partial u_\kappa}\,\bar\delta u_\kappa(x, u, p).$$

Thus the transformation formulae for variations are indeed satisfied, provided only that $\bar\delta v$ is taken to depend on the parameters, respectively arbitrary functions, r.[187]

It follows in particular that $\sum_i \psi_i \bar\delta u_i$ is relatively invariant; hence also, by (12), since the divergence relations are also fulfilled in y, v, the relative invariance of $\operatorname{Div} B$; and further, by (14) and (13), the relative invariance of $\operatorname{Div}\Gamma$ and of the left-hand sides of the dependencies combined with the $p^{(\lambda)}$'s, where in the transformed formulae the arbitrary $p(x)$'s (respectively the parameters) are everywhere to be replaced by the r's. From this follows also the relative invariance of $\operatorname{Div}(B - \Gamma)$, that is, of the divergence of a system of functions $B - \Gamma$ that does not vanish identically, but whose divergence vanishes identically.

From the relative invariance of $\operatorname{Div} B$, in the one-dimensional case and for a finite group, one can draw a further conclusion about the invariance of the first integrals. The transformation of the parameters corresponding to the infinitesimal transformation becomes, by (20), linear and homogeneous; and because all transformations are invertible, the ε's are also linear and homogeneous in the transformed parameters ε^*. This invertibility is certainly preserved when one sets $\psi = 0$, since no derivatives of u occur in (20). By equating the coefficients of the ε^* in

$$\operatorname{Div} B(x, u, \ldots, \varepsilon) = \frac{\mathrm{d}y}{\mathrm{d}x}\operatorname{Div} B(y, v, \ldots, \varepsilon^*)$$

the quantities $\frac{\mathrm{d}}{\mathrm{d}y}B^{(\lambda)}(y, v, \ldots)$ also become linear homogeneous functions of the $\frac{\mathrm{d}}{\mathrm{d}x}B^{(\lambda)}(x, u, \ldots)$. Thus from

$$\frac{\mathrm{d}}{\mathrm{d}x}B^{(\lambda)}(x, u, \ldots) = 0 \quad \text{or} \quad B^{(\lambda)}(x, u) = \text{const.}$$

it follows that

$$\frac{\mathrm{d}}{\mathrm{d}y}B^{(\lambda)}(y, v, \ldots) = 0 \quad \text{or} \quad B^{(\lambda)}(y, v) = \text{const.}$$

The ρ first integrals corresponding to a $\mathfrak{G}_\rho$ therefore each admit the group, so that the further integration is also simplified. The simplest example of this is that f is free of x or of a u, corresponding to the infinitesimal transformations $\Delta x = \varepsilon, \Delta u = 0$, respectively $\Delta x = 0, \Delta u = \varepsilon$. Then $\bar\delta u = -\varepsilon\,\mathrm{d}u/\mathrm{d}x$, respectively ε; and since B is derived from f and $\bar\delta u$ by differentiation and rational operations, it is also free of x, respectively u, and admits the corresponding groups.[188]

§6. A theorem of Hilbert

From the foregoing there finally results the proof of an assertion of Hilbert concerning the connection between the failure of proper energy theorems and "general relativity" (Klein's first note, Göttinger Nachr. 1917, Reply, first paragraph), in a generalized group-theoretic formulation.

Suppose the integral I admits a $\mathfrak{G}_{\infty\rho}$, and let $\mathfrak{G}_\sigma$ be any finite group arising by specialization of the arbitrary functions, thus a subgroup of $\mathfrak{G}_{\infty\rho}$. To the infinite group $\mathfrak{G}_{\infty\rho}$ there correspond dependencies (16), to the finite group $\mathfrak{G}_\sigma$ divergence relations (13); conversely, from the existence of any divergence relations follows the invariance of I with respect to a finite group, which is identical with $\mathfrak{G}_\sigma$ if and only if the $\bar\delta u$'s

[187] It is again seen that y must be assumed independent of u, and so on, if the conclusions are to hold. As an example, one may cite the $\delta g^{\mu\nu}$ and δq_σ indicated by Klein, which satisfy the transformations for variations as soon as the p's are subjected to a vector transformation.

[188] In those cases where the existence of first integrals already follows from the invariance of $\int(\sum \psi_i \delta u_i)\mathrm{d}x$, these do not admit the complete group $\mathfrak{G}_\rho$. For example, $\int(u''\delta u)\mathrm{d}x$ admits the infinitesimal transformation $\Delta x = \varepsilon_2, \Delta u = \varepsilon_1 + x\varepsilon_3$; whereas the first integral $u - u'x = \text{const.}$, corresponding to $\Delta x = 0, \Delta u = x\varepsilon_3$, does not admit the two other infinitesimal transformations, since it contains both u and x explicitly. To this first integral there correspond infinitesimal transformations for f that contain derivatives. Thus one sees that the invariance of $\int\cdots\int(\sum \psi_i \delta u_i)\mathrm{d}x$ in any case accomplishes less than the invariance of I, a point relevant to the question raised in a preceding note.

are linear combinations of those arising from $\mathfrak{G}_\sigma$. Hence the invariance with respect to $\mathfrak{G}_\sigma$ can lead to no divergence relations different from (13). But since from the existence of (16) follows the invariance of I with respect to the infinitesimal transformations $\Delta u, \Delta x$ of $\mathfrak{G}_{\infty\rho}$ for arbitrary $p(x)$, it follows in particular that I is already invariant with respect to the infinitesimal transformations of $\mathfrak{G}_\sigma$ arising from these by specialization, and hence with respect to $\mathfrak{G}_\sigma$. The divergence relations

$$\sum_i \psi_i \bar{\delta} u_i^{(\lambda)} = \operatorname{Div} B^{(\lambda)}$$

must therefore be consequences of the dependencies (16), which can also be written

$$\sum_i \psi_i a_i^{(\lambda)} = \operatorname{Div} \chi^{(\lambda)},$$

where the $\chi^{(\lambda)}$'s are linear combinations of the Lagrange expressions and their derivatives. Since the ψ's enter linearly both in (13) and in (16), the divergence relations must in particular be linear combinations of the dependencies (16). Thus

$$\operatorname{Div} B^{(\lambda)} = \operatorname{Div}\left(\sum \alpha_\mu \chi^{(\mu)}\right),$$

and the $B^{(\lambda)}$'s themselves are thus composed linearly from the χ's, that is, from the Lagrange expressions and their derivatives, and from functions whose divergence vanishes identically, as for instance the $B - \Gamma$ occurring at the end of §2, for which $\operatorname{Div}(B - \Gamma) = 0$, and where the divergence has at the same time the character of an invariant. I shall call divergence relations in which the $B^{(\lambda)}$'s can be composed in the indicated way from the Lagrange expressions and their derivatives "improper", and all the remaining ones "proper".

Conversely, if the divergence relations are linear combinations of the dependencies (16), hence "improper", then the invariance with respect to $\mathfrak{G}_\sigma$ follows from that with respect to $\mathfrak{G}_{\infty\rho}$; $\mathfrak{G}_\sigma$ becomes a subgroup of $\mathfrak{G}_{\infty\rho}$. Thus the divergence relations corresponding to a finite group $\mathfrak{G}_\sigma$ become improper if and only if $\mathfrak{G}_\sigma$ is a subgroup of an infinite group with respect to which I is invariant.

By specialization of the groups, Hilbert's original assertion follows from this. By the "translation group" one means the finite group

$$y_i = x_i + \varepsilon_i, \qquad v_i(y) = u_i(x);$$

hence

$$\Delta x_i = \varepsilon_i, \qquad \Delta u_i = 0, \qquad \bar{\delta} u_i = -\sum_\lambda \frac{\partial u_i}{\partial x_\lambda} \varepsilon_\lambda.$$

Invariance with respect to the translation group says, as is known, that in

$$I = \int \cdots \int f\left(x, u, \frac{\partial u}{\partial x}, \dots\right) \mathrm{d}x$$

the x's do not occur explicitly in f. The associated n divergence relations

$$\sum_i \psi_i \frac{\partial u_i}{\partial x_\lambda} = \operatorname{Div} B^{(\lambda)} \qquad (\lambda = 1, 2, \dots, n)$$

are to be called "energy relations", since the "conservation laws" $\operatorname{Div} B^{(\lambda)} = 0$ corresponding to the variational problem correspond to the "energy theorems", and the $B^{(\lambda)}$'s to the "energy components". Thus one obtains: if I admits the translation group, then the energy relations become improper if and only if I is invariant with respect to an infinite group containing the translation group as a subgroup.[189]

An example of such infinite groups is given by the group of all transformations of the x's and of the induced transformations of the $u(x)$'s in which only derivatives of the arbitrary functions $p(x)$ occur. The translation group arises by the specialization $p^{(i)}(x) = \varepsilon_i$. It must remain undecided, however, whether by this means — and by the groups arising through changing I by a boundary integral — the most general such groups have already been given. Induced transformations of the indicated kind arise, for example, by subjecting the u's to the coefficient transformations of a "total differential form", that is, of a form

$$\sum a \, \mathrm{d}^2 x_i + \sum b \, \mathrm{d}x_i \mathrm{d}x_k + \cdots,$$

[189] The energy theorems of classical mechanics, and likewise those of the old "theory of relativity" (where $\sum \mathrm{d}x^2$ goes over into itself), are "proper", since no infinite groups occur here.

which contains, besides the $\mathrm{d}x$'s, also higher differentials. More special induced transformations, in which the $p(x)$'s occur only in first derivatives, are given by the coefficient transformations of ordinary differential forms $\sum c\,\mathrm{d}x_{i_1}\cdots\mathrm{d}x_{i_\lambda}$; these are the ones that have usually been considered.

A further group of the indicated kind — which, because of the occurrence of the logarithmic term, cannot be a coefficient transformation — is, for example, the following:

$$y = x + p(x), \qquad v_i = u_i + \lg(1 + p'(x)) = u_i + \lg\frac{\mathrm{d}y}{\mathrm{d}x};$$

$$\Delta x = p(x), \qquad \Delta u_i = p'(x), \qquad \bar{\delta}u_i = p'(x) - u_i' p(x).$$

Here the dependencies (16) become

$$\sum_i \left(\psi_i u_i' + \frac{\mathrm{d}\psi_i}{\mathrm{d}x}\right) = 0,$$

and the improper energy relations become

$$\sum_i \left(\psi_i u_i' + \frac{\mathrm{d}(\psi_i + \text{const.})}{\mathrm{d}x}\right) = 0.$$

A simplest invariant integral of the group is

$$I = \int \frac{e^{-2u_1}}{u_1' - u_2'}\,\mathrm{d}x.$$

The most general I is determined by integration of the Lie differential equation (11)

$$\bar{\delta}f + \frac{\mathrm{d}}{\mathrm{d}x}(f \cdot \Delta x) = 0,$$

which, after substituting the values for Δx and $\bar{\delta}u$, becomes, as soon as one assumes f to depend on only first derivatives of the u's,

$$\frac{\partial f}{\partial x}p(x) + \left\{\sum_i \frac{\partial f}{\partial u_i} - \sum_i \frac{\partial f}{\partial u_i'}u_i' + f\right\}p'(x) + \left\{\sum_i \frac{\partial f}{\partial u_i'}\right\}p''(x) = 0$$

(identically in $p(x), p'(x), p''(x)$). Already for two functions $u(x)$, this system of equations has solutions that actually contain the derivatives, namely

$$f = (u_1' - u_2')\,\Phi\left(u_1 - u_2, \frac{e^{-u_1}}{u_1' - u_2'}\right),$$

where Φ denotes an arbitrary function of the indicated arguments.

14. The Arithmetic Theory of Algebraic Functions of One Variable in Its Relation to the Other Theories and to Algebraic Number Theory

Report by Emmy Noether in Göttingen.

Jahresbericht der Deutschen Mathematiker-Vereinigung 28 (1919), pp. 182–203

The following report arose from the wish to have a connecting link between the individual theories of algebraic functions; at the same time it may be regarded as a supplement to the report by Brill–Noether,[1] in which the discussion of the arithmetic theory is essentially absent.[2]

For discussions of the individual theories, besides Brill–Noether, the following encyclopedia articles, with the literature indicated there, come into consideration:

For the theory of Riemann: Wirtinger (II B 2), nos. 1–19;

for the theory of Weierstrass: Wirtinger (II B 2), nos. 23, 32, 33, 34;

for the algebraic-geometric theory of Brill–Noether: Wirtinger (II B 2), nos. 21–31; Berzolari (III C 4), nos. 23–38;

for the arithmetic theory of Dedekind–Weber and Hensel–Landsberg: Hensel (II C 5), [cited as Hensel];[3]

more generally, for the arithmetic theory of algebraic quantities: Landsberg (I C 5), and for the arithmetic theory of algebraic functions of several variables: Jung (II C 6).

For algebraic number theory compare Hilbert's "Zahlbericht"[4] and the lectures on number theory by Dirichlet–Dedekind [cited as Dedekind–number theory].[5]

Contents

1. Foundations of the various theories.

2. Parallelism between algebraic numbers and algebraic functions (conjugate elements, basis theorems, module concept).

3. Parallelism and differences in the ideal theory of algebraic numbers and functions.

4. Connection of the arithmetic foundation of series expansion with ideal theory.

5. Comparison of the arithmetic theory of algebraic functions with the geometric theory. Different concept of invariance.

6. Continuation of the comparison. Singular points.

7. Comparison between the residue theorem and theorems of ideal theory.

8. Transcendental questions for algebraic functions and algebraic numbers.

1. Foundations of the various theories

Riemann's theory is the only purely transcendental one, resting on existence theorems (Dirichlet's principle, Schwarz–Neumann methods). The integrals of algebraic functions are here primary, the algebraic functions themselves secondary. The functions on the Riemann surface are characterized by their zeros and poles, corresponding to the polygons (respectively divisors) of the arithmetic theory; whereas Weierstrass also speaks of the functions themselves together with their zeros and poles. The main problem, apart from the existence theorems, is the setting up of all functions with given poles, which is accomplished by integrals of the first and second kind; and, further, the question of the number of arbitrary constants that still enter when the points at infinity are prescribed. This latter question is answered by the Riemann–Roch theorem; corresponding to it in the arithmetic theory is the question of the dimension of a polygon class (respectively divisor class), and in the algebraic-geometric theory the question of the dimension of a complete linear system, whose answer is also provided here by the Riemann–Roch theorem. The actual construction of the functions

[1] The development of the theory of algebraic functions in earlier and more recent times. *Jahresbericht der Deutschen Mathematiker-Vereinigung* vol. 3 (1894) [cited as Brill–Noether].

[2] With the exception of a discussion of Kronecker's investigation of the discriminant. (*J. f. M.* vol. 91.)

[3] The parts concerning Dedekind–Weber are due to A. Ostrowski.

[4] The theory of algebraic number fields. *Jahresbericht der Deutschen Mathematiker-Vereinigung* vol. 4 (1894/95).

[5] Braunschweig, Vieweg, 4th ed. 1894.

is carried out in the arithmetic theory by means of the basis theorems; in the algebraic-geometric theory, by the residue theorem. In particular, the zeros of the integrands of the first kind correspond to the differential class in the arithmetic theory, and to the doctrine of special groups (that is, the pencil of point groups cut out by the adjoint curves of order $(n-3)$, the φ-curves) in the algebraic-geometric theory.

Just as Riemann's theory historically preceded the other theories, even though the rigorous proof of the existence theorems was obtained only later, so also later, with its transcendental aids, algebraic questions were settled which to this day are not yet accessible to a purely algebraic or arithmetic treatment; here above all Hurwitz's theory of singular correspondences is to be mentioned.[6]

Analogies with the transcendental questions in the theory of algebraic number fields will be discussed in the last section.

For the remaining theories the algebraic functions are primary, the integrals secondary. In this respect the Weierstrass theory rests on the transcendental foundations of power-series expansion and the residue theorem; but it then proceeds algebraically, by explicit specification of all functions under consideration.

The arithmetic theory in the form of Hensel–Landsberg also uses the transcendental foundations of series expansion. But by assigning divisors to the individual points on this foundation, it then proceeds purely arithmetically and can thus be viewed as a fusion of Weierstrass and Dedekind–Weber. In contrast with the latter, it simultaneously supplies methods for the actual construction of all basis functions in question. In detail it exhibits a number of simplifications compared with Dedekind–Weber, essentially by the introduction of "fractional" divisors. Recently Hensel[7] has given an arithmetic foundation for the theory of series expansions (apart from a majorant method for the convergence proof), whereby the theory has become almost purely arithmetic.

The algebraic-geometric theory of Brill–Noether presupposes only the concept of "successive points" of a branch, which is reduced to the series expansion at an ordinary point[8] and corresponds to the Weierstrass element concept; it then continues with algebraic-rational methods, essentially those of ternary elimination theory; it too reaches explicit representations.

The original, purely arithmetic theory of Dedekind–Weber[9] is akin to Riemann's in that its theorems again have the character of existence proofs; it preserves complete purity of method.[10] The arithmetic foundation of the theory, where the variables play only the role of indeterminates, runs parallel to the theory of algebraic numbers, as will be explained more closely in 2.[11] This foundation gives the means of introducing the point concept arithmetically (compare Hensel no. 10a) and thus of setting up the concept of the absolute Riemann surface without any consideration of continuity. The theory thereby acquires a formal character; for example, the concept of the differential is also introduced purely formally. On the basis obtained by the point concept, the close kinship with the methods and concepts of the algebraic-geometric theory can be demonstrated, since the latter too, apart from the element concept, is free of transcendental aids; this is to be done in the following sections.

2. Parallelism between algebraic numbers and algebraic functions. (Conjugate elements, basis theorems, module concept)

An algebraic number field is defined as a field of degree n over the field R of rational numbers; a field of algebraic functions of one variable as a field of degree n over the field $K(z)$ of all rational functions of one indeterminate z with arbitrary complex coefficients. Thus for both fields all theorems hold in common which abstract completely from the special nature of the ground field; these are the theorems on bases, norms, traces, and discriminants.[12] All these concepts are introduced by Dedekind–Weber without the use of conjugate elements. It should be noted, however, that the concept of the conjugate field can be defined in an entirely formal way, as Steinitz showed following Kronecker.[13] Namely, if K is an arbitrary field and $\varphi(x)$ a polynomial in x irreducible over K, then the system of residue classes modulo $\varphi(x)$ forms a field. If

[6] A. Hurwitz, Über algebraische Korrespondenzen und das erweiterte Korrespondenzprinzip. *Math. Ann.* vol. 28. (Compare Brill–Noether, section 10.)

[7] *Mathematische Zeitschrift* vol. 4; the foundation is also used as the basis of his report.

[8] For successive "singular" points compare Brill–Noether, section 6, especially nos. 10 and 11. Ordinary successive points are, for example, the points of intersection of the tangent with the curve or higher points of contact (branch points).

[9] *J. f. M.* 92 (cited as D.–W.).

[10] For this reason it is also more suitable for comparison with the other theories than, for instance, the theory of Hensel–Landsberg, which will occur only occasionally in the following comparisons. — The theory of Abelian integrals and their inversion, insofar as it presupposes continuity, is however not treated in D.–W. nor in the further development of the algebraic theory (M. Noether, *Ann.* 37).

[11] A comparison of the theory of Hensel–Landsberg with number theory, especially the theory of p-adic numbers, is found in Hensel.

[12] D.–W., ğ 1 and 2; Hensel no. 4 (with note 5).

[13] Steinitz, Algebraische Theorie der Körper. (*J. f. M.* 137, ğ 6 and 8.)

one assigns to the residue class of x an element ξ, then under the isomorphic assignment the element $f(\xi)$ corresponds to the residue class represented by the polynomial $f(x)$. Since all polynomials divisible by $\varphi(x)$ represent the zero class, $\varphi(\xi)$ is assigned to the zero class; the element ξ can thus symbolically be regarded as a zero of $\varphi(x) = 0$ and generates the algebraic field $K(\xi)$. Repetition of the procedure leads to the n conjugate fields $K(\xi), K(\xi'), \ldots, K(\xi^{(n-1)})$. Thus one may in particular speak of conjugate elements also for algebraic functions, without leaving the purely arithmetic theory.

The two ground fields R and $K(z)$ have the property in common that in them the system of all integral quantities is defined, as rational integers and as integral rational functions of one indeterminate, respectively. These integral quantities have the characteristic property that any two a and b possess a greatest common divisor d that is representable in the form $ma + nb$, where d, m, n are also integral quantities from R or $K(z)$; and indeed d is the absolutely smallest number, respectively the polynomial of lowest degree, representable in this form. On this property alone, which entails the unique decomposition into prime factors for rational integers and for functions of one indeterminate, rest the theorems on the integral quantities of the algebraic or upper field. The argument proving the existence of the greatest common divisor also gives the existence of a fundamental system or a basis of the integral quantities of the algebraic field. If one considers only such bases of the field as consist of integral quantities, then their discriminant becomes a rational integer, respectively a rational function of one indeterminate. Every basis that corresponds to the absolutely smallest number, respectively to the function of lowest degree, forms a fundamental system.

A more precise insight into the basis questions, also for more general fields, is given by the introduction of the module concept, which shall be formulated so as to include the definitions that occur differently in the literature according to the nature of the elements. A module — with respect to a basic domain of integrity $\mathfrak{S}$ — is a system of elements such that the difference of two elements again belongs to the system, and likewise the product of an element with an arbitrary quantity from $\mathfrak{S}$. (If $\mathfrak{S}$ consists of the rational integers, then the second requirement is a consequence of the first.)[14]

Every module that has a basis of finitely many elements through which every element can be represented linearly with coefficients from $\mathfrak{S}$ is called finite (finitely generated); in particular, every one-term module is therefore of the form $c \cdot \alpha$, where α denotes the basis element and c runs through all quantities from $\mathfrak{S}$. *A module whose elements themselves belong to $\mathfrak{S}$ is called an ideal in $\mathfrak{S}$;* whence follows the concept of a finite ideal, and in particular of a one-term ideal (principal ideal).

Now all basis theorems for integral quantities and ideals rest on the following theorem:

If M is a module with respect to $\mathfrak{S}$, whose elements consist of linear forms in n indeterminates with coefficients from $\mathfrak{S}$, and if every ideal in $\mathfrak{S}$ is finite, then M is also a finite module. If in particular every ideal in $\mathfrak{S}$ is a principal ideal, then M possesses a basis of linearly independent forms.[15]

Indeed, if the elements of M are given by $l(x) = a_1x_1 + \cdots + a_nx_n$, then the totality of the coefficients a_1 runs through an ideal in $\mathfrak{S}$, which by hypothesis is of the form $b_1a^{(1)} + \cdots + b_\rho a^{(\rho)}$. The linear form belonging to M,

$$m(x) = l(x) - b_1l^{(1)}(x) - \cdots - b_\rho l^{(\rho)}(x),$$

therefore depends only on $(n-1)$ indeterminates, from which the assertion follows by finitely many repetitions. If in each case $\rho = 1$, then the basis consists of n forms in respectively $n, n-1, \ldots, 1$ indeterminates, which gives the linear independence of the non-vanishing forms.

The theorem on the fundamental system follows from this in the various cases as follows:

If the algebraic field is obtained by adjoining the integral algebraic element δ to the ground field, and if $\mathfrak{S}$ denotes the totality of all integral quantities of the ground field, then every integral quantity of the upper field admits the representation (compare, for instance, Zahlbericht ğ 3)

$$\omega = \frac{a_1\delta^{n-1} + a_2\delta^{n-2} + \cdots + a_n}{\Delta(\delta)},$$

where the a_i are quantities from $\mathfrak{S}$ and $\Delta(\delta)$ denotes the discriminant of δ. By the substitution

$$x_i = \frac{\delta^{n-i}}{\Delta(\delta)}$$

[14]The module concept is due to Dedekind, who first introduced the number module ($\mathfrak{S}$ = rational integers) in the second edition of the number theory; the module of integral linear forms is also implicitly contained there. In Dedekind–Weber the "function modules" occur, whose elements consist of algebraic functions, whereas $\mathfrak{S}$ consists of all integral rational functions of one indeterminate. — The module of homogeneous forms in n indeterminates, more generally of polynomials, occurs first in Hilbert (*Annalen* 36); $\mathfrak{S}$ consists of all polynomials, and since the elements are also polynomials, this module falls under our ideal definition. Kronecker's "module systems" of polynomials start from the basis, not from the abstract definition.

[15]The theorem appears in the literature separately for the different coefficient domains $\mathfrak{S}$. For rational integers compare, for instance, Hilbert, Zahlbericht ğ 3 and 4; for polynomials in several indeterminates: Hilbert, Über die vollen Invariantensysteme: end of ğ 2 (*Math. Ann.* 42).

the module of all integral quantities is transformed into a module of linear forms; hence the existence of the fundamental system follows in all cases where every ideal in $\mathfrak{S}$ is finite. The same argument shows more generally that every ideal in the domain of integral quantities of the upper field is finite. Now in particular for rational integers and for functions of one indeterminate every ideal is a principal ideal; hence it follows that the fundamental systems in algebraic number fields and in fields of algebraic functions of one indeterminate consist of exactly n quantities, when n denotes the degree. And since, in these fields, every ideal is finite by the preceding argument, this at the same time yields the fundamental system for relative fields, which in general will consist of more quantities than the relative degree indicates.[16] Further, if $\mathfrak{S}$ denotes the domain of all polynomials in several indeterminates, every ideal in $\mathfrak{S}$ is also finite;[17] hence the existence of the fundamental system is obtained also for algebraic function fields of several indeterminates, and it will again consist of more quantities than the degree indicates.

3. Parallelism and differences in the ideal theory of algebraic numbers and functions

The proof of the fundamental theorem of ideal theory, that every ideal can be represented uniquely as a product of powers of prime ideals, can be carried out jointly for algebraic numbers and functions; solely on the basis of the property that, for rational integers and for functions of one indeterminate, every ideal is a principal ideal.[18] The main point of the proof lies in showing that, from the divisibility of an ideal $\mathfrak{c}$ by an ideal $\mathfrak{a}$ (that is, every element of $\mathfrak{c}$ is contained in $\mathfrak{a}$), the product representation $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ follows.[19] In Hurwitz this proof rests on the "extended Gauss theorem", which says that an integral quantity ω which divides every coefficient of the product of two polynomials φ and ψ also divides the product of all coefficients of φ and ψ; in Dedekind it rests on a module theorem equivalent to this theorem.[20]

Going further, the concept of the complementary module (Hensel no. 12), and from it the ramification ideal (ground ideal, different) $\mathfrak{D}$, can be defined jointly (its norm becomes the field discriminant D); and the fundamental theorem holds that the ramification ideal $\mathfrak{D}$ is the *greatest common divisor of all principal ideals* $F'(\delta)$; here δ runs through all integral quantities of the field and $F(\delta) = 0$ denotes in each case the corresponding irreducible equation. From this it follows that the *field discriminant contains all and only those rational primes, respectively linear factors in z, which are divisible by the square of a prime ideal.* For $F'(\delta)$ itself one obtains the representation

$$F'(\delta) = \mathfrak{f} \cdot \mathfrak{D},$$

and by taking norms

$$\Delta(\delta) = R^2 \cdot D;$$

here $\mathfrak{f}$ denotes the conductor of the ring derived from δ (order, domain of integrity), that is, $\mathfrak{f}$ consists of the totality of the (integral) quantities which, after multiplication by any integral quantity, are divisible by the module $[1, \delta, \ldots, \delta^{n-1}]$. $R^2 = \operatorname{Norm}\mathfrak{f}$ represents the square of the determinant of substitution that carries the basis $1, \delta, \ldots, \delta^{n-1}$ into a basis of the integral quantities.[21]

Differences in the further development are conditioned by special properties of the ground fields. Thus, in the case of algebraic numbers, the fact that the *elements of the ground field are at the same time exponents* leads to the possibility that the ramification ideal may be divisible by a higher power than the $(e-1)$-st power of a prime ideal $\mathfrak{p}$ which occurs in p to the e-th power (namely when e is divisible by p); and this leads to the further concepts of the inertia field and ramification field,[22] which have no analogue in the

[16] According to Steinitz's investigations on modules of linear forms, where $\mathfrak{S}$ consists of the integers of a (finite) algebraic number field, $\nu+1$ basis elements suffice when ν denotes the relative degree (*Math. Ann.* 71, ğ 4).

[17] By Hilbert's theorem on the module basis (*Math. Ann.* 36). The modules of polynomials here called ideals for the sake of consistency are usually called "form modules" or simply "modules". Hilbert's theorem that such a module N is finite can also be reduced to the theorem on linear forms. Namely, let f be a polynomial of degree n contained in N in the $r+1$ indeterminates $x_1, \ldots, x_r, x_{r+1}$, containing the term x_{r+1}^n (which can always be achieved by a linear transformation); then all polynomials from N are congruent mod. f to those representable in the form $a_1(x)x_{r+1}^{n-1} + \cdots + a_n(x)$; hence, by $x_{r+1}^{n-i} = X_i$, they form a module of linear forms for which every ideal in the domain of r indeterminates may be assumed finite, since this is the case for one indeterminate.

[18] Compare a remark in the introduction to Hurwitz: Über die Theorie der Ideale (*Gött. Nachr.* 1894). In Weber's textbook of algebra the proof, following Kronecker, is carried out in parallel for both fields by means of the introduction of functionals. [The connection between Kronecker's theory and ideal theory is mediated by the "extended Gauss theorem"; Hurwitz, loc. cit.]

[19] Emphasized especially by Dedekind (number theory); Supplement XI, theorem VII, ğ 177; compare the note on p. 554. The theorem uses the fact that algebraic fields are involved; it no longer holds for ideals (modules) of polynomials, where the least common multiple takes the place of the product.

[20] Number theory, Suppl. XI; theorem VI, ğ 173. Dedekind points out the equivalence of the two theorems (Über die Begründung der Idealtheorie, *Göttinger Nachr.* 1895).

[21] Dedekind, Über die Diskriminante endlicher Körper (*Abhandl. der Gött. Ges. d. Wissensch.* vol. 29, 1882). The definitions given there for algebraic numbers can be transferred directly to algebraic functions; the proofs too can be transferred almost exactly. The order of proof in D.–W. is different: see below. For the cited theorems compare also Zahlbericht, ğ 31 and 32. ($F'(\delta)$ is there called the "different" of the integer δ.)

[22] Compare Zahlbericht, ğ 39–45.

theory of algebraic functions. Above all, however, because of the *existence of infinitely many constants* in the ground field, the finiteness of the number of ideal classes disappears for algebraic functions, and with it all questions connected with determining the class number. Nevertheless, in a certain sense the domain of all (transcendental) prime forms[23] may be regarded as a transcendental analogue of the class field; for here every point is generated by a single form, a principal ideal.

On the other hand, the existence of infinitely many constants in the ground field $K(z)$ leads, for algebraic functions, to theorems and questions which have no analogue for algebraic numbers. First, a certain simplification in the arrangement of the proof follows from this; for example in the proof given by D.–W. of the unique factorization of ideals into prime ideals, where the "extended Gauss theorem" or a theorem equivalent to it can be avoided by using the fact that every linear form $(z - c)$ has infinitely many residue classes, namely all constants (whereas the number of residue classes modulo a prime number is finite).[24]

The further fact that every polynomial with integral rational functions of z as coefficients decomposes into linear factors mod. $(z - \alpha)$ (which is not the case for an integral polynomial mod. p) leads to genuinely new results; this fact also still holds if, instead of all constants, one takes only all algebraic numbers.[25] From this it follows, namely, that every prime ideal is an ideal of first degree;[26] and further, that the field discriminant D becomes the intersection of all discriminants $\Delta(\delta)$, where δ runs through all integral quantities;[27] both are in contrast to algebraic numbers. Subsequently it again follows from this that the ramification ideal is the intersection of all principal ideals $F'(\delta)$.

Further differences are conditioned by the fact that, for algebraic numbers, the ground field R of rational numbers is something absolutely distinguished, namely the prime field contained in the field (that is, the field derived from the unit); whereas the ground field $K(z)$ is something relative. Every nonconstant function ξ may be chosen as independent variable; the field then becomes an algebraic field over $K(\xi)$. The theorem that every prime ideal $\mathfrak{p}$ is an ideal of first degree, hence every function is congruent modulo $\mathfrak{p}$ to a constant, combined with the possibility of taking an arbitrary function as independent variable, leads to the most important concept going beyond algebraic numbers, the point concept in purely arithmetic form. (Compare Hensel 10a.) "Every point is represented here by a field of constants isomorphic to the function field."[28] The totality of points so defined forms the "absolute Riemann surface". This definition of point depends only on the field, not on a special variable. The existence proof, however, is carried out by distinguishing some function as independent variable z; a point P is generated by a prime ideal $\mathfrak{p}$ by assigning to every function its constant residue modulo $\mathfrak{p}$; thus in particular the functions divisible by $\mathfrak{p}$ vanish at P, and conversely. As $\mathfrak{p}$ runs through all prime ideals in z, all points in which z is finite are thereby obtained; the remaining points arise by introducing the independent variable $\xi = 1/z$ and correspond to the prime ideals which divide the principal ideal ξ. Naturally, the concepts attached to the point concept also can have no analogue for algebraic numbers; such as the concept of a polygon, of a polygon class, of the dimension of a polygon class, and so on.

It should also be noted that the free choice of the independent variable leads to a further interpretation of the decomposition $F'(\vartheta) = \mathfrak{f} \cdot \mathfrak{D}$. Namely, if one considers ϑ as independent variable, then correspondingly one obtains

$$\left(\frac{\partial F}{\partial z}\right) = \mathfrak{f} \cdot \mathfrak{a},$$

since the ring derived from ϑ was defined symmetrically with respect to z and ϑ; and $\mathfrak{f}$ becomes the greatest common divisor of the two principal ideals $\frac{\partial F}{\partial z}$ and $\frac{\partial F}{\partial \vartheta}$; the conductor $\mathfrak{f}$ becomes at the same time the "double-point ideal" with respect to ϑ, z.[29]

4. Connection of the arithmetic foundation of series expansion with ideal theory

In Hensel–Landsberg the transcendental aid of series expansion and the point concept borrowed from function theory take the place of ideal theory. Hensel's recently given arithmetic foundation of series expansion for algebraic numbers and functions[30] can therefore be regarded as an equivalent of ideal theory. In fact this

[23] Klein, Zur Theorie der Abelschen Funktionen (*Ann.* 36, 1890).

[24] D.–W. ğ 9. Compare the notes on pp. 212 and 213.

[25] D.–W. note in the introduction that in this case the whole theory remains intact.

[26] D.–W., ğ 9, no. 7.

[27] D.–W., p. 224.

[28] Two fields are, as is well known, called "isomorphic" if they can be put in one-to-one correspondence in such a way that sum, difference, product, and quotient also correspond.

[29] D.–W. p. 263.

[30] Eine neue Theorie der algebraischen Zahlen (*Math. Zeitschr.* vol. 2, 1918) and Neue Begründung der arithmetischen Theorie der algebraischen Funktionen einer Variablen (*Math. Zeitschr.* vol. 4, 1919). For a more detailed exposition compare Hensel no. 44ff.

arithmetic foundation amounts to passing, for each prime ideal, to such a (transcendental) extension field in which this prime ideal becomes a principal ideal, so that the usual decomposition theorems hold; and it suffices to carry out this consideration for all prime ideals occurring in one prime number p, respectively one linear function $z - a$.

First one introduces a transcendental extension field formed by all series expansions in integral powers of $z - a$, respectively p (p-adic numbers), with in each case at most finitely many negative powers. In this field the irreducible equation defining the algebraic number field or function field decomposes into the product of ρ irreducible factors, corresponding to the decomposition of p, respectively $z - a$, into the product of the ρ "primary" ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_\rho$. The further representation of each primary ideal as a power of a prime ideal,

$$\mathfrak{q}_i = \mathfrak{p}_i^{\ell_i},$$

corresponds in Hensel to the introduction of a further field, algebraic with respect to the transcendental extension field. And in the case of algebraic functions this field can be defined by a pure equation; in the case of algebraic numbers, more generally, by an algebraically solvable equation. The simplification for algebraic functions is due to the fact that here no inertia and ramification fields (compare no. 3) occur.

The "terminating series" in a prime element π[31] that occurs in these investigations (and which does not yet require a transcendental convergence proof)

$$v = c_0 + c_1\pi + \cdots + c_{\sigma-1}\pi^{\sigma-1} - v_\sigma\pi^\sigma,$$

where $c_0, \ldots, c_{\sigma-1}$ are constants and v_σ denotes an integral element of the field, is found in exactly corresponding form in D.–W.[32] There it is derived from ideal theory and gives the basis for defining the order of vanishing (respectively becoming infinite) of a function at a point.

5. Comparison of the arithmetic theory of algebraic functions with the geometric theory. Different concept of invariance

"Invariant" means any concept characterized by the field alone. In the arithmetic theory this invariance is in general already given in the definition, which is stated with respect to all elements of the field, not with respect to some basis or distinguished variable; the point concept given above is an example. By contrast, the remaining theories start from some special variable or basis and show afterwards the independence of the concept from this special choice; invariance here becomes invariance under birational transformation.

Namely, suppose that the field arises on the one hand by adjoining the algebraic element s to $K(z)$, and on the other by adjoining σ to $K(\xi)$, where $f(z, s) = 0$, respectively $F(\xi, \sigma) = 0$, denote the irreducible equations for s, respectively σ; or, still more generally, by adjoining a finite number of elements to $K(\eta)$, with the corresponding irreducible equations

$$g_1(\eta, \tau_1) = 0, \qquad g_2(\eta, \tau_1, \tau_2) = 0, \ldots.$$

Then, by definition, all elements can be expressed rationally by z and s, just as by ξ and σ, and also by $\eta, \tau_1, \tau_2, \ldots$. In particular z and s are therefore rationally expressible by ξ and σ, and conversely; likewise z and s rationally by $\eta, \tau_1, \tau_2, \ldots$, and conversely. The plane curve $f(z, s) = 0$ thus goes by "birational transformation" into the plane curve $F(\xi, \sigma) = 0$, or also into the curve in the space of variables $\eta, \tau_1, \tau_2, \ldots$ defined by $g_1(\eta, \tau_1) = 0; g_2(\eta, \tau_1, \tau_2) = 0, \ldots$. Invariance therefore appears in the fact that a definition stated for one special curve remains valid for all curves obtained from it by birational transformation (in a space of arbitrarily many dimensions); for all curves of the "class" in Riemann's sense. A "point" is here defined as a coherent system of values $z = a, s = b$, so that $f(a, b) = 0$; under birational transformation this point generally goes again into a coherent system of values α, β of $F(\xi, \sigma) = 0$, but in special cases, when a, b was a "singular" point, it can correspond to several "points" on $F(\xi, \sigma) = 0$; and one can always specify curves on which a "singular" point of $f(z, s) = 0$ corresponds to a finite number of simple points lying separately or successively (resolution of singularities).[33] Likewise a point group again goes into a point group; and the number of its points is invariant as soon as one counts a singular point as as many points as the simple points corresponding to it under a suitable transformation. Since every curve can be transformed birationally into one with "ordinary multiple" points,[33] the geometric theory develops its concepts only for such special curves

[31] Neue Begründung ..., formula (11).

[32] D.–W., p. 231 and ğ 15.

[33] Compare, for instance, Brill–Noether, section 6. More precise information on "singular" points appears in the next section.

and then proves the invariance under every birational transformation, including one which leads to the most general singular points.

In particular, as a distinguished curve of the "class" — excluding the hyperelliptic case — one can introduce the so-called "normal curve of the φ's" in the space of $(p-1)$ dimensions, which has no singular points; here the φ's are the p "adjoint curves of order $(n-3)$" for the homogenized $f(z,s)=0$. A birational transformation of $f(z,s)=0$ into $F(\xi,\sigma)=0$ corresponds to a linear transformation of the φ's, so that this is invariance in the projective sense. The representation of all functions of the field as rational functions of the φ's is called the "invariant representation" in the geometric theory.[34]

The linear system of the φ's, or also of the "special groups" cut out by them, therefore goes into itself under every birational transformation, and is consequently characterized by the field alone. It corresponds to the differential class in the arithmetic theory, where the invariance is again shown directly in the definition, which is given by properties with respect to every function of the field as independent variable.

6. Continuation of the comparison. Singular points

The different conception of the point concept is connected with the fact that the "singular points" of curves, which cause special difficulties in the algebraic-geometric theory, do not occur at all in the foundations of the arithmetic theory; and consequently the "adjoint functions" are not required for the construction of the arithmetic theory, as they are in the geometric theory, but belong to special higher parts of the theory. On the other hand, the branch points do not occur in the foundations of the geometric theory; in fact, they also drop out in the representation of the integrals in Aronhold's normal form (Hensel no. 27, formula 80).

The definition of singular point given in 5 can be formulated as follows: $f(z,s)=0$ (respectively a curve in a higher-dimensional space) has a singular point at $z=a, s=b$ (respectively $z=a; s_i=b_i$) if this system of values is assumed by more than one point of the absolute Riemann surface (point in the arithmetic sense), or if it is assumed at one or several points with higher order. In the latter case one has a point of the ramification polygon of z as well as of s; this corresponds to the "successive points" of the geometric theory; the point becomes a (higher) cusp point of $f(z,s)=0$ (respectively of the curve in the higher-dimensional space).

Since by hypothesis every arbitrary function η of the field can be represented rationally by z and s, because of the isomorphism every point of the absolute Riemann surface at which $z=a, s=b$ is obtained by assigning to every function η, represented by z and s, its value for $z=a, s=b$. Thus, for the point to be singular, there must be at least one function η which assumes several values or one system of values several times for $z=a, s=b$. And because of rational representability by z and s, this can be the case only when in this representation numerator and denominator vanish simultaneously for $z=a, s=b$. It follows that the above definition is identical with the usual one, namely that

$$f, \quad \frac{\partial f}{\partial z}, \quad \frac{\partial f}{\partial s}$$

vanish for $z=a, s=b$. For in this case

$$\eta = \frac{\frac{\partial f}{\partial z}}{\frac{\partial f}{\partial s}}$$

is a function of the indicated kind which is multivalued for $z=a, s=b$, whereas in the opposite case every function, even if it becomes $0/0$, assumes only one value.

With the arithmetic point concept the singular point cannot occur, since two points are regarded as different as soon as only one function is assigned different systems of values. But even in the ideal theory serving to found the arithmetic point concept, the concept of a singular point does not occur, precisely because the totality of all integral quantities of the field is always considered at the same time. All singular points in the finite part of $F(z,\delta)=0$, where δ is algebraically integral with respect to z, are generated (according to the second definition and the end of no. 3) by the "double-point ideal" $\mathfrak{f}$. Now, since by the fundamental theorem the ramification ideal $\mathfrak{D}$ is the greatest common divisor of all principal ideals $F'(\delta)$, for every prime ideal $\mathfrak{p}$ one can specify a δ such that the corresponding $\mathfrak{f}$ is not divisible by $\mathfrak{p}$, and consequently — since $\mathfrak{f}$ is the greatest common divisor of $F'(\delta)$ and $F'(z)$ — at least one of the two principal ideals $F'(\delta)$ and $F'(z)$ is not divisible by $\mathfrak{p}$. Thus there is *no system of values for which all $F'(\delta)$ and $F'(z)$ vanish simultaneously*, and consequently the system of values $z=a, \delta_i=b_i$ is assumed at only one point of the

[34] Compare, for instance, Brill–Noether, section 8. For algebraic functions of several variables the question whether invariance can be reduced to such invariance under linear transformation is not treated.

absolute Riemann surface; the *totality of integral algebraic functions of the field* (which may be interpreted as a curve in a space of infinitely many dimensions) *has no singular point in the finite part*; only finite values enter into consideration in ideal theory.

But the basis functions $\omega_1, \ldots, \omega_n$ of all integral quantities also have no singular points in the finite part. By the preceding, each point in the arithmetic sense is already uniquely determined by a system of constants isomorphically assigned to all integral functions. If, therefore, a "space curve" defined by any integral functions s_i has a singular point in the finite part for $s_i = \alpha_i$, then there must be at least one integral function η which assumes several systems of values for $s_i = \alpha_i$. If now $\omega_1, \ldots, \omega_n$ denotes a basis of all integral quantities, then, because $\delta = a_1\omega_1 + \cdots + a_n\omega_n$ with integral rational a_i, each system of values of the ω's corresponds to only one system of values of δ; hence the space curve defined by $\omega_1, \ldots, \omega_n$ can possess no singular point in the finite part; and *every point of the absolute Riemann surface at which z is finite is already uniquely defined by a system of constants isomorphically assigned to the ω's. The basis functions are precisely the functions η which become multivalued for $s_i = \alpha_i$.* Thus by introducing the basis of integral quantities, for example in place of a basis $1, \delta, \ldots, \delta^{n-1}$, the difficulty of singular points is avoided.

In the geometric theory the task of generating all points of the absolute Riemann surface uniquely — more generally, of forming all functions which become infinite at given points — is accomplished by means of adjoint forms and their quotients. A form ψ is called adjoint if $\psi = 0$ has at least an $(i-1)$-fold point at each i-fold point of the base curve $f(z, s) = 0$; a higher singular point must first be resolved into ordinary multiple points. It was shown above that, for the most general function $\eta = \frac{\psi}{\chi}$, numerator and denominator must vanish at all singular points of $f(z, s) = 0$; that they must be adjoint is shown by considering the everywhere finite differentials. That, conversely, the conditions of adjointness are also sufficient for forming the most general function is shown by the "residue theorem", which will be discussed more closely below. Thus the adjoint functions take the place of the basis functions of the arithmetic theory.

Arithmetically, an adjoint form corresponds to the numerator of a function of the field divisible by the "double-point ideal" $\mathfrak{f}$, as soon as one assumes the singular points — which can always be achieved by transformation — all to lie in the finite part. From this the representation of the basis quantities $\omega_1, \ldots, \omega_n$ as quotients of adjoint forms, and hence the connection among the various ways of representing them, is shown formally as follows:

Let $R(z)$ denote the determinant of substitution of a basis $1, \delta, \ldots, \delta^{n-1}$ into a basis $\omega_1, \ldots, \omega_n$. Conversely, every ω can then be expressed as a quotient of an integral function of z and δ by $R(z)$:

$$\omega_i = \frac{G_i(z, \delta)}{R(z)}.$$

Since $R(z)\omega_i$ belongs to the ring derived from δ, by the definition of the conductor $R(z)$ is divisible by $\mathfrak{f}$ [from $(R(z))^2 = \operatorname{Norm}\mathfrak{f}$ this divisibility follows only for $(R(z))^2$]. Since now ω_i, as an integral function, remains finite for all finite z, the numerator function $G_i(z, \delta)$ must also be divisible by $\mathfrak{f}$; numerator and denominator of all ω_i are therefore adjoint. From this representation of the ω's follows, however, the representation of all functions of the field by quotients of adjoints.

According to the preceding, the geometric theory can be characterized as the *theory of the ring derived from a quantity δ* (order), in contrast with the arithmetic theory, which considers *all integral quantities* simultaneously. Thus it is clear that the conductor of the ring — the singular points — plays a decisive role. Further analogies between the arithmetic theory of rings (orders) and the geometric theory can also be given. Thus the geometric theory does not count the intersection points that fall into the singular points in the intersection with adjoint curves, but considers only the point groups different from these. Corresponding to this is that Dedekind[35] considers only such ring ideals as are prime to the conductor ideal $\mathfrak{f}$, and for this domain of ideals sets up all divisibility laws, including unique decomposition into prime ideals.

Also the "fundamental theorem of algebraic functions"[36] underlying the geometric theory, or at least an immediate consequence of it, has in a certain sense an analogue in the arithmetic theory of rings. This theorem gives the conditions for a representability

$$\psi(z, s) = A(z, s)f(z, s) + B(z, s)\varphi(z, s),$$

where all quantities occurring are integral rational in s, z (more generally integral and homogeneous in x_1, x_2, x_3). From these conditions it follows,[37] by virtue of $f(z, s) = 0$, that the quotient $\frac{\psi}{\varphi}$ is always equal

[35] Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers. (Festschrift Braunschweig 1877); ğ 3–5. (The theorems stated in these paragraphs for algebraic numbers hold literally for algebraic functions of one variable.)

[36] M. Noether, Über einen Satz aus der Theorie der algebraischen Funktionen. *Math. Ann.* vol. 6 (1873).

[37] Brill–Noether, no. 55.

to an integral rational function $B(z,s)$ when it is adjoint to f. Corresponding to this is the theorem from no. 3, which underlies all these comparisons, that the conductor $\mathfrak{f}$ of a ring derived from δ is equal to the double-point ideal of $f(z,\delta)=0$. For, by the definition of the conductor, every algebraic integral quantity divisible by $\mathfrak{f}$ belongs to the ring, and is therefore integral and rationally representable by z and δ; whereas the cited theorem says that such a quantity is an adjoint function.[38]

7. Comparison between the residue theorem and theorems of ideal theory

The just mentioned consequence of the "fundamental theorem of algebraic functions" leads in the geometric theory directly to the "residue theorem", and thus to the foundation on which the whole geometric theory is built. In a certain respect, however, the residue theorem again has a more elementary character than the remaining foundations, insofar as it can be stated arithmetically as a direct consequence of the unique factorization of ideals into prime ideals, or rather of the facts underlying this decomposition theorem, and therefore does not rest on the higher theory of rings. One is led to this arithmetic formulation as follows:

Assume the base curve $f(z,\delta)=0$ — as can always be achieved by a linear fractional transformation of the variables — to be such that the singular points and the finitely many point groups under consideration lie in the finite part; and further that δ depends algebraically integrally on z, which can always be achieved by a subsequent linear transformation integral in the variables. Then to a prime ideal $\mathfrak{p}$ generating a point P of the absolute Riemann surface at which $z=a,\delta=b$, there corresponds the point $z=a,\delta=b$ of $f(z,\delta)=0$; more generally, an ideal $\mathfrak{a}=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_\rho^{e_\rho}$ generates the point group consisting of the points $z=a_i,\delta=b_i$ with the corresponding multiplicity; and all points of $f(z,\delta)=0$ lying in the finite part are so generated. Since at a point P all functions $g_1,g_2,\ldots$ divisible by $\mathfrak{p}$ vanish, and since conversely this totality of functions g generates the ideal $\mathfrak{p}$, the corresponding point on f is the intersection of

$$g_1(z,\delta)=0,\quad g_2(z,\delta)=0,\ldots$$

with $f=0$; the same holds for the point group corresponding to an ideal $\mathfrak{a}$. Indeed, by the theorem that every ideal is the greatest common divisor of two principal ideals, two such curves always suffice to cut out a point group. In particular, the point group corresponding to a principal ideal is cut out by a curve $g(z,\delta)=0$ and conversely; the principal ideal corresponds to the complete intersection.

Two point groups A and B are called *coresidual* in the geometric theory if they can be completed with the same point group R to a full intersection. If these point groups are generated respectively by the ideals $\mathfrak{a},\mathfrak{b},\mathfrak{r}$, then between these ideals one has the relation

$$\mathfrak{a}\cdot\mathfrak{r}=(\alpha),\qquad \mathfrak{b}\cdot\mathfrak{r}=(\beta),$$

which shows that the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent. Conversely, from the equivalence of two ideals, $\mathfrak{a}=\eta\mathfrak{b}$, this relation always follows on the basis of the theorem that every ideal can be transformed into a principal ideal by multiplication by another ideal;[39] *equivalent ideals and coresidual point groups are therefore identical concepts.*

The residue theorem now says: *If A and B are coresidual, then they can be cut out by adjoint curves with the same residue (outside the singular points).* Since the zeros and poles of a function are always coresidual, this proves at the same time that the most general functions of the field are representable as quotients of adjoint forms. In the language of ideal theory the residue theorem simply amounts to saying that, besides $\mathfrak{a}$ and $\mathfrak{b}$, $\mathfrak{a}\mathfrak{f}$ and $\mathfrak{b}\mathfrak{f}$ are also equivalent, where $\mathfrak{f}$ denotes the double-point ideal. For then, by the above, there always exists an ideal $\mathfrak{m}$ such that

$$\mathfrak{a}\mathfrak{f}\mathfrak{m}=(\alpha),\qquad \mathfrak{b}\mathfrak{f}\mathfrak{m}=(\beta)$$

become principal ideals; $\alpha=0$ and $\beta=0$ are the adjoint curves which cut out the point groups A and B, respectively their subgroups A' and B' different from the singular points.[40] The proof of the residue theorem is therefore arithmetically contained in the possibility of assigning points to prime ideals, and in the proof that equivalent ideals can be transformed into principal ideals by multiplication by one and the same ideal.

[38] Following Dedekind, the assumption is made here throughout that δ is an algebraic integer (which can always be achieved by transformation). The case more exactly corresponding to geometry, $f(z,s)=0$, where s may also depend algebraically fractionally on z, is treated by Hensel–Landsberg; compare Hensel no. 26 and 29.

[39] Compare Dedekind, number theory ğ 181; namely, if $\mathfrak{r}$ is chosen so that $\mathfrak{a}\mathfrak{r}$ becomes a principal ideal (α), then $\mathfrak{b}\mathfrak{r}=\eta^{-1}\cdot(\alpha)$; and since $\mathfrak{b}\mathfrak{r}$ contains only integral quantities, the same holds for $\eta^{-1}\cdot(\alpha)$, which is therefore also a principal ideal (β).

[40] If $\mathfrak{a}=\mathfrak{f}\mathfrak{a}_1,\ \mathfrak{b}=\mathfrak{f}\mathfrak{b}_1,\ \mathfrak{r}=\mathfrak{f}\mathfrak{r}_1$, where $\mathfrak{a}_1,\mathfrak{b}_1,\mathfrak{r}_1$ are relatively prime, then already $\mathfrak{a}_1\mathfrak{f}\mathfrak{n},\ \mathfrak{b}_1\mathfrak{f}\mathfrak{n}$ become principal ideals, where $\mathfrak{n}$ is prime to $\mathfrak{f}$. For every ideal can be transformed into a principal ideal by multiplication with an ideal that is prime to a given one (D.–W. p. 214; or number theory, ğ 178, theorem XI).

Corresidual point groups need not consist of the same number of points; just as equivalent ideals need not be of the same degree. Thus, for example, all principal ideals are equivalent, and all point groups generated by complete intersections are coresidual. This difference as against equivalent polygons (divisors)[41] is explained by the fact that those points at which z becomes infinite are not generated by prime ideals in z. In the representation of a function as an ideal quotient $\eta = \frac{\mathfrak{a}}{\mathfrak{b}}$, which states the equivalence of $\mathfrak{a}$ and $\mathfrak{b}$, the zeros or poles of η at which z becomes infinite therefore do not appear. For instance, the principal ideal (α) becomes the product of the prime ideals corresponding to the zeros of the integral function α; the poles of α do not occur, since α becomes infinite only at points where z becomes infinite. In this respect ideal theory is the exact analogue of form theory in the geometric theory, where there are likewise only zeros and no poles.

The passage from forms to functions is made geometrically by forming quotients of forms of the same order; arithmetically, this corresponds to the passage from ideal classes to the invariantly defined polygon (divisor) classes. For, since no variable is distinguished here any longer, the representation of a function by polygon quotients gives all zeros and poles. The relation of ideal class (class of coresidual point groups) to polygon class is the following: if $\mathcal{A}$ and $\mathcal{B}$ are the polygons generated by the ideals $\mathfrak{a}$ and $\mathfrak{b}$, and $\mathcal{N}$ is the polygon of the points at which z becomes infinite (the denominator polygon of z and of the integral functions of z), then from the equivalence of $\mathfrak{a}$ and $\mathfrak{b}$ follows the equivalence of $\mathcal{A}$ and $\mathcal{B}$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ have the same degree; in general only the equivalence of $\mathcal{A}\mathcal{N}^\nu$ with $\mathcal{B}\mathcal{N}^{\nu'}$ $(\nu \neq \nu')$ follows. The division of ideals (respectively of coresidual point groups) into classes is thus a gathering together of infinitely many polygon classes into one class; it may also be viewed as a division of the polygons into classes modulo a power of $\mathcal{N}$.[42]

The residue theorem for the case of coresidual point groups consisting of different numbers of points occurs only in purely geometric questions. In the application to algebraic functions, in fact only the case corresponding to polygon classes occurs, that of coresidual point groups of the same number. The "complete linear system" generated by a point group, that is, the totality of point groups coresidual to this point group and of the same number of points, corresponds exactly to the polygon class generated by the corresponding polygon; the concepts "sum of two complete systems" and "product of two polygon classes" also coincide. That such a complete system contains only finitely many linearly independent point groups is a direct consequence of the residue theorem, which reduces the dimension of the system (the number of linearly independent point groups) to the dimension of all adjoint curves of arbitrary but fixed order passing through the residual group. In order to arrive at the actual determination of this dimension, the Riemann–Roch theorem, the geometric theory first derives from the residue theorem the "reduction theorem" (theorem on the fixed points);[43] and from this the Riemann–Roch theorem.

Quite correspondingly, the arithmetic theory shows that every class of polygons is of finite dimension, and determines its dimension by a special basis of the integral quantities, a normal basis defined by means of the complementary module; thus it obtains the Riemann–Roch theorem as a consequence of the connection of the complementary module with the ramification polygon. In the presentation of D.–W. the reduction theorem also occurs,[44] though not as a foundation as in the geometric theory. In consequence of the correspondence mentioned in no. 6 between basis and adjoint functions, a certain correspondence of the auxiliary means in the two theories can also be established here. In summary, one may say that the formations of concepts in the two theories essentially coincide, even though, apart from formulation, they differ in their arrangement. The two theories arose independently of one another, the geometric one a decade earlier. It should also be noted that the Riemann–Roch theorem originally, in Riemann and Roch and also in Weierstrass, occurs as a rank theorem; what is at issue is the rank of the matrix $(\varphi_i(x_j))$, where the φ's run through the p adjoint curves of order $n-3$, and the x's through the points of the residual group.

8. Transcendental questions for algebraic functions and algebraic numbers

Hilbert in particular pointed out analogies between transcendental questions for algebraic functions and for algebraic numbers;[45] these are essentially existence questions. Thus Riemann's question concerning the existence of an algebraic function for a given Riemann surface (hence also for given branch points) corresponds

[41] A polygon A consists of finitely many points of the absolute Riemann surface; two polygons A and B are called equivalent if they are the zeros and poles of a function η; η then admits the representation by polygon quotients $\eta = \frac{A}{B}$. (D.–W. ğ 17 and 18.)

[42] Hensel–Landsberg, 25th lecture, p. 438. — If one represents the two variables z and s by polygon quotients, then this can be understood as binary homogenizing of each of these variables; if one chooses in particular z and s so that they have the same denominator polygon, then the ternary homogenizing customary in geometry arises.

[43] Brill–Noether, no. 58.

[44] D.–W., ğ 30, no. 2.

[45] Mathematische Probleme, problem 12. (*Göttinger Nachrichten* 1900).

to the question of the existence of algebraic number fields with prescribed group and discriminant.[46] Whereas in the case of algebraic functions the existence proof can be carried out in general, in the domain of algebraic number fields it has been achieved only for special ground fields (rational numbers, quadratic number fields) and only for Abelian groups.[47] This concerns Kronecker's theorem that every Abelian number field over the rational numbers can be assembled from fields of roots of unity, and the corresponding theorems of Fueter[48] and Hecke[49] for relatively Abelian number fields. Thus the desired number fields are actually supplied by a transcendental means, exponential functions, modular functions; in contrast with the pure existence proof for algebraic functions.

The existence proof of algebraic functions is preceded by the existence of everywhere finite integrals. An analogue of this is the existence of the "singular primary numbers" of an algebraic number field defined with respect to a prime number ℓ, whose ℓ-th roots are relatively unramified and supply the first building blocks for the class field.[50] This existence proof is carried out with essential help from the theorem that in the number field there always exist prime ideals with prescribed residue characters; this theorem may therefore be regarded as an analogue of the boundary-value problem on which the existence of the everywhere finite integrals rests.

The everywhere finite integrals provide a transcendental criterion for determining whether two polygons belong to the same class (two point groups of the same number are coresidual), namely by Abel's theorem, which says that the integrals of the first kind, extended over "coresidual paths", vanish; or by the corresponding differential theorem together with its converse.[51]

As the analogue of Abel's theorem for algebraic number fields one must take the "reciprocity law for ℓ-th power residues", which gives, for the field itself or at least for a suitable upper field, a criterion that two ideals belong to the same class. Its content can also be formulated by saying that in this upper field the singular primary numbers have the same residue character with respect to all ideals of the same class. This latter fact also holds in the field itself, but there it does not coincide with the reciprocity law.[52]

Finally, Hensel's theory of p-adic numbers supplies the analogue of the power-series expansion of algebraic functions; for this, see Hensel's report.

[46] The treatment of algebraic functions suggested thereby, starting from the group, was carried out by R. König as a special case of more general questions; compare especially: Riemannsche Funktionen- und Differentialsysteme in der Ebene (*J. f. M.* vol. 148) and *Math. Ann.* 78, 79. In place of the algebraic field, König has a special finite module with respect to $K(z)$: there is only "class property".

[47] Only the simple case of the groups occurring for equations of third and fourth degree, and some quite special groups for equations of degree 8, can be handled for arbitrary ground fields: G. Bucht, Über einige algebraische Körper 8. Grades (*Arkiv f. Math., Astron. och Physik*, vol. 6, no. 30.) Compare also E. Noether, Gleichungen mit vorgeschriebener Gruppe and the Seidelmann dissertation cited there. (*Math. Ann.* 78).

[48] *Math. Ann.* 75.

[49] *Math. Ann.* 76.

[50] Furtwängler, Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern. *Math. Ann.* 67 and 72.

[51] Compare, for example, the formulation in M. Noether (*Ann.* 37). Since the residue theorem historically grew out of Abel's theorem, the geometric theory speaks of the "sum" of point groups and linear systems, following the integral sums; in contrast to the "product" of the classes in the arithmetic theory.

[52] Furtwängler, loc. cit.

15. The Finiteness of the System of Integral Invariants of Binary Forms

15. The Finiteness of the System of Integral Invariants of Binary Forms

Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen 1919, pp. 138–156

By

Emmy Noether in Göttingen.

Presented by F. Klein in the session of 27 March 1919.

In what follows, as an extension of the known finiteness theorem, the following theorem is proved: *All polynomial integral invariants of a binary system of ground forms are polynomial rational functions, with integral coefficients, of a finite number among them.* Here, as usual, by an "invariant" one always means a polynomial rational invariant of a ground form or of a system of ground forms, namely an invariant with respect to the coefficient transformation induced by the group of all linear transformations.

The proof rests on an integrality sharpening of the Mertens-Hilbert proof of finiteness.[53] This proof of finiteness may be characterized as follows. One decomposes the ground forms into their linear factors - more precisely, one associates to each ground form a product of linear forms - whereby each invariant I is changed into an invariant of these linear forms, hence into a function of the homogenized roots. This function has to satisfy three conditions: 1) the condition of invariance, 2) weight conditions, and 3) symmetry conditions. Conditions 2) and 3) are necessary for I to become polynomial and rational in the coefficients of the ground forms. Condition 1) is satisfied by representing I as a polynomial rational function of the determinants of the linear forms; condition 2) by taking, instead of the individual determinants, certain products of powers of them as new arguments. Condition 3) then simply says that I becomes a polynomial rational symmetric function of rows of quantities, and that conversely every such symmetric function of rows of quantities becomes an invariant of the ground forms. The elementary symmetric functions of these rows of quantities therefore give the complete system.

If one considers only integral invariants, condition 1) can be satisfied just as above as soon as, for invariants of linear forms, the sharper theorem is proved that *all integral invariants of binary linear forms are polynomial integral functions of the determinants of these linear forms.* I show that this is in fact the case in ğ 3, in the form that the totality of all relations modulo any prime between these determinants coincides with the totality of all identical relations; that is, the module corresponding to these relations remains a prime module modulo every prime number. This verification is carried out by normalizing the residue classes with respect to the module of quadratic forms corresponding to the quadratic relations between the determinants; these quadratic forms thereby turn out to form an integral basis of the module, modulo every prime, whereas previously they were known as a module basis only when integrality was disregarded.

To satisfy condition 2) no alteration is needed, since the introduction of products of powers does not affect the integer coefficients. Condition 3) now says that $n_1! \cdots n_\mu! I$ (where $n_1, \ldots, n_\mu$ are the degrees of the individual ground forms) becomes an integral symmetric function of rows of quantities, and conversely every integral symmetric function of these rows becomes an integral invariant. But, as is easily shown, these integral symmetric functions of rows possess an integral basis, for which the elementary functions alone no longer suffice. The application of Hilbert's theorem on the integral module basis then also yields an integral basis for the I themselves.

Section 1 collects the special finiteness theorems corresponding to conditions 1), 2), and 3), from which the proof of finiteness follows in ğ 2. The special finiteness theorems corresponding to condition 3) also yield the finiteness of the integral invariants of finite groups of integral or algebraic-integral substitutions, as is briefly carried out in ğ 4.

[53] F. Mertens, Wiener Sitzungsberichte Jan. 1889; D. Hilbert, *Math. Ann.* vol. 33 (1889) [dated March 1888]. The two proofs, which arose independently of one another following Mertens, Crelle vol. 100, agree in content.

ğ 1. Special Finiteness Theorems

I first state the following special finiteness theorems, which will serve to satisfy the conditions of invariance, weight, and symmetry mentioned in the introduction.

I. Every integral invariant of a system of binary linear forms is a polynomial rational function, with integral coefficients, of the determinants of these linear forms. The proof will be given in ğ 3.

II. Every system $\mathfrak{S}$ of products of powers of n variables with nonnegative exponents, which together with any two products of powers f and g also contains their quotient whenever this quotient is polynomial in the variables, has a finite multiplicative basis $f_1, \ldots, f_k$ consisting of functions from $\mathfrak{S}$, such that for every f in $\mathfrak{S}$ one has a representation

$$f = f_1^{\lambda_1} \cdots f_k^{\lambda_k}$$

with nonnegative exponents $\lambda_1, \ldots, \lambda_k$.

Indeed, by Hilbert's theorem on the module basis there exists a finite number of functions from $\mathfrak{S}$, say $f_1, \ldots, f_k$, each of which really contains the x's, such that every nonconstant f from $\mathfrak{S}$ belongs to the module generated by them:

$$f \equiv 0 \pmod{(f_1, \ldots, f_k)}.$$

It follows that for every $f = x_1^{i_1} \cdots x_n^{i_n}$ there is at least one $f_\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$ such that $\nu_1 \leq i_1, \ldots, \nu_n \leq i_n$. In the representation

$$f = x_1^{i_1 - \nu_1} \cdots x_n^{i_n - \nu_n} f_\nu = A f_\nu$$

the factor A belongs to $\mathfrak{S}$ by hypothesis, but it has lower degree in the variables than f. Hence by repeating the argument finitely many times the assertion follows. In order that the representation also hold for $f = 1$, one need only put all exponents λ equal to zero.[54]

III. All polynomial integral symmetric functions of n rows of quantities are polynomial integral functions of a finite number among them.

Let $\tau_1(x), \ldots, \tau_n(x)$ denote the elementary symmetric functions of the indeterminates $x_1, \ldots, x_n$. Then for every exponent k there is an identity

$$x_i^k = G_0^{(k)}(\tau) + x_i G_1^{(k)}(\tau) + \cdots + x_i^{n-1} G_{n-1}^{(k)}(\tau), \qquad (i = 1, 2, \ldots, n),$$

where $G_0^{(k)}, \ldots, G_{n-1}^{(k)}$ are polynomial integral functions of the $\tau(x)$. If $x_i, y_i, \ldots, z_i$ are the elements of the i-th row, then by these identities and the corresponding ones for $y, \ldots, z$, all special, one-rowed symmetric functions

$$\sum_{i=1}^{n} x_i^a y_i^b \cdots z_i^c$$

become polynomial integral functions of the finitely many

$$\sum_{i=1}^{n} x_i^a y_i^b \cdots z_i^c \qquad (0 \leq a < n,\ 0 \leq b < n,\ \ldots,\ 0 \leq c < n)$$

and of the elementary symmetric functions $\tau(x), \tau(y), \ldots, \tau(z)$.[55] If one has the most general symmetric functions of the n rows - a case not occurring below - it is shown in the same way that the functions

$$\sum x_{i_1}^{a_1} y_{i_1}^{b_1} \cdots z_{i_1}^{c_1} x_{i_2}^{a_2} y_{i_2}^{b_2} \cdots z_{i_2}^{c_2} \cdots x_{i_n}^{a_n} y_{i_n}^{b_n} \cdots z_{i_n}^{c_n}$$

$$(0 \leq a_\nu < n,\ 0 \leq b_\nu < n,\ \ldots,\ 0 \leq c_\nu < n),$$

where $i_1, i_2, \ldots, i_n$ runs through all permutations, together with $\tau(x), \tau(y), \ldots, \tau(z)$, form an integral basis.

IV. Let $F_1(x), \ldots, F_k(x)$ be polynomial integral functions of $x_1, \ldots, x_n$, and let a be a fixed integer. Then all functions

$$\frac{G(F)}{a},$$

[54] This representation can also be proved directly, and conversely Hilbert's theorem follows from it: compare P. Gordan, Neuer Beweis des Hilbertschen Satzes über homogene Funktionen, Gött. Nachr. 1899. Another direct proof of this representation, from which Theorem II is also derived, is in A. Ostrowski, Über die Existenz einer endlichen Basis bei gewissen Funktionensystemen, *Math. Ann.* 78 (1916), ğ 2,1 and ğ 3,2. The special case of Theorem II used in ğ 2, where the exponents run through all nonnegative solutions of a Diophantine system of equations, is already found in Gordan-Kerschensteiner, *Vorlesungen über Invariantentheorie*, vol. I, p. 199.

[55] Hilbert, loc. cit., takes the power sums instead of the $\tau(x), \ldots, \tau(z)$ into the basis; this makes the basis consist only of one-rowed functions, but the integrality of the representation is then lost.

where G denotes a polynomial integral function, which become integral in the x's, are polynomial integral functions of a finite number among them.

Indeed, by Hilbert's theorem on the integral module basis, for each such $G(F)/a$ one has a representation

$$\frac{G(F)}{a} = A_1(F_1 \dots F_k)\frac{G_1(F)}{a} + \cdots + A_\rho(F_1 \dots F_k)\frac{G_\rho(F)}{a},$$

where $A_1, \dots, A_\rho$ are polynomial integral functions of the F's, and

$$\frac{G_1(F)}{a}, \dots, \frac{G_\rho(F)}{a}$$

belong to the system. The functions

$$F_1 = \frac{aF_1}{a}, \dots, F_k = \frac{aF_k}{a}; \quad \frac{G_1(F)}{a}, \dots, \frac{G_\rho(F)}{a}$$

therefore form the required basis.

ğ 2. Finiteness of the Integral Binary Invariants

Let x, y be binary variables subjected to a transformation with indeterminate coefficients

$$x = s_{11}x' + s_{12}y', \qquad y = s_{21}x' + s_{22}y', \tag{1}$$

and let f be a binary ground form whose coefficients are indeterminates. Then by (1),

$$f = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n = a'_0x'^n + a'_1x'^{n-1}y' + \cdots + a'_ny'^n. \tag{2}$$

By an integral invariant of f one understands, as is well known, a polynomial integral function $I(a)$ such that

$$I(a') = |s_{ik}|^\rho I(a), \qquad \text{identically in } a, s_{ik}. \tag{3}$$

The integral invariants of a system of ground forms are defined correspondingly; one may include homogeneity in the coefficients of the individual ground forms in the definition, since from such individually homogeneous invariants the remaining ones are composed in an integral-linear way.

In addition to (2), consider a special binary form g, namely the product of n linear forms whose coefficients are again indeterminates:[56]

$$\begin{aligned} g &= (\alpha_1x + \beta_1y)(\alpha_2x + \beta_2y)\cdots(\alpha_nx + \beta_ny) \\ &= \sigma_0(\alpha,\beta)x^n + \sigma_1(\alpha,\beta)x^{n-1}y + \cdots + \sigma_n(\alpha,\beta)y^n \\ &= (\alpha'_1x' + \beta'_1y')(\alpha'_2x' + \beta'_2y')\cdots(\alpha'_nx' + \beta'_ny') \\ &= \sigma'_0x'^n + \sigma'_1x'^{n-1}y' + \cdots + \sigma'_ny'^n. \end{aligned} \tag{4}$$

Thus $\sigma_0(\alpha,\beta), \sigma_1(\alpha,\beta), \dots, \sigma_n(\alpha,\beta)$ denote the homogenized elementary symmetric functions, and the transformed coefficients σ'_i become equal to $\sigma_i(\alpha',\beta')$.

Because of the algebraic independence of these elementary functions, to every relation

$$G(\sigma_0, \sigma_1, \dots, \sigma_n) = 0 \quad \text{identically in } \alpha, \beta \tag{5}$$

there corresponds a further relation

$$G(\sigma_0, \sigma_1, \dots, \sigma_n) = 0 \quad \text{identically in } \sigma_0, \dots, \sigma_n, \tag{6}$$

and hence, for indeterminates $a_0, \dots, a_n$,

$$G(a_0, a_1, \dots, a_n) = 0 \quad \text{identically in } a_0, \dots, a_n. \tag{7}$$

[56] If, as is often done in invariant theory, one writes f with binomial coefficients, $f = b_0x^n + \binom{n}{1}b_1x^{n-1}y + \cdots + b_ny^n$, then the domain of all integral invariants $I(b)$ is enlarged relative to that of the $I(a)$, and the finiteness arguments used here fail; $I(b)$ is no longer an integral function of the roots.

Now every integral invariant $I(a)$ of f, by the substitution $a_i = \sigma_i(\alpha, \beta)$, gives an integral invariant $I(\sigma) = H(\alpha, \beta)$ of g, where H becomes an integral function of α, β. For this invariant the relation (3) becomes

$$I(\sigma') = |s_{ik}|^\rho I(\sigma) \quad \text{identically in } \sigma, s_{ik}, \tag{8}$$

and since $\sigma' = \sigma(\alpha', \beta')$, (8) gives

$$H(\alpha', \beta') = |s_{ik}|^\rho H(\alpha, \beta) \quad \text{identically in } \alpha, \beta; s_{ik}. \tag{9}$$

Thus $I(\sigma) = H(\alpha, \beta)$ becomes an integral invariant of the n linear forms $(\alpha_i x + \beta_i y)$. Conversely, suppose $H(\alpha, \beta)$ is an integral invariant of these n linear forms, hence satisfies (9), and is at the same time equal to an integral function $I(\sigma)$ of the σ's. Since then

$$H(\alpha', \beta') = I(\sigma(\alpha', \beta')) = I(\sigma'),$$

equation (9) can also be written

$$I(\sigma') = |s_{ik}|^\rho I(\sigma) \quad \text{identically in } \alpha, \beta; s_{ik}. \tag{9a}$$

It follows from (5) and (6) that (8) holds, and from (7) that (3) holds. Therefore to every integral invariant $I(a)$ there corresponds an integral invariant $H(\alpha, \beta) = I(\sigma)$ of the n linear forms, and conversely. Moreover, if $I_1(a), \ldots, I_k(a)$ is an integral basis of all $I(a)$, then $H_1(\alpha, \beta), \ldots, H_k(\alpha, \beta)$ is an integral basis of all $H(\alpha, \beta)$ which are at the same time integral functions $I(\sigma)$; here too the converse holds by (5), (6), and (7). Thus, to prove the existence of an integral basis for all $I(a)$, it suffices to prove it for all integral invariants $H(\alpha, \beta)$ which are at the same time integral functions $I(\sigma)$; and the basis

$$H_1(\alpha, \beta) = I_1(\sigma), \ldots, H_k(\alpha, \beta) = I_k(\sigma)$$

then supplies the basis $I_1(a), \ldots, I_k(a)$ for the $I(a)$.

Let $H(\alpha, \beta) = I(\sigma)$ run through the totality of all integral invariants of (4). Since by (3) every invariant is homogeneous in the σ's, and by (4) each σ is homogeneous and linear in the coefficients of each linear form, $H(\alpha, \beta)$ is homogeneous in each row α_i, β_i and of the same dimension in each row; moreover it is of course a symmetric function of the n rows. Conversely, by the fundamental theorem on symmetric functions, every integral symmetric function $H(\alpha, \beta)$ of the n rows, homogeneous separately and of the same dimension in each row, is a polynomial integral function of the σ's. Thus, by the preceding argument, it is an invariant $I(\sigma)$ as soon as $H(\alpha, \beta)$ is invariant. The totality of the integral invariants of (4) is therefore characterized as the totality of integral functions $H(\alpha, \beta)$ with the following properties:

1) integral invariant of the n linear forms $\alpha_i x + \beta_i y$;
2) separately homogeneous and of the same dimension in each of the n rows α_i, β_i;
3) symmetric in the n rows α_i, β_i.

By the special finiteness theorem I, $H(\alpha, \beta)$, because of 1), becomes a polynomial integral function of the determinants

$$(ik) = \alpha_i \beta_k - \beta_i \alpha_k;$$

hence

$$H(\alpha, \beta) = G((ik)).$$

In this representation the symmetry can also be expressed formally by applying all permutations of the n rows to $G((ik))$:

$$n!\, H(\alpha, \beta) = G^{(1)}((ik)) + G^{(2)}((ik)) + \cdots + G^{(n!)}((ik)) = G^*((ik)). \tag{10}$$

Along with each product of powers P of the (ik), G^* therefore also contains the sum $Q = P^{(1)} + \cdots + P^{(n!)}$ over all permutations of P. In fact G^* becomes an integral linear combination of finitely many Q's, $G^* = \sum cQ$. Since the Q's satisfy conditions 1), 2), and 3), and hence themselves become invariants, it suffices to consider the Q's in place of $G^*((ik))$.

Now let P run through the system $\mathfrak{S}$ of all products of powers of the (ik) occurring in the Q's, i.e. satisfying condition 2). If the quotient of two P's is polynomial in the (ik), then it also satisfies condition

2), and hence belongs to $\mathfrak{S}$. Therefore, by Theorem II, there are finitely many such P's, say $P_1, \ldots, P_\rho$, such that every P is representable in the form

$$P = P_1^{\lambda_1} \cdots P_\rho^{\lambda_\rho}$$

with nonnegative exponents λ. Applying all permutations gives

$$Q = P_1^{(1)\lambda_1} \cdots P_\rho^{(1)\lambda_\rho} + \cdots + P_1^{(n!)\lambda_1} \cdots P_\rho^{(n!)\lambda_\rho}.$$

Thus Q becomes an integral symmetric function of the $n!$ rows of quantities, each with ρ elements:

$$P_1^{(1)} \ldots P_\rho^{(1)}; \quad P_1^{(2)} \ldots P_\rho^{(2)}; \quad \ldots; \quad P_1^{(n!)} \ldots P_\rho^{(n!)};$$

hence, by Theorem III, it is a polynomial integral function of finitely many symmetric functions of these rows. These basis functions are themselves quantities Q or elementary symmetric functions of the $n!$ elements $P_i^{(1)}, P_i^{(2)}, \ldots, P_i^{(n!)}$, and therefore satisfy conditions 1), 2), and 3) and become integral invariants

$$H_1(\alpha, \beta) = I_1(\sigma); \ldots; \quad H_l(\alpha, \beta) = I_l(\sigma). \tag{11}$$

By (10), since $G^* = \sum cQ$, every $H(\alpha, \beta) = I(\sigma)$ is therefore of the form

$$H(\alpha, \beta) = I(\sigma) = \frac{1}{n!}\Phi(I_1, \ldots, I_l),$$

where Φ denotes a polynomial integral function; conversely, $\frac{1}{n!}\Phi$ is an integral invariant as soon as it is polynomial in α, β. Hence by Theorem IV finitely many further invariants $I_{l+1}(\sigma), \ldots, I_k(\sigma)$ can be adjoined to (11) in such a way that

$$H_1(\alpha, \beta) = I_1(\sigma); \ldots; H_l(\alpha, \beta) = I_l(\sigma);$$

$$H_{l+1}(\alpha, \beta) = I_{l+1}(\sigma); \ldots; H_k(\alpha, \beta) = I_k(\sigma)$$

form an integral basis of all invariants $H(\alpha, \beta) = I(\sigma)$. This proves the theorem for the case of one ground form.

If one is dealing with a system of ground forms, then, as noted above, one may assume homogeneity of the invariants in the coefficients of each ground form. One again replaces the general ground forms by ones which are respectively products of linear forms. Their invariants then become: 1) invariants of these linear forms; 2) separately homogeneous in the rows formed from the coefficients of the linear forms, and of equal dimension in the rows belonging to each individual ground form; 3) symmetric in the rows belonging to each individual ground form. Conversely, each integral invariant of all the linear forms satisfying these conditions again corresponds to an integral invariant of the system of ground forms. The proof is absolutely parallel to that just given. To each product of powers $P = P_1^{\lambda_1} \cdots P_\rho^{\lambda_\rho}$ of the individual determinants satisfying the weight conditions (Theorems I and II) one must apply all

$$N = n_1! n_2! \cdots n_\mu!$$

permutations, where $n_1, \ldots, n_\mu$ denote the degrees of the ground forms. In this way $N \cdot I$ is converted into an integral symmetric function of N rows, each with ρ elements. From this one obtains the integral basis for all $N \cdot I$, and consequently, by Theorem IV, the integral basis for all I.

§ 3. The Basis of the Integral Invariants of Binary Linear Forms

It remains to supply the proof of the special finiteness theorem I. By a known theorem, first proved by Clebsch, all polynomial rational invariants of the n linear forms $\alpha_i x + \beta_i y$ are polynomial rational functions of the determinants (ik). In particular, therefore, all integral invariants of these linear forms become polynomial rational, though not necessarily integral, functions of these determinants.

It will be shown below that, in view of the identical relations existing between the (ik), this representation is always possible integrally.

In formulas, and in the language of module theory, this is expressed as follows. Let ξ_{ik}, $i < k$, be indeterminates. Then the totality of all integral polynomials $F(\xi_{ik})$ with the property that $F((ik))$ vanishes

identically in α, β forms a module $\mathfrak{M}$; the sum of two such F's, and also the product of such an F with an arbitrary integral polynomial in the ξ_{ik}, again belongs to this totality. In formulas:

$$F((ik)) = 0 \quad \text{identically in } \alpha, \beta$$

implies

$$F(\xi_{ik}) \equiv 0 \pmod{\mathfrak{M}} \quad \text{identically in } \xi_{ik},$$

and conversely.

I now show that the following completely analogous statement holds. From

$$F((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta$$

$$\text{it follows that} \qquad F(\xi_{ik}) \equiv 0 \pmod{(\mathfrak{M}, p)} \quad \text{identically in } \xi_{ik}, \tag{1}$$

and conversely, for every prime number p. Hence $\mathfrak{M}$ is also identical with the module $\mathfrak{M}_p$ corresponding to the totality of all relations modulo p among the (ik); this module consists of all integral polynomials $F(\xi_{ik})$ for which $F((ik))$ vanishes identically modulo p in α, β.

That (1) asserts the integral representability is seen as follows. It can also be written in the form: from $F((ik)) = p \cdot H(\alpha, \beta)$, identically in α, β, it follows that

$$F(\xi_{ik}) - p \cdot G(\xi_{ik}) \equiv 0 \pmod{\mathfrak{M}} \quad \text{identically in } \xi_{ik},$$

and hence, by the definition of $\mathfrak{M}$,

$$F((ik)) = p \cdot G((ik)) \quad \text{identically in } \alpha, \beta.^{57}$$

Thus $p \cdot H(\alpha, \beta) = p \cdot G((ik))$, or

$$H(\alpha, \beta) = G((ik)).$$

If, therefore, a representation is given

$$H(\alpha, \beta) = \frac{1}{p_1^{\lambda_1} \cdots p_\rho^{\lambda_\rho}} F((ik)),$$

where $p_1, \ldots, p_\rho$ are prime numbers, then it follows also that

$$H(\alpha, \beta) = \frac{1}{p_1^{\lambda_1 - 1} \cdots p_\rho^{\lambda_\rho}} G((ik)),$$

and by repeating this finitely many times one obtains the integrality of the representation.

For the proof of (1), denote by

$$f_{ik,rs} = \xi_{ik}\xi_{rs} - \xi_{ir}\xi_{ks} + \xi_{is}\xi_{kr}, \qquad i < k < r < s,$$

the forms in the indeterminates ξ_{ik} corresponding to the quadratic relations between the (ik),

$$(ik)(rs) - (ir)(ks) + (is)(kr) = 0,$$

and denote by $\mathfrak{N} = (f_{ik,rs})$ the module of integral polynomials generated from them. From

$$F(\xi_{ik}) \equiv 0 \pmod{\mathfrak{N}}$$

it follows that

$$F((ik)) = 0 \quad \text{identically in } \alpha, \beta,$$

and

$$\begin{aligned} \text{from } F(\xi_{ik}) &\equiv 0 \pmod{(\mathfrak{N}, p)} \\ \text{it follows that } F((ik)) &\equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta. \end{aligned} \tag{2}$$

I shall now show, by normalizing the residue classes with respect to $\mathfrak{N}$, that the converse of (2) also holds. Then $\mathfrak{N} = \mathfrak{M} = \mathfrak{M}_p$, and (1) will be proved. The equality $\mathfrak{N} = \mathfrak{M}$ is obtained as the special case $\mathfrak{N} = \mathfrak{M}_p$ for $p = 0$; the case $p = 0$ is always included in the following considerations. In other words, the $f_{ik,rs}$ form an integral module basis of $\mathfrak{M}_p$, and in particular also of $\mathfrak{M}_0 = \mathfrak{M}$.

[57] This latter conclusion simultaneously proves the converse of (1).

a) The case of two or three rows α_i, β_i

Since no four different indices occur, $\mathfrak{N}$ is the zero module. It must therefore be shown that from

$$F((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta \tag{3}$$

it follows that

$$F(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

This proves (1) with $\mathfrak{M} = \mathfrak{M}_p = 0$.

Since the condition $F((ik)) = p \cdot H(\alpha, \beta)$ must be satisfied separately by the components homogeneous in the individual rows, it is enough throughout to assume $F((ik))$ homogeneous in each individual row, and hence $F(\xi_{ik})$ homogeneous in each index. In the case of two rows there is only the one determinant (12) and the corresponding indeterminate ξ_{12}. By the assumed homogeneity,

$$F = c\,\xi_{12}^{\nu}.$$

From

$$c\,(12)^{\nu} \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta$$

it follows, since $(12) \not\equiv 0 \pmod{p}$ identically in α, β, that $c \equiv 0 \pmod{p}$; hence

$$F(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

This proves (3), and hence (1).

In the case of three rows there are the determinants $(12), (13), (23)$, corresponding to the indeterminates $\xi_{12}, \xi_{13}, \xi_{23}$. Thus

$$F = \sum c\,\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{23}^{\tau_{23}}.$$

Let F have respectively the degrees $\sigma_1, \sigma_2, \sigma_3$ in the indices $1, 2, 3$. Then

$$\sigma_1 = \tau_{12} + \tau_{13}, \qquad \sigma_2 = \tau_{12} + \tau_{23}, \qquad \sigma_3 = \tau_{13} + \tau_{23},$$

with the unique inverse

$$\tau_{12} = \frac{1}{2}(\sigma_1 + \sigma_2 - \sigma_3), \quad \tau_{13} = \frac{1}{2}(\sigma_1 - \sigma_2 + \sigma_3), \quad \tau_{23} = \frac{1}{2}(-\sigma_1 + \sigma_2 + \sigma_3).$$

Thus each separately homogeneous F contains at most one term,

$$F = c\,\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{23}^{\tau_{23}},$$

from which, as above, (3), and consequently (1), follows.

b) The case of four rows α_i, β_i

The six indeterminates $\xi_{12}, \xi_{13}, \xi_{14}, \xi_{23}, \xi_{24}, \xi_{34}$, and the corresponding determinants, occur; and $\mathfrak{N} = (f_{12,34})$. Since

$$\xi_{14}\xi_{23} \equiv \xi_{13}\xi_{24} - \xi_{12}\xi_{34} \pmod{\mathfrak{N}}, \tag{4}$$

every product of powers of the ξ_{ik} is congruent modulo $\mathfrak{N}$ to an integral linear combination of such products of powers in which the product $\xi_{14}\xi_{23}$ does not occur. Thus for every polynomial $F(\xi_{ik})$,

$$F(\xi_{ik}) \equiv F_0(\xi_{ik}) \pmod{\mathfrak{N}}, \tag{5}$$

where F_0 contains no product $\xi_{14}\xi_{23}$. The polynomial F_0 will be called the normalized polynomial of the residue class of F. Since (4) is separately homogeneous, a separately homogeneous F again corresponds to a separately homogeneous F_0.

Now put

$$F_0(\xi_{ik}) = G(\xi_{ik}) + \xi_{34} F_1(\xi_{ik}), \tag{6}$$

where G contains no product of powers divisible by ξ_{34}, and further put

$$[G]_{\xi_{14}=\xi_{13}} = K(\xi_{12}, \xi_{13}, \xi_{23}). \tag{7}$$

From

$$F((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta$$

it follows by (5), taking account of (2), that

$$F_0((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta. \tag{8}$$

By specializing $\alpha_4 = \alpha_3,\ \beta_4 = \beta_3$, (6) and (7) give

$$K((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta.$$

By the result proved under a), therefore,

$$K(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

From this follows what remains to be shown below:

$$G(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

Thus (6) gives

$$F_0(\xi_{ik}) \equiv \xi_{34} F_1(\xi_{ik}) \pmod{p} \quad \text{identically in } \xi_{ik}.$$

Since $(34) \not\equiv 0 \pmod{p}$ identically in α, β, it follows from (8) that

$$F_1((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta,$$

where $F_1(\xi_{ik})$ is again normalized and of lower degree in ξ_{34}. Repeating the procedure finitely many times yields

$$F_0(\xi_{ik}) \equiv \xi_{34}^{\lambda} F_\lambda(\xi_{ik}) \pmod{p},$$

where F_λ is of degree zero in ξ_{34}, and hence vanishes modulo p by what has just been proved. Therefore

$$\begin{array}{rcl} F_0(\xi_{ik}) & \equiv & 0 \pmod{p} \quad \text{identically in } \xi_{ik}, \quad \text{or} \\ F(\xi_{ik}) & \equiv & 0 \pmod{(\mathfrak{N}, p)} \quad \text{identically in } \xi_{ik}. \end{array} \tag{9}$$

This proves the converse of (2), and hence (1), at the same time in the sharper assertion for $F_0(\xi_{ik})$.[58]

It remains only to add that $G(\xi_{ik}) \equiv 0 \pmod{p}$ follows from $K(\xi_{ik}) \equiv 0 \pmod{p}$; equivalently, from $G(\xi_{ik}) \not\equiv 0 \pmod{p}$ it follows that $K(\xi_{ik}) \not\equiv 0 \pmod{p}$. The normalization is needed only for this part of the induction. Under the substitution $\xi_{14} = \xi_{13}$, the individual products of powers of G do not vanish. A vanishing of K could therefore occur only because distinct products of powers in G correspond to equal products in K; and that in turn can happen only when these products of powers differ merely by an interchange of the indices 3 and 4. Suppose that such a normalized product of powers is, for example,

$$\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{14}^{\tau_{14}} \xi_{24}^{\tau_{24}}.$$

Because of the assumed separate homogeneity in each index, a replacement of 3 by 4 in one ξ_{ik} must be accompanied by a replacement of 4 by 3 in another; a relevant term would therefore contain, instead of $\xi_{13}\xi_{24}$, the product $\xi_{14}\xi_{23}$, which is excluded by the normalization. In exactly the same way, against

$$\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{14}^{\tau_{14}} \xi_{24}^{\tau_{24}}$$

only a term containing the factor $\xi_{14}\xi_{23}$ could cancel, which is again excluded by the normalization. Hence $K(\xi_{ik}) \equiv 0 \pmod{p}$ implies $G(\xi_{ik}) \equiv 0 \pmod{p}$.

[58] This sharper assertion means that each residue class contains only one normalized polynomial.

c) The case of n rows α_i, β_i

The case of n rows is now settled by complete induction, as an exact generalization of the just treated case of four rows.[59] First I again show that for every polynomial F there is a congruence

$$F(\xi_{ik}) \equiv F_0(\xi_{ik}) \pmod{\mathfrak{N}} \quad \text{identically in } \xi_{ik}, \tag{10}$$

where $\mathfrak{N} = (f_{ik,rs})$ and where $F_0(\xi_{ik})$ is normalized. The normalization is to consist in the following: if i, k, r, s are four different indices and $i < k < r < s$, then F_0 is not to contain the product $\xi_{is}\xi_{kr}$; that is, the indices of one ξ are not both to lie between those of the other. This normalization imposes no restriction in the case of two and three rows, where every polynomial is already normalized; in the case of four rows, as shown, there also exists a normalized polynomial for every residue class. The existence of a normalized polynomial for every residue class may therefore be assumed proved for $(n-1)$ rows.

Let an arbitrary product of powers in F be written in the form

$$\xi_{i_1 n} \cdots \xi_{i_\nu n}\, P,$$

where P no longer contains the index n. By the induction hypothesis, P is congruent modulo $\mathfrak{N}$ to an integral normalized polynomial P_0:

$$\xi_{i_1 n} \cdots \xi_{i_\nu n} P \equiv \xi_{i_1 n} \cdots \xi_{i_\nu n} P_0 \pmod{\mathfrak{N}}.$$

If P_0 contains no ξ_{rs} such that for at least one index i_λ the two indices r, s lie between i_λ and n, i.e. $i_\lambda < r < s < n$, then the normalization has already been reached, since the hypotheses are fulfilled for the product of any two ξ's from P_0. Otherwise let i_λ be such an index, $i_\lambda < r < s < n$, and let P_0^* be the product of powers from P_0 containing ξ_{rs}. Since

$$\xi_{i_\lambda n}\xi_{rs} \equiv \xi_{i_\lambda s}\xi_{rn} - \xi_{i_\lambda r}\xi_{sn} \pmod{\mathfrak{N}},$$

one obtains

$$\begin{aligned}
&\xi_{i_1 n} \cdots \xi_{i_\lambda n} \cdots \xi_{i_\nu n} P_0^* \\
&\equiv \xi_{i_1 n} \cdots \xi_{rn} \cdots \xi_{i_\nu n} Q + \xi_{i_1 n} \cdots \xi_{sn} \cdots \xi_{i_\nu n} R \pmod{\mathfrak{N}} \\
&\equiv \xi_{i_1 n} \cdots \xi_{rn} \cdots \xi_{i_\nu n} Q_0 + \xi_{i_1 n} \cdots \xi_{sn} \cdots \xi_{i_\nu n} R_0 \pmod{\mathfrak{N}},
\end{aligned}$$

where Q_0 and R_0 again denote the normalized polynomials of the residue classes of Q and R. These exist by the induction hypothesis, since Q and R do not contain the index n, and they are certainly integral polynomials, since Q and R are simply products of powers. Since $i_\lambda < r < s < n$, one also has

$$((n-i_1) + \cdots + (n-r) + \cdots + (n-i_\nu)) < ((n-i_1) + \cdots + (n-i_\lambda) + \cdots + (n-i_\nu)),$$

$$((n-i_1) + \cdots + (n-s) + \cdots + (n-i_\nu)) < ((n-i_1) + \cdots + (n-i_\lambda) + \cdots + (n-i_\nu)).$$

Thus, in passing from P_0^* to Q_0, R_0, this sum of differences has decreased; since the sum is necessarily $\geq \sigma$, the procedure must terminate after finitely many steps for each product of powers P_0^*. Hence

$$F(\xi_{ik}) = \sum \xi_{i_1 n} \cdots \xi_{i_\nu n} P^{(1)} \equiv \sum \xi_{j_1 n} \cdots \xi_{j_\sigma n} S_0^{(j)} = F_0(\xi_{ik}) \pmod{\mathfrak{N}},$$

where the integral polynomial $F_0(\xi_{ik})$ is necessarily normalized, since otherwise the difference sum could be lowered further. This proves (10). Since, by the induction hypothesis for $(n-1)$ indices, every separately homogeneous F has a separately homogeneous normalized F_0, the procedure just given shows that this is also the case for n indices. Hence in what follows only separately homogeneous polynomials need be considered.

As in b), set

$$F_0(\xi_{ik}) = G(\xi_{ik}) + \xi_{n-1,n} F_1(\xi_{ik}),^{60} \tag{11}$$

[59] The proof still applies for $n = 3$.

[60] The identity corresponding to (10) and (11),

$$F((ik)) = F_0((ik)) = G((ik)) + (n-1, n) F_1((ik)),$$

is an analogue of the Clebsch-Gordan series expansion, as soon as the two rows $(n-1)$ and (n) are replaced by rows of variables x, y, so that $(n-1, n)$ is replaced by (xy). But whereas Clebsch-Gordan involves an expansion by polars, the normalization of F_0 corresponds to "initial terms" of polars, and thereby forces the integrality which does not hold for Clebsch-Gordan. The known proof that, when integrality is disregarded, the $f_{ik,rs}$ form a basis of $\mathfrak{M}$ is carried out precisely by means of the Clebsch-Gordan series expansion (Gordan-Kerschensteiner, *Vorlesungen über Invariantentheorie*, p. 132).

where G contains no product of powers divisible by $\xi_{n-1,n}$, and put further

$$[G]_{\xi_{in}=\xi_{i,n-1}} = K(\xi_{ik}). \tag{12}$$

As the definition of normalization shows, K, as well as G, is normalized.

Again there is a one-to-one correspondence between G and K. Distinct products of powers from G can correspond to the same product in K only if they differ merely by an interchange of the indices n and $(n-1)$. Suppose, for instance, that G is of degree ρ in the index $(n-1)$ and of degree σ in the index n, and that

$$\chi_1 \leq \chi_2, \ldots, \leq \chi_\rho \leq \chi_{\rho+1}, \ldots, \leq \chi_{\rho+\sigma}$$

are the indices connected with $(n-1)$ and n in a product of powers of G. Their number must be $\rho+\sigma$, since by (11) the indeterminate $\xi_{n-1,n}$ does not occur in G. By the normalization, the product of powers is therefore of the form

$$\xi_{\chi_1,n-1} \cdots \xi_{\chi_\rho,n-1} \xi_{\chi_{\rho+1},n} \cdots \xi_{\chi_{\rho+\sigma},n}\, P(\xi_{ik}),$$

where $P(\xi_{ik})$ no longer contains the indices n and $(n-1)$. Each interchange of n with $(n-1)$ would, for $i \neq j$, give the factor $\xi_{in}\xi_{j,n-1}$ with $i < j$; hence $j, n-1$ lies between i and n, and the term would not be normalized. Thus, for fixed $\chi_1, \chi_2, \ldots, \chi_{\rho+\sigma}$ and fixed P, G contains only one product of powers. This proves that different products of powers from G correspond to different products in K. Therefore

$$K(\xi_{ik}) \equiv 0 \pmod{p} \quad \Longrightarrow \quad G(\xi_{ik}) \equiv 0 \pmod{p}. \tag{13}$$

From

$$F((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta$$

it follows now from (10), taking account of (2), that

$$F_0((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta. \tag{14}$$

Specializing $\alpha_n = \alpha_{n-1},\ \beta_n = \beta_{n-1}$, (11) and (12) give

$$K((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta. \tag{15}$$

Since $K(\xi_{ik})$ is normalized and contains only $(n-1)$ indices, it follows by what was proved under a) and under b), formula (9), that

$$K(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

Then by (13)

$$G(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

Hence (11) gives

$$F_0(\xi_{ik}) \equiv \xi_{n-1,n} F_1(\xi_{ik}) \pmod{p} \quad \text{identically in } \xi_{ik}.$$

Since $(n, n-1) \not\equiv 0 \pmod{p}$ identically in α, β, it follows from (14) that

$$F_1((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta,$$

where $F_1(\xi_{ik})$ is again normalized and has lower degree in $\xi_{n-1,n}$ than F_0. Repeating the process finitely many times yields

$$F_0(\xi_{ik}) \equiv \xi_{n-1,n}^{\lambda} F_\lambda(\xi_{ik}) \pmod{p},$$

where F_λ is of degree zero in $\xi_{n-1,n}$, and hence vanishes modulo p by what has just been proved. Thus one obtains

$$\begin{aligned} F_0(\xi_{ik}) &\equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}, \quad \text{or} \\ F(\xi_{ik}) &\equiv 0 \pmod{(\mathfrak{N}, p)} \quad \text{identically in } \xi_{ik}. \end{aligned} \tag{16}$$

This proves the converse of (2), and hence (1). At the same time, it proves in the case of n indices, and therefore in general, the sharper assertion used in the induction step for $F_0(\xi_{ik})$.

ğ 4. Finiteness of the Integral Invariants of Finite Groups

The elementary proof of finiteness given in my note "The finiteness theorem for invariants of finite groups"[61] admits, by means of the special finiteness theorems III and IV of ğ 1, the sharpening to integrality, whereas the usual proof based on Hilbert's theorem on the module basis does not supply this integrality. Even the use of the integral module basis only gives a representation in which an arbitrarily high power of the integer h, the order of the group, appears in the denominator.

I use throughout the notation of the note just mentioned. Let the finite group $\mathfrak{H}$ consist of the h linear transformations $A_1, \ldots, A_h$ of nonzero determinant,[62] where A_k denotes the linear transformation

$$x_1^{(k)} = \sum_{\nu=1}^{n} a_{1\nu}^{(k)} x_\nu, \quad \ldots, \quad x_n^{(k)} = \sum_{\nu=1}^{n} a_{n\nu}^{(k)} x_\nu,$$

or, briefly, $(x^{(k)}) = A_k(x)$. Thus the group $\mathfrak{H}$ sends the row (x) with elements $x_1, \ldots, x_n$ into the rows $(x^{(k)})$ with elements $x_1^{(k)}, \ldots, x_n^{(k)}$. The coefficients $a_{i\nu}^{(k)}$ are assumed to be algebraic integers; this is no restriction of generality, since by a theorem of J. Schur[63] every finite group of linear transformations is similar to one for which the $a_{i\nu}^{(k)}$ become algebraic integers.

By an integral absolute invariant of the group is meant a polynomial rational function of $x_1, \ldots, x_n$, with algebraic integers of the number field $\mathfrak{K}$ generated by the $a_{i\nu}^{(k)}$ as coefficients, which remains identically unchanged under application of $A_1, \ldots, A_h$. For such an invariant $f(x)$ one has

$$f(x) = f(x^{(1)}) = \cdots = f(x^{(h)}) = \frac{1}{h} \sum_{k=1}^{h} f(x^{(k)}). \tag{1}$$

Conversely, every integral symmetric function of the h rows of quantities $(x^{(k)})$ also becomes an integral invariant of the group.

Let $\omega_1, \omega_2, \ldots, \omega_\rho$ denote a basis of all integers of $\mathfrak{K}$. Then every invariant can be represented as

$$f(x) = \omega_1 f_1(x) + \cdots + \omega_\rho f_\rho(x),$$

where $f_1(x), \ldots, f_\rho(x)$ have rational integer coefficients. Thus by (1)

$$h\, f(x) = \omega_1 \sum_{k=1}^{h} f_1(x^{(k)}) + \cdots + \omega_\rho \sum_{k=1}^{h} f_\rho(x^{(k)}).$$

Here the individual sums are symmetric functions of the h rows of quantities $(x^{(k)})$, and indeed with rational integer coefficients. By Theorem III they can therefore be expressed polynomially and rationally, with rational integer coefficients, in terms of finitely many integral-rational symmetric functions of these rows. By the preceding argument, these basis functions $I_1(x), \ldots, I_\sigma(x)$ become integral invariants of the group, in general with algebraic-integral coefficients, since $\mathfrak{H}$ need not contain together with A all of its algebraically conjugate transformations.

There is therefore a representation

$$h \cdot f(x) = \omega_1 G_1(I) + \cdots + \omega_\rho G_\rho(I), \tag{2}$$

where $G_1, \ldots, G_\rho$ have rational integer coefficients.

Now let $w_1, \ldots, w_\rho$ be indeterminates, and let

$$L = w_1 G_1(I) + \cdots + w_\rho G_\rho(I)$$

run through all linear forms in the w's which, by the substitution $w_i = \omega_i / h$, correspond to invariants $f(x)$ in the representation (2). Hilbert's theorem on the integral module basis gives

$$L = A_1(I) L_1 + \cdots + A_\tau(I) L_\tau, \tag{3}$$

[61] *Math. Ann.* 77, p. 89 (1915).

[62] It would suffice to suppose that $\mathfrak{H}$ is simply isomorphic to an abstract finite group; that is, if a transformation determinant of the A's vanishes, then $\mathfrak{H}$ should be similar to a group $\begin{pmatrix} \mathfrak{S} & 0 \\ 0 & 0 \end{pmatrix}$, where the determinants of the substitutions of $\mathfrak{S}$ do not vanish. In this case the invariants of $\mathfrak{H}$ coincide with the invariants of $\mathfrak{S}$, so the condition of the nonvanishing of the determinants is in fact no restriction of generality.

[63] Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlkörper. Satz VII. *Math. Ann.* 71, p. 555 (1912).

where the A_i have rational integer coefficients, and where, since all L's are linear in the w's, the A_i no longer contain the w's. If the substitution $\omega_i = w_i/h$ sends $L_1, \ldots, L_\tau$ to the invariants $\mathfrak{I}_1(x), \ldots, \mathfrak{I}_\tau(x)$, then (3) becomes

$$f(x) = A_1(I)\mathfrak{I}_1(x) + \cdots + A_\tau(I)\mathfrak{I}_\tau(x). \tag{4}$$

This representation shows that

$$I_1(x), \ldots, I_\sigma(x); \mathfrak{I}_1(x), \ldots, \mathfrak{I}_\tau(x)$$

form a basis of all integral invariants of the group $\mathfrak{H}$, such that every invariant is representable as a polynomial rational function, with rational integer coefficients, of these finitely many invariants.

If, in particular, the group $\mathfrak{H}$ has the property that with each transformation A it also contains all $A', A'', \ldots$ with algebraically conjugate number coefficients, then the integral-rational symmetric functions of the h rows $(x^{(k)})$ become functions of x with rational integer coefficients. This holds in particular also for the basis functions of the symmetric functions. Thus, if one restricts oneself to invariants $f(x)$ with rational integer coefficients, then the basis functions

$$I_1(x), \ldots, I_\sigma(x); \mathfrak{I}_1(x), \ldots, \mathfrak{I}_\tau(x)$$

also have rational integer coefficients. Under this special assumption, which is in general not satisfied by the groups $\mathfrak{H}$, integral finiteness therefore also holds for the subdomain of invariants with rational integer coefficients.

16. On Series Expansion in Form Theory.

On Series Expansion in Form Theory.

(Addendum and Correction to No. III of the paper "On the Polynomial Rational Representation of the Invariants of a System of Arbitrarily Many Ground Forms", Math. Ann. 77, p. 93.)

By

Emmy Noether in Göttingen.

Math. Ann. 81 (1920), pp. 25–30

By the "series expansion of form theory" one understands, as is well known, on the one hand the generalization of the Clebsch–Gordan series expansion – that is, the expansion of a form containing two binary rows according to powers of the determinant of these rows, where the coefficients are polars of forms in only one row of variables, or, what is identical with this, vanish under application of the Ω-process – to forms in arbitrarily many series of n variables each; and, on the other hand, as a generalization of the normal forms occurring for the "complex coordinates" t_{ik}, an expansion according to normal forms for forms which contain simultaneously the quantities of different levels $t_i, t_{ik}, t_{ikl}, \ldots$. This second kind of expansion can, however, be obtained from the first by invariant differentiation processes, as was carried out above all by Mertens and Deruyts.[64]

The various expansions of the first kind all arise – as is briefly sketched, for instance, in Math. Ann. 77, loc. cit. III – as consequences of the expansion of a form in n rows of n variables each according to powers of the determinant of these rows, where the coefficients are polars of forms in only $(n-1)$ rows, which themselves are derived from the initial form by polar formation and the Ω-process.[65] The original Clebsch–Gordan expansion ($n = 2$) had gone one step further: the special polar processes which occur there are given explicitly, even including the numerical coefficients.

What I now wish to add to the indicated note – where the series expansion is conceived more conceptually, as a problem of linear pencils of forms – is an explicit representation up to numerical coefficients, obtained by specializing E. Fischer's investigations concerning general module systems.[66]

[64] F. Mertens, Über invariante Gebilde quaternärer Formen (Sitzber. d. Ak. d. Wiss. Wien 98, Abt. IIa (1889)) for the quaternary case. The general normal forms are found in J. Deruyts: Sur la réduction des fonctions invariantes dans le système des variables géométriques, Bulletins de l'Ac. R. de Belgique 24 (1892). Without knowing this work, and in close dependence on Mertens, I gave the general expansion according to normal forms in § 7 of the paper: Zur Invariantentheorie der Formen von n Variabeln, J. f. M. 139 (1910).

[65] Compare the bibliographical references loc. cit. Since then there has appeared, also based on the formal method: Schouten, Over reeksontwikkelingen van algebraische vormen met verschillende rijen van variabelen van verschillenden graad, Verslag Ak. Amsterdam 27 (1919), p. 1481.

[66] E. Fischer, Über die Differentiationsprozesse der Algebra, J. f. M. 148 (1917).

This classification is led to by interpreting the normal form in the t_{ik}. Namely, if one replaces the "complex coordinates" t_{ik} by the "line coordinates"

$$p_{ik} = (x_i y_k - x_k y_i),$$

then, because of the identical relations existing among the p_{ik}, the representation of a form $F(p_{ik})$ is no longer unique. Uniqueness can be obtained by requiring that among the coefficients of F there hold the same linear relations as among the power products of the p_{ik} occurring in F.[67] Thus for this normal form Φ one has:

$$\begin{aligned} F(p_{ik}) &= \Phi(p_{ik}) \quad [\text{identically in } x, y], \quad \text{or} \\ F(t_{ik}) &\equiv \Phi(t_{ik}) \qquad \bmod M, \end{aligned} \tag{1}$$

where M denotes the module of all identical relations among the p_{ik}, that is, consists of the totality of all forms $G(t_{ik})$ for which $G(p_{ik})$ vanishes identically in x, y. $\Phi(t_{ik})$ is the "normal form" in complex coordinates, while the basis functions of M become quadratic forms in the t_{ik}. By iterating the procedure with respect to the factors of these basis functions, the complete series expansion arises. Corresponding considerations hold when $t_i, t_{ik}, t_{ikl}, \ldots$ occur simultaneously.

By an analogous line of thought one can reduce the expansion according to polars. If, for example, in a form $F(x, y, z)$ one replaces the three ternary rows $x = (x_1, x_2, x_3), y, z$ by rows ξ, η, ζ which are linearly composed of only two of them (for instance $\xi = x, \eta = y; \zeta = \lambda_1 x + \lambda_2 y$), then the representation of $F(\xi, \eta, \zeta)$ is again not unique. One can again prescribe for the coefficients the same linear relations as for the power products of ξ, η, ζ occurring in F. Since here the module M of all identical relations has as basis function the determinant $\Delta = (xyz)$ of the three rows (loc. cit. III, auxiliary lemma a)), [1] is replaced by:

$$\begin{aligned} F(\xi, \eta, \zeta) &= \Phi(\xi, \eta, \zeta) \quad [\text{identically in } x, y], \quad \text{or} \\ F(x, y, z) &\equiv \Phi(x, y, z) \qquad \bmod \Delta. \end{aligned} \tag{2}$$

It follows that Φ arises by polar formation (compare formula (2) loc. cit.); the complete series expansion is again obtained by iteration.

The formation of the normal forms Φ is therefore subordinated in both cases to the following problem: if in $F(z)$ the indeterminates z_i are replaced by polynomials $f_i(\xi)$ in parameters ξ, so that the representation $F(f_i(\xi))$ is therefore no longer unique, then the uniqueness is to be fixed by requiring that among the coefficients there hold the same linear relations as among the power products of the $f_i(\xi)$ occurring in F. Thus one has

$$\begin{aligned} F(f_i(\xi)) &= \Phi(f_i(\xi)) \quad [\text{identically in } \xi], \quad \text{or} \\ F(z) &\equiv \Phi(z) \qquad \bmod M, \end{aligned} \tag{3}$$

where M denotes the module of all identical relations among the $f_i(\xi)$.

For this normal form $\Phi(z)$, E. Fischer, in § 11, I of the cited paper, gave an explicit expansion up to numerical coefficients, namely by means of linear operations. At the same time, however, in Introduction III and in § 6 II, he also gave, for the difference $F - \Phi$ belonging to M – assuming knowledge of a module basis – an explicit expression in the same sense; and, by combining these developments in § 11 II, he thereby replaced formula [3] by an explicit representation. The question of the numerical coefficients, still open here, is according to § 12 of the same paper identical with the determination of the eigenvalues and eigenfunctions of the linear operations (formula 82).

I now specialize Fischer's formulas, in 1., to the case of the series expansion according to polars, and obtain from them, by iteration, the series expansion. The operation for determining Φ thereby passes into definite polar processes, which is considerably more precise than the previously known formulation given above. In the operation for determining $F - \Phi$, multiplication by the determinant Δ and the Ω-process occur in combination. To get to the usual, non-explicit form, one must also note that $\Omega\Delta$ can be expressed by polar processes.

At this point a correction should also be added. In the work cited above (p. 101, line 6 from the top) I inadvertently assumed as generally valid the identical transformation

$$\Omega(\Delta\psi) = c_1\psi + c_2\Delta \cdot \Omega(\psi),$$

which holds only in the binary domain, and thereby made the passage from the fundamental formula (2), which gives the expression for the normal form Φ in [2], to the series expansion (3). The considerations there

[67] Compare Clebsch, Über eine Fundamentalaufgabe der Invariantentheorie, § 4, Abh. d. K. G. d. Wissensch. zu Göttingen 17 (1872).

therefore yield only formula (2), and as a special case of it the reduction theorem (1); but, since an explicit expression for the difference $F - \Phi$ is missing, they do not suffice to justify the series expansion.

In 2. I similarly obtain, by specialization, the normal form $\Phi(t_{ik})$ of [1]; more generally, the normal form $\Phi(t_i, t_{ik}, t_{ikl}, \ldots)$, which leads to known explicit formulas. But since setting up the complete series expansion requires knowing a module basis of M, the invariant-theoretic route (compare the cited literature) is preferable here; it does not require this knowledge, but on the contrary supplies a module basis by means of the series expansion.

1. According to Fischer, § 11 (formula (19) and the following lines), the normal form $\Phi(z)$ of [3] – there denoted $N(\zeta)$ – is given by:

$$\Phi(z) = (a_1 S + a_2 S^2 + \cdots + a_r S^r) F(z), \tag{4}$$

where the constants $a_1 \ldots a_r$ belong to the coefficient domain of the $f(\xi)$ and depend only on the degree of $F(z)$; the operator S is defined by

$$\begin{gathered} S = AB; \qquad BF(z) = F(f(\xi)); \\ AF(f(\xi)) = \left\{ \sum z_i f_i \left(\frac{\partial}{\partial \xi} \right) \right\}^p F(f(\xi))^{68}. \end{gathered} \tag{5}$$

If in [2] one regards F as a form of p-th dimension in z alone, then $f_i(\xi)$ specializes to $\lambda_1 x_i + \lambda_2 y_i$; consequently one obtains:

$$\begin{gathered} BF = F(x, y, \lambda_1 x + \lambda_2 y), \\ SF = \left\{ \sum z_i \left(\frac{\partial}{\partial \lambda_1} \frac{\partial}{\partial x_i} + \frac{\partial}{\partial \lambda_2} \frac{\partial}{\partial y_i} \right) \right\}^p F(x, y, \lambda_1 x + \lambda_2 y), \end{gathered}$$

or, written in polar processes (compare loc. cit. II, 2 and 3; also for the abbreviated notation):

$$SF(x, y, z) = \frac{1}{p!} \left[z \left(\frac{\partial}{\partial \lambda_1} \frac{\partial}{\partial x} + \frac{\partial}{\partial \lambda_2} \frac{\partial}{\partial y} \right) \right]^p \left[(\lambda_1 x + \lambda_2 y) \frac{\partial}{\partial z} \right]^p F(x, y, z). \tag{6}$$

Equations [4] *and* [6] *give the desired explicit expression for* $\Phi(x, y, z)$; at the same time $\Phi(x, y, z)$ falls under the general form mentioned at the start ($\sum PH$ in (2), loc. cit.) – polars of expressions which depend on only 2 rows and are obtained from F by polar processes. The still undetermined coefficients a_i are rational numbers, since here the $f_i(\xi)$ have integral-rational numerical coefficients. If [2] is written in the form

$$F = \Phi + \Delta F_1, \tag{2a}$$

then specialization of the formula given by Fischer in Introduction III and in § 6 II (p. 41) gives

$$F_1 = (c_1 \Omega + c_2 \Omega \Delta \Omega + \cdots + c_i \Omega \Delta \Omega \cdots \Delta \Omega) F^{69}, \qquad \left[\Omega = \left(\frac{\partial}{\partial x} \frac{\partial}{\partial y} \frac{\partial}{\partial z} \right) \right], \tag{7}$$

where the c_i are again rational numbers depending only on the degree of F.

The iteration leads to:

$$F_1 = \Phi_1 + \Delta F_2; \quad F_2 = \Phi_2 + \Delta F_3; \quad \ldots; \quad F_i = \Phi_i + \Delta F_{i+1}; \quad \ldots,$$

where in each case the Φ_i are the normal forms corresponding to the F_i. Since the F_i have degree $(p - i)$ in z, [4] and [6] give:

$$\begin{gathered} \Phi_i = (a_{i1} S_i + a_{i2} S_i^2 + \cdots) F_i, \\ S_i F_i = \frac{1}{(p-i)!} \left[z \left(\frac{\partial}{\partial \lambda_1} \frac{\partial}{\partial x} + \frac{\partial}{\partial \lambda_2} \frac{\partial}{\partial y} \right) \right]^{p-i} \left[(\lambda_1 x + \lambda_2 y) \frac{\partial}{\partial z} \right]^{p-i} F_i. \end{gathered} \tag{8}$$

Formula [7] corresponds to

$$F_i = (\alpha_{i1} \Omega + \alpha_{i2} \Omega \Delta \Omega + \cdots) F_{i-1}, \quad \text{and by iteration}$$

$$F_i = (\beta_1 \Omega^i + \beta_2 \Omega^i \Delta \Omega + \cdots + \beta_\rho \Omega^{k_1} \Delta \Omega^{k_2} \cdots \Delta \Omega^{k_\lambda} + \cdots) F, \quad (k_1 + k_2 + \cdots + k_\lambda - \lambda + 1 = i). \tag{9}$$

[68] Compare formula (75). In the case of [3], the sum α runs over all power products of p-th dimension, and (75) therefore specializes to [5].

[69] Kerim uses this specialized formula in his Erlangen dissertation, soon to appear, in the application to "inertia forms".

By means of [8] *and* [9], *the expansion*

$$F = \Phi + \Delta\Phi_1 + \Delta^2\Phi_2 + \cdots + \Delta^i\Phi_i + \cdots + \Delta^p\Phi_p$$

has reached an explicit representation in the stated sense.

If one applies to [7] the identical transformation $\Omega\Delta F = PF$, where P denotes polar processes,[70] then, since these processes commute with the Ω-process, one obtains the known formula

$$F_1 = P\Omega F; \quad \ldots; \quad F_i = P\Omega^i F;$$

and from this, in conjunction with [8] or with the considerations loc. cit., follows the known formulation of the series expansion, as for instance in (3) loc. cit. If one is dealing with n rows of n variables, $x^{(1)}, x^{(2)}, \ldots, x^{(n-1)}, z$, then correspondingly

$$f_i(\xi) = \lambda_1 x_i^{(1)} + \lambda_2 x_i^{(2)} + \cdots + \lambda_{n-1} x_i^{(n-1)};$$

and likewise Δ and Ω are to be defined for n rows.

2. For the normal form of $F(t_i, t_{ik}, t_{ikl}, \ldots)$, the functions $f_i(\xi), f_{ik}(\xi), \ldots$ are given by the one-row, two-row, up to $(n-1)$-row determinants

$$\xi_i^{(1)}, \quad (\xi^{(1)}\xi^{(2)})_{ik}, \quad \ldots, \quad (\xi^{(1)}\xi^{(2)}\cdots\xi^{(n-1)})_{i_1 i_2 \cdots i_{n-1}}.$$

Thus, as a specialization of [5], one obtains:

$$S = AB; \qquad BF = F(\xi_i^{(1)}, (\xi^{(1)}\xi^{(2)})_{ik}, \ldots),$$

$$ABF = \left(\sum t_i \frac{\partial}{\partial \xi_i^{(1)}}\right)^{\lambda_1} \left(\sum t_{ik} \left(\frac{\partial}{\partial \xi^{(1)}} \frac{\partial}{\partial \xi^{(2)}}\right)_{ik}\right)^{\lambda_2} \cdots F(\xi_i^{(1)}, (\xi^{(1)}\xi^{(2)})_{ik}, \ldots),$$

where $\lambda_1, \lambda_2, \ldots$ denote the degrees in $t_i, t_{ik}, \ldots$.

From invariant-theoretic considerations (namely, all invariants of F which are linear in the coefficients can be linearly composed from Φ and from forms out of M, thus in particular also the SF not belonging to M)[71] the congruence follows here: $\Phi \equiv a_1 SF \mod M$; and because of the normal-form property one obtains from this, instead of [4], the simple relation

$$\Phi = a_1 SF = a_1 S\Phi. \tag{10}$$

The second equality holds because applying S makes every form from M vanish. Formula [10] shows that the normal form Φ is itself at the same time an eigenfunction; and indeed, by the invariant-theoretic consideration above, there are no further eigenfunctions which are at the same time invariants of F (compare, concerning [10], Deruyts, formulas (10) and (10')).

Corrections.

1. In the paper "Die allgemeinsten Bereiche aus ganzen transzendenten Zahlen" (Math. Ann. 77), on p. 121, line 8 from the top, line 9 from the top, and line 11 from the bottom, the field (H, Y) is to be replaced by the "field $(H, Y, Y', \ldots, Y^{(\lambda_0-1)})$, where $Y', \ldots, Y^{(\lambda_0-1)}$ denote the conjugates of Y with respect to H." Correspondingly, on p. 120, line 5 from the top, and p. 121, line 9 from the top, (H, y) is to be replaced by $(H, y, y', \ldots, y^{(\lambda_0-1)})$.

2. In the paper "Gleichungen mit vorgeschriebener Gruppe" (Math. Ann. 78), in the formulation of Hilbert's irreducibility theorem – p. 222, line 3 from the bottom – instead of "number field Ω" it must more precisely say "finite algebraic number field Ω", as Mr. Ostrowski has pointed out to me. In fact, with respect to the field of all algebraic numbers, for instance, the group of every equation with algebraic numerical coefficients is the identity group. – Correspondingly, in the introduction, "arbitrary domain of rationality" is to be understood as a finite algebraic number field to which finitely many parameters can still be adjoined, or as one of the intermediate fields which arise in this way.

(Accepted September 1919.)

[70] Compare, for example, F. Mertens, Über ganze Funktionen von m Systemen von je n Unbestimmten, Monatsh. f. Math. u. Phys. 4, formula (5).

[71] This follows, for instance, from § 6 and § 7, 2. of my cited paper "Zur Invariantentheorie der Formen von n Variabeln".

Modules in Noncommutative Domains, Especially from Differential and Difference Expressions.

By

Emmy Noether and Werner Schmeidler in Göttingen.

Contents.

Introduction.
§ 1. Formal Matters Concerning Differential and Difference Expressions.
§ 2. The General Polynomial Domain.
§ 3. One-Sided Modules and Their Residue Groups.
§ 4. Reducibility of the Residue Group into Two Subgroups and Its Relation to the Module.
§ 5. Computation with Units and Reducibility into k Subgroups.
§ 6. Finiteness Theorems.
§ 7. A Case of Unique Decomposition.
§ 8. Additive Decomposition of Completely Reducible Groups into Prime Groups. The Theorem on Isomorphism.
§ 9. Connection Between the Concepts "Isomorphic" and "of the Same Kind".
§ 10. Existence of Infinitely Many Decompositions of a Group.
§ 11. Relations to Systems of Differential Equations and Their Integrals.
§ 12. Examples.

Introduction.

The formal theory of differential expressions in one variable leads to a decomposition into irreducible factors which is unique in a certain sense.[1] But whereas the corresponding theorem in algebra can be carried over to polynomials in several variables, this is no longer possible for partial differential expressions.[2] For differential expressions in one variable, however, alongside the product representation there is also a representation as least common multiple, with similar laws holding; for, in two different decompositions, the individual constituents can be assigned to one another pairwise: they are "of the same kind".[3]

This concept of the least common multiple can now be interpreted as a module concept and so transferred to n variables; in the present paper this gives the natural generalization of the theorems just mentioned. Beyond this, however, we also note that for differential expressions only the following fact is used: they can be interpreted as polynomials with noncommutative multiplication, for which the degree of a product is equal to the sum of the degrees of the factors. These conditions are fulfilled, for example, by difference expressions as well, and hence the theorems also hold for these, where until now they were likewise known only for one variable.[4]

We therefore develop, in general, a theory of modules whose elements are polynomials with noncommutative multiplication; in doing so we reduce the study of the modules to that of residue classes.[5] In contrast with the commutative special case, one can indeed speak here of the sum of residue classes, but not of their product; one can speak only of the product of a residue class with a polynomial. The concept of a "residue group" is therefore to be modified relative to the commutative case. In the special case of polynomials in one variable, the residue group is moreover "finite", that is, it possesses only a finite number of linearly independent residue classes. In general there is no such finite "order"; the groups are "infinite". For our methods, however, this difference is immaterial.

Just as in the commutative case, to the representation of a module as the least common multiple of relatively prime modules there corresponds the simpler process of additive decomposition of the residue group.

1) Cf. E. Landau, Ein Satz über die Zerlegung homogener linearer Differentialausdrücke in irreduzible Faktoren, Journal für die reine und angewandte Mathematik 124 (1902), pp. 115–120, and subsequently A. Loewy, Über reduzible lineare homogene Differentialgleichungen, Mathematische Annalen 56 (1903), pp. 549–584.

2) Cf. a counterexample of Landau published in H. Blumberg, Über algebraische Eigenschaften von linearen homogenen Differentialausdrücken, dissertation, Göttingen 1912, 52 pp., pp. 51–52.

3) Cf., besides the papers just cited, A. Loewy, Über vollständig reduzible lineare homogene Differentialgleichungen, Mathematische Annalen 62 (1906), pp. 89–117; cited as Loewy.

4) Cf. G. Wallenberg–A. Guldberg, Theorie der linearen Differenzengleichungen, Leipzig and Berlin 1911.

5) For the case of commutative domains, cf. W. Schmeidler, Über Moduln und Gruppen hyperkomplexer GröSSen, Mathematische Zeitschrift 3 (1919), pp. 29–42.

In this connection the isomorphism of residue groups proves essential; upon specialization to differential expressions in one variable this isomorphism becomes the concept of the same kind for the associated modules, while upon specialization to commutative modules it becomes identity. Incidentally, the concept of the same kind can also be transferred to n variables, and its agreement with the isomorphism concept can be proved. The fact that in the additive decomposition of the residue group only finitely many summands ever occur follows by transferring Hilbert's theorem on the module basis, using Gordan's method of proof; Hilbert's original method of proof would require restrictions on the multiplication laws (in formula (6), a on the right instead of a_i, which is fulfilled for differential expressions but not for difference expressions).

In order to arrive at a uniqueness theorem, we must specialize the modules – as Loewy also does – to "completely reducible" ones, that is, to those representable as least common multiples of prime modules. Given two different decompositions, the constituents are then either pairwise identical, or at least to every constituent of one decomposition there corresponds an isomorphic constituent of the other decomposition, and conversely; at the same time, each decomposition then contains at least two isomorphic constituents. Furthermore, from the occurrence of two isomorphic constituents in one and the same decomposition there follows the existence of infinitely many decompositions; this even holds without the restriction to prime modules, which until now was not known even in the special case of differential expressions in one variable.

Finally, for modules from differential expressions, we discuss the connection with integrals and show that, for finite residue groups, the order is equal to the largest number of linearly independent integrals. Thus arbitrary functions occur in the general integral precisely when the residue group is not finite. The concept that two modules are of the same kind means, here as in the one-variable case, a "birational" relation between the integrals. Some examples conclude the paper.

The first impulse for the present paper was given several years ago by a question of E. Landau to E. Noether concerning the generalization of the product theorem. At that time E. Noether only observed that the question was one of module theory in the noncommutative polynomial domain, but could not yet be attacked. The Lasker module theorems then known were not directly transferable to this domain, because Lasker's method of proof rests on the theorem that a polynomial is uniquely decomposable into irreducible factors.[6] Only Schmeidler's methods offered the possibility of a transfer, which we then carried out jointly. In detail, let it be mentioned that the generalization of the residue group, the transfer and application of Hilbert's finiteness theorem, and the existence of infinitely many decompositions are due to E. Noether; the generalization of Loewy's concept of complete reducibility, the concept of isomorphism, and its connection with the concept of the same kind are due to W. Schmeidler.

§ 1.
Formal Matters Concerning Differential and Difference Expressions.

1. For differential expressions in one variable, a symbolic product formation has been introduced. Let

$$a_0(x)\frac{\mathrm{d}^n y}{\mathrm{d}x^n} + a_1(x)\frac{\mathrm{d}^{n-1} y}{\mathrm{d}x^{n-1}} + \cdots + a_n(x)y = A(y),$$

$$b_0(x)\frac{\mathrm{d}^m y}{\mathrm{d}x^m} + b_1(x)\frac{\mathrm{d}^{m-1} y}{\mathrm{d}x^{m-1}} + \cdots + b_m(x)y = B(y).$$

Then one defines the symbolic product $AB(y)$ as the differential expression

$$a_0(x)\frac{\mathrm{d}^n B(y)}{\mathrm{d}x^n} + a_1(x)\frac{\mathrm{d}^{n-1} B(y)}{\mathrm{d}x^{n-1}} + \cdots + a_n(x)B(y).$$

This product formation is in reality a multiplication of two operators; it is most simply written by replacing, as usual, $\frac{\mathrm{d}^n}{\mathrm{d}x^n}$ by $\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^n$. Then AB becomes

$$\left(a_0\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^n + \cdots + a_n\right)\left(b_0\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^m + \cdots + b_m\right)y,$$

where the ordinary rules for differentiating sums and products apply in carrying out the product. Every such operator can now be regarded as a polynomial in the single variable $\frac{\mathrm{d}}{\mathrm{d}x} = \xi$, by not writing explicitly the

6) Recently E. Noether observed that the Lasker theorems too can be established without using this theorem, by methods related to those used here.

function to which the operator is applied and by fixing for the variable ξ the multiplication rule corresponding to product differentiation:

$$\frac{\mathrm{d}}{\mathrm{d}x}(a(x)y) = a(x)\frac{\mathrm{d}}{\mathrm{d}x}(y) + a'(x)y,$$

or, in our notation ($n = 1, m = 0$),

$$\xi \cdot a = a \cdot \xi + a'. \tag{1}$$

One proceeds in exactly the same way for linear partial differential expressions

$$\left(\sum a_{\alpha_1 \dots \alpha_n}(x_1, \dots, x_n)\frac{\partial^{\alpha_1+\dots+\alpha_n}}{\partial x_1^{\alpha_1} \cdots \partial x_n^{\alpha_n}}\right) y$$

of a function y. For the n operators $\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n}$ we introduce variables $\xi_1, \dots, \xi_n$ and thereby obtain the polynomial

$$\sum a_{\alpha_1 \dots \alpha_n}(x_1, \dots, x_n)\xi_1^{\alpha_1} \cdots \xi_n^{\alpha_n}.$$

The product of two polynomials is then computed according to the laws

$$\xi_i a = a\xi_i + a_i \qquad (i = 1, \dots, n), \tag{2}$$

where a_i denotes the partial derivative of a with respect to x_i; the products of the ξ's among themselves are commutative. Apart from the commutative law of multiplication, all laws of addition and multiplication hold for the polynomials so defined just as in ordinary algebra. In particular, for the product of two such polynomials the total degree, and the degree in each individual variable, is equal to the sum of the corresponding degrees of the two factors.

2. For difference expressions (cf. Wallenberg, loc. cit.) of the form

$$a_x^{(0)} y_{x+n} + a_x^{(1)} y_{x+n-1} + \dots + a_x^{(n)} y_x = A_x,$$

$$b_x^{(0)} y_{x+m} + b_x^{(1)} y_{x+m-1} + \dots + b_x^{(m)} y_x = B_x$$

one has a corresponding product definition

$$(AB)_x = a_x^{(0)} B_{x+n} + a_x^{(1)} B_{x+n-1} + \dots + a_x^{(n)} B_x,$$

which can be carried out with the aid of the multiplication rule

$$(ay)_{x+1} = a_{x+1} y_{x+1}.$$

If we introduce the operator ξ for the transition from x to $x + 1$, then we obtain $\xi\{ay\} = a^*\xi\{y\}$, where $a^* = a_{x+1}$. Again one can omit the function y to which the operator is applied and obtains the law

$$\xi a = a^* \xi, \tag{3}$$

where, along with a, also a^* does not vanish identically. In exactly the same way, for n variables,

$$\xi_i a = a_i \xi_i \qquad (i = 1, \dots, n), \tag{4}$$

where ξ_i stands for the transition from x_i to $x_i + 1$, and a_i denotes the function obtained from a by replacing x_i by $x_i + 1$; hence it does not vanish identically if a does not. With these conventions, all rules of addition and multiplication, including the rule concerning the degree of a product, again hold, except for the commutative law.

Both cases will be subordinated, in the following section, to a quite generally defined polynomial domain with arbitrary coefficients.

§ 2.
The General Polynomial Domain.

We start from an arbitrary abstractly defined field P (whose elements we denote by small Latin letters), for which all rules of algebra hold, in particular also the commutative law of multiplication with unique inversion. To this field we adjoin n indeterminates $\xi_1, \ldots, \xi_n$; that is, we consider the integral domain J consisting of the products $a\xi_1^{\nu_1}\xi_2^{\nu_2}\cdots\xi_n^{\nu_n}$ and their finite sums, where all laws of addition and multiplication are to hold with the exception of the commutative law of multiplication. In particular, we call finite sums of the form

$$F(\xi_1, \ldots, \xi_n) = \sum a_{\nu_1 \ldots \nu_n}\xi_1^{\nu_1}\cdots\xi_n^{\nu_n}$$

"polynomials" (which throughout are to be denoted by capital Latin letters). In place of the commutative law, we now subject the elements of J to product laws such that *the product of two polynomials is again a polynomial*; thus the domain of all polynomials from J already exhausts J. For this it is plainly necessary and sufficient that, for the elements $\xi_1, \ldots, \xi_n$ and an arbitrary element a of P, product rules of the form

$$\xi_i a = F_i(\xi_1, \ldots, \xi_n) \qquad (i = 1, \ldots, n) \tag{5}$$

hold, where $F_i(\xi_1, \ldots, \xi_n)$ denotes some polynomial depending naturally on ξ_i and a. (In particular, the rules (2) and (4) for differential and difference expressions, respectively, are of this form.) For since $\xi_i a$ is not in itself a polynomial, while by hypothesis it belongs to the domain, the equation is necessary. Conversely, by finitely repeated application of formula (5), every element of the domain J can be transformed into a polynomial.

For the unit of the field, which we denote by 1, we shall further require $\xi_i \cdot 1 = 1 \cdot \xi_i = \xi_i$. We shall also stipulate that the multiplication of $\xi_1, \ldots, \xi_n$ among themselves is commutative.[7] Every polynomial in J then writes itself just like an ordinary polynomial in $\xi_1, \ldots, \xi_n$ with coefficients from P, and two polynomials agree only when all their coefficients agree.

More specifically, in what follows[8] we require that, in place of (5), the rule

$$\xi_i a = a_i \xi_i + b_i \qquad (a_i \neq 0) \quad (i = 1, \ldots, n) \tag{6}$$

shall hold. Here too, in particular, the laws (2) and (4) are included. Then the degree of a product is equal to the sum of the degrees of the factors; this holds both for total degree and for the degree in each individual variable, so that the product of two polynomials which do not vanish identically is likewise different from 0.

§ 3.
One-Sided Modules and Their Residue Groups.

For our domain J, because multiplication is noncommutative, the following kinds of modules[9] can be distinguished:[10]

1. The *right-sided module*, which, along with M, contains also FM for an arbitrary polynomial F, and along with M_1 and M_2 contains also $M_1 + M_2$.

2. The *left-sided module*, which, along with M, contains also MF, and along with M_1 and M_2 contains also $M_1 + M_2$.

We refer to these two kinds by the common name *one-sided modules*; modules which are both right-sided and left-sided will be called *two-sided*. In what follows we restrict ourselves to right-sided modules and note that the theory of the left-sided ones can be built up in exactly the same way.

We call two polynomials F and G congruent modulo $\mathfrak{M}$, written $F \equiv G(\mathfrak{M})$, if their difference is divisible by $\mathfrak{M}$, that is, if it belongs to $\mathfrak{M}$. The totality of all polynomials congruent to a given polynomial forms a *residue class* modulo $\mathfrak{M}$. (Residue classes are to be denoted by small German letters.) Since from

$$F_1 \equiv F_2(\mathfrak{M}) \qquad \text{and} \qquad G_1 \equiv G_2(\mathfrak{M})$$

it follows that $F_1 + G_1 \equiv F_2 + G_2(\mathfrak{M})$, the sum of two residue classes $\mathfrak{x}$ and $\mathfrak{y}$ is defined and is again a residue class $\mathfrak{x} + \mathfrak{y}$. By contrast, because the module is one-sided, one cannot speak of the product of two residue classes. Indeed, from

$$F_1 = F_2 + M_1, \qquad G_1 = G_2 + M_2$$

7) This is needed only from § 6 onward for the finiteness theorem and its consequences.

8) This too is used only from § 6 onward.

9) We denote modules by capital German letters.

10) One-sided ideals were already considered by A. Hurwitz; cf. Vorlesungen über die Zahlentheorie der Quaternionen (Berlin, Springer 1919), Lecture 6. There, however, what is essentially involved are principal ideals; the same holds for the works of Du Pasquier cited there in note 1.

there follows only

$$F_1G_1 = F_2G_2 + F_2M_2 + M_1G_2 + M_1M_2;$$

but since M_1G_2 need not belong to $\mathfrak{M}$ when M_1 belongs to $\mathfrak{M}$, F_1G_1 and F_2G_2 need not be congruent in general. On the other hand, if $M_1 = 0$, hence $F_1 = F_2 = F$, one sees that $G_1 \equiv G_2$ implies $FG_1 \equiv FG_2$. Thus an arbitrary residue class $\mathfrak{y}$ can be multiplied from the front by a polynomial F, and this gives a well-defined residue class $F\mathfrak{y} = \mathfrak{z}$.

For computation with residue classes, the commutative and associative laws of addition hold, as does the law of unique reversal of addition; moreover, for multiplication of residue classes by polynomials and addition, the distributive law $F(\mathfrak{y}_1 + \mathfrak{y}_2) = F\mathfrak{y}_1 + F\mathfrak{y}_2$ holds, as follows directly from computing with polynomials modulo $\mathfrak{M}$.

The residue class to which the unit belongs will be called the unit class, or unit, and denoted $\mathfrak{e}$. Then $F\mathfrak{e} = \mathfrak{x}$ is the residue class to which the polynomial F belongs. In contrast to the general residue classes, however, here the product $\mathfrak{x}\mathfrak{e}$ is also well-defined and equal to $\mathfrak{x}$; for from

$$F_1 = F_2 + M_1, \qquad G_1 = 1 + M_2$$

and $M_1 \cdot 1 = M_1$ it follows that

$$F_1G_1 = F_2 + M.$$

The totality of the residue classes modulo $\mathfrak{M}$ is called the *residue group of* $\mathfrak{M}$. A residue group therefore has the following properties: 1. Along with every residue class $\mathfrak{x}$ and an arbitrary polynomial F, it contains the residue class $F\mathfrak{x}$; and along with the residue classes $\mathfrak{x}_1$ and $\mathfrak{x}_2$ it contains the residue class $\mathfrak{x}_1 + \mathfrak{x}_2$.[11] 2. It possesses a unit $\mathfrak{e}$, so that $F\mathfrak{e}$ represents, for every polynomial F, the residue class $\mathfrak{x}$ of F. *Thus, as F runs through all polynomials, $F\mathfrak{e}$ runs through the whole residue group.*

§ 4.
Reducibility of the Residue Group into Two Subgroups and Its Relation to the Module.

For one-sided modules, the concepts *divisibility*, *greatest common divisor*, and *least common multiple* remain as in the two-sided case, as the following definitions show.

A module $\mathfrak{M}$ is said to be divisible by another module $\mathfrak{N}$ if from $M \equiv 0(\mathfrak{M})$ it follows also that $M \equiv 0(\mathfrak{N})$.

For two modules $\mathfrak{M}$ and $\mathfrak{N}$, the *greatest common divisor* $(\mathfrak{M}, \mathfrak{N})$ is defined as the totality of all polynomials representable in the form $M + N$, where $M \equiv 0(\mathfrak{M})$ and $N \equiv 0(\mathfrak{N})$; it is again a module. The same holds for several modules.

The totality of all polynomials divisible both by $\mathfrak{M}$ and by $\mathfrak{N}$ forms a module $[\mathfrak{M}, \mathfrak{N}]$, the *least common multiple* of $\mathfrak{M}$ and $\mathfrak{N}$. This definition too applies correspondingly to several modules, indeed even to a set of modules of arbitrary cardinality.

Two modules are called relatively prime when their greatest common divisor is the unit module, that is, the totality of all polynomials.

We now start from a module $\mathfrak{M}$ which is representable as the least common multiple of two relatively prime modules $\mathfrak{N}$ and $\mathfrak{L}$, both assumed to be proper divisors:

$$\mathfrak{M} = [\mathfrak{N}, \mathfrak{L}]. \tag{7}$$

We investigate the residue group $\mathfrak{G}$ of $\mathfrak{M}$. By hypothesis,

$$1 \equiv N + L(\mathfrak{M}) \tag{8}$$

for two polynomials $N \equiv 0(\mathfrak{N})$ and $L \equiv 0(\mathfrak{L})$. From this we show

$$\mathfrak{L} = (\mathfrak{M}, L), \qquad \mathfrak{N} = (\mathfrak{M}, N), \tag{9}$$

where, for example, $(\mathfrak{M}, L)$ means the module consisting of all polynomials of the form $M + FL$. In fact, first $(\mathfrak{M}, L) \equiv 0(\mathfrak{L})$. Conversely, from (8) it follows, for an arbitrary polynomial F, that

$$F \equiv FN(\mathfrak{L}). \tag{10}$$

11) This property could, in a more general sense, be called the "module property" of the residue group.

Now if $F \equiv 0(\mathfrak{L})$, then $FN \equiv 0(\mathfrak{L})$, hence $\equiv 0(\mathfrak{M})$, and consequently $F \equiv FL(\mathfrak{M})$. In the same way one proves $\mathfrak{N} = (\mathfrak{M}, N)$. It follows incidentally, since $\mathfrak{N}$ and $\mathfrak{L}$ are proper divisors of $\mathfrak{M}$, that neither $L \equiv 0$ nor $N \equiv 0(\mathfrak{M})$ can hold.

Let $\mathfrak{a}$ be the residue class of N modulo $\mathfrak{M}$, and $\mathfrak{b}$ the residue class of L modulo $\mathfrak{M}$. Then by (8)

$$\mathfrak{e} = \mathfrak{a} + \mathfrak{b} \qquad (\mathfrak{a} \neq 0,\ \mathfrak{b} \neq 0).$$

Since every residue class is of the form $F\mathfrak{e}$, the distributive law gives, for every residue class,

$$F\mathfrak{e} = F\mathfrak{a} + F\mathfrak{b} \qquad (\mathfrak{a} \neq 0,\ \mathfrak{b} \neq 0). \tag{11}$$

This representation of an arbitrary residue class as a sum of two residue classes of the form $G\mathfrak{a}$ and $H\mathfrak{b}$ is, however, *unique*. For from a relation $0 = G\mathfrak{a} + H\mathfrak{b}$, if K is a polynomial in the residue class $G\mathfrak{a} = -H\mathfrak{b}$, then plainly $K \equiv GN(\mathfrak{M})$, $K \equiv -HL(\mathfrak{M})$, hence $K \equiv 0(\mathfrak{N})$, $K \equiv 0(\mathfrak{L})$, and therefore $K \equiv 0(\mathfrak{M})$; that is, $G\mathfrak{a} = 0$, $H\mathfrak{b} = 0$.

Conversely, suppose now that relation (11) is fulfilled for every polynomial F, and indeed uniquely in the above sense. Let N then be a polynomial from $\mathfrak{a}$ and L a polynomial from $\mathfrak{b}$. We form the two modules (9) and assert (7) and (8). The latter follows from (11) for $F = 1$. Furthermore, by the definition of $\mathfrak{N}$ and $\mathfrak{L}$, $\mathfrak{M}$ is a common multiple of these two modules, and indeed the least one. For from $F \equiv 0(\mathfrak{L})$ and $F \equiv 0(\mathfrak{N})$ there follows $F \equiv HL \equiv GN(\mathfrak{M})$; hence $G\mathfrak{a} = H\mathfrak{b}$, $G\mathfrak{a} - H\mathfrak{b} = 0$, and therefore, by uniqueness of the representation, $G\mathfrak{a} = 0$, $H\mathfrak{b} = 0$, $F \equiv 0(\mathfrak{M})$. It has therefore been shown that the *representation of a module $\mathfrak{M}$ as the least common multiple of two relatively prime modules is equivalent to the unique additive decomposition of the residue group $\mathfrak{G}$ of $\mathfrak{M}$, as given by formula* (11).

We now investigate the system $\mathfrak{A}$ of residue classes of the form $F\mathfrak{a}$, which we wish to relate to the residue group $\overline{\mathfrak{A}}$ of $\mathfrak{L}$. By (11), every polynomial F in $\mathfrak{L}$ belongs to the residue class $F\mathfrak{a}$ when $\overline{\mathfrak{a}}$ is the residue class of N modulo $\mathfrak{L}$, and hence the unit class of $\overline{\mathfrak{A}}$. If we now associate the residue classes $F\mathfrak{a}$ in $\mathfrak{A}$ with the residue classes $F\overline{\mathfrak{a}}$ in $\overline{\mathfrak{A}}$, then to every residue class of $\mathfrak{A}$ there is assigned a residue class of $\overline{\mathfrak{A}}$, in such a way that the sum of two residue classes of $\mathfrak{A}$ corresponds to the sum of the assigned residue classes of $\overline{\mathfrak{A}}$, and the product of a residue class of $\mathfrak{A}$ with a polynomial corresponds to the product of the assigned residue class of $\overline{\mathfrak{A}}$ with the same polynomial. This assignment is moreover one-to-one: from $F\mathfrak{a} = 0$ follows $F \equiv 0(\mathfrak{L})$ by (11), hence $F\overline{\mathfrak{a}} = 0$; conversely, $F\overline{\mathfrak{a}} = 0$, hence $F \equiv 0(\mathfrak{L})$, also says by (10) that $FN \equiv 0(\mathfrak{L})$, hence $FN \equiv 0(\mathfrak{M})$, that is, $F\mathfrak{a} = 0$.

This leads us to a fundamental concept, which we define as follows:

A one-to-one correspondence between two systems $\mathfrak{A}$ and $\overline{\mathfrak{A}}$ of residue classes is called isomorphic if the sum of two residue classes of $\mathfrak{A}$ is assigned the sum of the corresponding residue classes of $\overline{\mathfrak{A}}$, and the product of an arbitrary residue class of $\mathfrak{A}$ with a polynomial is assigned the product of the corresponding residue class of $\overline{\mathfrak{A}}$ with the same polynomial.

A subsystem $\mathfrak{A}$ of residue classes in $\mathfrak{G}$ which is isomorphic to the residue group of a module is called a *subgroup* of $\mathfrak{G}$. As the proof above shows, the assignment here is specifically such that every residue class of $\mathfrak{A}$ arises from the corresponding residue class of $\overline{\mathfrak{A}}$ by adjoining certain polynomials, namely all polynomials belonging to $\mathfrak{L}$ but not to $\mathfrak{M}$.

Similarly one shows that the totality of all residue classes of the form $F\mathfrak{b}$ forms a subgroup $\mathfrak{B}$ of $\mathfrak{G}$ which is isomorphic to the residue group $\overline{\mathfrak{B}}$ of $\mathfrak{N}$.

A residue group $\mathfrak{G}$ whose residue classes admit a unique additive decomposition (11) will be called *reducible* into the two subgroups $\mathfrak{A}$ and $\mathfrak{B}$, written $\mathfrak{G} = \mathfrak{A} + \mathfrak{B}$; a group which is not reducible is called *irreducible*. We also occasionally call the associated modules reducible or irreducible. Thus the following holds.

Theorem 1.[12] *A module $\mathfrak{M}$ is representable as the least common multiple of two relatively prime proper divisors $\mathfrak{L}$ and $\mathfrak{N}$ if and only if its residue group $\mathfrak{G}$ is reducible into two subgroups $\mathfrak{A}$ and $\mathfrak{B}$. In this case $\mathfrak{A}$ and $\mathfrak{B}$ are respectively isomorphic to the residue groups of $\mathfrak{L}$ and $\mathfrak{N}$.*

§ 5.
Computation with Units and Reducibility into k Subgroups.

The residue classes $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{G}$ share with the unit $\mathfrak{e}$ the property that the product of $\mathfrak{a}$ and $\mathfrak{b}$ with an arbitrary residue class $\mathfrak{x}$ is defined; we therefore likewise call $\mathfrak{a}$ and $\mathfrak{b}$ units of $\mathfrak{G}$. Indeed, from (11), for $F = M$, there follows

$$0 = M\mathfrak{e} = M\mathfrak{a} + M\mathfrak{b},$$

12) Cf. Schmeidler, loc. cit., p. 39.

and hence, by uniqueness, $M\mathfrak{a} = 0$, $M\mathfrak{b} = 0$, and therefore

$$(F + M)\mathfrak{a} = F\mathfrak{a} = \mathfrak{x}\mathfrak{a},$$

where $\mathfrak{x}$ denotes the residue class of F. In place of relation (11), we may therefore write the equivalent class relation

$$\mathfrak{x}\mathfrak{e} = \mathfrak{x}\mathfrak{a} + \mathfrak{x}\mathfrak{b}.$$

In particular, putting $\mathfrak{x} = \mathfrak{a}$ gives

$$\mathfrak{a} = \mathfrak{a}^2 + \mathfrak{a}\mathfrak{b},$$

and hence, by uniqueness, $\mathfrak{a}^2 = \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} = 0$. Similarly one obtains $\mathfrak{b}^2 = \mathfrak{b}$, $\mathfrak{b}\mathfrak{a} = 0$.

Corresponding to the representation of a residue group as a sum of two constituents, we may now also define such a representation as a sum of k constituents. Namely, suppose a unique representation is given

$$F\mathfrak{e} = F\mathfrak{a}_1 + F\mathfrak{a}_2 + \cdots + F\mathfrak{a}_k \qquad (\mathfrak{a}_1 \neq 0, \ldots, \mathfrak{a}_k \neq 0),$$

where from $0 = G_1\mathfrak{a}_1 + \cdots + G_k\mathfrak{a}_k$ it also follows that $G_i\mathfrak{a}_i = 0$. Then, in particular for $F = M$, one obtains the relation $M\mathfrak{a}_i = 0$, so that the representation may also be written in the form[13]

$$\mathfrak{x}\mathfrak{e} = \mathfrak{x}\mathfrak{a}_1 + \cdots + \mathfrak{x}\mathfrak{a}_k \qquad (\mathfrak{a}_1 \neq 0, \ldots, \mathfrak{a}_k \neq 0). \tag{12}$$

This representation may also be regarded as having arisen from a successive decomposition into two constituents. If this can be continued without limit, with all $\mathfrak{a}_i \neq 0$, then we speak of a sum of infinitely many constituents.

Putting $\mathfrak{x} = \mathfrak{a}_i$ in (12) gives

$$\mathfrak{a}_i^2 = \mathfrak{a}_i, \qquad \mathfrak{a}_i\mathfrak{a}_j = 0 \quad (i \neq j), \qquad i, j = 1, \ldots, k, \tag{13}$$

with $\mathfrak{a}_i \neq 0$. Conversely, suppose a system of residue classes $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ in $\mathfrak{G}$ is present for which the orthogonality conditions (13) are fulfilled and for which

$$\mathfrak{e} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_k \tag{14}$$

holds. We shall show that this gives a representation of the group as a sum of k constituents. First, from the hypothesis, for every polynomial A_i from $\mathfrak{a}_i$, since $A_i\mathfrak{a}_i = (A_i + M)\mathfrak{a}_i$, it follows that $M\mathfrak{a}_i = 0$; hence $\mathfrak{a}_i$ can be multiplied by every class. Thus (14) implies representation (12), and this representation is unique. For if $0 = \mathfrak{x}_1\mathfrak{a}_1 + \cdots + \mathfrak{x}_k\mathfrak{a}_k$, then right multiplication by $\mathfrak{a}_i$ gives, by (13), $0 = \mathfrak{x}_i\mathfrak{a}_i$, proving uniqueness and hence the assertion. The residue classes $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ occurring in the decomposition of the unit class will be called the units belonging to the decomposition; equivalently they are characterized by the orthogonality relations (13) and condition (14). The later developments will essentially amount to computation with units.

It remains to establish the connection between the additive decomposition of the group into k constituents and the corresponding decomposition of the module. As in the case $k = 2$, a representation of the module as the least common multiple of k relatively prime modules will result, by induction.

Let the decomposition (12) be given, which we write in the form

$$\mathfrak{x}\mathfrak{e} = \mathfrak{x}\mathfrak{b} + \mathfrak{x}\mathfrak{a}_k, \tag{15}$$

$$\mathfrak{x}\mathfrak{b} = \mathfrak{x}\mathfrak{a}_1 + \cdots + \mathfrak{x}\mathfrak{a}_{k-1}. \tag{16}$$

From (15) it follows by Theorem I that the residue classes $\mathfrak{x}\bar{\mathfrak{b}}$ are isomorphic to the residue group of the module

$$\mathfrak{N} = (\mathfrak{M}, A_k). \tag{17}$$

For their residue classes $\mathfrak{x}\bar{\mathfrak{b}}$, the representation corresponding to (16) is therefore also valid:

$$\mathfrak{x}\bar{\mathfrak{b}} = \mathfrak{x}\bar{\mathfrak{a}}_1 + \cdots + \mathfrak{x}\bar{\mathfrak{a}}_{k-1}. \tag{18}$$

Suppose now it has already been proved that

$$\mathfrak{N} = [\mathfrak{M}_1, \ldots, \mathfrak{M}_{k-1}], \tag{19}$$

13) For the additive decomposition of residue groups, the commutative and associative laws hold; in contrast to the commutative case, however, $\mathfrak{U}_1 + \mathfrak{U}_2 = \mathfrak{U}_1 + \mathfrak{U}_3$ does not imply $\mathfrak{U}_2 = \mathfrak{U}_3$; cf. example 1 in § 12.

where

$$\begin{cases} \mathfrak{M}_1 = (\mathfrak{N}, A_2 + \cdots + A_{k-1}), \\ \mathfrak{M}_2 = (\mathfrak{N}, A_1 + A_3 + \cdots + A_{k-1}), \\ \qquad\qquad \vdots \\ \mathfrak{M}_{k-1} = (\mathfrak{N}, A_1 + \cdots + A_{k-2}). \end{cases} \tag{20}$$

For two summands this assertion agrees with our earlier result. Moreover, the polynomials A_i may here be chosen specifically as polynomials from $\bar{\mathfrak{a}}_i$ which at the same time are contained in $\mathfrak{a}_i$, since by § 4 the polynomials of the latter residue class are contained in the former. Then, by (15),

$$\mathfrak{M} = [\mathfrak{N}, \mathfrak{M}_k], \tag{21}$$

where

$$\mathfrak{M}_k = (\mathfrak{M}, A_1 + \cdots + A_{k-1}).$$

From (19) and (21) one obtains

$$\mathfrak{M} = [[\mathfrak{M}_1, \ldots, \mathfrak{M}_{k-1}], \mathfrak{M}_k] = [\mathfrak{M}_1, \ldots, \mathfrak{M}_{k-1}, \mathfrak{M}_k]$$

by the definition of least common multiple; and from (17) and (20) one gets

$$\mathfrak{M}_1 = (\mathfrak{M}, A_k, A_2 + \cdots + A_{k-1}).$$

It follows that

$$\mathfrak{M}_1 = (\mathfrak{M}, A_2 + \cdots + A_k),$$

for the latter module contains, by (13), also the polynomial

$$A_k = A_k(A_2 + \cdots + A_k) \pmod{\mathfrak{M}}.$$

Corresponding expressions are obtained for $\mathfrak{M}_2, \ldots, \mathfrak{M}_{k-1}$. Furthermore, the modules $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$ are relatively prime, since by (14)

$$\frac{1}{k-1}\Big((A_2 + \cdots + A_k) + (A_1 + A_3 + \cdots + A_k) + \cdots + (A_1 + \cdots + A_{k-1})\Big) \equiv 1 \pmod{\mathfrak{M}}.$$

They moreover form a totally relatively prime system, that is, the least common multiple of any of them is relatively prime to the least common multiple of the remaining ones.[14] This follows directly by grouping the summands in formula (12) into two suitable groups.

It has thus been shown that to a decomposition of the residue group into k summands there corresponds a representation of the module as the least common multiple of k modules forming a totally relatively prime system. We now prove the converse theorem, likewise by induction.

Suppose therefore that

$$\mathfrak{M} = [\mathfrak{M}_1, \ldots, \mathfrak{M}_k] = [[\mathfrak{M}_1, \ldots, \mathfrak{M}_{k-1}], \mathfrak{M}_k] = [\mathfrak{N}, \mathfrak{M}_k],$$

where $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$ form a totally relatively prime system. In combination with Theorem I this gives representation (15) for the residue group. The modules $\mathfrak{M}_1, \ldots, \mathfrak{M}_{k-1}$ also form a totally relatively prime system. For if, under some division of the modules of this system into two groups, the least common multiple of one group and the least common multiple of the other had a divisor in common, this divisor would remain if the module $\mathfrak{M}_k$ were added to one of the two groups and the least common multiple were then formed.[15] For $k = 2$, "totally relatively prime" means the same as "relatively prime"; hence our assertion may be assumed proved up to $k - 1$. Thus for the residue class $\mathfrak{x}\bar{\mathfrak{b}}$ the unique representation (18) holds, hence, by the isomorphism, also (16), and so the assertion follows.

Theorem II. *A module $\mathfrak{M}$ is representable as the least common multiple of k modules $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$ which form a totally relatively prime system if and only if its residue group $\mathfrak{G}$ is reducible into k subgroups $\mathfrak{U}_1, \ldots, \mathfrak{U}_k$. With suitable notation, $\mathfrak{U}_i$ is then isomorphic to the residue group of $\mathfrak{M}_i$.*

14) This is a generalization of a concept introduced by Loewy.

15) Continuing this argument shows that among $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$ every two are relatively prime; the converse, that this would imply $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$ to form a totally relatively prime system, is generally valid only in the commutative case; cf. the counterexample 1 in § 12.

§ 6.
Finiteness Theorems.

In this paragraph it will be shown that every residue group can be represented as a sum of finitely many irreducible constituents. To do this we first transfer Hilbert's theorem on the module basis.

From now on we use the more special hypotheses formulated in § 2: the multiplication of $\xi_1, \ldots, \xi_n$ among themselves is commutative, and the multiplication law of the polynomials has the form

$$\xi_i a = a_i \xi_i + b_i, \qquad (a_i \neq 0) \quad (i = 1, \ldots, n). \tag{6}$$

It suffices to prove the assertion for modules only. For if $\mathfrak{S}$ is any system of polynomials, we form the module $\mathfrak{M}$ derived from it by adjoining to $\mathfrak{S}$ all polynomials which can be composed from finitely many polynomials $G_1, \ldots, G_k$ of $\mathfrak{S}$ in the form $A_1 G_1 + \cdots + A_k G_k$. If $F_1, \ldots, F_l$ is then a module basis of $\mathfrak{M}$, and if

$$F_i = \sum_j A_{ij} G_j \qquad (i = 1, \ldots, l),$$

then the finitely many polynomials G_j occurring in these representations form a basis of $\mathfrak{S}$.

We prove the module-basis theorem following Gordan (Göttingen Nachrichten 1899). The proof splits into two parts. The first concerns a system $\mathfrak{P}$ of infinitely many power products and remains essentially unchanged because of the commutativity of $\xi_1, \ldots, \xi_n$. The power products

$$P = \xi_1^{a_1} \cdots \xi_n^{a_n},$$

each of which is entered into the system only once, are to be ordered by increasing degree and, within the same degree, in some fixed way. We now consider the subsystem $\mathfrak{Q}$ of $\mathfrak{P}$ consisting of all power products $P = Q$ not divisible by any preceding P. Then no Q is divisible by a later Q either, since later ones are either of higher degree or, in the same degree, different from the earlier ones. On the other hand, every P of $\mathfrak{P}$ is divisible by at least one Q. For suppose, to the contrary, that P_m is the first P divisible by no Q. Then P_m cannot itself be a Q, and so it is divisible by at least one preceding P; since by hypothesis this preceding P is divisible by some Q, P_m itself is divisible by a Q, a contradiction.

We now assert that the number of the Q is finite. Indeed, let

$$Q_0 = \xi_1^{h_1} \cdots \xi_n^{h_n}$$

be the first Q. Since an arbitrary $Q_\lambda = \xi_1^{h_{1\lambda}} \cdots \xi_n^{h_{n\lambda}}$ is not divisible by Q_0, for every Q at least one $h_{\rho\lambda} < h_\rho$ must hold; let λ denote the smallest index for which this is the case. We group all Q for which $h_{\rho\lambda}$ has the same fixed value c_λ into one class $K(c_\lambda)$. Since $c_\lambda < h_\lambda$, the number of these classes is finite. But each class contains only finitely many elements. For if we put a Q in the class $K(c_\lambda)$ equal to $\xi_\lambda^{c_\lambda} Q'$, then the Q' also form a system of power products none of which is divisible by another, and they contain only $n-1$ variables. For $n = 2$ the Q' contain only one variable; their number is then 1, hence finite, so that the number may also be assumed finite for $n-1$ variables. This proves the assertion.

Second, let $\mathfrak{M}$ be a module of polynomials whose terms are lexicographically ordered. Let $\mathfrak{P}$ be the system of the power products which occur in the highest term, each written only once. Then to the system $\mathfrak{Q} = (Q_1, \ldots, Q_\rho)$ there corresponds a system of finitely many polynomials $F_1, \ldots, F_\rho$, obtained by assigning to each Q_i some polynomial from $\mathfrak{M}$ whose highest term is equal to $b_i Q_i$, so that $F_i = b_i Q_i + \cdots$ with lower terms.

Now let $F = bP + \cdots$ be an arbitrary polynomial from $\mathfrak{M}$, where $P = \xi_1^{\beta_1} \cdots \xi_n^{\beta_n} Q_i$. Form the product

$$\xi_1^{\beta_1} \cdots \xi_n^{\beta_n} F_i = \xi_1^{\beta_1} \cdots \xi_n^{\beta_n} (b_i Q_i + \cdots) = c\, \xi_1^{\beta_1} \cdots \xi_n^{\beta_n} Q_i + \cdots = cP + \cdots .$$

Here $c \neq 0$ by (6), and all following terms are lower terms in the lexicographic order, since multiplication is commutative as regards the exponents, up to lower terms.[16] The difference

$$F - \frac{b}{c}\, \xi_1^{\beta_1} \cdots \xi_n^{\beta_n} F_i$$

16) This shows that in place of law (6) one could also use the somewhat less restrictive law

$$\xi_i a = a_i \xi_i + a_{i,i+1} \xi_{i+1} + \cdots + a_{in} \xi_n + b_i \qquad (a_i \neq 0)$$

for some fixed numbering of the ξ.

then contains only lower terms and again belongs to $\mathfrak{M}$. The procedure therefore terminates after finitely many steps, so that $F_1, \ldots, F_\rho$ are recognized as a module basis.

Theorem III. *Every system $\mathfrak{S}$ of infinitely many polynomials has a finite module basis $G_1, \ldots, G_k$, so that every polynomial G from $\mathfrak{S}$ admits a representation $G = A_1 G_1 + \cdots + A_k G_k$.*

The following is immediate.

Corollary. *Every system $\mathfrak{S}$ of infinitely many residue classes mod $\mathfrak{M}$ has a basis $\mathfrak{x}_1, \ldots, \mathfrak{x}_k$, so that every $\mathfrak{x}$ from $\mathfrak{S}$ is representable in the form $\mathfrak{x} = A_1\mathfrak{x}_1 + \cdots + A_k\mathfrak{x}_k$.*

Namely, assign to each residue class some representative and consider the system of these representatives together with all polynomials from $\mathfrak{M}$.

We now turn to the proof of the following theorem.

Theorem IV. *Every residue group can be represented as a sum of finitely many irreducible constituents; equivalently, by Theorem II, every module can be represented as the least common multiple of finitely many irreducible modules forming a totally relatively prime system.*

Suppose, to the contrary, that $\mathfrak{G}$ is a sum of infinitely many constituents $\mathfrak{U}_1, \mathfrak{U}_2, \ldots$ (cf. § 5), and let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ be the corresponding units, all of which are nonzero by definition. We form the system $\mathfrak{S}$ of all these units; by the corollary to Theorem III it has a finite basis $\mathfrak{a}_{i_1}, \ldots, \mathfrak{a}_{i_v}$ with $i_1 < \cdots < i_v$. Let $\mu > i_v$. Then

$$\mathfrak{a}_\mu = \mathfrak{x}_1\mathfrak{a}_{i_1} + \cdots + \mathfrak{x}_v\mathfrak{a}_{i_v}.$$

This is a linear relation between units, which is excluded by the definition. Hence in every additive decomposition of a residue group an irreducible constituent occurs after finitely many steps; because of commutativity of the decomposition, we can place it at the beginning. Thus, without loss of generality, we may assume that the $\mathfrak{U}_i$ themselves are irreducible. But by the preceding argument only finitely many constituents $\mathfrak{U}_i$ can occur. The assertion is proved.

§ 7.
A Case of Unique Decomposition.

Let

$$\mathfrak{G} = \mathfrak{U}_1 + \cdots + \mathfrak{U}_k = \mathfrak{B}_1 + \cdots + \mathfrak{B}_l$$

be a residue group whose constituents $\mathfrak{U}_1, \ldots, \mathfrak{U}_k$, $\mathfrak{B}_1, \ldots, \mathfrak{B}_l$ are irreducible. Then

$$\mathfrak{x}\mathfrak{e} = \mathfrak{x}\mathfrak{a}_1 + \cdots + \mathfrak{x}\mathfrak{a}_k = \mathfrak{x}\mathfrak{b}_1 + \cdots + \mathfrak{x}\mathfrak{b}_l, \tag{22}$$

where $\mathfrak{a}_\varkappa$ is the residue class of $\mathfrak{G}$ isomorphically assigned to the unit class of $\mathfrak{U}_\varkappa$, and $\mathfrak{b}_\lambda$ is the one assigned to the unit class of $\mathfrak{B}_\lambda$. Replacing $\mathfrak{x}$ by $\mathfrak{x}\mathfrak{b}_\lambda$, with λ a fixed index in the range $1, \ldots, l$, gives

$$\mathfrak{x}\mathfrak{b}_\lambda = \mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_1 + \cdots + \mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_k. \tag{23}$$

This representation of the group $\mathfrak{B}_\lambda$ is unique, but it is not an additive decomposition of $\mathfrak{B}_\lambda$, since the individual residue classes on the right need not belong to $\mathfrak{B}_\lambda$. Since $\mathfrak{b}_\lambda$ does not vanish, not every product $\mathfrak{b}_\lambda\mathfrak{a}_\varkappa$ can be zero. Without loss of generality, let

$$\mathfrak{b}_\lambda\mathfrak{a}_1 \neq 0, \ldots, \mathfrak{b}_\lambda\mathfrak{a}_\rho \neq 0, \qquad \mathfrak{b}_\lambda\mathfrak{a}_{\rho+1} = 0, \ldots, \mathfrak{b}_\lambda\mathfrak{a}_k = 0.$$

Then

$$\mathfrak{x}\mathfrak{b}_\lambda = \mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_1 + \cdots + \mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_\rho.$$

For a fixed $\varkappa$ in the range $1, \ldots, \rho$, consider the totality of those residue classes $\mathfrak{x}\mathfrak{b}_\lambda$ which are nonzero and for which also $\mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_\varkappa \neq 0$. The two systems $\mathfrak{x}\mathfrak{b}_\lambda$ and $\mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_\varkappa$ are isomorphic. First, the assignment is one-to-one: from $\mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_\varkappa = 0$ follows, by hypothesis, $\mathfrak{x}\mathfrak{b}_\lambda = 0$, and from the latter, by uniqueness of representation (23), $\mathfrak{x}\mathfrak{b}_\lambda\mathfrak{a}_\varkappa = 0$. Furthermore, sums correspond to sums, and products with arbitrary polynomials to the corresponding products. Keeping $\varkappa$ fixed, the same argument can be made for every λ with $\mathfrak{b}_\lambda\mathfrak{a}_\varkappa \neq 0$. For each $\mathfrak{a}_\varkappa$ there must be at least one such $\mathfrak{b}_\lambda$, since $\mathfrak{a}_\varkappa = (\mathfrak{b}_1 + \cdots + \mathfrak{b}_l)\mathfrak{a}_\varkappa \neq 0$.

We first assume that for each $\varkappa$ there is only one λ, and for each λ only one $\varkappa$, such that $\mathfrak{b}_\lambda\mathfrak{a}_\varkappa \neq 0$.

This correspondence implies $k = l$; moreover the notation may be chosen so that $\mathfrak{b}_\varkappa\mathfrak{a}_\varkappa \neq 0$ and $\mathfrak{b}_\lambda\mathfrak{a}_\varkappa = 0$ for $\lambda \neq \varkappa$. We then say that the products $\mathfrak{b}_\lambda\mathfrak{a}_\varkappa$ form a diagonal scheme. In this case, by (23), the unit is $\mathfrak{b}_\varkappa = \mathfrak{b}_\varkappa\mathfrak{a}_\varkappa$, and since

$$\mathfrak{a}_\varkappa = \mathfrak{b}_1\mathfrak{a}_\varkappa + \cdots + \mathfrak{b}_l\mathfrak{a}_\varkappa = \mathfrak{b}_\varkappa\mathfrak{a}_\varkappa = \mathfrak{b}_\varkappa, \tag{24}$$

one has, in general, $\mathfrak{U}_\varkappa = \mathfrak{B}_\varkappa$. Thus there is uniqueness of decomposition, and the products $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$ form a diagonal scheme.

If, for example, the commutative law holds specifically for the residue classes $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$, then the preceding hypothesis is always fulfilled. For in (23) each constituent $\mathfrak{x}\mathfrak{b}_\lambda \mathfrak{a}_\varkappa = \mathfrak{x}\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$ is then contained in $\mathfrak{B}_\lambda$, so that (23) gives an additive decomposition of the group $\mathfrak{B}_\lambda$. Since $\mathfrak{B}_\lambda$ is irreducible, all but one of the $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa$ are zero. By (24), correspondingly, for fixed $\varkappa$ only one $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa$ is different from zero, since otherwise (24), by interchangeability of $\mathfrak{a}_\varkappa$ and $\mathfrak{b}_\lambda$, would yield an additive decomposition of $\mathfrak{U}_\varkappa$, which is supposed to be irreducible.[17]

The same conclusions hold in the case where the conditions $\mathfrak{b}_\lambda \mathfrak{a}_\lambda \neq 0$, $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa = 0$ for $\lambda \neq \varkappa$, $\varkappa = 1, \ldots, k$, and likewise, for each $\mu = 1, \ldots, l$, $\mathfrak{b}_\mu \mathfrak{a}_\varkappa = 0$, $\mathfrak{b}_\mu \mathfrak{a}_\mu \neq 0$, $\varkappa = 1, \ldots, \sigma$, are fulfilled not for all, but only for part of the $\mathfrak{b}_\lambda$ ($\lambda = 1, \ldots, \sigma$). One finds $\mathfrak{U}_\varkappa = \mathfrak{B}_\varkappa$ for $\varkappa = 1, \ldots, \sigma$; and if one puts

$$\mathfrak{U}_{\sigma+1} + \cdots + \mathfrak{U}_k = \mathfrak{U}, \qquad \mathfrak{B}_{\sigma+1} + \cdots + \mathfrak{B}_l = \mathfrak{B},$$

then, also for the units $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{U}$ and $\mathfrak{B}$, the conditions $\mathfrak{b}\mathfrak{a}_\varkappa = 0$, $\mathfrak{b}_\varkappa \mathfrak{a} = 0$ ($\varkappa = 1, \ldots, \sigma$), and $\mathfrak{b}\mathfrak{a} \neq 0$ are fulfilled, whence $\mathfrak{U} = \mathfrak{B}$.

§ 8.
Additive Decomposition of Completely Reducible Groups into Prime Groups. The Theorem on Isomorphism.

We now consider another case, in which uniqueness does not hold, but isomorphism of the different decompositions does. This is the generalization of the case considered by Loewy.

Definition. *A module is called a prime module if it has no divisor other than itself and the unit module containing all polynomials. The residue group of a prime module is called a prime group.*

Every prime group is, a fortiori, irreducible. There are also infinite prime groups (cf. the definition in § 11 and example § 12, 2).

Let the given residue group $\mathfrak{G}$ now be representable in two ways as a sum of finitely many prime groups $\mathfrak{U}_1, \ldots, \mathfrak{U}_k$ and $\mathfrak{B}_1, \ldots, \mathfrak{B}_l$. A residue group which admits at least one such representation as a sum of prime groups, and the corresponding module $\mathfrak{M}$, will be called completely reducible, following Loewy's terminology.

We consider the products $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$ ($\varkappa = 1, \ldots, k$, $\lambda = 1, \ldots, l$), and show that either $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda = 0$, or else $\mathfrak{x}\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$ runs through the whole group $\mathfrak{B}_\lambda$ as $\mathfrak{x}$ runs through all residue classes of $\mathfrak{G}$. Indeed, the module belonging to $\mathfrak{B}_\lambda$ is

$$(\mathfrak{M}, \mathfrak{b}_1 + \cdots + \mathfrak{b}_{\lambda-1} + \mathfrak{b}_{\lambda+1} + \cdots + \mathfrak{b}_l) = \mathfrak{M}_{\mathfrak{b}_\lambda};$$

it arises from $\mathfrak{M}$ by adjoining all polynomials of the residue class $\mathfrak{b}_1 + \cdots + \mathfrak{b}_{\lambda-1} + \mathfrak{b}_{\lambda+1} + \cdots + \mathfrak{b}_l$. This module has the divisor

$$(\mathfrak{M}, \mathfrak{b}_1 + \cdots + \mathfrak{b}_{\lambda-1} + \mathfrak{b}_{\lambda+1} + \cdots + \mathfrak{b}_l, \mathfrak{a}_\varkappa \mathfrak{b}_\lambda).$$

But since $\mathfrak{M}_{\mathfrak{b}_\lambda}$ is, by hypothesis, a prime module, the divisor is either equal to $\mathfrak{M}_{\mathfrak{b}_\lambda}$ or to the unit module. In the first case $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$ belongs to $\mathfrak{M}_{\mathfrak{b}_\lambda}$; hence there is a relation

$$\mathfrak{a}_\varkappa \mathfrak{b}_\lambda = \mathfrak{x}(\mathfrak{b}_1 + \cdots + \mathfrak{b}_{\lambda-1} + \mathfrak{b}_{\lambda+1} + \cdots + \mathfrak{b}_l),$$

which gives $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda = 0$. In the second case there are two classes $\mathfrak{x}_0$ and $\mathfrak{x}_1$ such that

$$\mathfrak{x}_0 \mathfrak{a}_\varkappa \mathfrak{b}_\lambda + \mathfrak{x}_1(\mathfrak{b}_1 + \cdots + \mathfrak{b}_{\lambda-1} + \mathfrak{b}_{\lambda+1} + \cdots + \mathfrak{b}_l) = \mathfrak{e} = \mathfrak{b}_1 + \cdots + \mathfrak{b}_{\lambda-1} + \mathfrak{b}_{\lambda+1} + \cdots + \mathfrak{b}_l + \mathfrak{b}_\lambda,$$

and therefore, by uniqueness, $\mathfrak{x}_0 \mathfrak{a}_\varkappa \mathfrak{b}_\lambda = \mathfrak{b}_\lambda$. Thus $F\mathfrak{x}_0 \mathfrak{a}_\varkappa \mathfrak{b}_\lambda$, and hence also $\mathfrak{x}\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$, runs through the whole group $\mathfrak{B}_\lambda$ as F or $\mathfrak{x}$ runs through all polynomials or all residue classes of $\mathfrak{G}$. This proves the assertion.

If $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda \neq 0$, then $\mathfrak{U}_\varkappa$ is also isomorphic to $\mathfrak{B}_\lambda$. For by § 7 the totality of all classes $\mathfrak{x}\mathfrak{a}_\varkappa \neq 0$ for which $\mathfrak{x}\mathfrak{a}_\varkappa \mathfrak{b}_\lambda \neq 0$ is isomorphic to the system of classes $\mathfrak{x}\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$; and these exhaust the subgroup $\mathfrak{B}_\lambda$. It remains only to show that the indicated classes $\mathfrak{x}\mathfrak{a}_\varkappa$ exhaust $\mathfrak{U}_\varkappa$. To this end, consider all residue classes $\mathfrak{x}\mathfrak{a}_\varkappa$ for which $\mathfrak{x}\mathfrak{a}_\varkappa \mathfrak{b}_\lambda = 0$. This system has the property that the sum of two of its classes and the product with an arbitrary

17) The same applies in the noncommutative two-sided case treated by Schmeidler, loc. cit., where the product of every residue class of one subgroup with every residue class of the other subgroup vanishes. Then, since $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa = \mathfrak{b}_\lambda \mathfrak{a}_\varkappa \mathfrak{b}_1 + \cdots + \mathfrak{b}_\lambda \mathfrak{a}_\varkappa \mathfrak{b}_l$ and $\mathfrak{b}_\lambda(\mathfrak{a}_\varkappa \mathfrak{b}_\mu) = 0$ for $\lambda \neq \mu$, one has $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa = \mathfrak{b}_\lambda \mathfrak{a}_\varkappa \mathfrak{b}_\lambda$, hence this class is contained in $\mathfrak{B}_\lambda$; by irreducibility of $\mathfrak{B}_\lambda$, it follows that for only one, and hence for exactly one, $\varkappa$ the product $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa \neq 0$. In the same way one shows that for every $\mathfrak{a}_\varkappa$ there is one and only one $\mathfrak{b}_\lambda$ with $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda \neq 0$, whence $k = l$. Thus the $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa$ form a diagonal scheme, proving the uniqueness established there.

polynomial again belong to the system. If all these residue classes are adjoined to the module $\mathfrak{M}_{\mathfrak{a}_\varkappa}$, one again obtains a module which is a divisor of $\mathfrak{M}_{\mathfrak{a}_\varkappa}$; thus it is either $\mathfrak{M}_{\mathfrak{a}_\varkappa}$ or the unit module. In the latter case, however, $\mathfrak{a}_\varkappa$ itself would be contained in it, so that $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda = 0$, contrary to the hypothesis. Hence there are no classes $\mathfrak{x}\mathfrak{a}_\varkappa \neq 0$ for which $\mathfrak{x}\mathfrak{a}_\varkappa \mathfrak{b}_\lambda = 0$, and the isomorphism of $\mathfrak{U}_\varkappa$ with $\mathfrak{B}_\lambda$ is proved.

Suppose now, for a fixed $\varkappa$, that $\mathfrak{a}_\varkappa \mathfrak{b}_{\lambda_1} \neq 0, \ldots, \mathfrak{a}_\varkappa \mathfrak{b}_{\lambda_i} \neq 0$ with $i > 1$. Then $\mathfrak{U}_\varkappa$ is isomorphic to the groups $\mathfrak{B}_{\lambda_1}, \ldots, \mathfrak{B}_{\lambda_i}$, so these groups are mutually isomorphic.

We now show that at least two of the $\mathfrak{U}$ must then also be isomorphic. For if in the products $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa$ there belonged to each $\mathfrak{b}_\lambda$ only a single $\mathfrak{a}_\varkappa$ with $\mathfrak{b}_\lambda \mathfrak{a}_\varkappa \neq 0$, so that $\mathfrak{b}_\lambda = \mathfrak{b}_\lambda \mathfrak{a}_\varkappa$, then $\mathfrak{B}_\lambda = \mathfrak{U}_\varkappa$, since $\mathfrak{U}_\varkappa$, as a prime group, cannot contain a proper subgroup. Thus $k = l$ and, with a correct numbering, $\mathfrak{a}_\varkappa = \mathfrak{b}_\varkappa$; but then the scheme $\mathfrak{a}_\varkappa \mathfrak{b}_\lambda$ would be a diagonal scheme, which is not the case. The following theorem is therefore proved.

Theorem V. *If a completely reducible group $\mathfrak{G}$ is represented in two ways as a sum of prime groups,*

$$\mathfrak{G} = \mathfrak{U}_1 + \cdots + \mathfrak{U}_k = \mathfrak{B}_1 + \cdots + \mathfrak{B}_l,$$

then every group $\mathfrak{U}$ is isomorphic to at least one group $\mathfrak{B}$, and conversely. If every $\mathfrak{U}$ is isomorphic to exactly one $\mathfrak{B}$, then the decompositions are identical. In the other case at least two groups $\mathfrak{U}$ are mutually isomorphic, and likewise at least two groups $\mathfrak{B}$ are mutually isomorphic.

§ 9.
Connection Between the Concepts "Isomorphic" and "of the Same Kind".

In this paragraph we show that the concept "of the same kind", known for differential expressions in one variable, when generalized in the natural way, leads to the isomorphism of the associated residue groups.

Definition.[18] *Two modules $\mathfrak{M}$ and $\mathfrak{N}$ are called of the same kind if there are two polynomials P and Q, with P relatively prime to $\mathfrak{M}$ and Q relatively prime to $\mathfrak{N}$, such that for every $M \equiv 0(\mathfrak{M})$ and $N \equiv 0(\mathfrak{N})$*

$$MQ \equiv 0(\mathfrak{N}), \tag{25}$$

$$NP \equiv 0(\mathfrak{M}) \tag{26}$$

hold. Relative primeness here means the existence of two polynomials X and Y such that

$$YQ \equiv 1(\mathfrak{N}), \tag{27}$$

$$XP \equiv 1(\mathfrak{M}) \tag{28}$$

hold.

We now have the following theorem.

Theorem VI. *Two modules are of the same kind if and only if their residue groups are isomorphic.*

1. Let $\mathfrak{A}$ be the residue group of $\mathfrak{M}$, $\mathfrak{B}$ the residue group of $\mathfrak{N}$, and suppose $\mathfrak{A}$ is isomorphic to $\mathfrak{B}$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be the unit classes of $\mathfrak{A}$ and $\mathfrak{B}$. Further, let $Q\mathfrak{b}$ be the class in $\mathfrak{B}$ corresponding to the unit $\mathfrak{a}$ in $\mathfrak{A}$, and let $P\mathfrak{a}$ be the class in $\mathfrak{A}$ corresponding to the unit $\mathfrak{b}$ of $\mathfrak{B}$. We write this assignment as

$$\mathfrak{a} \sim Q\mathfrak{b}, \tag{29}$$

$$P\mathfrak{a} \sim \mathfrak{b}. \tag{30}$$

It follows that

$$0 = M\mathfrak{a} \sim MQ\mathfrak{b}, \qquad \text{that is,} \qquad MQ \equiv 0(\mathfrak{N}),$$

which proves (25). Likewise,

$$NP\mathfrak{a} \sim N\mathfrak{b} = 0, \qquad \text{that is,} \qquad NP \equiv 0(\mathfrak{M}),$$

which proves (26). Moreover, by (29), $P\mathfrak{a} \sim PQ\mathfrak{b}$; since by (30) $P\mathfrak{a} \sim \mathfrak{b}$ was assumed, uniqueness of the assignment gives $PQ\mathfrak{b} = \mathfrak{b}$, hence $PQ \equiv 1(\mathfrak{N})$, and similarly $QP \equiv 1(\mathfrak{M})$. Thus (27) and (28) are proved, with $X = Q$, $Y = P$.

2. Conversely, suppose $\mathfrak{M}$ and $\mathfrak{N}$ are of the same kind, so that relations (25) through (28) hold. We assign to an arbitrary class $F\mathfrak{a}$ of $\mathfrak{A}$ the class $FQ\mathfrak{b}$ of $\mathfrak{B}$. This assigns to each class in $\mathfrak{A}$ only one class in $\mathfrak{B}$: for

18) For differential expressions in one variable, cf. Blumberg's formal definition, loc. cit., p. 25.

from $F\mathfrak{a} = 0$, hence $F = M$, it follows by (25) that $FQ\mathfrak{b} = 0$. Moreover, the whole group $\mathfrak{B}$ is exhausted by this assignment, since the special class $Y\mathfrak{a}$ corresponds to $YQ\mathfrak{b}$, which equals $\mathfrak{b}$ by (27). Thus we have an unambiguous map Φ from $\mathfrak{A}$ onto $\mathfrak{B}$; it has not yet been shown to be one-to-one. Similarly, equations (26) and (28) give an unambiguous map Ψ from $\mathfrak{B}$ onto $\mathfrak{A}$, which again has not yet been shown to be one-to-one.

If either of these two maps is one-to-one, then the isomorphism is proved, since the requirements concerning sums and products are fulfilled. But if both maps Φ and Ψ were not one-to-one, then there would be classes $G\mathfrak{a}$ in $\mathfrak{A}$ corresponding to the class $GQ\mathfrak{b} = 0$ in $\mathfrak{B}$. The classes $FQ\mathfrak{b}$ corresponding to all the other residue classes $F\mathfrak{a}$ would then already exhaust the group $\mathfrak{B}$, and consequently the map Ψ would return the whole group $\mathfrak{A}$ in the classes $FQP\mathfrak{a}$. As we know, there are also nonzero classes in $\mathfrak{B}$ which, under Ψ, correspond to the zero class in $\mathfrak{A}$; we denote by $G_1\mathfrak{a}$ all those classes for which $G_1\mathfrak{a} \neq 0$ but $G_1QP\mathfrak{a} = 0$. All remaining polynomials F have the property that $FQP\mathfrak{a}$ exhausts the group $\mathfrak{A}$. Those polynomials F for which $FQP\mathfrak{a} = G_1\mathfrak{a}$ will be denoted by G_2; such polynomials exist whenever polynomials G_1 exist. For each G_2 one has $G_2QP\mathfrak{a} \neq 0$, but $G_2(QP)^2\mathfrak{a} = 0$. Correspondingly, for every integer ν there are classes $G_\nu\mathfrak{a}$ such that $G_\nu(QP)^{\nu-1}\mathfrak{a} \neq 0$ but $G_\nu(QP)^\nu\mathfrak{a} = 0$.

Now consider the system $\mathfrak{S}$ consisting of all polynomials $G_1, G_2, \ldots$. It has a finite module basis $G_{\lambda_1}, \ldots, G_{\lambda_e}$. Choose ν greater than the largest of the indices $\lambda_1, \ldots, \lambda_e$, which we denote by λ. Then

$$G_\nu = A_1 G_{\lambda_1} + \cdots + A_e G_{\lambda_e}.$$

Multiplying by $(QP)^\lambda$ gives

$$G_\nu (QP)^\lambda \equiv 0(\mathfrak{M}),$$

a contradiction to our hypothesis. Hence the isomorphism follows, and therefore, by part 1, the sharper relations (27), (28) hold with $X = Q$, $Y = P$.

By Theorem VI, Theorem V may also be expressed as follows.

Theorem VII.[19] *If a completely reducible module $\mathfrak{M}$ is representable in two ways as the least common multiple of prime modules $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ and $\mathfrak{D}_1, \ldots, \mathfrak{D}_l$, each forming a totally relatively prime system, then every $\mathfrak{P}$ is of the same kind as at least one $\mathfrak{D}$, and conversely. If every $\mathfrak{P}$ is of the same kind as exactly one $\mathfrak{D}$, then the decompositions are identical. In the other case at least two of the modules $\mathfrak{P}$ are of the same kind as one another, and likewise at least two of the modules $\mathfrak{D}$ are of the same kind as one another.*

§ 10.
Existence of Infinitely Many Decompositions of a Group.

If the representation of a completely reducible group as a sum is not unique, then by Theorem V every representation contains at least two mutually isomorphic subgroups. We now consider the subgroup formed from such a system of isomorphic subgroups,

$$\mathfrak{H} = \mathfrak{A}_1 + \cdots + \mathfrak{A}_\alpha,$$

where $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\alpha$ are all isomorphic, and assert that $\mathfrak{H}$ then admits infinitely many distinct decompositions of this kind, provided only that the rationality domain P contains infinitely many "constants", that is, quantities a for which $\xi_i a = a\xi_i$. This theorem is valid even when no further hypothesis is imposed on the groups $\mathfrak{A}_i$, not even irreducibility. Thus we have:

Theorem VIII. *If $\mathfrak{G}$ can be represented as a sum of finitely many mutually isomorphic subgroups, then this representation is possible in infinitely many distinct ways, provided only that the rationality domain P contains infinitely many constants. Here constants mean those quantities a of the domain for which $\xi_i a = a\xi_i$.*

Proof. Let

$$\mathfrak{G} = \mathfrak{A}_1 + \cdots + \mathfrak{A}_\alpha,$$

and let $\mathfrak{A}_i$ be isomorphic to $\mathfrak{A}_\varkappa$ for $i, \varkappa = 1, \ldots, \alpha$ ($\alpha \geq 2$). In order to specify a definite isomorphic assignment, we first single out one subgroup, say $\mathfrak{A}_1$. Let the isomorphism between $\mathfrak{A}_1$ and $\mathfrak{A}_i$ be fixed by

$$a_1 \sim t_{1i} a_i, \qquad a_i \sim t_{i1} a_1, \qquad t_{11} a_1 = a_1 \quad (i, \varkappa = 1, \ldots, \alpha), \tag{31}$$

so that, in the group $\mathfrak{A}_1$, each residue class is assigned to itself. Since $Ma_1 = 0$ and $Ma_i = 0$, it follows that $Mt_{1i}a_i = 0$ and $Mt_{i1}a_1 = 0$; hence the classes $t_{1i}a_i$ and $t_{i1}a_1$, analogously to units, admit multiplication

19) Cf. Loewy, pp. 100–101.

by classes, not merely by polynomials. It follows from the definition of isomorphism that, for two assigned classes $\mathfrak{y}$ and $\bar{\mathfrak{y}}$ admitting this class multiplication, the classes $\mathfrak{r}\mathfrak{y}$ and $\mathfrak{r}\bar{\mathfrak{y}}$ are again assigned to each other. Therefore the relations $a_r a_s = 0$ $(r \neq s)$ $(r = 1, \ldots, \alpha;\ s = 1, \ldots, \alpha)$ give, for $s = 1$,

$$\begin{cases} & a_r t_{1\varkappa} a_\varkappa = 0 & (\varkappa = 1, \ldots, \alpha,\ r \neq 1), \\ \text{and for } s > 1 & a_r t_{s1} a_1 = 0 & (r \neq s), \\ \text{hence also} & t_{1\varkappa} a_\varkappa = a_1 t_{1\varkappa} a_\varkappa, \quad t_{i1} a_1 = a_i t_{i1} a_1. \end{cases} \tag{32}$$

Furthermore, from (31), generalizing (27) and (28), the uniqueness of the assignment gives

$$t_{1i} t_{i1} a_1 = a_1, \qquad t_{\varkappa 1} t_{1\varkappa} a_\varkappa = a_\varkappa. \tag{33}$$

Let the isomorphism between $\mathfrak{A}_i$ and $\mathfrak{A}_\varkappa$ now be the relation obtained by composing (31); such a stipulation is necessary, since the individual groups may admit isomorphisms into themselves. From (31), (32), and (33) we therefore get

$$a_i \sim t_{i1} t_{1\varkappa} a_\varkappa = t_{i\varkappa} a_\varkappa, \qquad t_{ii} a_i = a_i; \qquad a_r t_{s\varkappa} a_\varkappa = 0 \quad (r \neq s), \tag{34}$$

where $t_{i1} t_{1\varkappa} = t_{i\varkappa}$ has been put. From (33) and (34) one obtains further

$$t_{i\varkappa} t_{\varkappa l} a_l = t_{i1} t_{1\varkappa} t_{\varkappa 1} t_{1l} a_l = t_{i1} t_{1l} a_l = t_{il} a_l;$$

thus the singling out of the group $\mathfrak{A}_1$ is again removed. The isomorphic relation between $\mathfrak{A}_i$ and $\mathfrak{A}_\varkappa$ remains the same, whichever group $\mathfrak{A}_\varkappa$ is used in place of $\mathfrak{A}_1$ for the definition. Hence the $t_{i\varkappa}$ are classes which, in summary, satisfy the relations

$$M t_{i\varkappa} a_\varkappa = 0; \quad a_r t_{i\varkappa} a_\varkappa = 0 \ (r \neq i); \quad t_{i\varkappa} t_{\varkappa l} a_l = t_{il} a_l; \quad t_{\varkappa i} a_i = t_{\varkappa i} t_{i\varkappa} a_\varkappa = a_\varkappa. \tag{35}$$

These relations say precisely that the modules $\mathfrak{M}_i$ and $\mathfrak{M}_\varkappa$ belonging to $\mathfrak{A}_i$ and $\mathfrak{A}_\varkappa$ are of the same kind (cf. the definition in § 9); in place of the P and Q there we have here the classes $t_{i\varkappa}$ and $t_{\varkappa i}$, and the first two relations (35), taken together, correspond to formula (25) or (26). Conversely, these relations imply the isomorphism by Theorem VI.[20]

From the classes $t_{i\varkappa} a_\varkappa$ we now compose classes b_ρ which will again turn out to be units of groups $\mathfrak{B}_\rho$, whence a representation

$$\mathfrak{G} = \mathfrak{B}_1 + \cdots + \mathfrak{B}_\alpha$$

will follow. Let $\lambda_{i\varkappa}$ be constants whose determinant $|\lambda_{i\varkappa}|$ is nonzero, and let $\lambda^{\varkappa r}$ be the corresponding cofactors divided by $|\lambda_{i\varkappa}|$, so that the relations

$$\begin{cases} \sum_{r=1}^{\alpha} \lambda_{ri} \lambda^{r\varkappa} = \delta_{i\varkappa} = \begin{cases} 0, & i \neq \varkappa, \\ 1, & i = \varkappa, \end{cases} \\ \sum_{r=1}^{\alpha} \lambda_{ir} \lambda^{\varkappa r} = \delta_{i\varkappa} \end{cases} \tag{36}$$

hold. We then define

$$b_\rho = \sum_{i,\varkappa} \lambda_{\rho i} \lambda^{\rho\varkappa} t_{i\varkappa} a_\varkappa \qquad (\rho = 1, \ldots, \alpha). \tag{37}$$

From (35), (36), and (37) one obtains $M b_\rho = 0$ and

$$\sum_{\rho=1}^{\alpha} b_\rho = \sum_{i,\varkappa,\rho} \lambda_{\rho i} \lambda^{\rho\varkappa} t_{i\varkappa} a_\varkappa = \sum_{i,\varkappa} \delta_{i\varkappa} t_{i\varkappa} a_\varkappa = \sum_i t_{ii} a_i = \sum_i a_i = e, \tag{38}$$

and also

$$\begin{aligned} b_\rho b_\sigma &= \sum_{\substack{i,\varkappa \\ \mu,\nu}} \lambda_{\rho i} \lambda^{\rho\varkappa} \lambda_{\sigma\mu} \lambda^{\sigma\nu} t_{i\varkappa} a_\varkappa t_{\mu\nu} a_\nu \\ &= \sum_{i,\mu,\nu} \lambda_{\rho i} \lambda^{\rho\mu} \lambda_{\sigma\mu} \lambda^{\sigma\nu} t_{i\nu} a_\nu = \delta_{\rho\sigma} \sum_{i,\nu} \lambda_{\rho i} \lambda^{\sigma\nu} t_{i\nu} a_\nu = \begin{cases} 0 & (\rho \neq \sigma), \\ b_\rho & (\rho = \sigma), \end{cases} \end{aligned}$$

20) And in fact without applying the finiteness theorem, since the formulas already display respectively a map $\varphi_{i\varkappa}$ and its inverse $\varphi_{\varkappa i}$. For from $r a_i = r a_i t_{i\varkappa} a_\varkappa t_{\varkappa i} a_i$ it follows that $r a_i \neq 0$ also implies $r a_i t_{i\varkappa} a_\varkappa \neq 0$.

$(\rho, \sigma = 1, \ldots, \alpha)$. Thus the representation $\mathfrak{r}e = \mathfrak{r}b_1 + \cdots + \mathfrak{r}b_\alpha$ is an additive decomposition of the group $\mathfrak{G}$. The groups $\mathfrak{B}_\rho$ are distinct from the groups $\mathfrak{A}_\sigma$ as soon as the $\lambda_{i\varkappa}$ do not merely form a diagonal matrix. For if we form $a_\sigma b_\rho$, then by (35) we get

$$a_\sigma b_\rho = \sum_{i,\varkappa} \lambda_{\rho i} \lambda^{\rho\varkappa} a_\sigma t_{i\varkappa} a_\varkappa = \lambda_{\rho\sigma} \sum_{\varkappa} \lambda^{\rho\varkappa} t_{\sigma\varkappa} a_\varkappa \neq 0 \quad \text{for } \lambda_{\rho\sigma} \neq 0,$$

since otherwise each individual summand in the last sum would have to vanish, which is not the case. Thus if, for fixed σ, there are at least two ρ with $\lambda_{\rho\sigma} \neq 0$, then $\mathfrak{A}_\sigma$ cannot be identical with any $\mathfrak{B}_\rho$.

But the groups $\mathfrak{B}_\rho$ are also mutually isomorphic and isomorphic to the groups $\mathfrak{A}_\sigma$. We first show the existence of classes $r_{\rho\sigma} a_\sigma$ and $r^{\sigma\rho} b_\rho$ which mediate the isomorphism of $\mathfrak{A}_\sigma$ and $\mathfrak{B}_\rho$ $(\rho, \sigma = 1, \ldots, \alpha)$. Indeed, we show that for the classes

$$r_{\rho\sigma} a_\sigma = \sum_i \lambda_{\rho i} t_{i\sigma} a_\sigma, \qquad r^{\sigma\rho} = \sum_{\varkappa} \lambda^{\rho\varkappa} t_{\sigma\varkappa} a_\varkappa = r^{\sigma\rho} b_\rho$$[20]

the relations "of the same kind" are fulfilled between the modules

$$(\mathfrak{M}, b_1 + \cdots + b_{\rho-1} + b_{\rho+1} + \cdots + b_\alpha)$$

and

$$\begin{gathered}(\mathfrak{M}, a_1 + \cdots + a_{\sigma-1} + a_{\sigma+1} + \cdots + a_\alpha) : \\ \begin{cases} b_\varkappa r_{\rho\sigma} a_\sigma = 0 \quad (\varkappa \neq \rho), \quad r^{\sigma\rho} r_{\rho\sigma} a_\sigma = a_\sigma, \\ a_\varkappa r^{\sigma\rho} b_\rho = 0 \quad (\varkappa \neq \sigma), \quad r_{\rho\sigma} r^{\sigma\rho} b_\rho = b_\rho, \end{cases}\end{gathered} \tag{39}$$

from which, as in (35), the isomorphism follows through the assignment

$$b_\rho \sim r_{\rho\sigma} a_\sigma, \qquad a_\sigma \sim r^{\sigma\rho} b_\rho. \tag{40}$$

Indeed,

$$\begin{aligned} b_\varkappa r_{\rho\sigma} a_\sigma &= \sum_{\mu,\nu,i} \lambda_{\varkappa\mu} \lambda^{\varkappa\nu} t_{\mu\nu} a_\nu \lambda_{\rho i} t_{i\sigma} a_\sigma \\ &= \sum_{\mu,i} \lambda_{\varkappa\mu} \lambda^{\varkappa i} \lambda_{\rho i} t_{\mu\sigma} a_\sigma = \delta_{\varkappa\rho} \sum_\mu \lambda_{\varkappa\mu} t_{\mu\sigma} a_\sigma = \delta_{\varkappa\rho} r_{\rho\sigma} a_\sigma = 0 \quad (\varkappa \neq \rho), \end{aligned}$$

and further

$$r^{\sigma\rho} r_{\rho\sigma} a_\sigma = \sum_{\nu,i} \lambda^{\rho\nu} t_{\sigma\nu} a_\nu \lambda_{\rho i} t_{i\sigma} a_\sigma = \sum_i \lambda^{\rho i} \lambda_{\rho i} a_\sigma = a_\sigma.$$

Conversely, in the same way one finds

$$a_\varkappa r^{\sigma\rho} b_\rho = a_\varkappa \sum_\mu \lambda^{\rho\mu} t_{\sigma\mu} a_\mu = 0 \quad (\varkappa \neq \sigma),$$

and

$$r_{\rho\sigma} r^{\sigma\rho} b_\rho = \sum_{i,\mu} \lambda_{\rho i} t_{i\sigma} a_\sigma \lambda^{\rho\mu} t_{\sigma\mu} a_\mu = \sum_{i,\mu} \lambda_{\rho i} \lambda^{\rho\mu} t_{i\mu} a_\mu = b_\rho.$$

From the relations of the same kind just proved, the isomorphism of $\mathfrak{A}_\sigma$ and $\mathfrak{B}_\rho$ follows (again without the finiteness theorem). The isomorphism between $\mathfrak{B}_\rho$ and $\mathfrak{B}_\tau$ is obtained from this by composition; we record the formulas. Put

$$\ell_{\rho\tau} b_\tau = r_{\rho\varkappa} r^{\varkappa\tau} b_\tau = \sum_{i,j} \lambda_{\rho i} t_{i\varkappa} a_\varkappa \lambda^{\tau j} t_{\varkappa j} a_j = \sum_{i,j} \lambda_{\rho i} \lambda^{\tau j} t_{ij} a_j;$$

then the assignment is $b_\rho \sim \ell_{\rho\tau} b_\tau$. Here too the relations of the same kind can again be verified formally; if the $\ell_{\rho\tau}$ are put in place of the $t_{i\varkappa}$, they satisfy (35). Indeed,

$$b_\sigma \ell_{\rho\tau} b_\tau = b_\sigma r_{\rho\varkappa} r^{\varkappa\tau} b_\tau = 0 \quad (\sigma \neq \rho),$$

$$\ell_{\rho\sigma} \ell_{\sigma\tau} b_\tau = r_{\rho\varkappa} r^{\varkappa\sigma} r_{\sigma\lambda} r^{\lambda\tau} b_\tau = r_{\rho\varkappa} a_\varkappa r^{\varkappa\tau} b_\tau = \ell_{\rho\tau} b_\tau.$$

20) Because of (37), $r^{\sigma\rho} b_\rho = \sum_{\varkappa,i,\mu} \lambda^{\rho\varkappa} t_{\sigma\varkappa} a_\varkappa \lambda_{\rho i} \lambda^{\rho\mu} t_{i\mu} a_\mu = \sum_{\varkappa,\mu} \lambda^{\rho\varkappa} \lambda_{\rho\varkappa} \lambda^{\rho\mu} t_{\sigma\mu} a_\mu = \sum_\mu \lambda^{\rho\mu} t_{\sigma\mu} a_\mu = r^{\sigma\rho}$.

20) The number of formulas is doubled in comparison with (35), since the inverse is not obtained here, as it was there, by interchanging the indices.

This proves Theorem VIII, since one need only choose the $\lambda_{i\varkappa}$ in infinitely many ways so that they form no diagonal matrix and also are not transformed into one another by diagonal matrices.

A consequence of Theorem VIII, in connection with Theorem V or VII, is:

Theorem IX.[23] *Let the module $\mathfrak{M}$ be completely reducible and the least common multiple of prime modules $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ which form a totally relatively prime system, and suppose the rationality domain P contains infinitely many constants. Then the necessary and sufficient condition that $\mathfrak{M}$ be representable in infinitely many distinct ways as the least common multiple of prime modules is that at least two of the modules $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ be of the same kind.*

We shall now derive general criteria for a module $\mathfrak{M}$ to be divisible by infinitely many prime modules, and first prove the following:

Auxiliary theorem.[24] *If a completely reducible module $\mathfrak{M} = [\mathfrak{P}_1, \ldots, \mathfrak{P}_k]$ is divisible by a prime module $\mathfrak{P}'$ different from all the $\mathfrak{P}_i$, then at least two of the $\mathfrak{P}_i$ are of the same kind.*

We first select from $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ a totally relatively prime system by successively deleting every one of these prime modules that is contained in the least common multiple of those not yet deleted. Hence assume now that $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ themselves form a totally relatively prime system. Let a' be a class of $\mathfrak{M}$ corresponding to the unit class modulo $\mathfrak{P}'$. Then

$$Fa' = Fa'a_1 + \cdots + Fa'a_k$$

for every polynomial F. At least two of the products $a'a_i$ are nonzero, say $a'a_1$ and $a'a_2$; for if, for instance, only $a'a_1 \neq 0$, then $Fa' = Fa'a_1$, and the residue classes Fa' would form a subgroup of $\mathfrak{A}_1$, hence, since $\mathfrak{A}_1$ is a prime group, would be identical with $\mathfrak{A}_1$, so that the modules $\mathfrak{P}'$ and $\mathfrak{P}_1$ would also coincide. By the reasoning of § 8, it follows that $\mathfrak{A}'$ is isomorphic to $\mathfrak{A}_1$ and $\mathfrak{A}_2$.

Let $\mathfrak{M}$ now be an arbitrary module. We consider the least common multiple $\mathfrak{N}$ of all prime modules by which $\mathfrak{M}$ is divisible.[25] Two cases are possible. Either $\mathfrak{N}$ is not representable as the least common multiple of finitely many prime modules; in this case $\mathfrak{N}$, and hence also $\mathfrak{M}$, has infinitely many prime modules as divisors. Or $\mathfrak{N}$ is representable as the least common multiple of finitely many prime modules; then $\mathfrak{N}$ is called the greatest completely reducible module of $\mathfrak{M}$ (following a corresponding construction of Loewy). If among these finitely many prime modules two are of the same kind, then by Theorem IX the module $\mathfrak{N}$, and therefore $\mathfrak{M}$, is divisible by infinitely many prime modules. Conversely, if the latter is the case, then there is at least one prime divisor of $\mathfrak{N}$ different from all the finitely many modules whose least common multiple represents $\mathfrak{N}$. By the auxiliary theorem, $\mathfrak{N}$, hence $\mathfrak{M}$, has two prime divisors of the same kind. Thus we have proved:

Theorem X. *If the rationality domain P contains infinitely many constants, then the necessary and sufficient condition that a module be divisible by infinitely many distinct prime modules is that either no greatest completely reducible module exists, or, if such a module exists, that it be divisible by at least two distinct prime modules of the same kind.*

§ 11.
Relations to Systems of Differential Equations and Their Integrals.

By virtue of the finiteness theorem, to every module of differential expressions there can be assigned as a basis a system of finitely many differential expressions, so that the totality of simultaneous integrals of all differential equations obtained by setting a differential expression of the module equal to zero coincides with the totality of integrals of the finite system of differential equations obtained by setting the basis differential expressions equal to zero. This gives the connection with the theory of systems of linear partial differential equations; we pursue this connection a little further in the case where the residue group of the module is "finite".

Definition. *A residue group is called finite if there is a number μ, the order of the group, such that between any $\mu + 1$ residue classes there is a linear relation with coefficients from P, while there is at least one system of μ residue classes between which no relation exists, and which we shall call a linear basis of the residue group. In the other case the residue group is called infinite.*

23) Cf. Loewy, pp. 106–107.

24) Cf. Loewy, p. 96.

25) If there are infinitely many of these, then by Theorem IV no additive decomposition of the residue group can correspond to this representation. Cf. also the example § 12, 4.

The sum of two finite residue groups has finite order, namely the sum of their orders. The sum of two infinite groups, or of a finite and an infinite group, is an infinite group. Examples of finite groups are furnished by all residue groups of modules in one variable; but for several variables the order can also be finite, for instance for the module with basis ξ_1^2, ξ_2^2, where all residue classes can be linearly composed from those of $1, \xi_1, \xi_2, \xi_1\xi_2$. For examples of infinite groups see § 12.

We now have the following:

Theorem XI: *If a module has a finite residue group, then every system of differential equations obtained by setting a basis of the module equal to zero admits exactly as many linearly independent integrals as the order of its residue group indicates. Conversely, for a given system of finitely many linear partial differential equations that possess only a finite number of linearly independent integrals, this number is equal to the order of the residue group of the module generated by the differential expressions.*

Here the rationality domain P consists of analytic functions of n variables $x_1, \ldots, x_n$, with the occurring singularities, inside a certain n-dimensional domain, forming at most manifolds of lower dimensions, so that there are arbitrarily many points with regular n-dimensional neighborhoods.

Let $\mathfrak{M}$ be a module with finite residue group. We show that there is a linear basis of power products with the property that *when an arbitrary residue class is expressed through this basis, only powers of finitely many different quantities from P can occur in the denominator.*

For this purpose we order all power products $\xi_1^{a_1} \cdots \xi_n^{a_n}$ lexicographically and take as representatives $Q_1, \ldots, Q_m$ of the residue classes all those that are linearly independent modulo $\mathfrak{M}$ of the preceding ones. By hypothesis there are only finitely many such products. All the others can be expressed linearly through these.

Let $\mathfrak{S}$ be the system of all power products not admitted into the linear basis. Then, by the first part of the proof of Theorem III, $\mathfrak{S}$ has a finite subsystem $\mathfrak{T}$ of power products such that every power product from $\mathfrak{S}$ is divisible by at least one from $\mathfrak{T}$. Let $P_1, \ldots, P_\rho$ be the power products of $\mathfrak{T}$, and let $M_1 \equiv 0, \ldots, M_\rho \equiv 0$ $(\mathfrak{M})$ be the relations by means of which $P_1, \ldots, P_\rho$ are each expressed modulo $\mathfrak{M}$ by a linear combination of lower power products; for example,

$$M_i = b_i P_i + \text{lower terms.}$$

If P is an arbitrary power product from $\mathfrak{S}$, hence of the form

$$\xi_1^{h_1} \cdots \xi_n^{h_n} P_i,$$

then

$$\begin{aligned} \xi_1^{h_1} \cdots \xi_n^{h_n} M_i &= b_i \xi_1^{h_1} \cdots \xi_n^{h_n} P_i + \text{lower terms} \\ &= b_i P + \text{lower terms.} \end{aligned}$$

Assume now that it has already been proved for all power products lower than P that only powers of $b_1, \ldots, b_\rho$ occur in denominators, while the numerators are formed from the coefficients of the M_i by addition, multiplication, and differentiation. Then the same holds for P itself. This assumption is permitted, since it is fulfilled for P_1, the first element from $\mathfrak{S}$ and $\mathfrak{T}$.

By Theorem III, moreover, $M_1, \ldots, M_\rho$ is a module basis of $\mathfrak{M}$. Now consider a system of values $\beta_1, \ldots, \beta_n$ of $x_1, \ldots, x_n$ for which $b_1 \neq 0, \ldots, b_\rho \neq 0$ and the remaining coefficients of the M_i are regular, that is, a regular point of the system of differential equations $M_1 = 0, \ldots, M_\rho = 0$. The power products $Q_i = \xi_1^{h_{i1}} \cdots \xi_n^{h_{in}}$ $(i = 1, \ldots, m)$ correspond to the partial derivatives

$$\frac{\partial^{h_{i1}+\cdots+h_{in}}}{\partial x_1^{h_{i1}} \cdots \partial x_n^{h_{in}}} y,$$

for which we prescribe arbitrary constant values $(\gamma_1, \ldots, \gamma_m)$ at the point $(\beta_1, \ldots, \beta_n)$. Then the differential equations $M_i = 0$ determine uniquely, as finite values at this point, the values of all higher derivatives of y, since only the b_i occur in denominators; and it is known that this implies the existence of m linearly independent analytic integrals.

On the other hand, under our hypotheses there cannot exist more than m linearly independent integrals, since otherwise at a regular point one could prescribe arbitrarily the values of $m+1$ suitably chosen derivatives, contrary to the fact that linear dependencies modulo $\mathfrak{M}$ must exist among any $m+1$ power products.

Conversely, if a module has an infinite residue group, the same method shows that there are infinitely many linearly independent integrals; therefore, in the case of only m linearly independent integrals, the residue group is finite, and its order is, by the above, equal to m.

To close this paragraph we show that, for two modules of differential expressions, the concept of isomorphism, or equivalently of being of the same kind, has for the integrals of the associated systems of differential equations the same meaning as Poincaré's concept of kind for one variable (cf. Blumberg, loc. cit., Appendix I).

Theorem XII. *If two modules $\mathfrak{M}$ and $\mathfrak{N}$ of differential expressions are of the same kind, then there are two differential expressions P and Q such that $P(y)$ and $Q(z)$ run through all integrals of $\mathfrak{N}$ and $\mathfrak{M}$, respectively, when y runs through all integrals of $\mathfrak{M}$ and z through all integrals of $\mathfrak{N}$.*

By hypothesis, namely (by § 9), for two suitably chosen polynomials P and Q the relations

$$MQ \equiv 0(\mathfrak{N}), \qquad PQ \equiv 1(\mathfrak{N}),$$

$$NP \equiv 0(\mathfrak{M}), \qquad QP \equiv 1(\mathfrak{M})$$

hold. Thus, since $NP(y) = 0$, the function $P(y)$ is an integral of $\mathfrak{N}$. Likewise $Q(z)$ is an integral of $\mathfrak{M}$. Since $PQ(z) = z$ and $QP(y) = y$, $P(y)$ runs through all integrals of $\mathfrak{N}$, and $Q(z)$ all integrals of $\mathfrak{M}$. In this way, to each nonzero y there corresponds a nonzero z, and conversely.

§ 12.
Examples.

1. As a first example we consider an ordinary linear differential equation of second order whose coefficients are represented as symmetric functions of the integrals. The rationality domain P consists here of all rational functions of the integrals and their derivatives; we restrict ourselves to a sufficiently small neighborhood of a regular point of the differential equation. We define the module $\mathfrak{M}$ as the totality of all differential expressions that have y_1 and y_2 as integrals, and for which we again write polynomials in one indeterminate ξ. The module basis is then one-membered, and is given by the polynomial

$$M = \begin{vmatrix} y_1 & y_2 \\ y_1' & y_2' \end{vmatrix} \xi^2 - \begin{vmatrix} y_1 & y_2 \\ y_1'' & y_2'' \end{vmatrix} \xi + \begin{vmatrix} y_1' & y_2' \\ y_1'' & y_2'' \end{vmatrix},$$

which is uniquely determined up to a factor from P. Now

$$\mathfrak{M} = [\mathfrak{M}_1, \mathfrak{M}_2], \tag{41}$$

where $\mathfrak{M}_i$ consists of all differential expressions having the integral y_i, and whose basis is determined up to a factor from P by

$$M_i = y_i\xi - y_i' \qquad (i = 1, 2).$$

Indeed, $\mathfrak{M}$ is divisible by $\mathfrak{M}_1$ and $\mathfrak{M}_2$, since it vanishes for the integrals y_1 and y_2, and hence is divisible by $[\mathfrak{M}_1, \mathfrak{M}_2]$; and since the order of the basis polynomial of $[\mathfrak{M}_1, \mathfrak{M}_2]$ must be at least 2, one has $\mathfrak{M} = [\mathfrak{M}_1, \mathfrak{M}_2]$. Further, $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are relatively prime, because

$$\frac{y_2}{D}(y_1\xi - y_1') - \frac{y_1}{D}(y_2\xi - y_2') = 1, \qquad D = D(y) = \begin{vmatrix} y_1 & y_2 \\ y_1' & y_2' \end{vmatrix}. \tag{42}$$

They are also prime modules, since their residue group has order 1.

But besides y_1 and y_2, $\mathfrak{M}$ also has all integrals

$$z_1 = \alpha_{11}y_1 + \alpha_{12}y_2, \qquad z_2 = \alpha_{21}y_1 + \alpha_{22}y_2, \qquad A = |\alpha_{ik}| \neq 0,$$

and hence is identical with the least common multiple of the two relatively prime modules $\mathfrak{N}_1$ and $\mathfrak{N}_2$, which have respectively the integrals z_1 and z_2, with basis polynomials

$$N_i = z_i\xi - z_i' = (\alpha_{i1}y_1 + \alpha_{i2}y_2)\xi - (\alpha_{i1}y_1' + \alpha_{i2}y_2').$$

Thus $\mathfrak{M}$ admits infinitely many distinct representations as the least common multiple of relatively prime prime modules; by Theorem VII the two modules $\mathfrak{N}_1$ and $\mathfrak{N}_2$ are therefore of the same kind as one another and as all $\mathfrak{M}_1$ and $\mathfrak{M}_2$. Indeed, the residue groups of all these modules have order 1, and so are isomorphic.

We shall now write the additive decomposition of the residue group $\mathfrak{G} = \mathfrak{A}_1 + \mathfrak{A}_2$ corresponding to the representation (41). To do this we start, as in § 4, from relation (42), which expresses the relative primeness of $\mathfrak{M}_1$ and $\mathfrak{M}_2$. For the units a_1 and a_2 we obtain the residue classes generated by the polynomials

$$-\frac{y_1}{D}(y_2\xi - y_2') \quad \text{and} \quad \frac{y_2}{D}(y_1\xi - y_1').$$

Thus

$$\mathfrak{M}_1 = \left(\mathfrak{M}, \frac{y_2}{D}(y_1\xi - y_1')\right), \qquad \mathfrak{M}_2 = \left(\mathfrak{M}, -\frac{y_1}{D}(y_2\xi - y_2')\right).$$

If we now form in the same way the units b_1 and b_2 corresponding to the decomposition $\mathfrak{M} = [\mathfrak{N}_1, \mathfrak{N}_2]$, replacing y_i by z_i, we get

$$-\frac{z_1}{D(z)}(z_2\xi - z_2') = -\frac{\alpha_{11}y_1 + \alpha_{12}y_2}{AD(y)}((\alpha_{21}y_1 + \alpha_{22}y_2)\xi - (\alpha_{21}y_1' + \alpha_{22}y_2')),$$

$$\frac{z_2}{D(z)}(z_1\xi - z_1') = \frac{\alpha_{21}y_1 + \alpha_{22}y_2}{AD(y)}((\alpha_{11}y_1 + \alpha_{12}y_2)\xi - (\alpha_{11}y_1' + \alpha_{12}y_2')),$$

and therefore

$$\begin{cases} b_1 = \dfrac{\alpha_{11}y_1 + \alpha_{12}y_2}{y_1}\left(\dfrac{\alpha_{22}}{A}\right)a_1 + \dfrac{\alpha_{11}y_1 + \alpha_{12}y_2}{y_2}\left(-\dfrac{\alpha_{21}}{A}\right)a_2 = \dfrac{z_1}{y_1}\alpha^{11}a_1 + \dfrac{z_1}{y_2}\alpha^{12}a_2, \\ b_2 = \dfrac{\alpha_{21}y_1 + \alpha_{22}y_2}{y_1}\left(-\dfrac{\alpha_{12}}{A}\right)a_1 + \dfrac{\alpha_{21}y_1 + \alpha_{22}y_2}{y_2}\left(\dfrac{\alpha_{11}}{A}\right)a_2 = \dfrac{z_2}{y_1}\alpha^{21}a_1 + \dfrac{z_2}{y_2}\alpha^{22}a_2. \end{cases} \tag{43}$$

Here (α^{ik}) is the inverse matrix of (α_{ik}).

Conversely, exchanging z_i with y_i gives

$$\begin{cases} a_1 = \dfrac{y_1}{z_1}\alpha_{11}b_1 + \dfrac{y_1}{z_2}\alpha_{12}b_2, \\ a_2 = \dfrac{y_2}{z_1}\alpha_{21}b_1 + \dfrac{y_2}{z_2}\alpha_{22}b_2. \end{cases} \tag{44}$$

These formulas display the isomorphism of the groups $\mathfrak{A}$ and $\mathfrak{B}$. Namely, by our general considerations, if $a_1 b_\sigma \neq 0$ the corresponding assignment is $a_1 \sim a_1 b_\sigma$, and hence by (44)

$$a_1 \sim \frac{y_1}{z_\sigma}\alpha_{1\sigma}b_\sigma, \qquad \text{provided } \alpha_{1\sigma} \neq 0,$$

and by (43) likewise

$$b_\sigma \sim \frac{z_\sigma}{y_2}\alpha^{\sigma 2}a_2, \qquad \text{provided } \alpha^{\sigma 2} \neq 0,$$

so that

$$\frac{y_1}{z_\sigma}\alpha_{1\sigma}b_\sigma \sim \frac{y_1}{z_\sigma}\alpha_{1\sigma}\frac{z_\sigma}{y_2}\alpha^{\sigma 2}a_2 = \frac{y_1}{y_2}\alpha_{1\sigma}\alpha^{\sigma 2}a_2.$$

Hence

$$a_1 \sim \alpha_{1\sigma}\alpha^{\sigma 2}\frac{y_1}{y_2}a_2 \quad \text{for } \alpha_{1\sigma}\alpha^{\sigma 2} \neq 0, \qquad \frac{1}{\alpha_{1\sigma}\alpha^{\sigma 2}}\frac{y_2}{y_1}a_1 \sim a_2,$$

which gives the inverse. If (α_{ik}) is not a diagonal matrix, this condition $\alpha_{1\sigma}\alpha^{\sigma 2} \neq 0$ is always fulfilled for some σ. The case of a diagonal matrix must be excluded, since then the modules are identical. If, for example, only $\alpha_{12} = 0$, then $\mathfrak{A}_1 = \mathfrak{B}_1$, but not $\mathfrak{A}_2 = \mathfrak{B}_2$. Thus from $\mathfrak{A}_1 + \mathfrak{A}_2 = \mathfrak{B}_1 + \mathfrak{B}_2$ and $\mathfrak{A}_1 = \mathfrak{B}_1$ it does not follow that $\mathfrak{A}_2 = \mathfrak{B}_2$ (cf. note 12). The three modules $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{N}_2$ are then pairwise relatively prime, but do not form a totally relatively prime system, since $[\mathfrak{M}_1, \mathfrak{M}_2]$ is divisible by $\mathfrak{N}_2$ (cf. note 15).

Putting further

$$t_{12} = \alpha_{1\sigma}\alpha^{\sigma 2}\frac{y_1}{y_2}a_2, \qquad t_{21} = \frac{1}{\alpha_{1\sigma}\alpha^{\sigma 2}}\frac{y_2}{y_1}a_1,$$

one verifies by direct calculation that the relations (35) are fulfilled.

2. Every module in more than one variable whose basis consists of a single polynomial gives an example of an infinite group. The following somewhat more complicated example is meant to show that infinite

groups can also occur for multi-membered modules, that is, for modules whose basis contains more than one polynomial.[26]

$$\mathfrak{M} = [(\xi + x\eta), (\xi + 1)] = [(P), (Q)] \qquad \left(\xi = \frac{\partial}{\partial x},\ \eta = \frac{\partial}{\partial y}\right).$$

The multiplication rule is that for differential expressions. The residue group is here infinite because the residue groups of $(\xi + x\eta)$ and $(\xi + 1)$ are both infinite, whereas the modules $(\xi + x\eta)$ and $(\xi + 1)$ are relatively prime, since

$$1 = (-x\xi - x^2\eta + 1)Q + (x\xi + x - 1)P.$$

It is now very easy to show that $\mathfrak{M}$ possesses no polynomial of the second degree: one sets

$$(u_1\xi + u_2\eta + u_3)(\xi + x\eta) = (v_1\xi + v_2\eta + v_3)(\xi + 1),$$

which gives $u_1 = u_2 = u_3 = v_1 = v_2 = v_3 = 0$. If one next looks for polynomials of the third degree in $\mathfrak{M}$, one finds two linearly independent ones, for example

$$(\xi^2 + x\xi\eta + \xi + (2 + x)\eta)Q = (\xi^2 + 2\xi + 1)P$$

and

$$(\xi^2 + 2x\xi\eta + x^2\eta^2 + \eta)Q = (\xi^2 + x\xi\eta + \xi + (x - 1)\eta)P.$$

If $\mathfrak{M}$ were a one-membered module, then both would have to be divisible by the basis polynomial, and, since $\mathfrak{M}$ contains no polynomial of the second degree, by a polynomial of the third degree; they would therefore have to be proportional, which they are not. The multi-memberedness of $\mathfrak{M}$ is the internal reason for the failure of Landau's product theorems, which are valid in the case of one variable.

3. A further example shows that infinite groups can also occur for prime modules.[27] Let P be the domain of all rational functions of two variables x, y. The module $\mathfrak{M}$ with basis

$$\xi - \frac{y}{x}\eta = \xi - a$$

has an infinite group, since this group contains the residue class of every power of y; on the other hand, $\mathfrak{M}$ is a prime module. Indeed, we show that every divisor

$$\mathfrak{M}_1 = (\xi - a, F(\xi, \eta))$$

is equal to the unit module. Every polynomial $F(\xi, \eta)$ can be represented modulo $(\xi - a)$ by a polynomial $G(\eta)$:

$$F(\xi, \eta) \equiv c_0\eta^\nu + c_1\eta^{\nu-1} + \cdots + c_\nu \quad (\mathfrak{M}).$$

Without loss of generality let $c_0 = 1$. By the multiplication law, $\xi\eta^\nu - \eta^\nu\xi = 0$; hence, since

$$\xi \equiv a(\mathfrak{M}_1), \qquad \eta^\nu \equiv F_1(\mathfrak{M}_1),$$

where $F_1 = -(c_1\eta^{\nu-1} + \cdots + c_\nu)$, one has

$$\xi F_1 - \eta^\nu a \equiv 0(\mathfrak{M}_1).$$

Expanding

$$\eta^\nu a = a\eta^\nu + \nu\frac{\partial a}{\partial y}\eta^{\nu-1} + \cdots,$$

and again replacing η^ν by F_1, one obtains

$$\xi(c_1\eta^{\nu-1} + \cdots + c_\nu) - a(c_1\eta^{\nu-1} + \cdots + c_\nu) + \nu\frac{\partial a}{\partial y}\eta^{\nu-1} + \cdots \equiv 0(\mathfrak{M}_1),$$

or

$$c_1\eta^{\nu-1}a + \frac{\partial c_1}{\partial x}\eta^{\nu-1} + \cdots - ac_1\eta^{\nu-1} + \cdots + u\frac{\partial a}{\partial y}\eta^{\nu-1} + \cdots \equiv 0(\mathfrak{M}_1),$$

26) Cf. the example of Landau communicated by Blumberg (loc. cit., pp. 51–52). Here and below we denote the independent variables by x and y.

27) Our definition of "prime module" differs from what is called a prime module in the commutative case, since there divisors of lower dimension always exist, except when the dimension is 0, that is, when the residue group is finite.

or finally

$$\left(\frac{\partial c_1}{\partial x} + \nu\frac{\partial a}{\partial y}\right)\eta^{\nu-1} + \cdots \equiv 0(\mathfrak{M}_1).$$

On the left now stands a polynomial in η of exact degree $\nu - 1$ which does not vanish identically, for the highest coefficient

$$\frac{\partial c_1}{\partial x} + \nu\frac{\partial a}{\partial y} = \frac{\partial c_1}{\partial x} + \nu\frac{1}{x} \quad \text{is } \neq 0,$$

since otherwise $c_1 = -\nu \log x + \varphi(y)$ would not be rational. Thus the procedure can be continued and leads to a non-identically-vanishing polynomial of degree zero, proving that the unit is also contained in $\mathfrak{M}_1$.[28]

4. On the other hand, if one adjoins the function $\log x$ to the rationality domain, then $\mathfrak{M}$ has the divisors

$$\left(\xi - \frac{y}{x},\ \eta - \log x + \varphi(y)\right),$$

where $\varphi(y)$ runs through all rational functions of y. These divisors are all distinct, the integrability condition is fulfilled for each, and the corresponding integral is

$$y \log x - \int \varphi(y)\, dy + c.$$

Therefore the unit cannot be contained in the module, since otherwise the zero function would be the only possible integral. On the other hand, ξ and η are congruent, with respect to the module, to a quantity of the domain; hence the residue group is finite and of order 1. Further, any two of the infinitely many divisors are relatively prime, and the given module $\mathfrak{M}$ is equal to the least common multiple $\mathfrak{N}$ of all these divisors. Indeed, it is divisible by all divisors, hence also by $\mathfrak{N}$. If $\mathfrak{N}$ were a proper divisor of $\mathfrak{M}$, then $\mathfrak{N}$ would still have to contain at least one polynomial F, say of degree ρ, depending only on η alone. Letting $\varphi(y)$ run through the functions $y, \ldots, y^{\rho+1}$, there is no linear relation with coefficients independent of y between the corresponding integrals

$$y \log x - \frac{y^{i+1}}{i+1} + c_i \qquad (i = 1, \ldots, \rho + 1).$$

But the differential equation of order ρ, $F = 0$, cannot possess $\rho + 1$ linearly independent integrals.

The module $\mathfrak{M} = \mathfrak{N}$ is, however, not completely reducible.[29] For otherwise it would be the least common multiple of finitely many of these prime modules, and its residue group would therefore be of finite order; yet the residue group of $\xi - y/x$ contains the residue classes of all powers of η, and so is infinite.

Göttingen, August 1, 1919.

(Received August 4, 1919.)

28) This procedure amounts to proving that the integrability conditions necessary for a system of differential equations are not fulfilled.

29) Thus we have an example of the first case of Theorem X.

11th Session, Friday, September 23, 1921, at 11 a.m.
(Chair: Loewy.)

1. E. Noether: On a Work in Elimination Theory by K. Hentzelt, Who Fell in the War.

Kurt Hentzelt has been missing near Dixmude since October 1914 and must be counted among the dead. I intend shortly to publish in the *Mathematische Annalen*, in a free reworking, the most essential parts of his Erlangen dissertation, which he left behind fully developed but presented in an almost incomprehensible form.

The subject is the *general problem of elimination theory*: to determine the common zeroes of all polynomials in an ideal $\mathfrak{M}$ of polynomials. If the variables are first subjected to a linear transformation with indeterminate coefficients, the principal result can be stated as follows:

A resultant form can be uniquely assigned to the ideal $\mathfrak{M}$:

$$R_{\mathfrak{M}} = R^{(1)}(x_1 \dots x_n) \cdots R^{(i)}(x_i \dots x_n) \cdots R^{(n)}(x_n) \equiv 0(\mathfrak{M}),$$

in such a way that $R_{\mathfrak{M}}$ vanishes at all the zeroes of $\mathfrak{M}$, and only at those zeroes. If $\mathfrak{N}$ is a divisor of $\mathfrak{M}$, and $R_{\mathfrak{N}}$ and $R_{\mathfrak{M}}$ agree, then $\mathfrak{N}$ and $\mathfrak{M}$ themselves also agree.

The second part of the theorem shows that the resultant form gives the zeroes with their characteristic multiplicities. It rests on the fact that $\mathfrak{M}$ can be regarded as a module of linear forms in the power products of $x_1, \dots, x_{i-1}$; the individual factors $R^{(i)}(x_i \dots x_n)$ of $R_{\mathfrak{M}}$ then become the norms of the respective "base module" with respect to this module, after $x_{i+1}, \dots, x_n$ have been adjoined to the coefficient domain. Invoking abstract ideal theory gives the following interpretation. If $\mathfrak{M} = [\mathfrak{Q}, \mathfrak{Q}_1, \dots, \mathfrak{Q}_r] = [\mathfrak{Q}, \mathfrak{L}]$ is a decomposition of $\mathfrak{M}$ into primary ideals $\mathfrak{Q}_i$, with $\mathfrak{L}$ the complement of $\mathfrak{Q}$, then the ideal $\mathfrak{Q}$ corresponds to a primary factor $Q^{(i)}(x_i \dots x_n)$ of $R^{(i)}(x_i \dots x_n)$ which, in the sense given above, represents the norm of $\mathfrak{L}$ with respect to $\mathfrak{Q}$.

Ideal Theory in Ring Domains.

By
Emmy Noether in Göttingen.

Table of Contents.

Introduction.
§ 1. **Ring Domain, Ideal, Finiteness Condition.**
§ 2. **Representation of an Ideal as the Least Common Multiple of Finitely Many Irreducible Ideals.**
§ 3. **Equality of the Number of Components in Two Different Decompositions into Irreducible Ideals.**
§ 4. **Primary Ideals. Uniqueness of the Associated Prime Ideals in Two Different Decompositions into Irreducible Ideals.**
§ 5. **Representation of an Ideal as the Least Common Multiple of Greatest Primary Ideals. Uniqueness of the Associated Prime Ideals.**
§ 6. **Unique Representation of an Ideal as the Least Common Multiple of Relatively Prime Irreducible Ideals.**
§ 7. **Uniqueness of the Isolated Ideals.**
§ 8. **Unique Representation of an Ideal as a Product of Coprime-Irreducible Ideals.**
§ 9. **Extension of the Investigation to Modules. Equality of the Number of Components in Decompositions into Irreducible Modules.**
§ 10. **Special Case of the Polynomial Domain.**
§ 11. **Examples from Number Theory and from the Theory of Differential Expressions.**
§ 12. **Example from Elementary-Divisor Theory.**

Introduction.

The content of the present paper is the *transfer of the decomposition theorems for the rational integers, respectively of the ideals in algebraic number fields, to ideals in arbitrary integral domains, and more generally ring domains.* To understand this transfer, let us first state the decomposition theorems for the rational integers in a form somewhat different from the usual formulation.

If in

$$a = p_1^{\varrho_1} p_2^{\varrho_2} \cdots p_\sigma^{\varrho_\sigma} = q_1 q_2 \cdots q_\sigma$$

one regards the prime-power factors q_i as the components of the decomposition, then these components have the following characteristic properties:

1. They are *pairwise coprime*; but no q_i can be represented as a product of pairwise coprime numbers, so that in this sense irreducibility holds. From the pairwise coprimeness it further follows that the product $q_1 \cdots q_\sigma$ is equal to the least common multiple $[q_1 \cdots q_\sigma]$.

2. Any two of the components, q_i and q_k, are *relatively prime*; that is, if bq_i is divisible by q_k, then b is divisible by q_k. In this sense too irreducibility holds.

3. Every q is *primary*; that is, if a product $b \cdot c$ is divisible by q, but b is not divisible, then a power[1] of c is divisible. The representation is moreover one by *greatest primary components*, since the product of two distinct q is no longer primary. Also with respect to decomposition into greatest primary components the q are irreducible.

4. Every q is *irreducible* in the sense that it cannot be represented as the least common multiple of two proper divisors.

The connection of these primary numbers q with the prime numbers p consists in this: to each q there exists one, and apart from sign only one, p which is a divisor of q and a power of which is divisible by q: the associated prime number. If p^ϱ is the lowest power of this kind – ϱ the exponent of q – then here, in particular, p^ϱ is equal to q. The uniqueness theorem may now be stated as follows:

[1] If this power is always the first, then one is, as is well known, dealing with prime numbers.

For two different decompositions of a rational integer into the irreducible, greatest primary components q, the number of components, the associated prime numbers (up to sign), and the exponents coincide. Since $p^\varrho = q$, it follows from this also that the q themselves coincide (up to sign).

The indeterminacy arising from the sign is, as is well known, removed when one considers, instead of the numbers, the ideals derived from them (all numbers divisible by a); then the formulation holds in exactly the same way for the unique decomposition of the ideals of finite algebraic number fields into powers of prime ideals.

In what follows (§ 1), the basis will be a general ring domain satisfying only the finiteness condition that each ideal of the domain possess a finite ideal basis. Without such a finiteness condition, irreducible and prime ideals need not exist at all, as is shown by the domain of all algebraic integers, in which there is no decomposition into prime ideals.

It turns out that – corresponding to the four characteristic properties of the components q – in general four separate decompositions exist, each arising from the preceding one by subdivision. The decomposition into coprime-irreducible ideals is a product representation; the other three decompositions are reduced (§ 2) representations as least common multiples. The connection between a primary ideal – the irreducible ideals too are primary – and the associated prime ideal also persists: to every primary ideal $\mathfrak{Q}$ there is uniquely determined an associated prime ideal $\mathfrak{P}$ which is a divisor of $\mathfrak{Q}$ and a power of which is divisible by $\mathfrak{Q}$. If $\mathfrak{P}^\varrho$ is the lowest such power – ϱ the exponent of $\mathfrak{Q}$ – then here $\mathfrak{P}^\varrho$ need not coincide with $\mathfrak{Q}$. The uniqueness theorem is expressed as follows:

Decompositions 1 and 2 are unique; in two different decompositions 3 or 4 the number of components and the associated prime ideals coincide[2]*; the isolated ideals occurring among the components (§ 7) are uniquely determined.*

For the proof of the decomposition theorems, the finiteness condition first yields the "theorem on the finite chain", first stated by Dedekind for finite number modules; from it the representation 4 of each ideal as the least common multiple of finitely many irreducible ideals is derived. By transforming the concept of reducibility of a component, one obtains from this the fundamental uniqueness theorem for decomposition 4 into irreducible ideals. By combining finitely many components at a time one rises to the remaining decompositions, whose uniqueness theorems then follow from the uniqueness theorem 4.

Finally it is shown (§ 9) that the representation by finitely many irreducible components still holds under weaker hypotheses; commutativity of the ring domain is not required, and it is enough to consider, in place of an ideal, a module with respect to the domain. In this more general case the equality of the number of components in two different decompositions still holds, whereas the notions prime and primary are tied to commutativity and to the ideal concept; by contrast, the notion coprime remains valid for ideals in noncommutative domains.

The simplest ring domain for which the four separate decompositions actually occur is the domain of all polynomials in n variables with arbitrary complex coefficients. Here the individual decompositions can be interpreted, irrationally, by the behavior of algebraic configurations, and the uniqueness theorem for the associated prime ideals corresponds to the fundamental theorem of elimination theory on the unique decomposability of algebraic configurations into irreducible ones. Further examples are given by all finite integral domains made of polynomials (§ 10). But even the simple domain of all even numbers, more generally of all numbers divisible by a fixed number, already gives an example of partially separated decompositions (§ 11). An example of ideal theory in noncommutative domains is provided by elementary-divisor theory (§ 12), where unique decomposition into irreducible ideals, respectively classes, holds. These irreducible classes completely characterize the irreducible constituents of the elementary divisors, and may perhaps be viewed as their equivalent for domains in which the usual elementary-divisor theory fails.

On the existing literature the following is to be said. The decomposition into greatest primary ideals for the polynomial domain with arbitrary complex, respectively integral, coefficients was given by Lasker, and in individual points further developed by Macaulay.[3] Both rely on elimination theory, and hence use the fact that a polynomial can be represented uniquely as a product of irreducible polynomials. In fact the decomposition theorems for ideals are independent of this prerequisite, as ideal theory in algebraic number fields suggests and as the present paper shows. The primary ideal is also defined by Lasker and Macaulay on the basis of concepts from elimination theory.

The decomposition into irreducible ideals and the decomposition into relatively-prime irreducible ideals

[2] Presumably, beyond this, the exponents also coincide, and still more generally corresponding components are isomorphic.

[3] E. Lasker, Zur Theorie der Moduln und Ideale. Math. Ann. 60 (1905), p. 20, Theorems VII and XIII. – F. S. Macaulay, On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers. Math. Ann. 74 (1913), p. 66.

do not seem to have been noticed in the literature even for the polynomial domain; only in Macaulay is there a remark on the uniqueness of isolated primary ideals.

The decomposition into coprime-irreducible ideals was given for the polynomial domain by Schmeidler,[4] using elimination theory for the proof of finiteness. There, however, the uniqueness theorem is stated only for classes of ideals, not for the ideals themselves. This latter uniqueness theorem appears in a joint paper,[5] where ideals in noncommutative polynomial domains are involved. Only the finite ideal basis is used there; hence theorems and methods remain valid for general ring domains, and are sharpened in the present paper with respect to equality of number (§ 11). The present investigations are a strong generalization and further development of the conceptual formations underlying those two papers. The essential feature of the two papers is the passage from representation as a least common multiple to an additive decomposition of the system of residue classes. Here, for simplicity of presentation, we remain with the least common multiple; the additive decomposition is then matched by the transformation of the notion of reducibility into a property of the complement (§ 3). Yet by considerations essentially corresponding to those of the joint paper, all the theorems stated here can also be understood as additive decomposition theorems for the system of residue classes and certain partial systems. This system of residue classes forms a ring of the same generality as the ring originally taken as basis; indeed every ring may be regarded as the system of residue classes of the ideal corresponding to the totality of identical relations among the ring elements; or also of a partial system of these relations, if the remaining relations are assumed to be satisfied already in the domain.

This remark also gives the place of Fraenkel's papers.[6] Fraenkel considers additive decompositions of rings that are subjected to such restrictive conditions (existence of regular elements, division by these, decomposability condition) that, for the corresponding ideal, the four decompositions coincide. Because of this coincidence, his finiteness condition, that the ideal should have only finitely many proper divisors – from which he in part departs – also means no stronger restriction than ours. Fraenkel's starting point is conditioned by the different, essentially algebraic, aims of his papers; by algebraic extension he then arrives at more general rings with less restrictive conditions.

§ 1.
Ring Domain, Ideal, Finiteness Condition.

1. The domain Σ taken as basis is to be a (commutative) ring in the abstract definition;[7] that is, Σ consists of a system of elements $a, b, c, \ldots, f, g, h, \ldots$ in which a relation satisfying the usual conditions is defined as equality; and in which by two operations (modes of composition), addition and multiplication, from any two ring elements a and b a third is always uniquely obtained, respectively as sum $a + b$ and as product $a \cdot b$. The ring and the otherwise wholly arbitrary operations must satisfy the following laws:

1. The associative law of addition: $(a + b) + c = a + (b + c)$.
2. The commutative law of addition: $a + b = b + a$.
3. The associative law of multiplication: $(a \cdot b)c = a(b \cdot c)$.
4. The commutative law of multiplication: $a \cdot b = b \cdot a$.
5. The distributive law: $a(b + c) = ab + ac$.
6. The law of unrestricted and unique subtraction. There is in Σ a single element x satisfying the equation $a + x = b$. (One denotes $x = b - a$.)

From these properties follows the existence of zero; but a ring need not possess a unit; and the product of two elements can vanish without one of the factors vanishing. Rings for which, from the vanishing of a product, the vanishing of a factor always follows, and which in addition possess a unit, will be called proper integral domains. For the finite sum $a+a+\cdots+a$ we introduce the usual abbreviated notation na, where the

[4] W. Schmeidler, Über Moduln und Gruppen hyperkomplexer GröSSen. Math. Zeitschr. 3 (1919), p. 29.

[5] E. Noether–W. Schmeidler, Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzenausdrücken. Math. Zeitschr. 8 (1920), p. 1.

[6] A. Fraenkel, Über die Teiler der Null und die Zerlegung von Ringen. J. f. M. 145 (1914), p. 139. Über gewisse Teilbereiche und Erweiterungen von Ringen. Habilitationsschrift, Leipzig, Teubner, 1916. Über einfache Erweiterungen zerlegbarer Ringe. J. f. M. 151 (1920), p. 121.

[7] The definition is taken from Fraenkel's habilitation thesis, omitting his restrictive conditions 6, I and II; for this the commutative law of addition had to be included. Thus these are the laws defining a field with the invertibility of multiplication omitted.

integers n are to be regarded merely as abbreviating signs, not as ring elements, and are defined recursively by $a = 1a$, $na + a = (n+1)a$.

2. By an ideal $\mathfrak{M}$[8] in Σ is meant a system of elements from Σ satisfying the two conditions:

1. $\mathfrak{M}$ contains, together with f, also $a \cdot f$, where a is an arbitrary element of Σ.

2. $\mathfrak{M}$ contains, together with f and g, also the difference $f - g$; hence with f also nf for every integer n.

If f is an element of $\mathfrak{M}$, we express this as usual by $f \equiv 0(\mathfrak{M})$ and say that f is divisible by $\mathfrak{M}$. If every element of $\mathfrak{N}$ is at the same time an element of $\mathfrak{M}$, and hence divisible by $\mathfrak{M}$, we say: $\mathfrak{N}$ is divisible by $\mathfrak{M}$; in symbols, $\mathfrak{N} \equiv 0(\mathfrak{M})$. $\mathfrak{M}$ is called a proper divisor of $\mathfrak{N}$ when it contains elements different from those of $\mathfrak{N}$, and hence is not conversely divisible by $\mathfrak{N}$. From $\mathfrak{N} \equiv 0(\mathfrak{M})$ and $\mathfrak{M} \equiv 0(\mathfrak{N})$ follows $\mathfrak{N} = \mathfrak{M}$.

The other familiar notions are also retained word for word. By the greatest common divisor of two ideals $\mathfrak{A}$ and $\mathfrak{B}$ – $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$ – we mean the totality of elements that can be represented in the form $a + b$, where a runs through all elements of $\mathfrak{A}$ and b through all elements of $\mathfrak{B}$; $\mathfrak{D}$ is again an ideal. Likewise, the greatest common divisor of infinitely many ideals – $\mathfrak{D} = (\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\nu, \ldots)$ – is defined as the totality of elements d representable as sums of elements from finitely many of the ideals at a time: $d = a_{i_1} + a_{i_2} + \cdots + a_{i_n}$; here too $\mathfrak{D}$ is again an ideal.

If, in particular, the ideal $\mathfrak{M}$ contains a finite number of elements $f_1, f_2, \ldots, f_\varrho$ such that

$$\mathfrak{M} = (f_1 \ldots f_\varrho), \qquad f = a_1 f_1 + \cdots + a_\varrho f_\varrho + n_1 f_1 + \cdots + n_\varrho f_\varrho$$

for every $f \equiv 0(\mathfrak{M})$, where the a_i are quantities of the ring domain and the n_i are integers, then $\mathfrak{M}$ is called a finite ideal; $f_1, \ldots, f_\varrho$ an ideal basis.

In what follows we take as basis only rings Σ satisfying the finiteness condition: *Every ideal in Σ is finite, hence possesses an ideal basis.*

3. From the finiteness condition there follows directly the result on which all subsequent considerations rest.

Theorem I (theorem on the finite chain).[9] *Let $\mathfrak{M}, \mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_\nu, \ldots$ be a countably infinite system of ideals in Σ, each of which is divisible by the following one. Then from some finite index n onward all ideals are identical, $\mathfrak{M}_n = \mathfrak{M}_{n+1} = \cdots$. In other words: if $\mathfrak{M}, \mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_s, \ldots$ form a simply ordered chain of ideals such that every ideal is a proper divisor of the one immediately preceding it, then the chain breaks off after finitely many steps.*

Indeed, let $\mathfrak{D} = (\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_\nu, \ldots)$ be the greatest common divisor of the system, and let $f_1, \ldots, f_k$ be a basis of $\mathfrak{D}$, which always exists by the finiteness condition. From the divisibility assumption it follows that every element of $\mathfrak{D}$ is at the same time an element of one ideal of the chain; for from

$$f = g + h, \qquad g \equiv 0(\mathfrak{M}_r), \qquad h \equiv 0(\mathfrak{M}_s), \qquad (r \leq s)$$

one gets $g \equiv 0(\mathfrak{M}_s)$ and hence $f \equiv 0(\mathfrak{M}_s)$. The same holds when f is a sum of several constituents. Hence there is a finite index n such that

$$f_1 \equiv 0(\mathfrak{M}_n); \quad \ldots; \quad f_k \equiv 0(\mathfrak{M}_n); \quad \mathfrak{D} = (f_1 \ldots f_k) \equiv 0(\mathfrak{M}_n).$$

Since conversely $\mathfrak{M}_n \equiv 0(\mathfrak{D})$, we have $\mathfrak{M}_n = \mathfrak{D}$; and since further $\mathfrak{M}_n \equiv 0(\mathfrak{D})$ and $\mathfrak{D} = \mathfrak{M}_n \equiv 0(\mathfrak{M}_r)$, we also have $\mathfrak{M}_r = \mathfrak{D} = \mathfrak{M}_n$ for every $r > n$, proving the theorem.

We note that conversely the existence of an ideal basis again follows from this theorem, so that the finiteness condition could also have been stated in this basis-free form.

§ 2.

Representation of an Ideal as the Least Common Multiple of Finitely Many Irreducible Ideals.

The least common multiple $[\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_k]$ of the ideals $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_k$ is defined as usual as the totality of the elements divisible by $\mathfrak{B}_1$, by $\mathfrak{B}_2$, ..., and by $\mathfrak{B}_k$; in symbols,

$$\text{from } f \equiv 0(\mathfrak{B}_i), \quad (i = 1, 2, \ldots, k), \quad \text{follows} \quad f \equiv 0([\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_k]),$$

[8] Ideals are denoted by capital German letters. $\mathfrak{M}$ is meant to recall the example of the ideal in polynomials usually called a "module" or form module. Incidentally, §§ 1–3 use only the module property and not the ideal property; compare § 9.

[9] First stated for number modules by Dedekind: Zahlentheorie, Suppl. XI, § 172, Theorem VIII (4th ed.); our proof and the designation "chain" are taken from there. For ideals in polynomials, see Lasker, loc. cit., p. 56 (lemma). But in both cases the theorem finds only isolated application. Our applications rest throughout on the principle of choice.

and conversely. The least common multiple is again an ideal; the ideals $\mathfrak{B}_i$ are also called the components of the decomposition.

Definition I. *A representation $\mathfrak{M} = [\mathfrak{B}_1 \cdots \mathfrak{B}_k]$ is called a reduced representation if no $\mathfrak{B}_i$ is absorbed into the least common multiple $\mathfrak{A}_i$ of the remaining ideals, and if no $\mathfrak{B}_i$ can be replaced by a proper divisor.*[10] *If the conditions are satisfied only for the ideal $\mathfrak{B}_i$, the representation is called reduced with respect to $\mathfrak{B}_i$. The least common multiple $\mathfrak{A}_i = [\mathfrak{B}_1, \ldots, \mathfrak{B}_{i-1}, \mathfrak{B}_{i+1}, \ldots, \mathfrak{B}_k]$ is called the complement of $\mathfrak{B}_i$. Representations in which only the first condition is satisfied are called shortest representations.*

For representing an ideal as a least common multiple it therefore suffices to restrict to reduced representations, by the following result.

Lemma I. *Every representation of an ideal as the least common multiple of finitely many ideals can be replaced, in at least one way, by a reduced representation; such a representation can in particular be attained by successive decomposition.*

Indeed, let $\mathfrak{M} = [\mathfrak{B}_1^* \cdots \mathfrak{B}_l^*]$ be an arbitrary representation of $\mathfrak{M}$. We omit, in order, those $\mathfrak{B}_i^*$ which are absorbed into the least common multiple of the ideals retained. Since the remaining ideals still yield $\mathfrak{M}$, in the resulting representation

$$\mathfrak{M} = [\mathfrak{B}_1 \cdots \mathfrak{B}_k] = [\mathfrak{A}_i, \mathfrak{B}_i]$$

the first condition is satisfied, hence it is a shortest representation; and this condition remains satisfied if any $\mathfrak{B}_i$ is replaced by a proper divisor. The second condition, however, is always attainable by the theorem on the finite chain (Theorem I). For if

$$\mathfrak{B}_i \supset \mathfrak{B}_i' \supset \mathfrak{B}_i'' \supset \cdots \supset \mathfrak{B}_i^{(\nu)} \supset \cdots, \qquad \mathfrak{M} = [\mathfrak{A}_i, \mathfrak{B}_i] = [\mathfrak{A}_i, \mathfrak{B}_i'] = \cdots = [\mathfrak{A}_i, \mathfrak{B}_i^{(\nu)}] = \cdots,$$

where every $\mathfrak{B}_i^{(\nu)}$ is a proper divisor of the one immediately preceding, then by that theorem the chain $\mathfrak{B}_i, \mathfrak{B}_i', \ldots, \mathfrak{B}_i^{(\nu)}, \ldots$ must terminate after finitely many steps; hence in the representation $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{B}_i^{(\nu)}]$ the ideal $\mathfrak{B}_i^{(\nu)}$ can no longer be replaced by a proper divisor; and this holds a fortiori if $\mathfrak{A}_i$ is replaced by a proper divisor. Applying the procedure successively to each $\mathfrak{B}_i$, always forming the complement with the already reduced $\mathfrak{B}$, gives a reduced representation.[11]

In order to obtain such a representation successively, it remains to show that from the individual reduced representations

$$\mathfrak{M} = [\mathfrak{B}_1, \mathfrak{C}_1], \qquad \mathfrak{C}_1 = [\mathfrak{B}_2, \mathfrak{C}_2], \quad \ldots, \quad \mathfrak{C}_{k-1} = [\mathfrak{B}_k, \mathfrak{C}_k]$$

it follows that the resulting representation $\mathfrak{M} = [\mathfrak{B}_1 \cdots \mathfrak{B}_k, \mathfrak{C}_k]$ is reduced. For this it suffices to show that from reduced representations

$$\mathfrak{M} = [\mathfrak{B}, \mathfrak{C}], \qquad \mathfrak{C} = [\mathfrak{C}_1, \mathfrak{C}_2]$$

one obtains a reduced representation $\mathfrak{M} = [\mathfrak{B}, \mathfrak{C}_1, \mathfrak{C}_2]$. In fact, by hypothesis no $\mathfrak{B}$ lies in its complement; if this happened for a $\mathfrak{C}_i$, then, contrary to the hypothesis in the first representation, $\mathfrak{C}$ would be replaceable by a proper divisor, since by the second reduced representation $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are proper divisors of $\mathfrak{C}$; so the representation is shortest. Moreover, by hypothesis no $\mathfrak{B}$ can be replaced by a proper divisor; if this were possible for a $\mathfrak{C}_i$, it would, contrary to the hypothesis, correspond to replacing $\mathfrak{C}$ by a proper divisor, since the representation for $\mathfrak{C}$ is reduced. Thus the lemma is proved.

Definition II. An ideal $\mathfrak{M}$ is called reducible if it can be represented as the least common multiple of two proper divisors; in the contrary case $\mathfrak{M}$ is called irreducible.

We now prove, by means of Theorem I on the finite chain and using reduced representations:

Theorem II. *Every ideal is representable as the least common multiple of finitely many irreducible ideals.*[12]

For an arbitrary ideal $\mathfrak{M}$ is either irreducible; then $\mathfrak{M} = [\mathfrak{M}]$ is a representation of the kind required by Theorem II; or else $\mathfrak{M} = [\mathfrak{B}_1, \mathfrak{C}_1]$, where $\mathfrak{B}_1$ and $\mathfrak{C}_1$ are proper divisors of $\mathfrak{M}$, and the representation may, by Lemma I, be assumed reduced. For $\mathfrak{C}_1$ the same alternative holds: either it is irreducible, or there is a reduced representation $\mathfrak{C}_1 = [\mathfrak{B}_2, \mathfrak{C}_2]$.

[10] An example of a non-reduced representation is $(x^2, xy) = [(x), (x^2, xy, y^\lambda)]$ for every exponent $\lambda \geq 2$; the representation $[(x), (x^2, y)]$ corresponding to $\lambda = 1$ is an associated reduced one. (This representation was given to me by K. Hentzelt, who was killed in the war, as the simplest example of a nonunique decomposition into primary ideals.)

[11] That such a representation is not uniquely defined by the given representation is shown by the previous example. For $(x^2, xy) = [(x), (x^2, xy, y^\lambda)]$, $\lambda \geq 2$, besides $[(x), (x^2, y)]$ also $[(x), (x^2, ux + y)]$, for arbitrary u, is a reduced representation.

[12] That such a representation is not unique in general is shown by the previous example: $(x^2, xy) = [(x), (x^2, ux + y)]$ for arbitrary u. The two components are irreducible for arbitrary u. Indeed, all divisors of (x) are of the form $(x, g(y))$, where $g(y)$ denotes a polynomial in y; the least common multiple of any two therefore also has this form, hence is a proper divisor of (x). The ideal $(x^2, ux + y)$ possesses only the single divisor (x, y), and therefore is necessarily irreducible as well.

Continuing in this way, one obtains the series of reduced representations

$$\mathfrak{M} = [\mathfrak{B}_1, \mathfrak{C}_1] = [\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{C}_2] = \cdots = [\mathfrak{B}_1, \ldots, \mathfrak{B}_n, \mathfrak{C}_n] = \cdots . \tag{1}$$

In the chain $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_n, \ldots$ each $\mathfrak{C}_n$ is a proper divisor of the one immediately preceding, and therefore the chain terminates after finitely many steps; there is an index n such that $\mathfrak{C}_n$ is irreducible. By Lemma I, moreover, the representation $\mathfrak{M} = [\mathfrak{A}_n, \mathfrak{C}_n]$ is reduced; $\mathfrak{C}_n$ therefore cannot lie in its complement $\mathfrak{A}_n$, and in the representation $\mathfrak{M} = [\mathfrak{A}_n, \mathfrak{C}_n]$ the ideal $\mathfrak{A}_n$ cannot be replaced by a proper divisor. Replacing, if necessary, $\mathfrak{A}_n$ by a proper divisor,[13] so that the representation becomes reduced, shows that every reducible ideal admits a reduced representation as the least common multiple of an irreducible ideal and a complementary ideal. In the series (1), therefore, all $\mathfrak{B}_i$ may be assumed irreducible without loss of generality; repeating the preceding argument gives the existence of an irreducible $\mathfrak{C}_n$, proving Theorem II.

§ 3.
Equality of the Number of Components in Two Different Decompositions into Irreducible Ideals.

To prove equality of number, the reducibility or irreducibility of an ideal must first be expressed in terms of properties of its complement, as follows.

Theorem III.[14] *Let the shortest representation $\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}]$ be reduced with respect to $\mathfrak{C}$. Then the necessary and sufficient condition for $\mathfrak{C}$ to be reducible is the existence of two ideals $\mathfrak{N}_1$ and $\mathfrak{N}_2$ that are proper divisors of $\mathfrak{M}$, such that*

$$\mathfrak{N}_1 \equiv 0(\mathfrak{A}); \qquad \mathfrak{N}_2 \equiv 0(\mathfrak{A}); \qquad [\mathfrak{N}_1, \mathfrak{N}_2] = \mathfrak{M}. \tag{2}$$

It follows further: if conditions (2) are satisfied and $\mathfrak{C}$ is irreducible, then at least one $\mathfrak{N}_i$ is not a proper divisor of $\mathfrak{M}$; $\mathfrak{N}_i = \mathfrak{M}$.

Let $\mathfrak{C} = [\mathfrak{C}_1, \mathfrak{C}_2]$, where $\mathfrak{C}_1, \mathfrak{C}_2$ are proper divisors of $\mathfrak{C}$. Then

$$\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}] = [\mathfrak{A}, \mathfrak{C}_1, \mathfrak{C}_2] = [[\mathfrak{A}, \mathfrak{C}_1], [\mathfrak{A}, \mathfrak{C}_2]].$$

Here the ideals $[\mathfrak{A}, \mathfrak{C}_i]$ are proper divisors of $\mathfrak{M}$, since otherwise $[\mathfrak{A}, \mathfrak{C}]$ would not be reduced with respect to $\mathfrak{C}$. Since divisibility by $\mathfrak{A}$ is also satisfied, condition (2) has been proved necessary. (The representation (2) is not reduced, since one $[\mathfrak{A}, \mathfrak{C}_i]$ can be replaced by $\mathfrak{C}_i$.)

Conversely, suppose (2) is satisfied. We form the ideals

$$\mathfrak{C}_1 = (\mathfrak{C}, \mathfrak{N}_1), \qquad \mathfrak{C}_2 = (\mathfrak{C}, \mathfrak{N}_2), \qquad \mathfrak{C}^* = [\mathfrak{C}_1, \mathfrak{C}_2].$$

Then $\mathfrak{C}$ is divisible both by $\mathfrak{C}_1$ and by $\mathfrak{C}_2$, and hence also by their least common multiple $\mathfrak{C}^*$. To show that $\mathfrak{C}^*$ is divisible by $\mathfrak{C}$, let

$$f \equiv 0(\mathfrak{C}^*); \quad f \equiv 0(\mathfrak{C}_1); \quad f \equiv 0(\mathfrak{C}_2), \quad \text{or equivalently} \quad f = c + n_1 = \bar{c} + n_2,$$

where $c, \bar{c}$ are elements of $\mathfrak{C}$ and n_1, n_2 are elements of $\mathfrak{N}_1, \mathfrak{N}_2$, respectively; in particular, n_i is divisible by $\mathfrak{N}_i$. Thus the difference

$$g = c - \bar{c} = n_2 - n_1$$

is divisible both by $\mathfrak{C}$ and by $\mathfrak{A}$, hence by $\mathfrak{M}$. Since $n_1 = n_2 + m$, moreover, n_1 (and similarly n_2) is divisible both by $\mathfrak{N}_1$ and by $\mathfrak{N}_2$, hence by $\mathfrak{M}$. Therefore

$$f = c + m, \qquad f \equiv 0(\mathfrak{C}), \qquad \mathfrak{C}^* = \mathfrak{C}.$$

The ideals $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are proper divisors of $\mathfrak{C}$; for if $\mathfrak{C}_1 = (\mathfrak{C}, \mathfrak{N}_1) = \mathfrak{C}$, then $\mathfrak{N}_1$ would be divisible by $\mathfrak{C}$ and hence, because it is also divisible by $\mathfrak{A}$, would equal $\mathfrak{M}$, contrary to the hypothesis. Thus $\mathfrak{C} = [\mathfrak{C}_1, \mathfrak{C}_2]$ has been shown to be reducible; Theorem III is proved.

It may be noted that almost the same argument also proves the following.

Lemma II. *If, in a shortest representation $\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}]$, the ideal $\mathfrak{C}$ can be replaced by a proper divisor, then $\mathfrak{C}$ is reducible.*

[13] In fact the representation is also reduced with respect to $\mathfrak{A}_n$, as will be shown in § 3 (Lemma IV) as the converse of Lemma I.

[14] Theorem III corresponds to the passage from modules to residue groups in the works of Schmeidler and Noether–Schmeidler (cf. the Introduction). The residue group corresponds to $\mathfrak{C}$, and the subgroups into which the residue group is decomposed correspond to $\mathfrak{N}_1$ and $\mathfrak{N}_2$.

Indeed, suppose

$$\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}] = [\mathfrak{A}, \mathfrak{C}_1],$$

and put

$$\mathfrak{C}^* = [\mathfrak{C}_1, (\mathfrak{A}, \mathfrak{C})].$$

Again $\mathfrak{C}$ is divisible by $\mathfrak{C}^*$. From $f \equiv 0(\mathfrak{C}^*)$ it follows that

$$f = c_1 = a + c.$$

The difference $a = c_1 - c$ is therefore divisible both by $\mathfrak{A}$ and by $\mathfrak{C}_1$, hence by $\mathfrak{M}$; thus $c_1 = c + m$, $f \equiv 0(\mathfrak{C})$, and $\mathfrak{C}^* = \mathfrak{C}$. Since, by hypothesis, both $\mathfrak{C}_1$ and $(\mathfrak{A}, \mathfrak{C})$ are proper divisors of $\mathfrak{C}$, the ideal $\mathfrak{C} = \mathfrak{C}^*$ has thereby been shown to be reducible.

An irreducible $\mathfrak{C}$ therefore cannot be replaced by a proper divisor.

Now let two different shortest representations of $\mathfrak{M}$ as the least common multiple of finitely many irreducible ideals be given:

$$\mathfrak{M} = [\mathfrak{B}_1 \cdots \mathfrak{B}_k] = [\mathfrak{D}_1 \cdots \mathfrak{D}_l].$$

By the remark following Lemma II, these representations are at the same time reduced. We first prove:

Lemma III. *For every complement* $\mathfrak{A}_i = [\mathfrak{B}_1 \cdots \mathfrak{B}_{i-1}\mathfrak{B}_{i+1} \cdots \mathfrak{B}_k]$ *there is an ideal* $\mathfrak{D}_j$ *such that* $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{D}_j]$.

Indeed, put $\mathfrak{M} = [\mathfrak{D}_1, \mathfrak{C}_1]$, $\mathfrak{C}_1 = [\mathfrak{D}_2, \mathfrak{C}_{12}]$, and so on. Then

$$\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{M}] = [\mathfrak{A}_i, \mathfrak{D}_1, \mathfrak{C}_1] = [[\mathfrak{A}_i, \mathfrak{D}_1], [\mathfrak{A}_i, \mathfrak{C}_1]].$$

Here, for $\mathfrak{N}_1 = [\mathfrak{A}_i, \mathfrak{D}_1]$ and $\mathfrak{N}_2 = [\mathfrak{A}_i, \mathfrak{C}_1]$, the conditions (2) of Theorem III are satisfied, since $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{B}_i]$ is reduced with respect to $\mathfrak{B}_i$ and the representation is a shortest one. Since $\mathfrak{B}_i$ was assumed irreducible, one $\mathfrak{N}_i$ must necessarily equal $\mathfrak{M}$.

If $\mathfrak{N}_1 = \mathfrak{M}$, the lemma is proved. If $\mathfrak{N}_2 = \mathfrak{M}$, then correspondingly $\mathfrak{M} = [[\mathfrak{A}_i, \mathfrak{D}_2], [\mathfrak{A}_i, \mathfrak{C}_{12}]]$, where the same argument again shows that one component must equal $\mathfrak{M}$. Continuing in this way, either $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{D}_j]$ with $j < l$, or $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{C}_{1\ldots l-1}]$; since $\mathfrak{C}_{1\ldots l-1} = \mathfrak{D}_l$, the lemma is proved.

It now follows that:

Theorem IV. *In two different shortest representations of an ideal as the least common multiple of irreducible ideals, the number of components is the same.*

Indeed, the lemma gives, for $i = 1$,

$$\mathfrak{M} = [\mathfrak{A}_1, \mathfrak{B}_1] = [\mathfrak{A}_1, \mathfrak{D}_{j_1}] = [\mathfrak{D}_{j_1}, \mathfrak{B}_2, \ldots, \mathfrak{B}_k].$$

Now consider the two decompositions

$$\mathfrak{M} = [\mathfrak{D}_{j_1}, \mathfrak{B}_2, \ldots, \mathfrak{B}_k] = [\mathfrak{D}_1, \mathfrak{D}_2, \ldots, \mathfrak{D}_l],$$

and repeat the preceding argument with respect to the complement $\bar{\mathfrak{A}}_2 = [\mathfrak{D}_{j_1}, \mathfrak{B}_3, \ldots, \mathfrak{B}_k]$ of $\mathfrak{B}_2$. This gives

$$\mathfrak{M} = [\bar{\mathfrak{A}}_2, \mathfrak{B}_2] = [\bar{\mathfrak{A}}_2, \mathfrak{D}_{j_2}] = [\mathfrak{D}_{j_1}, \mathfrak{D}_{j_2}, \mathfrak{B}_3, \ldots, \mathfrak{B}_k],$$

and, by continuing the procedure,

$$\mathfrak{M} = [\mathfrak{D}_{j_1}, \mathfrak{D}_{j_2}, \ldots, \mathfrak{D}_{j_k}].$$

Since by hypothesis the representation $\mathfrak{M} = [\mathfrak{D}_1 \cdots \mathfrak{D}_l]$ is a shortest one, so that no $\mathfrak{D}$ can be omitted, the distinct ideals among the $\mathfrak{D}_{j_i}$ must exhaust all the $\mathfrak{D}$; hence $k \geq l$. Interchanging the $\mathfrak{B}$ and $\mathfrak{D}$ throughout the lemma and the subsequent arguments gives correspondingly $l \geq k$, and therefore $k = l$, proving equality of number. It follows further that the ideals $\mathfrak{D}_{j_i}$ are all mutually distinct, since otherwise a shortest representation by the $\mathfrak{D}_{j_i}$ would have fewer than k components; the notation may therefore be chosen so that $\mathfrak{D}_{j_i} = \mathfrak{D}_i$. For the same reason, all the intermediate representations $\mathfrak{M} = [\mathfrak{D}_{j_1} \cdots \mathfrak{D}_{j_r}, \mathfrak{B}_{r+1}, \ldots, \mathfrak{B}_k]$ are shortest and hence, by the remark following Lemma II, reduced.

Equality of number yields a converse of Lemma I:

Lemma IV. *If, in a reduced representation, the components are combined into groups and their least common multiples are formed, then the resulting representation is reduced. In other words: from a reduced representation*

$$\mathfrak{M} = [\mathfrak{C}_{11} \cdots \mathfrak{C}_{1\mu_1};\ \ldots;\ \mathfrak{C}_{\sigma 1} \cdots \mathfrak{C}_{\sigma\mu_\sigma}]$$

it follows that $\mathfrak{M} = [\mathfrak{N}_1 \cdots \mathfrak{N}_\sigma] = [\mathfrak{N}_i, \mathfrak{L}_i]$ *is also reduced, if* $\mathfrak{N}_i = [\mathfrak{C}_{i1} \cdots \mathfrak{C}_{i\mu_i}]$.

First, $\mathfrak{N}_i$ cannot be absorbed into its complement $\mathfrak{L}_i$, since this is true of none of its divisors $\mathfrak{C}_{ij}$; the representation is therefore a shortest one. To show that $\mathfrak{N}_i$ cannot be replaced by a proper divisor, decompose the $\mathfrak{C}$ into their irreducible ideals $\mathfrak{B}$,[15] so that the representations, reduced by Lemma I, become

$$\mathfrak{M} = [\mathfrak{B}_{11} \cdots \mathfrak{B}_{1\lambda_1};\ \ldots;\ \mathfrak{B}_{\sigma 1} \cdots \mathfrak{B}_{\sigma\lambda_\sigma}]; \qquad \mathfrak{N}_i = [\mathfrak{B}_{i1} \cdots \mathfrak{B}_{i\lambda_i}].$$

Now let $\mathfrak{M} = [\mathfrak{N}_i^*, \mathfrak{L}_i]$ be reduced with respect to $\mathfrak{N}_i^*$, and let $\mathfrak{N}_i^*$ be a proper divisor of $\mathfrak{N}_i$. By Lemma II,

$$\mathfrak{N}_i = [\mathfrak{N}_i^*, (\mathfrak{N}_i, \mathfrak{L}_i)],$$

and this representation is necessarily reduced with respect to $\mathfrak{N}_i^*$, since otherwise $\mathfrak{N}_i^*$ could also be replaced in $\mathfrak{M}$ by a proper divisor. If necessary, also replace $(\mathfrak{N}_i, \mathfrak{L}_i)$ by a proper divisor so that a reduced representation of $\mathfrak{N}_i$ results. If the two components of $\mathfrak{N}_i$ are now decomposed into irreducible ideals, the number λ_i of irreducible ideals of $\mathfrak{N}_i$ is the sum of the numbers belonging to the components; the number of irreducible ideals corresponding to the proper divisor $\mathfrak{N}_i^*$ is therefore necessarily smaller than λ_i. But then the decomposition of $\mathfrak{M} = [\mathfrak{N}_i^*, \mathfrak{L}_i]$ into irreducible ideals would also yield fewer than $\sum_i \lambda_i$ ideals, contradicting equality of number. As the special case $\sigma = 2$, it follows further that the representation $\mathfrak{M} = [\mathfrak{N}_i, \mathfrak{L}_i]$ is also reduced with respect to the complement $\mathfrak{L}_i$.

§ 4.
Primary Ideals. Uniqueness of the Associated Prime Ideals in Two Different Decompositions into Irreducible Ideals.

What follows concerns the connection between primary and irreducible ideals.

Definition III. *An ideal* $\mathfrak{Q}$ *is called primary if* $a \cdot b \equiv 0(\mathfrak{Q})$ *and* $a \not\equiv 0(\mathfrak{Q})$ *necessarily imply* $b^\varkappa \equiv 0(\mathfrak{Q})$, *where the exponent* $\varkappa$ *is finite.*

The definition may also be stated as follows: if a product $a \cdot b$ is divisible by $\mathfrak{Q}$, then either one factor is divisible by $\mathfrak{Q}$, or a power of each factor is. *In particular, if* $\varkappa$ *is always equal to 1, the ideal is called a prime ideal.*

By virtue of the existence of bases, the definition of a primary (respectively prime) ideal yields the following formulation, which involves only products of ideals[16]:

Definition IIIa. *An ideal* $\mathfrak{Q}$ *is called primary if* $\mathfrak{A} \cdot \mathfrak{B} \equiv 0(\mathfrak{Q})$ *and* $\mathfrak{A} \not\equiv 0(\mathfrak{Q})$ *necessarily imply* $\mathfrak{B}^\lambda \equiv 0(\mathfrak{Q})$. *If* λ *is always equal to 1, the ideal is called a prime ideal. Thus, for a prime ideal* $\mathfrak{P}$, $\mathfrak{A} \cdot \mathfrak{B} \equiv 0(\mathfrak{P})$ *and* $\mathfrak{A} \not\equiv 0(\mathfrak{P})$ *always imply* $\mathfrak{B} \equiv 0(\mathfrak{P})$.

Indeed, since Definition III is contained in IIIa as the special case $\mathfrak{A} = (a)$, $\mathfrak{B} = (b)$, every ideal primary according to IIIa is also primary according to III. Conversely, let $\mathfrak{Q}$ be primary according to III and suppose the hypothesis of IIIa is satisfied: $\mathfrak{A} \cdot \mathfrak{B} \equiv 0(\mathfrak{Q})$. Then either $\mathfrak{A} \equiv 0(\mathfrak{Q})$, or there is at least one element $a \equiv 0(\mathfrak{A})$ such that $a \cdot \mathfrak{B} \equiv 0(\mathfrak{Q})$ and $a \not\equiv 0(\mathfrak{Q})$. If $b_1, \ldots, b_r$ is an ideal basis of $\mathfrak{B}$, then Definition III, since $a \cdot b_i \equiv 0(\mathfrak{Q})$, gives

$$b_1^{\varkappa_1} \equiv 0(\mathfrak{Q}); \quad \ldots; \quad b_r^{\varkappa_r} \equiv 0(\mathfrak{Q}).$$

Since

$$b = f_1 b_1 + \cdots + f_r b_r + n_1 b_1 + \cdots + n_r b_r,$$

the product of any $\lambda = \varkappa_1 + \cdots + \varkappa_r$ elements b is therefore divisible by $\mathfrak{Q}$, proving that ideals primary according to III satisfy Definition IIIa. In the special case of prime ideals $\mathfrak{P}$, however, $a \cdot \mathfrak{B} \equiv 0(\mathfrak{P})$, and hence $a \cdot b \equiv 0(\mathfrak{P})$ for every $b \equiv 0(\mathfrak{B})$, together with $a \not\equiv 0(\mathfrak{P})$, imply $b \equiv 0(\mathfrak{P})$ and thus $\mathfrak{B} \equiv 0(\mathfrak{P})$. This proves the equivalence of the two definitions.

The connection between primary and prime ideals is established by observing that the totality $\mathfrak{P}$ of all elements p having the property that some power of p is divisible by $\mathfrak{Q}$ forms a prime ideal. First, it is clear that $\mathfrak{P}$ is an ideal, since, along with p_1 and p_2, the elements ap_1 and $p_1 - p_2$ also have the stated property. By the same basis argument used in Definition IIIa, there is furthermore a number λ such that $\mathfrak{P}^\lambda \equiv 0(\mathfrak{Q})$.

Now let

$$ab \equiv 0(\mathfrak{P}), \qquad a \not\equiv 0(\mathfrak{P}).$$

[15] This always means a shortest, and therefore reduced, representation by the $\mathfrak{B}$.

[16] As usual, the product $\mathfrak{A} \cdot \mathfrak{B}$ of two ideals means the ideal consisting of all elements $a \cdot b$ and their finite sums.

Then, by the definition of $\mathfrak{P}$,

$$a^\lambda b^\lambda \equiv 0(\mathfrak{Q}), \qquad a^\lambda \not\equiv 0(\mathfrak{Q}),$$

and therefore, by the definition of $\mathfrak{Q}$,

$$b^{\lambda\varkappa} \equiv 0(\mathfrak{Q}), \qquad \text{and consequently} \qquad b \equiv 0(\mathfrak{P}),$$

which proves that $\mathfrak{P}$ is a prime ideal. The ideal $\mathfrak{P}$ is also characterized as the greatest common divisor of all ideals $\mathfrak{B}$ having the property that some power of $\mathfrak{B}$ is divisible by $\mathfrak{Q}$. For every such $\mathfrak{B}$ is divisible by $\mathfrak{P}$, and hence so is their greatest common divisor $\mathfrak{D}$. Conversely, $\mathfrak{P}$ itself is one of these ideals $\mathfrak{B}$, and hence is divisible by $\mathfrak{D}$, proving $\mathfrak{P} = \mathfrak{D}$. Thus $\mathfrak{P}$ is a prime ideal that is a divisor of $\mathfrak{Q}$ and some power of which is divisible by $\mathfrak{Q}$; this property determines it uniquely. For from

$$\mathfrak{Q} \equiv 0(\mathfrak{P}), \qquad \mathfrak{P}^\lambda \equiv 0(\mathfrak{Q}), \qquad \mathfrak{Q} \equiv 0(\bar{\mathfrak{P}}), \qquad \bar{\mathfrak{P}}^\mu \equiv 0(\mathfrak{Q})$$

it follows that

$$\mathfrak{P}^\lambda \equiv 0(\bar{\mathfrak{P}}), \qquad \bar{\mathfrak{P}}^\mu \equiv 0(\mathfrak{P}),$$

and hence, by the property of prime ideals,

$$\mathfrak{P} \equiv 0(\bar{\mathfrak{P}}), \qquad \bar{\mathfrak{P}} \equiv 0(\mathfrak{P}), \qquad \mathfrak{P} = \bar{\mathfrak{P}}.$$

In summary, we have:

Theorem V. *For every primary ideal $\mathfrak{Q}$ there exists one and only one prime ideal $\mathfrak{P}$ that is a divisor of $\mathfrak{Q}$ and some power of which is divisible by $\mathfrak{Q}$; $\mathfrak{P}$ will be called the "associated prime ideal".*[17] *$\mathfrak{P}$ is characterized as the greatest common divisor of all ideals $\mathfrak{B}$ having the property that some power of $\mathfrak{B}$ is divisible by $\mathfrak{Q}$. If ϱ is the least number such that $\mathfrak{P}^\varrho \equiv 0(\mathfrak{Q})$, then ϱ will be called the exponent of $\mathfrak{Q}$.*[18]

We now prove, as the connection between primary and irreducible ideals:

Theorem VI. *Every nonprimary ideal is reducible; in other words, every irreducible ideal is primary.*[19]

Let $\mathfrak{K}$ be a nonprimary ideal, so that by Definition III there is at least one pair of elements a, b such that

$$a \cdot b \equiv 0(\mathfrak{K}); \qquad a \not\equiv 0(\mathfrak{K}); \qquad b^\varkappa \not\equiv 0(\mathfrak{K}) \quad \text{for every } \varkappa. \tag{3}$$

We now form the two ideals

$$\mathfrak{L}_0 = (\mathfrak{K}, a); \qquad \mathfrak{N}_0 = (\mathfrak{K}, b),$$

which by (3) are proper divisors of $\mathfrak{K}$ and for which, again by (3),

$$\mathfrak{L}_0 \cdot \mathfrak{N}_0 \equiv 0(\mathfrak{K}). \tag{4}$$

For the elements f of the least common multiple $\mathfrak{K}_0 = [\mathfrak{L}_0, \mathfrak{N}_0]$, the following alternative holds.

Either from

$$f \equiv 0(\mathfrak{L}_0); \qquad f \equiv 0(\mathfrak{N}_0), \qquad \text{i.e.} \qquad f \equiv a_1 \cdot b\ (\mathfrak{K})$$

there always follows a representation

$$f \equiv l_0 \cdot b\ (\mathfrak{K}); \qquad l_0 \equiv 0(\mathfrak{L}_0);$$

then by (4), $f \equiv 0(\mathfrak{K})$, hence $\mathfrak{K}_0 \equiv 0(\mathfrak{K})$, and, since also $\mathfrak{K} \equiv 0(\mathfrak{K}_0)$, $\mathfrak{K} = \mathfrak{K}_0$, which shows that $\mathfrak{K}$ is reducible.

Or there is at least one $f \equiv 0(\mathfrak{K}_0)$ for which no such l_0 exists. With the a_1 belonging to this f, we then form

$$\mathfrak{L}_1 = (\mathfrak{L}_0, a_1) = (\mathfrak{K}, a, a_1); \qquad \mathfrak{N}_1 = (\mathfrak{K}, b^2).$$

Then, since $a_1 \cdot b \equiv 0(\mathfrak{L}_0)$, (4) also gives

$$\mathfrak{L}_1 \cdot \mathfrak{N}_1 \equiv 0(\mathfrak{K}); \tag{4'}$$

and $\mathfrak{L}_1$ is a proper divisor of $\mathfrak{L}_0$.

The same alternative holds for the elements f of $\mathfrak{K}_1 = [\mathfrak{L}_1, \mathfrak{N}_1]$.

---

[17] That the converse does not hold is shown by the example $\mathfrak{M} = (x^2, xy)$. The prime ideal (x) satisfies all the conditions, but $\mathfrak{M}$ is not primary.

[18] That in general $\mathfrak{P}^\varrho = \mathfrak{Q}$ need not hold, as it does in the domain of rational integers and in that of algebraic integers, is shown by the example $\mathfrak{Q} = (x^2, y)$; $\mathfrak{P} = (x, y)$; $\mathfrak{P}^2 = (x^2, xy, y^2) \equiv 0(\mathfrak{Q})$, but $\mathfrak{Q} \not\equiv 0(\mathfrak{P}^2)$; thus $\mathfrak{Q}$ differs from $\mathfrak{P}^2$.

[19] That the converse does not hold here is shown, for example, by $\mathfrak{Q} = (x^2, xy, y^\lambda) = [(x^2, y), (x, y^\lambda)]$, where $\lambda \geq 2$. Here $\mathfrak{Q}$ is primary but reducible. That $\mathfrak{Q}$ is primary follows from the fact that it contains all power products of degree λ in x, y; thus, for every polynomial without a constant term, some power is divisible by $\mathfrak{Q}$. But if, in $a \cdot b \equiv 0(\mathfrak{Q})$, the polynomial b contains a constant term—so that $b^\varkappa \not\equiv 0(\mathfrak{Q})$ for every $\varkappa$—then, since every homogeneous component of $a \cdot b$ is divisible by $\mathfrak{Q}$ because the basis polynomials of $\mathfrak{Q}$ are homogeneous, a must be divisible by $\mathfrak{Q}$.

Either from

$$f \equiv 0(\mathfrak{L}_1); \qquad f \equiv 0(\mathfrak{N}_1);$$

$$\text{i.e.} \qquad f \equiv a_2 \cdot b^2 \ (\mathfrak{K}) \quad \text{there always follows} \quad f \equiv l_1 \cdot b^2; \qquad l_1 \equiv 0(\mathfrak{L}_1);$$

and therefore by (4'), $\mathfrak{K} = \mathfrak{K}_1$.

Or for at least one f there is no such l_1, which leads to the formation of $\mathfrak{L}_2 = (\mathfrak{L}_1, a_2)$ and $\mathfrak{N}_2 = (\mathfrak{K}, b^{2^2})$, with $\mathfrak{L}_2 \cdot \mathfrak{N}_2 \equiv 0(\mathfrak{K})$, where $\mathfrak{L}_2$ is a proper divisor of $\mathfrak{L}_1$. Continuing in this way, we define in general

$$\mathfrak{L}_0 = (\mathfrak{K}, a); \quad \mathfrak{L}_1 = (\mathfrak{L}_0, a_1); \quad \ldots; \quad \mathfrak{L}_\nu = (\mathfrak{L}_{\nu-1}, a_\nu); \quad \ldots,$$

$$\mathfrak{N}_0 = (\mathfrak{K}, b); \quad \mathfrak{N}_1 = (\mathfrak{K}, b^2); \quad \ldots; \quad \mathfrak{N}_\nu = (\mathfrak{K}, b^{2^\nu}); \quad \ldots,$$

where the a_i are defined by the existence of an f such that

$$f \equiv 0(\mathfrak{L}_{i-1}); \qquad f \equiv 0(\mathfrak{N}_{i-1}),$$

$$\text{i.e.} \qquad f \equiv a_i \cdot b^{2^{i-1}} \ (\mathfrak{K}); \qquad \text{but} \qquad a_i \not\equiv 0(\mathfrak{L}_{i-1}).$$

It then follows in general that $\mathfrak{L}_i \cdot \mathfrak{N}_i \equiv 0(\mathfrak{K})$, that $\mathfrak{N}_i$ is a proper divisor of $\mathfrak{K}$ by (3), and that $\mathfrak{L}_i$ is a proper divisor of $\mathfrak{L}_{i-1}$. By Theorem I on the finite chain, the chain of the $\mathfrak{L}_i$ must therefore terminate after finitely many steps, say with $\mathfrak{L}_n$. Thus, for every $f \equiv 0(\mathfrak{L}_n)$ and $f \equiv 0(\mathfrak{N}_n)$, one has $f \equiv l_n \cdot b^{2^n}$ $(\mathfrak{K})$ with $l_n \equiv 0(\mathfrak{L}_n)$, and consequently the preceding argument gives $\mathfrak{K} = [\mathfrak{L}_n, \mathfrak{N}_n]$, which shows that $\mathfrak{K}$ is reducible.

The *uniqueness of the associated prime ideals* follows from what has just been proved, as follows.

Let

$$\mathfrak{M} = [\mathfrak{B}_1 \cdots \mathfrak{B}_k] = [\mathfrak{D}_1 \cdots \mathfrak{D}_k]$$

be two shortest, hence reduced, representations of $\mathfrak{M}$ as the least common multiple of irreducible ideals, whose numbers of components agree by Theorem IV. By that theorem the intermediate representations occurring there (where, as noted there, the index $j_i = i$ may be put)

$$\mathfrak{M} = [\mathfrak{D}_1 \cdots \mathfrak{D}_{i-1}\mathfrak{B}_i\mathfrak{B}_{i+1} \cdots \mathfrak{B}_k] = [\mathfrak{D}_1 \cdots \mathfrak{D}_{i-1}\mathfrak{D}_i\mathfrak{B}_{i+1} \cdots \mathfrak{B}_k] = [\bar{\mathfrak{U}}_i, \mathfrak{B}_i] = [\bar{\mathfrak{U}}_i, \mathfrak{D}_i]$$

are also shortest representations. Hence

$$\bar{\mathfrak{U}}_i \cdot \mathfrak{B}_i \equiv 0(\mathfrak{D}_i), \qquad \bar{\mathfrak{U}}_i \not\equiv 0(\mathfrak{D}_i), \qquad \bar{\mathfrak{U}}_i \cdot \mathfrak{D}_i \equiv 0(\mathfrak{B}_i), \qquad \bar{\mathfrak{U}}_i \not\equiv 0(\mathfrak{B}_i).$$

Since by Theorem VI the irreducible ideals $\mathfrak{B}_i$ and $\mathfrak{D}_i$ are primary, it follows that there are two numbers λ_i and μ_i such that

$$\mathfrak{B}_i^{\lambda_i} \equiv 0(\mathfrak{D}_i); \qquad \mathfrak{D}_i^{\mu_i} \equiv 0(\mathfrak{B}_i). \tag{5}$$

Let $\mathfrak{P}_i$ and $\bar{\mathfrak{P}}_i$ denote the associated prime ideals of $\mathfrak{B}_i$ and $\mathfrak{D}_i$, respectively; thus $\mathfrak{P}_i^{\varrho_i} \equiv 0(\mathfrak{B}_i)$ and $\bar{\mathfrak{P}}_i^{\sigma_i} \equiv 0(\mathfrak{D}_i)$. Then (5) gives

$$\mathfrak{P}_i^{\lambda_i\varrho_i} \equiv 0(\bar{\mathfrak{P}}_i), \qquad \bar{\mathfrak{P}}_i^{\mu_i\sigma_i} \equiv 0(\mathfrak{P}_i),$$

and hence, by the property of prime ideals,

$$\mathfrak{P}_i \equiv 0(\bar{\mathfrak{P}}_i), \qquad \bar{\mathfrak{P}}_i \equiv 0(\mathfrak{P}_i), \qquad \mathfrak{P}_i = \bar{\mathfrak{P}}_i.$$

This proves:

Theorem VII. *In two different shortest representations of an ideal as the least common multiple of irreducible ideals, the associated prime ideals agree; equal prime ideals may occur among them,*[20] *and occur equally often in every decomposition. Consequently, the ideals themselves can be paired in at least one way so that, in each pair, a power of one ideal $\mathfrak{B}_i$ is divisible by the assigned ideal $\mathfrak{D}_i$, and conversely. Their numbers agree by Theorem IV.*[21]

§ 5.

Representation of an ideal as the least common multiple of greatest primary ideals. Uniqueness of the associated prime ideals.

[20] This is shown, for example, by the example in footnote 19: $(x^2, xy, y^\lambda) = [(x^2, y), (x, y^\lambda)]$, where $\lambda \geq 2$. The two associated prime ideals here are (x, y).

[21] For the uniqueness of the "isolated" ideals among the irreducible ideals, cf. § 7.

Definition IV. *A shortest representation* $\mathfrak{M} = [\mathfrak{Q}_1 \cdots \mathfrak{Q}_\alpha]$ *will be called a least common multiple of greatest primary ideals if all* $\mathfrak{Q}$ *are primary, but the least common multiple of two* $\mathfrak{Q}$ *is no longer primary.*

That at least one such representation always exists follows from the representation of $\mathfrak{M}$ as a least common multiple of irreducible ideals. These ideals are primary; either there is already a representation by greatest primary ideals, or the least common multiple of some two ideals is again primary. Since the number of ideals has thereby decreased by one, repetition of the procedure leads after finitely many steps to the desired representation.

This representation is reduced by Lemma IV. Conversely, every reduced representation by greatest primary ideals arises in this way, as the decomposition of the $\mathfrak{Q}$ into irreducible ideals shows.

In order to derive here from Theorem VII a corresponding uniqueness theorem, the connection with the associated prime ideals has to be investigated.

Theorem VIII. *If the primary ideals* $\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_\lambda$ *all possess the same associated prime ideal* $\mathfrak{P}$*, then their least common multiple* $\mathfrak{Q} = [\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_\lambda]$ *is also primary and has* $\mathfrak{P}$ *as associated prime ideal. Conversely, if* $\mathfrak{Q} = [\mathfrak{N}_1 \cdots \mathfrak{N}_\lambda]$ *is a reduced representation of the primary ideal* $\mathfrak{Q}$*, then all* $\mathfrak{N}_i$ *are primary and have, as associated prime ideal, the associated prime ideal* $\mathfrak{P}$ *of* $\mathfrak{Q}$*.*

For the proof of the first part, first observe that from $\mathfrak{P}^{\varrho_i} \equiv 0(\mathfrak{N}_i)$ for every i it also follows that $\mathfrak{P}^\tau \equiv 0(\mathfrak{Q})$, where τ denotes the largest of the indices ϱ_i. Since $\mathfrak{P}$ is also a divisor of $\mathfrak{Q}$, $\mathfrak{P}$ is necessarily the associated prime ideal if $\mathfrak{Q}$ is primary. From

$$\mathfrak{A}\mathfrak{B} \equiv 0(\mathfrak{Q}), \qquad \mathfrak{B}^k \not\equiv 0(\mathfrak{Q}) \quad \text{(for every } k\text{)}$$

it follows that

$$\mathfrak{B} \not\equiv 0(\mathfrak{P}), \quad \text{hence} \quad \mathfrak{B}^k \not\equiv 0(\mathfrak{N}_i) \quad \text{(for every } k\text{)},$$

and consequently $\mathfrak{A} \equiv 0(\mathfrak{N}_i)$; hence $\mathfrak{A} \equiv 0(\mathfrak{Q})$. Thus $\mathfrak{Q}$ is proved primary, and $\mathfrak{P}$ the associated prime ideal.

Conversely, let first

$$\mathfrak{Q} = [\mathfrak{N}_1 \cdots \mathfrak{N}_\lambda] = [\mathfrak{N}_i, \mathfrak{L}_i]$$

be a shortest representation of $\mathfrak{Q}$ by primary ideals $\mathfrak{N}_i$, and let $\mathfrak{P}_i$ denote the corresponding associated prime ideals. From

$$\mathfrak{L}_i \cdot \mathfrak{N}_i \equiv 0(\mathfrak{Q}), \qquad \mathfrak{L}_i \not\equiv 0(\mathfrak{Q})$$

(because the representation is shortest) it follows that

$$\mathfrak{N}_i^{\sigma_i} \equiv 0(\mathfrak{Q}), \qquad \text{or} \qquad \mathfrak{P}_i^{\varrho_i \sigma_i} \equiv 0(\mathfrak{Q}).$$

Since $\mathfrak{P}_i$ is at the same time a divisor of $\mathfrak{Q}$, $\mathfrak{P}_i$ therefore agrees, for every i, with the associated prime ideal $\mathfrak{P}$ of $\mathfrak{Q}$.

It remains to show that in every reduced representation $\mathfrak{Q} = [\mathfrak{N}_1 \cdots \mathfrak{N}_\lambda]$ the $\mathfrak{N}_i$ are primary.[22] To this end, decompose the $\mathfrak{N}_i$ into their irreducible ideals $\mathfrak{B}$; in the resulting shortest representation $\mathfrak{Q} = [\mathfrak{B}_1 \cdots \mathfrak{B}_s]$, every ideal is primary and, by what has just been proved, has $\mathfrak{P}$ as associated prime ideal. Then by the first part of the theorem proved above the same holds for each $\mathfrak{N}_i$, completing the proof of Theorem VIII.

Addendum. It also follows that a prime ideal is necessarily irreducible. For from the reduced representation $\mathfrak{P} = [\mathfrak{N}, \mathfrak{K}]$ one obtains by Theorem VIII $\mathfrak{N} \equiv 0(\mathfrak{P})$; hence, since $\mathfrak{P} \equiv 0(\mathfrak{N})$, also $\mathfrak{P} = \mathfrak{N}$, and similarly $\mathfrak{P} = \mathfrak{K}$. The irreducibility of $\mathfrak{P}$ also follows directly: for from $\mathfrak{P} = [\mathfrak{N}, \mathfrak{K}]$ follows $\mathfrak{N}\mathfrak{K} \equiv 0(\mathfrak{P})$, $\mathfrak{N} \not\equiv 0(\mathfrak{P})$, $\mathfrak{K} \not\equiv 0(\mathfrak{P})$, contrary to the defining property of a prime ideal.

Now let

$$\mathfrak{M} = [\mathfrak{Q}_1 \cdots \mathfrak{Q}_\alpha] = [\bar{\mathfrak{Q}}_1 \cdots \bar{\mathfrak{Q}}_\beta]$$

be two reduced representations of $\mathfrak{M}$ as the least common multiple of greatest primary ideals. Decomposing the $\mathfrak{Q}$ into irreducible ideals $\mathfrak{B}$, and the $\bar{\mathfrak{Q}}$ correspondingly into irreducible ideals $\mathfrak{D}$, gives two reduced representations of $\mathfrak{M}$ as the least common multiple of irreducible ideals; by Theorem VII, both the number of components and the associated prime ideals coincide. By Theorem VIII, all irreducible ideals $\mathfrak{B}$ occurring for a fixed $\mathfrak{Q}_i$ have the same associated prime ideal $\mathfrak{P}_i$; whereas the $\mathfrak{P}_j$ associated to $\mathfrak{Q}_j$ is necessarily different from this, since otherwise, by Theorem VIII, there would be no representation by greatest primary ideals. Hence the number α of the $\mathfrak{Q}$ is equal to the number of different associated prime ideals $\mathfrak{P}$ of the

[22] That the reduced representation is essential here is shown by the example of the non-reduced representation $\mathfrak{Q} = [x^2, xy, y^\lambda] = [(x^2, xy, y^2, yz), (x, y^\lambda)]$, where $\lambda \geq 2$. Here $(x^2, xy, y^2, yz) = [(x^2, y), (x, y^2, z)]$ is not primary by what has just been proved; for the latter representation is a shortest one by primary ideals, but the associated prime ideals (x, y) and (x, y, z) are different. ($\mathfrak{Q}$ is primary by footnote 19.)

$\mathfrak{B}$; these different $\mathfrak{P}$ form the associated prime ideals of the $\mathfrak{Q}$. The same holds for the $\bar{\mathfrak{Q}}$ with respect to their decomposition into the $\mathfrak{D}$. Theorem VII therefore gives equality of number for the $\mathfrak{Q}$ and $\bar{\mathfrak{Q}}$, and agreement of their associated prime ideals. At the same time it is seen that the grouping of the irreducible ideals into greatest primary ideals described at the beginning of the paragraph consists in combining all, and only those, with the same associated prime ideal. Theorem VIII further shows the irreducibility property of the greatest primary ideals: they admit no reduced representation as the least common multiple of greatest primary ideals.

In summary:

Theorem IX. *In two reduced representations of an ideal as the least common multiple of greatest primary ideals, the number of components and the associated prime ideals, all of which are distinct from each other, coincide. In other words, to each $\mathfrak{Q}$ there can be assigned one and only one $\bar{\mathfrak{Q}}$ such that a power of $\mathfrak{Q}$ is divisible by $\bar{\mathfrak{Q}}$, and conversely.*[23] *The $\mathfrak{Q}$ and $\bar{\mathfrak{Q}}$ have the irreducibility property with respect to decomposition into greatest primary ideals.*

Addendum. It should be noted that Theorem IX remains essentially valid if one assumes only a shortest representation instead of a reduced one. If, say,

$$\mathfrak{M} = [\mathfrak{Q}_1 \cdots \mathfrak{Q}_i^* \cdots \mathfrak{Q}_\alpha]$$

is reduced with respect to $\mathfrak{Q}_i^*$, and $\mathfrak{Q}_i^*$ is a proper divisor of $\mathfrak{Q}_i$, while $\mathfrak{L}_i$ is the complement of $\mathfrak{Q}_i$, then by Lemma IV

$$\mathfrak{Q}_i = [\mathfrak{Q}_i^*; (\mathfrak{L}_i, \mathfrak{Q}_i)],$$

and this representation is reduced with respect to $\mathfrak{Q}_i^*$. By Theorem VIII – replacing $(\mathfrak{L}_i, \mathfrak{Q}_i)$ by a proper divisor if necessary when applying the theorem – $\mathfrak{Q}_i^*$ is therefore primary and has the same associated prime ideal $\mathfrak{P}_i$ as $\mathfrak{Q}_i$. Continuing the procedure shows that to every such representation there can be assigned a reduced representation by greatest primary ideals in such a way that the number of components and the associated prime ideals coincide. Thus even for shortest representations it holds that in two different representations the number of components and the associated prime ideals coincide.

The associated, mutually distinct prime ideals thereby uniquely defined will be called simply "the associated prime ideals of $\mathfrak{M}$."

§ 6.

Unique representation of an ideal as the least common multiple of relatively-prime irreducible ideals.

Definition V. *An ideal $\mathfrak{R}$ is called relatively prime to $\mathfrak{S}$ if $\mathfrak{T} \cdot \mathfrak{R} \equiv 0(\mathfrak{S})$ necessarily implies $\mathfrak{T} \equiv 0(\mathfrak{S})$. If both $\mathfrak{R}$ is relatively prime to $\mathfrak{S}$ and $\mathfrak{S}$ is relatively prime to $\mathfrak{R}$, then $\mathfrak{R}$ and $\mathfrak{S}$ are called mutually relatively prime.*[24]

An ideal is called relatively-prime irreducible if it cannot be represented as the least common multiple of mutually relatively prime proper divisors.

In particular, if instead of $\mathfrak{T}$ one takes the greatest common divisor $\mathfrak{T}_0$ of all $\mathfrak{T}$ for which $\mathfrak{T}\mathfrak{R} \equiv 0(\mathfrak{S})$, then also $\mathfrak{T}_0\mathfrak{R} \equiv 0(\mathfrak{S})$ and $\mathfrak{S} \equiv 0(\mathfrak{T}_0)$. Thus $\mathfrak{T}_0 = \mathfrak{S}$ when $\mathfrak{R}$ is relatively prime to $\mathfrak{S}$; and $\mathfrak{T}_0$ is a proper divisor of $\mathfrak{S}$ when $\mathfrak{R}$ is not relatively prime to $\mathfrak{S}$.[25]

The uniqueness proof rests on:

Theorem X. *1. If $\mathfrak{R}$ is relatively prime to the ideals $\mathfrak{S}_1, \ldots, \mathfrak{S}_\lambda$, then $\mathfrak{R}$ is also relatively prime to their least common multiple $\mathfrak{S}$.*

2. If the ideals $\mathfrak{S}_1, \ldots, \mathfrak{S}_\lambda$ are relatively prime to $\mathfrak{R}$, then their least common multiple $\mathfrak{S}$ is also relatively prime to $\mathfrak{R}$.

3. If $\mathfrak{R}$ is relatively prime to $\mathfrak{S}$ and $\mathfrak{S} = [\mathfrak{S}_1 \cdots \mathfrak{S}_\lambda]$ is a reduced representation for $\mathfrak{S}$, then $\mathfrak{R}$ is also relatively prime to each $\mathfrak{S}_i$.

4. If $\mathfrak{S}$ is relatively prime to $\mathfrak{R}$, then every divisor $\mathfrak{S}_i$ of $\mathfrak{S}$ is also relatively prime to $\mathfrak{R}$.

1. Since $\mathfrak{T}\mathfrak{R} \equiv 0(\mathfrak{S})$ necessarily gives $\mathfrak{T}\mathfrak{R} \equiv 0(\mathfrak{S}_i)$, the hypothesis gives $\mathfrak{T} \equiv 0(\mathfrak{S}_i)$, and hence $\mathfrak{T} \equiv 0(\mathfrak{S})$.

[23] An example of different representations is the one given in footnote 12 for Theorem II: $(x^2, xy) = [(x), (x^2, \mu x + y)]$ for arbitrary μ. Since the associated prime ideals $\mathfrak{P}_1 = (x)$ and $\mathfrak{P}_2 = (x, y)$ are distinct, these are greatest primary ideals. – For the uniqueness of the "isolated" greatest primary ideals, compare § 7.

[24] The condition of being relatively prime is not symmetric. For example, $\mathfrak{R} = (x^2, y)$ is relatively prime to $\mathfrak{S} = (x)$; but $\mathfrak{S}$ is not relatively prime to $\mathfrak{R}$, since $\mathfrak{S}^2 \equiv 0(\mathfrak{R})$, whereas $\mathfrak{S} \not\equiv 0(\mathfrak{R})$.

[25] The $\mathfrak{T}_0$ so defined agrees with Lasker's "residual module"; and, in its extension to number modules in place of ideals, with Dedekind's "quotient" of two modules. Lasker, loc. cit., p. 49; Dedekind (Zahlentheorie), p. 504.

2. Put

$$\mathfrak{C}_1 = [\mathfrak{S}_2 \cdots \mathfrak{S}_\lambda], \quad \mathfrak{C}_{12} = [\mathfrak{S}_3 \cdots \mathfrak{S}_\lambda], \quad \ldots, \quad \mathfrak{C}_{12\ldots\lambda-1} = \mathfrak{S}_\lambda.$$

From $\mathfrak{T} \cdot \mathfrak{S} \equiv 0(\mathfrak{R})$ it follows that $\mathfrak{T} \cdot \mathfrak{S}_1 \cdot \mathfrak{C}_1 \equiv 0(\mathfrak{R})$; hence, by the hypothesis, $\mathfrak{T} \cdot \mathfrak{C}_1 \equiv 0(\mathfrak{R})$. It follows in turn that $\mathfrak{T} \cdot \mathfrak{S}_2 \cdot \mathfrak{C}_{12} \equiv 0(\mathfrak{R})$, hence $\mathfrak{T} \cdot \mathfrak{C}_{12} \equiv 0(\mathfrak{R})$, and finally $\mathfrak{T} \cdot \mathfrak{C}_{12\ldots\lambda-1} = \mathfrak{T} \cdot \mathfrak{S}_\lambda \equiv 0(\mathfrak{R})$; hence $\mathfrak{T} \equiv 0(\mathfrak{R})$.

3. Let $\mathfrak{C}_i$ denote the complement of $\mathfrak{S}_i$. From $\mathfrak{T}_0 \cdot \mathfrak{R} \equiv 0(\mathfrak{S}_i)$, together with $\mathfrak{C}_i \cdot \mathfrak{R} \equiv 0(\mathfrak{S}_i)$, it follows that $[\mathfrak{T}_0, \mathfrak{C}_i] \cdot \mathfrak{R} \equiv 0(\mathfrak{S})$. If $\mathfrak{T}_0$ were a proper divisor of $\mathfrak{S}_i$, then, since $\mathfrak{S} = [\mathfrak{S}_i, \mathfrak{C}_i]$ is reduced, $[\mathfrak{T}_0, \mathfrak{C}_i]$ would be a proper divisor of $\mathfrak{S}$, contrary to the hypothesis.

4. From $\mathfrak{T}\mathfrak{S}_i \equiv 0(\mathfrak{R})$, where $\mathfrak{T}$ is a proper divisor of $\mathfrak{R}$, it follows also that $\mathfrak{T}\mathfrak{S} \equiv 0(\mathfrak{R})$; hence $\mathfrak{T}$ would be a proper divisor of $\mathfrak{R}$, contrary to the hypothesis.

Definition V shows in particular that every ideal is relatively prime to the unit ideal $\mathfrak{D}$ consisting of all elements of Σ;[26] the following theorems, however, apply only to ideals distinct from $\mathfrak{D}$.

From Theorem X one first obtains:

Lemma V. *Every representation of an ideal as the least common multiple of mutually relatively prime ideals distinct from $\mathfrak{D}$ is reduced.*

Let

$$\mathfrak{M} = [\mathfrak{R}_1\mathfrak{R}_2 \cdots \mathfrak{R}_\sigma] = [\mathfrak{R}_i, \mathfrak{L}_i]$$

be such a representation. By Theorem X, 2, $\mathfrak{L}_i$ is also relatively prime to $\mathfrak{R}_i$; hence $\mathfrak{R}_i$ cannot be contained in $\mathfrak{L}_i$, and the representation is shortest. For from $\mathfrak{L}_i \equiv 0(\mathfrak{R}_i)$, with $\mathfrak{L}_i$ relatively prime to $\mathfrak{R}_i$, it would follow from $\mathfrak{D}\mathfrak{L}_i \equiv 0(\mathfrak{R}_i)$ that $\mathfrak{D} \equiv 0(\mathfrak{R}_i)$, hence $\mathfrak{R}_i = \mathfrak{D}$, contrary to the hypothesis.

If now $\mathfrak{R}_i$ could be replaced by a proper divisor $\mathfrak{R}_i^*$, then by Lemma II $\mathfrak{R}_i$ would be reducible and

$$\mathfrak{R}_i = [\mathfrak{R}_i^*, (\mathfrak{R}_i, \mathfrak{L}_i)].$$

If necessary, replace $(\mathfrak{R}_i, \mathfrak{L}_i)$ by a proper divisor $(\mathfrak{R}_i, \mathfrak{L}_i)^*$ and likewise replace $\mathfrak{R}_i^*$ by a proper divisor so that a reduced representation of $\mathfrak{R}_i$ is obtained. Then Theorem X, 3 shows that $\mathfrak{L}_i$ is also relatively prime to $(\mathfrak{R}_i, \mathfrak{L}_i)^*$, and this ideal is distinct from $\mathfrak{D}$ because the original representation was shortest. But $(\mathfrak{R}_i, \mathfrak{L}_i)^*$ is contained in $(\mathfrak{R}_i, \mathfrak{L}_i)$ and $(\mathfrak{R}_i, \mathfrak{L}_i)$ is contained in $\mathfrak{L}_i$, giving the contradiction.

Theorem X further gives the following theorem, which mediates the connection with the associated prime ideals.

Theorem XI. *If $\mathfrak{R}$ is relatively prime to $\mathfrak{S}$ and $\mathfrak{S}$ is distinct from $\mathfrak{D}$, then no associated prime ideal of $\mathfrak{R}$*[27] *is divisible by an associated prime ideal of $\mathfrak{S}$. Conversely, if no such divisibility holds, then $\mathfrak{R}$ is relatively prime to $\mathfrak{S}$, and of course $\mathfrak{S}$ is distinct from $\mathfrak{D}$.*

Let

$$\mathfrak{R} = [\mathfrak{Q}_1 \cdots \mathfrak{Q}_\alpha], \qquad \mathfrak{S} = [\mathfrak{Q}_1^* \cdots \mathfrak{Q}_\beta^*]$$

be reduced representations of $\mathfrak{R}$ and $\mathfrak{S}$ by greatest primary ideals, and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_\alpha$ and $\mathfrak{P}_1^*, \ldots, \mathfrak{P}_\beta^*$ be their associated prime ideals. We prove the assertion in the form: if some $\mathfrak{P}$ is divisible by some $\mathfrak{P}^*$, then $\mathfrak{R}$ cannot be relatively prime to $\mathfrak{S}$, and conversely.

Suppose then that $\mathfrak{P}_\mu \equiv 0(\mathfrak{P}_\nu^*)$, and consequently also $\mathfrak{Q}_\mu \equiv 0(\mathfrak{P}_\nu^*)$. By the definition of $\mathfrak{P}_\nu^*$ this gives $\mathfrak{Q}_\mu^{\sigma_\nu} \equiv 0(\mathfrak{Q}_\nu^*)$, hence also $\mathfrak{R}^{\sigma_\nu} \equiv 0(\mathfrak{Q}_\nu^*)$. Let $\mathfrak{R}^\tau$ be the lowest power of $\mathfrak{R}$ divisible by $\mathfrak{Q}_\nu^*$. If $\tau = 1$, then $\mathfrak{R}$ is divisible by $\mathfrak{Q}_\nu^*$; but since $\mathfrak{S} \neq \mathfrak{D}$, $\mathfrak{R}$ is not relatively prime to $\mathfrak{Q}_\nu^*$. If $\tau \geq 2$, then $\mathfrak{R}^{\tau-1}\mathfrak{R} \equiv 0(\mathfrak{Q}_\nu^*)$ while $\mathfrak{R}^{\tau-1} \not\equiv 0(\mathfrak{Q}_\nu^*)$, so again $\mathfrak{R}$ is not relatively prime to $\mathfrak{Q}_\nu^*$;[28] in both cases Theorem X, 3 then implies that $\mathfrak{R}$ is not relatively prime to $\mathfrak{S}$.

Conversely, if $\mathfrak{R}$ is not relatively prime to $\mathfrak{S}$, then by Theorem X, 1 it is not relatively prime to at least one $\mathfrak{Q}_\nu^*$. Thus

$$\mathfrak{T}_0\mathfrak{R} \equiv 0(\mathfrak{Q}_\nu^*), \qquad \mathfrak{T}_0 \not\equiv 0(\mathfrak{Q}_\nu^*),$$

and since $\mathfrak{Q}_\nu^*$ is primary,

$$\mathfrak{R}^\tau \equiv 0(\mathfrak{Q}_\nu^*), \qquad \text{hence also} \quad \mathfrak{Q}_1^\tau \cdots \mathfrak{Q}_\alpha^\tau \equiv 0(\mathfrak{Q}_\nu^*).$$

For the associated prime ideals this implies

$$\mathfrak{P}_1^{\tau\varrho_1} \cdots \mathfrak{P}_\alpha^{\tau\varrho_\alpha} \equiv 0(\mathfrak{P}_\nu^*),$$

[26] $\mathfrak{D}$ plays the role of the unit only with respect to divisibility and least common multiple, not with respect to product formation. For instance, $\mathfrak{D} = (x)$ for the domain of all integral polynomials in x without constant term; and $\mathfrak{D} = (2)$ for the domain of all even numbers.

[27] The associated prime ideals of $\mathfrak{R}$ were defined at the end of § 5.

[28] $\mathfrak{R}^0$ is not defined, because Σ need not contain a unit; hence the case $\tau = 1$ had to be dealt with first. The case $\tau = 0$ is also excluded, if Σ has a unit, by the hypothesis on $\mathfrak{S}$.

and therefore, by the property of prime ideals, $\mathfrak{P}_\nu^*$ is contained in at least one of the $\mathfrak{P}$. This proves Theorem XI.

Theorems X and XI now give the existence[29] and uniqueness of decomposition into relatively-prime irreducible ideals as follows.

Let $\mathfrak{M} = [\mathfrak{Q}_1 \cdots \mathfrak{Q}_\alpha]$ be a reduced (or at least shortest) representation of $\mathfrak{M}$ by greatest primary ideals, and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_\alpha$ be the associated prime ideals. We collect the $\mathfrak{P}$ into groups so that no ideal of one group is divisible by an ideal of a different group, while a single group cannot be split into two subgroups both having this property.

To construct such a grouping, note that by definition an individual group G must contain, together with each ideal $\mathfrak{P}$, all its divisors and multiples occurring among $\mathfrak{P}_1, \ldots, \mathfrak{P}_\alpha$ (that is, all ideals divisible by $\mathfrak{P}$). Let $\mathfrak{P}^{(i_1)}$ denote all multiples of $\mathfrak{P}$, $\mathfrak{P}_{j_1}^{(i_1)}$ all divisors of $\mathfrak{P}^{(i_1)}$, $\mathfrak{P}_{j_1}^{(i_1 i_2)}$ all multiples of $\mathfrak{P}_{j_1}^{(i_1)}$, and so on; in general, let $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$ denote all multiples of $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_{\lambda-1})}$, and $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$ all divisors of $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$. Since only finitely many ideals $\mathfrak{P}$ are involved altogether, the procedure must terminate after finitely many steps, that is, must cease to produce an ideal different from all preceding ones. The totality of ideals $\mathfrak{P}$ so obtained does indeed form a group G with the required properties.

For by definition G contains, together with each $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_{\lambda-1})}$, all multiples $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$, and, together with each $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$, all divisors $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$. These include all divisors of $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_{\lambda-1})}$, while the multiples of $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$ are themselves again among the $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$. Thus the ideals not contained in G can be neither divisors nor multiples of those contained in G.

The group G also satisfies the irreducibility condition. For if a division into two subgroups $G^{(1)}$ and $G^{(2)}$ were possible, and $G^{(1)}$ contained, say, $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$ (respectively $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$), it would also contain all preceding ideals, since these are alternately multiples and divisors (respectively divisors and multiples), hence also $\mathfrak{P}$ and therefore the entire group G. Applying the same procedure to the ideals not contained in G yields a grouping $G_1, \ldots, G_\sigma$ of all the $\mathfrak{P}$ with the required properties. Such a grouping is unique: for if $G_1', \ldots, G_\tau'$ were a second grouping and $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$ (respectively $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$) were an element of G_i', then by the preceding argument G_i' would contain the entire group G and hence, by the irreducibility property, would be identical with G.

Let $\mathfrak{Q}_{i\mu}$, where μ runs from 1 to λ_i, denote the ideals $\mathfrak{Q}$ whose associated prime ideals are collected in a group G_i. Since the $\mathfrak{P}$ are all distinct, the primary ideals $\mathfrak{Q}_{i\mu}$ belonging to a shortest representation are uniquely determined. Put

$$\mathfrak{R}_i = [\mathfrak{Q}_{i1} \cdots \mathfrak{Q}_{i\lambda_i}], \qquad \text{then} \quad \mathfrak{M} = [\mathfrak{R}_1 \cdots \mathfrak{R}_\sigma].$$

Theorem XI remains applicable even if $\mathfrak{R}_i$ is only a shortest representation, since by the addendum to Theorem IX its associated prime ideals are already well-defined. Because no associated prime ideal of $\mathfrak{R}_i$ is divisible by one of $\mathfrak{R}_j$, and conversely, Theorem XI shows that $\mathfrak{R}_i$ and $\mathfrak{R}_j$ are mutually relatively prime; and each $\mathfrak{R}_i$ is relatively-prime irreducible by the irreducibility property of the group G_i. By Lemma V the representation is reduced. Conversely, every decomposition into relatively-prime irreducible ideals leads, by Theorem XI, to the grouping just described.

Now let

$$\mathfrak{M} = [\bar{\mathfrak{R}}_1 \cdots \bar{\mathfrak{R}}_\tau]$$

be a second representation of $\mathfrak{M}$ by relatively-prime irreducible ideals. It is reduced by Lemma V. Decomposing the $\mathfrak{R}$ into greatest primary ideals shows that the associated prime ideals agree, and hence the groupings of these prime ideals agree. Thus $\tau = \sigma$, and the notation may be chosen so that $\mathfrak{R}_i$ and $\bar{\mathfrak{R}}_i$ belong to the same group. If

$$\mathfrak{M} = [\mathfrak{R}_i, \mathfrak{L}_i] = [\bar{\mathfrak{R}}_i, \bar{\mathfrak{L}}_i]$$

is the representation by ideal and complement, then, since $\bar{\mathfrak{R}}_i$ is assigned to the same group as $\mathfrak{R}_i$, Theorem XI gives that $\mathfrak{L}_i$ is relatively prime to $\bar{\mathfrak{R}}_i$, and $\bar{\mathfrak{L}}_i$ is relatively prime to $\mathfrak{R}_i$. From

$$\mathfrak{R}_i \mathfrak{L}_i \equiv 0(\bar{\mathfrak{R}}_i), \qquad \bar{\mathfrak{R}}_i \bar{\mathfrak{L}}_i \equiv 0(\mathfrak{R}_i)$$

therefore follows

$$\mathfrak{R}_i \equiv 0(\bar{\mathfrak{R}}_i), \qquad \bar{\mathfrak{R}}_i \equiv 0(\mathfrak{R}_i), \qquad \mathfrak{R}_i = \bar{\mathfrak{R}}_i.$$

[29] The existence of the decomposition can also be proved directly, in exact analogy with the proof in § 2 of the existence of a decomposition into finitely many irreducible ideals.

Thus:

Theorem XII. *Every ideal can be represented uniquely as the least common multiple of finitely many mutually relatively prime and relatively-prime irreducible ideals.*

§ 7.
Uniqueness of the Isolated Ideals.

Definition VI. *If the shortest representation* $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$ *is reduced with respect to* $\mathfrak{L}$*, then* $\mathfrak{R}$ *is called an isolated ideal if no associated prime ideal of* $\mathfrak{R}$ *is contained in an associated prime ideal of* $\mathfrak{L}$*; equivalently, if* $\mathfrak{L}$ *is relatively prime to* $\mathfrak{R}$*.*

Then the representation $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$ satisfies the conditions of the representation $\mathfrak{M} = [\mathfrak{R}_i, \mathfrak{L}_i]$ in Lemma V, and Lemma V proves:

Lemma VI. *If* $\mathfrak{R}$ *is an isolated ideal of the shortest representation* $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$*, reduced with respect to* $\mathfrak{L}$*, then the representation is also reduced with respect to* $\mathfrak{R}$*.*

Thus isolated ideals occur only in reduced representations. The associated prime ideals arising in the decompositions of $\mathfrak{R}$ and $\mathfrak{L}$ into irreducible ideals complement one another to the uniquely determined associated prime ideals arising in the corresponding decomposition of $\mathfrak{M}$. Hence no associated prime ideal belonging to the decomposition of $\mathfrak{R}$ into irreducible ideals is contained in the remaining associated prime ideals of $\mathfrak{M}$. Conversely, if this condition is satisfied and $\mathfrak{R}$ occurs in at least one representation $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$ reduced with respect to $\mathfrak{R}$, and hence also in a reduced representation $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}^*]$, then $\mathfrak{R}$ is isolated by Definition VI. This gives the following definition, independent of the particular complement $\mathfrak{L}$.

Definition VIa. $\mathfrak{R}$ *is called an isolated ideal if the prime ideals belonging to its decomposition into irreducible ideals are not contained in the other associated prime ideals belonging to the corresponding decomposition of* $\mathfrak{M}$*, and if* $\mathfrak{R}$ *occurs in at least one representation* $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$ *reduced with respect to* $\mathfrak{R}$*.*[30]

Suppose

$$\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}] = [\bar{\mathfrak{R}}, \bar{\mathfrak{L}}]$$

are two representations of $\mathfrak{M}$ by isolated ideals $\mathfrak{R}$ and $\bar{\mathfrak{R}}$, with complements $\mathfrak{L}$ and $\bar{\mathfrak{L}}$, such that the associated prime ideals of $\mathfrak{R}$ and $\bar{\mathfrak{R}}$ agree. Replace $\mathfrak{L}$ and $\bar{\mathfrak{L}}$ by divisors $\mathfrak{L}^*$ and $\bar{\mathfrak{L}}^*$ so that the representations become reduced. Then the associated prime ideals of $\mathfrak{L}^*$ and $\bar{\mathfrak{L}}^*$ also agree; by Theorem XI, $\mathfrak{L}^*$ is relatively prime to $\bar{\mathfrak{R}}$ and $\bar{\mathfrak{L}}^*$ is relatively prime to $\mathfrak{R}$. Since

$$\mathfrak{R}\mathfrak{L}^* \equiv 0(\bar{\mathfrak{R}}), \qquad \bar{\mathfrak{R}}\bar{\mathfrak{L}}^* \equiv 0(\mathfrak{R}),$$

we obtain

$$\mathfrak{R} \equiv 0(\bar{\mathfrak{R}}), \qquad \bar{\mathfrak{R}} \equiv 0(\mathfrak{R}), \qquad \mathfrak{R} = \bar{\mathfrak{R}}.$$

Thus isolated ideals are uniquely determined by their associated prime ideals. This sharpens Theorems VII and IX on decompositions into irreducible, respectively greatest primary, ideals; by the addendum to Theorem IX it is enough to assume a shortest representation. In summary:

Theorem XIII. *In every shortest representation of an ideal as the least common multiple of irreducible, respectively greatest primary, ideals, the isolated irreducible, respectively greatest primary, ideals are uniquely determined; the ambiguity concerns only the non-isolated irreducible, respectively greatest primary, ideals.*[31] *In general, isolated ideals are uniquely determined by their associated prime ideals.*

If in such a shortest representation by irreducible, respectively greatest primary, ideals the ideals $\mathfrak{B}_i$, respectively $\mathfrak{Q}_j$, are non-isolated, then by definition their complements $\mathfrak{U}_i$, respectively $\mathfrak{L}_j$, are divisible by $\mathfrak{P}_i$, respectively $\mathfrak{P}_j$. Hence

$$\mathfrak{U}_i^{\varrho_i} \equiv 0(\mathfrak{B}_i) \qquad \text{respectively} \qquad \mathfrak{L}_j^{\sigma_j} \equiv 0(\mathfrak{Q}_j).$$

Conversely, if these relations hold, then $\mathfrak{P}_i$, respectively $\mathfrak{P}_j$, is contained in at least one associated prime ideal of the complement, and hence, by the addendum to Theorem IX, in an associated prime ideal of the divisor $\mathfrak{L}_j^*$ of $\mathfrak{L}_j$ that supplies a representation reduced with respect to $\mathfrak{L}_j^*$. Thus $\mathfrak{B}_i$, respectively $\mathfrak{Q}_j$, is non-isolated. In particular, irreducible ideals $\mathfrak{B}_i$ whose associated prime ideal occurs more than once in the decomposition of $\mathfrak{M}$ are always non-isolated. *Non-isolated primary ideals are therefore also characterized by the fact that a power of every complement is divisible by them; isolated primary ideals by the fact that this cannot occur.*

[30] If one introduced ordinary associated prime ideals (end of § 5), then one would have to add the special condition that those of $\mathfrak{L}$ are all distinct from those of $\mathfrak{R}$. With Definition VIa, the representation no longer has to be assumed reduced with respect to the complement.

[31] For ideals in polynomial domains, this theorem was already stated without proof by Macaulay in the case of decomposition into greatest primary ideals; his definition of isolated and non-isolated (imbedded) primary ideals can be regarded as an irrational form of the one given below.

§ 8.

Unique Representation of an Ideal as a Product of Coprime-Irreducible Ideals.

If the underlying ring domain Σ has a unit, that is, an element ε such that $\varepsilon a = a$ for every element of Σ,[32] then coprime ideals can be defined as follows.

Definition VIII. *Two ideals $\mathfrak{R}$ and $\mathfrak{S}$ are called coprime if their greatest common divisor is the unit ideal $\mathfrak{D} = (\varepsilon)$ consisting of all elements of Σ. An ideal is called coprime-irreducible if it cannot be represented as the least common multiple of pairwise coprime ideals.*

Note that two coprime ideals are always mutually relatively prime. By definition there are elements $r \equiv 0(\mathfrak{R})$ and $s \equiv 0(\mathfrak{S})$ with $\varepsilon = r + s$. From $\mathfrak{T}\mathfrak{R} \equiv 0(\mathfrak{S})$ it follows that $\mathfrak{T}r \equiv 0(\mathfrak{S})$, hence $\mathfrak{T}\varepsilon = \mathfrak{T} \equiv 0(\mathfrak{S})$; correspondingly, from $\bar{\mathfrak{T}}\mathfrak{S} \equiv 0(\mathfrak{R})$ it follows that $\bar{\mathfrak{T}} \equiv 0(\mathfrak{R})$.[33] Thus Lemma V implies that every representation by pairwise coprime ideals is also reduced.

The uniqueness proof rests on the analogue of Theorem X:

Theorem XIV. *If $\mathfrak{R}$ is coprime to each of the ideals $\mathfrak{S}_1, \ldots, \mathfrak{S}_\lambda$, then $\mathfrak{R}$ is also coprime to $\mathfrak{S} = [\mathfrak{S}_1 \cdots \mathfrak{S}_\lambda]$. Conversely, if $\mathfrak{R}$ and $\mathfrak{S}$ are coprime, then $\mathfrak{R}$ is coprime to each $\mathfrak{S}_j$. If $\mathfrak{R} = [\mathfrak{R}_1 \cdots \mathfrak{R}_\mu]$ and every $\mathfrak{R}_i$ is coprime to every $\mathfrak{S}_j$, then $\mathfrak{R}$ and $\mathfrak{S}$ are coprime; here too the converse holds.*

Indeed, if $\mathfrak{R}$ is coprime to every $\mathfrak{S}_j$, then there are elements s_j such that

$$s_j \equiv 0(\mathfrak{S}_j), \qquad s_j \equiv \varepsilon(\mathfrak{R}).$$

Consequently

$$s_1 s_2 \cdots s_\lambda \equiv 0(\mathfrak{S}), \qquad s_1 s_2 \cdots s_\lambda \equiv \varepsilon(\mathfrak{R}), \qquad (\mathfrak{R}, \mathfrak{S}) = (\varepsilon).$$

Since $(\mathfrak{R}, \mathfrak{S})$ is divisible by each $(\mathfrak{R}, \mathfrak{S}_j)$, the converse follows. Repeated application of the same argument gives the second part. For if $\mathfrak{R}_i$ is coprime to $\mathfrak{S}_1, \ldots, \mathfrak{S}_\lambda$ for a fixed i, then $\mathfrak{R}_i$ is coprime to $\mathfrak{S}$; if this holds for every i, then, since coprimeness is mutual, $\mathfrak{S}$ is coprime to $\mathfrak{R}$. Conversely, coprimeness of $\mathfrak{R}$ and $\mathfrak{S}$ gives coprimeness of $\mathfrak{S}$ with $\mathfrak{R}_i$, and hence of $\mathfrak{R}_i$ with $\mathfrak{S}$.

The proof of existence and uniqueness[34] of the decomposition into coprime-irreducible ideals is, as in the corresponding proof for relatively-prime ideals, a matter of a unique grouping. Since, however, the relatively-prime irreducible ideals $\mathfrak{R}_1, \ldots, \mathfrak{R}_\sigma$ of $\mathfrak{M}$ are uniquely defined by Theorem XII, it is unnecessary here to go back to the associated prime ideals.

We collect the uniquely defined relatively-prime irreducible ideals $\mathfrak{R}_1, \ldots, \mathfrak{R}_\sigma$ of $\mathfrak{M}$ into groups so that *every ideal of one group is coprime to every ideal of any different group, while a single group cannot be split into two subgroups such that every ideal of one subgroup is coprime to every ideal of the other subgroup.* Such a grouping is obtained as follows. By definition a group G must contain, together with every ideal $\mathfrak{R}$, all ideals not coprime to $\mathfrak{R}$. Let these be $\mathfrak{R}_{i_1}$; let $\mathfrak{R}_{i_1 i_2}$ be the ideals not coprime to these; in general let $\mathfrak{R}_{i_1 \ldots i_\lambda}$ be not coprime to $\mathfrak{R}_{i_1 \ldots i_{\lambda-1}}$. Since only finitely many ideals occur, this process terminates after finitely many steps. The set of ideals so obtained forms a group G with the desired properties: all ideals outside G are, by construction, coprime to all ideals in G. If G were split into two subgroups $G^{(1)}$ and $G^{(2)}$, and if $\mathfrak{R}_{i_1 \ldots i_\lambda}$ belonged to $G^{(1)}$, then, because coprimeness is mutual, $G^{(1)}$ would also have to contain $\mathfrak{R}_{i_1 \ldots i_{\lambda-1}}, \ldots, \mathfrak{R}_{i_1}$, hence also $\mathfrak{R}$ and therefore the whole group G. This proves irreducibility. Repeating the construction with the remaining ideals gives a grouping $G_1, \ldots, G_\tau$ of all $\mathfrak{R}$.

The grouping is unique: if $G'_1, \ldots, G'_\tau$ is a second grouping and $\mathfrak{R}_{i_1 \ldots i_\lambda}$ is an element of G'_i, then G'_i contains $\mathfrak{R}$ and hence G_1, and, by the irreducibility condition, cannot contain elements different from G_1; therefore $G'_i = G_1$.

Let $\mathfrak{T}_i$ be the least common multiple of the ideals $\mathfrak{R}$ united in a group G_i. We show that

$$\mathfrak{M} = [\mathfrak{T}_1 \cdots \mathfrak{T}_\tau]$$

is a representation of $\mathfrak{M}$ by coprime-irreducible ideals. Decomposing the $\mathfrak{T}$ into the $\mathfrak{R}$ first shows that $[\mathfrak{T}_1 \cdots \mathfrak{T}_\tau]$ really represents $\mathfrak{M}$. By Theorem XIV the $\mathfrak{T}$ are pairwise coprime, and each $\mathfrak{T}$ is coprime-irreducible. This proves the existence of such a representation.

For uniqueness, let $\mathfrak{M} = [\bar{\mathfrak{T}}_1 \cdots \bar{\mathfrak{T}}_\tau]$ be a second representation of this type. Decomposing the $\bar{\mathfrak{T}}$ into relatively-prime irreducible ideals $\mathfrak{R}$, Theorem XIV shows that ideals $\mathfrak{R}$ occurring in different $\bar{\mathfrak{T}}$ are coprime

[32] Because multiplication is commutative, Σ can of course have at most one unit: for any two units ε_1 and ε_2, one has $\varepsilon_1 \varepsilon_2 = \varepsilon_2 = \varepsilon_1$.

[33] The converse is false: for example, $\mathfrak{R} = (x)$ and $\mathfrak{S} = (y)$ are mutually relatively prime, but not coprime.

[34] The existence of the decomposition can again be proved directly in analogy with § 2; the uniqueness proof too can be carried out directly (compare what was said in the introduction about Schmeidler and Noether–Schmeidler). The proof given here also gives insight into the structure of coprime-irreducible ideals.

to one another, hence also mutually relatively prime; therefore they agree with the uniquely defined relatively-prime irreducible ideals $\mathfrak{R}$ of $\mathfrak{M}$. The ideals $\bar{\mathfrak{T}}_i$ also induce, by Theorem XIV, a grouping G_i' of the $\mathfrak{R}$ with the stated properties. Since this grouping is unique and each $\bar{\mathfrak{T}}_i$ is uniquely determined by the group $G_i' = G_i$, one has $\bar{\mathfrak{T}}_i = \mathfrak{T}_i$; uniqueness is proved.

For pairwise coprime ideals, the least common multiple is moreover equal to the product. For by Theorem XIV, if $\mathfrak{M} = [\mathfrak{T}_1 \cdots \mathfrak{T}_\tau]$, the complement $\mathfrak{L}_i$ is also coprime to $\mathfrak{T}_i$; hence there are elements

$$t_i \equiv 0(\mathfrak{T}_i), \qquad l_i \equiv 0(\mathfrak{L}_i), \qquad \varepsilon = t_i + l_i.$$

From $f \equiv 0(\mathfrak{T}_i)$ and $f \equiv 0(\mathfrak{L}_i)$ it follows that

$$f = f\varepsilon = ft_i + fl_i, \qquad f \equiv 0(\mathfrak{L}_i\mathfrak{T}_i).$$

Conversely $\mathfrak{L}_i\mathfrak{T}_i$ is divisible by $[\mathfrak{L}_i, \mathfrak{T}_i]$, whence $[\mathfrak{L}_i, \mathfrak{T}_i] = \mathfrak{L}_i\mathfrak{T}_i$; continuing the procedure on $\mathfrak{L}_i$ gives

$$\mathfrak{M} = [\mathfrak{T}_1 \cdots \mathfrak{T}_\tau] = \mathfrak{T}_1\mathfrak{T}_2 \cdots \mathfrak{T}_\tau.$$

Therefore:

Theorem XV. *Every ideal can be represented uniquely as a product of finitely many pairwise coprime and coprime-irreducible ideals.*

§ 9.
Extension of the investigation to modules. Equality of the number of components in decompositions into irreducible modules.

We now show that the content of the first three paragraphs, which concerns irreducible ideals and not primary and prime ideals, remains valid under weaker hypotheses. Those paragraphs do not use the commutative law of multiplication and refer only to the property of ideals of being modules. They therefore remain valid for modules with respect to non-commutative domains, which are now to be defined. The definition of modules is to be based on a double domain (Σ, T) with the following properties.

Σ *is an abstractly defined non-commutative ring*; that is, Σ is a system of elements $a, b, c, \ldots$ for which two modes of combination are defined, ring addition $(\#)$ and ring multiplication $(\times)$, satisfying the laws stated in § 1, with the exception of the commutative law 4 for ring multiplication.

T is a system of elements $\alpha, \beta, \gamma, \ldots$, for which, in connection with Σ, two combinations are likewise defined: addition, which from any two elements α, β produces a unique third element $\alpha + \beta$; and multiplication of an element α of T by an element c of Σ, which uniquely produces an element $c\alpha$ of T.[35]

For these combinations the following laws hold:

1. The associative law of addition: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
2. The commutative law of addition: $\alpha + \beta = \beta + \alpha$.
3. The law of unrestricted and unique subtraction: there is in T one and only one element ξ satisfying the equation $\alpha + \xi = \beta$ (one writes $\xi = \beta - \alpha$).
4. The associative law of multiplication: $a \cdot (b \cdot \gamma) = (a \times b) \cdot \gamma$.
5. The distributive law:

$$(a\#b) \cdot \gamma = a \cdot \gamma + b \cdot \gamma, \qquad c \cdot (\alpha + \beta) = c \cdot \alpha + c \cdot \beta.$$

From these conditions there follow, as is well known, the existence of the zero element and the validity of the distributive law also for the combination of subtraction and multiplication:

$$(a - b) \cdot \gamma = a \cdot \gamma - b \cdot \gamma, \qquad c \cdot (\alpha - \beta) = c \cdot \alpha - c \cdot \beta,$$

where $(-)$ denotes subtraction in Σ. *If* Σ *contains a unit* ε*, then* $\varepsilon \cdot \alpha = \alpha$ *is to hold for every element* α *of* T.

By a module M in (Σ, T) we mean a system of elements of T satisfying the two conditions:

[35] Thus here one is dealing with a "right-sided" multiplication, a "right-sided" domain T, and consequently with "right-sided" modules and ideals. If one were to base T instead on a left-sided multiplication αc, a corresponding theory of left-sided modules and ideals would result; M would contain αc along with α. The associative law would then have the form $(\gamma b)a = \gamma(b \times a)$.

1. *Along with α, M contains $c \cdot \alpha$, where c is any element of Σ.*

2. *Along with α and β, M contains the difference $\alpha - \beta$*; hence also $n\alpha$ for every integer n.[36]

By this definition, T itself forms a module in (Σ, T). If in particular the domain T and the combinations established there coincide with the domain Σ and the combinations valid there, then the module M becomes a right ideal M in Σ. If Σ is also assumed commutative, the ordinary concept of ideal results, and is thus a special case of the concept of module.[37]

For modules all definitions of § 1 remain valid. Thus $\alpha \equiv 0\,(M)$, respectively $N \equiv 0\,(M)$, means that α, respectively every element of N, is an element of M; in other words, α, respectively N, is divisible by M. M is a proper divisor of N if M contains elements different from those of N; from $N \equiv 0\,(M)$ and $M \equiv 0\,(N)$ follows $M = N$. The definitions of greatest common divisor and least common multiple likewise remain literally the same. If, in particular, the module M contains a finite number of elements $\alpha_1, \ldots, \alpha_e$ such that $M = (\alpha_1 \ldots \alpha_e)$, that is,

$$\alpha = c_1\alpha_1 + \cdots + c_e\alpha_e + n_1\alpha_1 + \cdots + n_e\alpha_e$$

for every $\alpha \equiv 0\,(M)$, where the c_i are elements of Σ and the n_i are integers, then M is called a *finite module*, and $\alpha_1, \ldots, \alpha_e$ a *module basis*.

In what follows we assume, just as in § 1, only those domains (Σ, T) that satisfy the finiteness condition: every module in (Σ, T) is finite, and hence has a module basis.

For such a domain (Σ, T), Theorem I on finite chains holds also for modules, as the proof given there shows, and therefore all hypotheses for §§ 2 and 3 are satisfied. Definition I and Lemma I on shortest and reduced representations carry over directly; likewise Theorem II on the representability of every module as the least common multiple of finitely many irreducible modules, where Lemma II shows that every shortest representation of this kind is at the same time reduced. Theorem III also remains valid, expressing reducibility of a module through properties of its complement; from it follows Lemma III, and finally Theorem IV, which asserts equality of the number of components in two different shortest representations of a module as the least common multiple of irreducible modules. Theorem IV also gives Lemma IV as the converse of Lemma I on reduced representations.

Addendum. The same argument shows that all these theorems and definitions remain valid if, for two-sided domains T, that is, domains which are both right- and left-sided, one everywhere understands by a module a two-sided module: one which, along with α, also contains $c\alpha$ and αc, and along with α and β also contains $\alpha - \beta$.

While all these theorems rest only on the concept of divisibility and of least common multiple, the further uniqueness theorems rest essentially on the product concept and therefore do not admit a direct transfer. Thus the definition of a primary ideal and of a prime ideal cannot be transferred to modules, since the product of two elements of T is not defined. The formally possible transfer to non-commutative rings loses its meaning, since here the existence of the associated prime ideal cannot be proved[38] and the proof that an irreducible ideal is primary also fails. These two facts form the basis of the following uniqueness theorems. By contrast, if the non-commutative ring has a unit, coprime and coprime-irreducible ideals can be defined, and the arguments used in the proof of Theorem II show that every ideal can be represented as the least common multiple of finitely many pairwise coprime and coprime-irreducible ideals.[39]

Finally, we mention a sufficient criterion for the finiteness condition to hold in (Σ, T): if Σ contains a unit and satisfies the finiteness condition, and if T itself is a finite module in (Σ, T), then every module in (Σ, T) is finite.

Indeed, from the existence of the unit in Σ, for

$$\mathfrak{M} = (f_1, \ldots, f_e), \qquad f = \bar{b}_1 f_1 + \cdots + \bar{b}_e f_e + n_1 f_1 + \cdots + n_e f_e,$$

where the $\bar{b}_i$ are elements of Σ and the n_i are integers, there follows also a representation

$$f = b_1 f_1 + \cdots + b_e f_e$$

[36] The integers are again to be understood as abbreviating symbols, not as ring elements.

[37] The simplest example of a module is the module of integral linear forms: here Σ consists of all rational integers and T of all integral linear forms. A somewhat more general module arises when, in Σ and T, one takes algebraic integers instead of rational integers, or for instance all even integers. If, instead of the linear forms, one considers each complex of coefficients as an element, then the combinations in Σ and T are in fact different. Ideals in non-commutative polynomial ring domains are the subject of the joint paper of Noether–Schmeidler. Ideals in other special non-commutative domains are treated in Hurwitz's lectures on the number theory of quaternions (Berlin, Springer 1919) and in the works of Du Pasquier cited there.

[38] For from $p_1^\rho \equiv 0\,(\mathfrak{Q})$ and $p_2^\sigma \equiv 0\,(\mathfrak{Q})$ it does not follow here that $(p_1 - p_2)^{\rho+\sigma} \equiv 0\,(\mathfrak{Q})$; likewise, from $(ab)^\rho \equiv 0\,(\mathfrak{Q})$ it does not follow that $a^\rho b^\rho \equiv 0\,(\mathfrak{Q})$. Thus $\mathfrak{P}$ can be proved neither to be an ideal nor to have the property of a prime ideal. For two-sided ideals $\mathfrak{P}$ can indeed be proved to be an ideal, but not a prime ideal.

[39] For special, "completely reducible" ideals, uniqueness theorems can be set up here too; compare the joint paper Noether–Schmeidler.

with the b_i in Σ. For since $f_i = \varepsilon f_i$, one has $n_i f_i = n_i \varepsilon f_i$, and since $n_i \varepsilon = (\varepsilon + \cdots + \varepsilon)$ belongs to Σ, $b_i = \bar{b}_i + n_i \varepsilon$ is an element of Σ. The hypothesis on T says that every element α of T admits a representation

$$\alpha = \bar{a}_1 \tau_1 + \cdots + \bar{a}_k \tau_k + n_1 \tau_1 + \cdots + n_k \tau_k,$$

and hence

$$\alpha = a_1 \tau_1 + \cdots + a_k \tau_k,$$

the second representation following from the first just as above because $\varepsilon \tau_i = \tau_i$.

As α runs through the elements of a module M in (Σ, T), the coefficients a_k of τ_k run through an ideal $\mathfrak{M}_k$ of Σ; by the preceding, for every $a_k \equiv 0\,(\mathfrak{M}_k)$ one has

$$a_k = b_1 a_k^{(1)} + \cdots + b_e a_k^{(e)}.$$

Let $\alpha^{(i)}$ be an element of M for which the coefficient of τ_k is $a_k^{(i)}$. Then $\alpha - b_1 \alpha^{(1)} - \cdots - b_e \alpha^{(e)}$ is an element belonging to M which depends only on $\tau_1, \ldots, \tau_{k-1}$. The procedure can be repeated for the totality of these elements, which no longer contain τ_k and which form a module M', and the assertion is proved by finitely many repetitions.

§ 10.
Special case of the polynomial domain.

1. Let the underlying ring domain Σ consist of all polynomials in $x_1, \ldots, x_n$ with arbitrary complex coefficients. By Hilbert's basis theorem (Ann. 36) the finiteness condition holds for it. The issue is the relation of our theorems to the known theorems of elimination theory and module theory.

This relation is established by the following special case of a known theorem of Hilbert:[40]

If f vanishes for every finite system of values of $x_1, \ldots, x_n$ that is a zero of all polynomials of a prime ideal $\mathfrak{P}$ (a zero of $\mathfrak{P}$), then f is divisible by $\mathfrak{P}$. In other words, a prime ideal $\mathfrak{P}$ consists of the totality of polynomials which vanish at its zeros.[41]

Thus, if a product fg vanishes for all zeros of $\mathfrak{P}$, at least one factor vanishes; the zeros form an irreducible algebraic variety. Conversely, if this definition of irreducible variety is adopted, then the totality of polynomials vanishing on an irreducible variety forms a prime ideal. Prime ideal and irreducible variety therefore correspond one-to-one. Since $\mathfrak{Q} \equiv 0\,(\mathfrak{P})$ and $\mathfrak{P}^e \equiv 0\,(\mathfrak{Q})$, the zeros of a primary ideal coincide with those of its associated prime ideal.[42] Therefore the representation of an ideal as the least common multiple of greatest primary ideals gives a resolution of all zeros of the ideal into irreducible varieties; and, as Lasker showed, the converse also holds. The proof of uniqueness of the associated prime ideals thus corresponds here to the fundamental theorem of elimination theory on the unique decomposability of an algebraic variety into irreducible varieties, and for special polynomial domains, where no unique product representation of the polynomials by irreducible polynomials of the domain and consequently no elimination theory exists, it can serve as an equivalent of that theorem of elimination theory.

The irreducible varieties corresponding to the isolated primary ideals are exactly those which occur in the "minimal resolvent";[43] for the zeros of every non-isolated greatest primary ideal are at the same time zeros of at least one isolated one, namely one whose associated prime ideal is divisible by that of the non-isolated ideal. The uniqueness of isolated primary ideals therefore gives, in the exponents, new invariant multiplicity numbers. The uniqueness theorems for the resolution of primary ideals into irreducible ones can likewise be regarded as supplements to elimination theory in the sense of multiplicity.

After these remarks the different decompositions can be interpreted in terms of their behavior with respect to algebraic varieties. Pairwise coprime ideals correspond to varieties having no common zero; for mutually relatively prime ideals, no irreducible variety of one ideal is at the same time a common zero; the

[40] Über die vollen Invariantensysteme. Math. Ann. 42 (1893), § 3, p. 313.

[41] As Lasker showed [Math. Ann. 60 (1905), p. 607], this special case can also be proved directly for homogeneous forms; conversely, Hilbert's theorem follows again from it in the homogeneous and inhomogeneous cases. We can express that theorem as follows: if an ideal $\mathfrak{R}$ vanishes at all zeros of M, then a power of $\mathfrak{R}$ is divisible by M. This theorem, and also the special case, holds only if the range of values of the x is algebraically closed; hence it cannot follow from our theorems alone, but must use the existence of roots, for example at the point where one uses that an ideal whose zeros consist only of $x_1 = 0, \ldots, x_n = 0$ contains all products of powers of the x from some dimension on. The remaining proof can be somewhat simplified in comparison with Lasker by using our theorems. For Lasker must also appeal to Hilbert's theorem to prove the decomposition of an ideal into greatest primary ideals.

[42] Macaulay (compare the introduction) takes this property of a primary ideal, namely to possess an irreducible variety, as the definition; Lasker includes only the concept of the manifold of a variety in the definition and otherwise defines abstractly. The primary ideals vanishing only for $x_1 = 0, \ldots, x_n = 0$ occupy a special position for Lasker.

[43] Compare, for example, J. König, Einleitung in die allgemeine Theorie der algebraischen GröSSen (Leipzig, Teubner, 1903), p. 235.

greatest primary ideals vanish only on irreducible varieties which are all distinct from one another; in the decomposition into irreducible ideals the same irreducible varieties may occur with multiplicity.

It should also be noted that, instead of the general polynomial domain, the domain of all homogeneous forms may also be taken as the basis; for one readily verifies that the general theorems remain valid for the combinations there in force, where addition is defined only for forms of the same dimension.[44]

A simplest example of the four different decompositions - for which the formulas follow below - is given, according to the preceding, by a line and two intersecting lines skew to it, one of the latter containing, with higher multiplicity, a point different from the point of intersection. The decomposition into coprime-irreducible ideals corresponds to the decomposition into the line and the variety skew to it; in the decomposition into relatively-prime irreducible ideals this variety splits into the two lines; the decomposition into greatest primary ideals corresponds to separating off the point of higher multiplicity, while the decomposition into irreducible ideals forces a resolution of that point.

Taking this point as the origin, the running line as the y-axis, the line intersecting it parallel to the x-axis, and the line skew to it parallel to the z-axis, such a configuration is represented, for example, by the following *irreducible ideals*[45]:

$$\mathfrak{B}_1 = (x-1, y); \qquad \mathfrak{B}_2 = (y-1, z); \qquad \mathfrak{B}_3 = (x, z); \qquad \mathfrak{B}_4 = (x^3, y, z);$$
$$\mathfrak{B}_5 = (x^2, y^2, z).$$

The *associated prime ideals* are:

$$\mathfrak{P}_1 = \mathfrak{B}_1; \qquad \mathfrak{P}_2 = \mathfrak{B}_2; \qquad \mathfrak{P}_3 = \mathfrak{B}_3; \qquad \mathfrak{P}_4 = \mathfrak{P}_5 = (x, y, z).$$

The *greatest primary ideals* are:

$$\mathfrak{Q}_1 = \mathfrak{B}_1; \qquad \mathfrak{Q}_2 = \mathfrak{B}_2; \qquad \mathfrak{Q}_3 = \mathfrak{B}_3; \qquad \mathfrak{Q}_4 = [\mathfrak{B}_4, \mathfrak{B}_5] = (x^3, y^2, x^2y, z).$$

The *relatively-prime irreducible ideals* are:

$$\mathfrak{R}_1 = \mathfrak{Q}_1; \qquad \mathfrak{R}_2 = \mathfrak{Q}_2; \qquad \mathfrak{R}_3 = [\mathfrak{Q}_3, \mathfrak{Q}_4] = (x^3, x^2y, xy^2, z).$$

The *coprime-irreducible ideals* are:

$$\mathfrak{S}_1 = \mathfrak{R}_1; \qquad \mathfrak{S}_2 = [\mathfrak{R}_2, \mathfrak{R}_3] = ((y-1)x^3, (y-1)x^2y, (y-1)xy^2, z).$$

This gives the *total ideal*:

$\mathfrak{M} = [\mathfrak{S}_1, \mathfrak{S}_2] = \mathfrak{S}_1 \cdot \mathfrak{S}_2$
$= ((x-1)(y-1)x^3, (y-1)x^2y, (y-1)xy^2, (x-1)z, y(y-1)x^3, yz),$

where
$$1 = -(y-1)x^3 + (y-1)(x^3-1) + y,$$
$$(y-1)(x^3-1) + y \equiv 0\,(\mathfrak{S}_1); \qquad -(y-1)x^3 \equiv 0\,(\mathfrak{S}_2).$$

Here the ideals $\mathfrak{B}_1$, $\mathfrak{B}_2$, and $\mathfrak{B}_3$ are isolated, and hence uniquely determined also in the decompositions into irreducible and greatest primary ideals. The ideals $\mathfrak{B}_4$ and $\mathfrak{B}_5$, respectively $\mathfrak{Q}_4$, are non-isolated; they are not uniquely determined, but can, for example, be replaced by

$$\mathfrak{D}_4 = (x^3, y + \lambda x^2, z); \qquad \mathfrak{D}_5 = (x^2 + \mu xy, y^2, z).$$

Likewise, $\mathfrak{Q}_4$ can be replaced by

$$\overline{\mathfrak{Q}}_4 = (x^3, x^2y, y^2 + \lambda xy, z).$$

2. Just as the general, and the integral, polynomial domains satisfy the finiteness condition, so does every finite integral domain of polynomials, by Hilbert's theorem on module bases;[46] the coefficients may be assigned to an arbitrary field. We give one more example, for the domain of all even polynomials, the simplest domain in which, because $x^2y^2 = (xy)^2$, no unique product representation of the polynomials by irreducible polynomials of the domain exists. It is the same configuration as in the preceding example, now given by the irreducible ideals

$$\mathfrak{B}_1 = (x^2-1, xy, y^2, yz), \quad \mathfrak{B}_2 = (y^2-1, xz, yz, z^2),$$
$$\mathfrak{B}_3 = (x^2, xy, xz, yz, z^2), \quad \mathfrak{B}_4 = (x^4, x^3y, y^2, xz, yz, z^2),$$
$$\mathfrak{B}_5 = (x^2, y^2, xz, yz, z^2).$$

[44] That in the ambiguous case inhomogeneous decompositions can exist beside homogeneous ones is shown by the example $(x^3, xy, y^3) = [(x^3, y), (y^3, x)] = [(xy, x^3, y^3, x+y^3), (xy, x^3, y^3, y+x^2)]$.

[45] Of these, the first three are irreducible as prime ideals; $\mathfrak{B}_4$ because it has only the divisors (x^2, y, z) and (x, y, z); $\mathfrak{B}_5$ because every divisor contains the polynomial xy.

[46] Conversely, if a polynomial domain satisfies the finiteness condition and every polynomial has at least one representation in which the multipliers are of lower degree in x, then the domain is a finite integral domain.

The associated prime ideals are

$$\mathfrak{P}_1 = \mathfrak{B}_1, \quad \mathfrak{P}_2 = \mathfrak{B}_2, \quad \mathfrak{P}_3 = \mathfrak{B}_3, \quad \mathfrak{P}_4 = \mathfrak{P}_5 = (x^2, xy, y^2, xz, yz, z^2).$$

That $\mathfrak{P}_1$ is a prime ideal follows from the fact that every polynomial of the domain has the form

$$f = \varphi(z^2) + xz\,\psi(z^2) \pmod{\mathfrak{P}_1}.$$

Thus if

$$f_1 = \varphi_1(z^2) + xz\,\psi_1(z^2), \qquad f_2 = \varphi_2(z^2) + xz\,\psi_2(z^2),$$

then from $f_1 f_2 \equiv 0\,(\mathfrak{P}_1)$ one obtains the equations

$$\varphi_1\varphi_2 + z^2\psi_1\psi_2 = 0, \qquad \varphi_2\psi_1 + \varphi_1\psi_2 = 0,$$

and hence $f_1 \equiv 0\,(\mathfrak{P}_1)$ or $f_2 \equiv 0\,(\mathfrak{P}_1)$. In exactly the same way one sees that $\mathfrak{P}_2$ is a prime ideal; $\mathfrak{P}_3$ is a prime ideal because every polynomial of the domain modulo $\mathfrak{P}_3$ is congruent to a polynomial in y^2; $\mathfrak{P}_4$ consists of all polynomials of the domain. Thus $\mathfrak{B}_1$, $\mathfrak{B}_2$, and $\mathfrak{B}_3$ are irreducible as prime ideals, while $\mathfrak{B}_4$ and $\mathfrak{B}_5$ each have only the single proper divisor $\mathfrak{P}_4$, and hence are necessarily irreducible.

From the irreducible ideals one obtains the greatest primary ideals

$$\mathfrak{Q}_1 = \mathfrak{B}_1, \quad \mathfrak{Q}_2 = \mathfrak{B}_2, \quad \mathfrak{Q}_3 = \mathfrak{B}_3, \quad \mathfrak{Q}_4 = [\mathfrak{B}_4, \mathfrak{B}_5] = (x^4, x^3y, y^2, xz, yz, z^2),$$

the relatively-prime irreducible ideals

$$\mathfrak{R}_1 = \mathfrak{Q}_1, \quad \mathfrak{R}_2 = \mathfrak{Q}_2, \quad \mathfrak{R}_3 = [\mathfrak{Q}_3, \mathfrak{Q}_4] = (x^4, x^3y, x^2y^2, xy^3, xz, yz, z^2),$$

and the coprime-irreducible ideals

$$\mathfrak{S}_1 = \mathfrak{R}_1, \quad \mathfrak{S}_2 = [\mathfrak{R}_2, \mathfrak{R}_3] = ((y^2-1)x^4, (y^2-1)x^3y, (y^2-1)x^2y^2, (y^2-1)xy^3, xz, yz, z^2).$$

As in the first example,

$$[\mathfrak{B}_4, \mathfrak{B}_5] = [\mathfrak{D}_4, \mathfrak{D}_5], \qquad [\mathfrak{Q}_3, \mathfrak{Q}_4] = [\mathfrak{Q}_3, \overline{\mathfrak{Q}}_4],$$

where

$$\mathfrak{D}_4 = (x^4, xy + \lambda x^2, \ldots), \qquad \mathfrak{D}_5 = (x^2 + \mu xy, \ldots), \qquad \lambda\mu \neq 1,$$

and

$$\overline{\mathfrak{Q}}_4 = (x^4, x^3y, y^2 + \lambda xy, \ldots).$$

The remaining irreducible, respectively greatest primary, ideals $\mathfrak{B}_1$, $\mathfrak{B}_2$, $\mathfrak{B}_3$ are uniquely determined as isolated ideals.

§ 11.
Examples from Number Theory and the Theory of Differential Expressions.

1. Let the underlying domain Σ consist of all even rational integers. Thus Σ can be put in one-to-one correspondence with the domain of all rational integers, by assigning to each number $2a$ in Σ the number a. It follows at once that every ideal in Σ is a principal ideal $(2a)$, where in the basis representation $2c = n \cdot 2a$ for every element $2c$ of the ideal, the odd integers n are only abbreviations for finite sums.

The prime ideals of the domain are $\mathfrak{P}_0 = \mathfrak{D} = (2)$ and $\mathfrak{P} = (2p)$, where p denotes an odd prime number; every prime ideal is therefore divisible by $\mathfrak{P}_0$, but by no further prime ideal. The primary ideals are

$$\mathfrak{Q}_{e_0} = (2 \cdot 2^{e_0}) \qquad \text{and} \qquad \mathfrak{Q}_e = (2p^e).$$

They are at the same time irreducible ideals, and by what was said about the prime ideals, two ideals belonging to different odd prime numbers are mutually relatively prime, but no $\mathfrak{Q}$ is relatively prime to any $\mathfrak{Q}_{e_0}$.[47] Thus the $\mathfrak{Q}_{e_0}$ are the only non-isolated primary ideals. The unique decomposition of a into prime

[47] Indeed, from $2b \cdot 2p_1^{e_1} \equiv 0\,(2p_2^{e_2})$ for odd $p_1 \neq p_2$ one always obtains $2b \equiv 0\,(2p_2^{e_2})$; but from $2b \cdot 2p^e \equiv 0\,(2 \cdot 2^{e_0})$ one obtains only $2b \equiv 2 \cdot 2^{e_0-1}\,(2 \cdot 2^{e_0})$.

powers corresponds to the unique representation of the ideal $(2a)$ by greatest primary, at the same time irreducible, ideals:

$$(2a) = [(2 \cdot 2^{e_0}), (2p_1)^{e_1}, \ldots, (2p_\alpha)^{e_\alpha}].$$

Thus here, in contrast to the examples from the polynomial domain, even the non-isolated greatest primary ideals are uniquely determined. If $e_0 = 0$ this is at the same time a representation by mutually relatively prime ideals, while if $e_0 > 0$ the ideal is relatively-prime-irreducible.

Thus, while in the domain of all integers the four different decompositions coincide, here this happens only for the two decompositions into greatest primary and into irreducible ideals on the one hand, and, for $e_0 > 0$, for coprime-irreducible (every ideal is coprime-irreducible, since the domain has no unit) and relatively-prime-irreducible ideals on the other; for $e_0 = 0$, however, the coprime-irreducible and relatively-prime-irreducible decompositions become different. At the same time one already obtains here an example in which one prime ideal can be divisible by another without being identical with it; more generally, one sees that product representation does not follow from divisibility. The latter fact - a consequence of the absence of a unit in the domain - is also why no unique product representation of the numbers of the domain by irreducible numbers of the domain exists, even though every ideal is a principal ideal; the introduction of least common multiples therefore proves necessary. It should also be noted that the situation remains exactly the same if, instead of all even integers, one takes all integers divisible by a fixed prime number or power of a prime.

Irreducible and primary ideals also become different, however, if Σ consists of all numbers divisible by a composite number $g = p_1^{\sigma_1} \cdots p_\nu^{\sigma_\nu}$. Again every ideal is a principal ideal $(g \cdot a)$, and the prime ideals are again $\mathfrak{P}_0 = \mathfrak{D} = (g)$ and $\mathfrak{P} = (g \cdot p)$, where p is a prime different from the primes occurring in g. But the irreducible ideals are $\mathfrak{B}_{\lambda_i} = (g \cdot p_i^{\lambda_i})$ and $\mathfrak{B}_e = (g \cdot p^e)$; the primary ideals are $\mathfrak{Q}_e = \mathfrak{B}_e$ and the ideals, different from the irreducible ones,

$$\mathfrak{Q}_{\lambda_1 \ldots \lambda_\nu} = (g \cdot p_1^{\lambda_1} \cdots p_\nu^{\lambda_\nu}),$$

where the $\mathfrak{B}_{\lambda_i}$ and $\mathfrak{Q}_{\lambda_1 \ldots \lambda_\nu}$ all have the same associated prime ideal $\mathfrak{P}_0 = (g)$. Here too the decomposition into irreducible ideals is unique, and consequently so is the decomposition into greatest primary ideals; thus here again the non-isolated ideals are uniquely determined.

2. An example of a non-commutative ring domain is supplied by the ideal theory in non-commutative polynomial domains treated in the paper of Noether–Schmeidler. In particular one has "completely reducible" ideals, that is, ideals for which the components of the decomposition are pairwise coprime and have no proper divisors; the components are therefore a fortiori irreducible. Thus, in addition to the isomorphism proved there according to § 9, one obtains equality of the number of components in two different decompositions. For the decomposition of systems of partial or ordinary linear differential expressions, which arises as a special case of that paper, this gives a result which does not seem to have been noticed even in the known case of a single ordinary linear differential expression.

At the same time the system T of all residue classes of a fixed ideal $\mathfrak{M}$, together with the non-commutative polynomial domain Σ, supplies a double domain (Σ, T), where T has the module property with respect to Σ. For the difference of two residue classes is again a residue class, and likewise the product of a residue class by an arbitrary polynomial; whereas the product of two residue classes does not exist (loc. cit., § 3). Thus the systems of residue classes called "subgroups" there furnish examples of modules in double domains (Σ, T), where the underlying ring domain Σ is non-commutative.

§ 12.

Example from Elementary-Divisor Theory.

This is a conception of elementary divisor theory dictated by the general developments, but the theory itself is assumed as known.

Let Σ be the domain of all integral matrices with n^2 elements, with addition and multiplication defined in the usual sense for matrices. Then Σ is a non-commutative ring domain; the ideals are therefore in general one-sided, with two-sided ideals only as a special case.[48]

We first show that every ideal is principal. For this purpose, in the case of right ideals, to each matrix $A = (a_{ik})$ we assign the module

$$A = (a_{11}\xi_1 + \cdots + a_{1n}\xi_n, \ldots, a_{n1}\xi_1 + \cdots + a_{nn}\xi_n)$$

[48] The ideal theory of these domains is the subject of the works of Du Pasquier: Zahlentheorie der Tettarionen, dissertation, Zürich, Vierteljahrsschr. d. Naturf. Ges. Zürich, 51 (1906); Zur Theorie der Tettarionenideale, ibid., 52 (1907). The content of the second paper is the proof that every ideal is a principal ideal.

of integral linear forms. Conversely, to this module there corresponds every matrix that supplies a basis of A, hence, beside A, also UA, where U is unimodular. More generally, to the product PA there corresponds a module B which is a multiple of A. A single linear form from A is given by such matrices P as contain only one non-zero row.

Let now $A_1, A_2, \ldots, A_\nu, \ldots$ be all elements of an ideal $\mathfrak{M}$; let $A_1, A_2, \ldots, A_\nu, \ldots$ be the modules assigned to them; let A be their greatest common divisor and UA the most general matrix assigned to this module A. To each single linear form in A there then corresponds, by the definition of greatest common divisor, a matrix $P_1 A_{i_1} + \cdots + P_\sigma A_{i_\sigma}$, where, as above, the P have only one non-zero row. It follows that the matrix A corresponding to a basis of A also admits such a representation, now with general P, and hence becomes an element of $\mathfrak{M}$. Since, furthermore, every module A_i is divisible by A, every matrix A_i is divisible by A; A, and in general UA, forms a basis of $\mathfrak{M}$. If one is dealing with left ideals, then correspondingly the columns of each matrix are to be regarded as the basis of a module; every ideal is a principal ideal, for which, beside A, also AV is a basis, with V an arbitrary unimodular matrix.

For the connection with elementary divisor theory, we now base the following on two-sided ideals; hence in particular PAQ belongs to the ideal whenever A does. By the preceding, the most general basis of such an ideal is UAV, where U and V are unimodular. The basis elements therefore exhaust a class of equivalent matrices,[49] and there is a one-to-one relation between ideal and class, hence also between ideal and the elementary divisor system $(a_1 \mid a_2 \mid \cdots \mid a_n)$ of the class, where the a_i are, as is well known, non-negative integers, each dividing the following one. Thus the matrix of the class that occurs in the normal form determined by the elementary divisors may be regarded as a special basis of the ideal; divisibility of ideals, respectively of classes, implies divisibility of the elementary divisors, and conversely.

But Du Pasquier has shown, loc. cit. § 11, that for every two-sided ideal the rank is n and all elementary divisors agree. To be able to consider the case of general elementary divisors, we must therefore start not from the ideals but directly from the two-sided classes (which are likewise to be denoted by capital German letters). A class $\mathfrak{A} = UAV$ is divisible by another class $\mathfrak{B}$ if $A = PBQ$.

In general: *the least common multiple (the greatest common divisor) of two classes is obtained by forming the least common multiple (the greatest common divisor) of the corresponding elementary divisor systems.*[50] For let

$$(a_1 \mid a_2 \mid \cdots \mid a_n), \quad (b_1 \mid b_2 \mid \cdots \mid b_n), \quad (c_1 \mid c_2 \mid \cdots \mid c_n),$$

where $c_i = [a_i, b_i]$, be respectively the elementary divisor systems of $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}^*$, and let $\mathfrak{C} = [\mathfrak{A}, \mathfrak{B}]$. Then $\mathfrak{C}^*$ is divisible by $\mathfrak{A}$ and $\mathfrak{B}$, hence by $\mathfrak{C}$; conversely, the elementary divisors of $\mathfrak{C}$ are divisible by those of $\mathfrak{C}^*$, so $\mathfrak{C}$ is divisible by $\mathfrak{C}^*$ and therefore $\mathfrak{C} = \mathfrak{C}^*$. The proof for the greatest common divisor is obtained correspondingly.

The unique representation of the elementary divisors a_i as least common multiples of prime powers therefore corresponds to a representation of $\mathfrak{A}$ as the least common multiple of classes $\mathfrak{Q}$ whose elementary divisors are given by powers of one prime number, in symbols

$$\mathfrak{Q} \sim (p^{r_1} \mid p^{r_2} \mid \cdots \mid p^{r_e} \mid 0 \mid \cdots \mid 0), \qquad r_1 \leqq r_2 \leqq \cdots \leqq r_e.$$

If in particular the rank ϱ is equal to n, then one has here a decomposition into coprime and coprime-irreducible classes which is unique despite the non-commutative domain.

The classes $\mathfrak{Q}$ can be further decomposed into classes corresponding to the elementary divisor systems

$$\mathfrak{B}_1 \sim (p^{r_1} \mid \cdots \mid p^{r_1}), \quad \mathfrak{B}_2 \sim (1 \mid p^{r_2} \mid \cdots \mid p^{r_2}), \quad \ldots,$$
$$\mathfrak{B}_e \sim (1 \mid \cdots \mid 1 \mid p^{r_e} \mid \cdots \mid p^{r_e}), \quad \mathfrak{B}_{e+1} \sim (1 \mid \cdots \mid 1 \mid 0 \mid \cdots \mid 0),$$

where in $\mathfrak{B}_\nu$ the number 1 occurs $(\nu - 1)$ times. If, for example, $r_1 = r_2 = \cdots = r_\mu = 0$, then $\mathfrak{B}_1, \ldots, \mathfrak{B}_\mu$ are equal to the unit class and are to be omitted from the decomposition; the same holds for $\mathfrak{B}_{e+1}$ if $\varrho = n$. If, furthermore, say $r_\nu = r_{\nu+1} = \cdots = r_{\nu+\lambda}$, then $\mathfrak{B}_{\nu+1}, \ldots, \mathfrak{B}_{\nu+\lambda}$ are proper divisors of $\mathfrak{B}_\nu$, and are likewise to be discarded. Denote by $\mathfrak{B}_{i_1}, \ldots, \mathfrak{B}_{i_k}$ those that remain and now give a shortest representation. Then

$$\mathfrak{Q} = [\mathfrak{B}_{i_1}, \ldots, \mathfrak{B}_{i_k}]$$

[49] The basis elements of one-sided ideals correspond to right or left classes.

[50] In the paper Zur Theorie der Moduln, Math. Ann. 52 (1899), p. 1, E. Steinitz defines the least common multiple (the greatest common divisor) of classes by the least common multiples and greatest common divisors of the elementary systems. Independently, the least common multiple of classes occurs as "congruence composition" in H. Brandt, Komposition der binären quadratischen Formen relativ einer Grundform, J. f. M. 150 (1919), p. 1.

is the unique decomposition of $\mathfrak{Q}$ into irreducible classes. Indeed, suppose

$$\mathfrak{B}_\nu \sim (1 \mid \cdots \mid 1 \mid p^{r_\nu} \mid \cdots \mid p^{r_\nu})$$

can be represented as the least common multiple of

$$\mathfrak{C} \sim (1 \mid \cdots \mid 1 \mid p^{s_1} \mid \cdots \mid p^{s_\lambda}) \quad \text{and} \quad \mathfrak{D} \sim (1 \mid \cdots \mid 1 \mid p^{t_1} \mid \cdots \mid p^{t_\mu}).$$

Then in the elementary divisor systems of $\mathfrak{C}$ and $\mathfrak{D}$ the number 1 must stand in the first $(\nu-1)$ places; in the ν-th place one of the exponents s_ν or t_ν, say s_ν, must become equal to r_ν. But since

$$r_\nu = s_1 \leqq s_2 \leqq \cdots \leqq s_\lambda \leqq r_\nu,$$

one obtains $\mathfrak{C} = \mathfrak{B}_\nu$, and $\mathfrak{B}_\nu$ is therefore irreducible.[51] The same holds for $\mathfrak{B}_{e+1}$, where p is to be replaced by 0. But, as the formation of the least common multiple shows, each of these irreducible classes gives a definite exponent and the place where this exponent first occurs in the elementary divisor system of $\mathfrak{Q}$, respectively $\mathfrak{A}$, while $\mathfrak{B}_{e+1}$ gives the rank. Since these numbers are uniquely determined by the elementary divisor system of $\mathfrak{Q}$, respectively $\mathfrak{A}$, and since the relation between elementary divisors and class is one-to-one, the decomposition of $\mathfrak{Q}$, and likewise of any class, into irreducible classes is unique.

In summary: *Every two-sided class $\mathfrak{A}$ of integral matrices with bounded number of entries can be represented uniquely as the least common multiple of finitely many irreducible two-sided classes. Each irreducible class represents a fixed prime divisor of the elementary divisor system of $\mathfrak{A}$, an associated exponent, and the place where that exponent first occurs. The irreducible class corresponding to the divisor 0 gives the rank of $\mathfrak{A}$.*

Erlangen, October 1920.

(Received 16. 10. 1920.)

[51] The $\mathfrak{B}$ are still reducible into one-sided classes; here there is no longer a unique relation between elementary divisors and class, and hence no unique decomposition into irreducible one-sided classes. The following example, supplied to me by H. Brandt, shows this for decomposition into right-sided classes (where the classes are represented by a basis matrix, or by the corresponding module):

$$\mathfrak{B} = [\mathfrak{C}_1, \mathfrak{C}_2] = [\mathfrak{D}_1, \mathfrak{D}_2], \quad \mathfrak{B} \sim \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, \quad \mathfrak{C}_1 \sim \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \quad \mathfrak{C}_2 \sim \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix},$$
$$\mathfrak{D}_1 \sim \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \quad \mathfrak{D}_2 \sim \begin{pmatrix} p & 0 \\ (p-1) & 1 \end{pmatrix}.$$

Indeed, the modules $(\xi, p\eta)$, $(p\xi, \eta)$, and $(p\xi, (p-1)\xi + \eta)$ each have as their only proper divisor the module (ξ, η), and are therefore irreducible and mutually distinct.

20. An Algebraic Criterion for Absolute Irreducibility.

By

Emmy Noether in Göttingen.

Math. Ann. 85 (1922), pp. 26–33

A polynomial—with coefficients in an arbitrary abstractly defined field—is called *absolutely irreducible* if it remains irreducible in an algebraically closed field to which the coefficient field can be extended[1)]. In what follows I show that absolute irreducibility, in contrast to irreducibility with respect to a prescribed field, admits an *algebraic* formulation; more precisely, the following theorem holds:

To every polynomial in $n \geq 2$ indeterminates with indeterminate coefficients one can associate a polynomial with integer coefficients in these coefficients and in further indeterminates, the reducibility form, in such a way that for every particular polynomial of the same degree the necessary and sufficient condition for absolute irreducibility is the nonvanishing of the reducibility form. In other words: *For every particular system of coefficient values for which the reducibility form vanishes identically in the indeterminates and which entails no lowering of degree, the particular polynomial is reducible, and conversely.*

If, instead of polynomials, one considers homogeneous forms in one more indeterminate, the degree condition is replaced by the simpler condition that the coefficient system not vanish identically.

As a direct consequence of the theorem one also obtains the following result, first stated by A. Ostrowski[2]:

Every absolutely irreducible polynomial with algebraic numbers as coefficients remains irreducible modulo every prime ideal of a finite algebraic number field Ω containing the coefficient field, with the possible exception of a finite number of prime ideals of Ω. In particular, Ω may also be the field of rational numbers.

I intend to discuss elsewhere further applications to the theory of relatively integral functions.[3]

1. We first show that *every polynomial in $n \geq 2$ indeterminates with indeterminate coefficients is absolutely irreducible.* Put

$$
\begin{aligned}
F(x) &= \sum A_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} && (i_1 + \cdots + i_n \leq l),\\
G(x) &= \sum B_{j_1 \dots j_n} x_1^{j_1} \cdots x_n^{j_n} && (j_1 + \cdots + j_n \leq m),\\
H(x) &= F(x)G(x) = \sum C_{k_1 \dots k_n}(A,B) x_1^{k_1} \cdots x_n^{k_n} && (k_1 + \cdots + k_n \leq l+m),
\end{aligned} \tag{1}
$$

where the A and B denote indeterminates and the $C(A,B)$ are integral bilinear combinations of the A and B. The quotients $D = C(A,B)/C_{0\dots0}(A,B)$ are therefore rational functions of the quotients $A/A_{0\dots0}$ and $B/B_{0\dots0}$; but the number of these functions is greater than the number of their arguments, for the respective numbers are $\binom{l+m+n}{n} - 1$, $\binom{l+n}{n} - 1$, and $\binom{m+n}{n} - 1$, and

$$
\binom{l+m+n}{n} + 1 > \binom{l+n}{n} + \binom{m+n}{n} \quad \text{for } n \geq 2,\ l > 0,\ m > 0.
$$

Thus there exists at least *one* algebraic relation among the $D(A,B)$, and consequently also among the $C(A,B)$:

$$
\Phi(Z) \neq 0 \quad [\text{identically in } Z_{k_1 \dots k_n}],\ \Phi(C(A,B)) = 0 \quad [\text{identically in } A, B], \tag{2}
$$

where Φ denotes a polynomial with integer coefficients.

A polynomial having *indeterminates* Z as coefficients,

$$
E(x) = \sum Z_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n} \qquad (k_1 + \cdots + k_n \leq l+m), \tag{3}
$$

is therefore necessarily *absolutely irreducible* for $n \geq 2$[4)].

[1)] E. Steinitz showed in his "Algebraic Theory of Fields" (J. f. M. 137 (1910), p. 167) that every field can be extended, in an essentially unique way, to an algebraically closed field, that is, to one in which every polynomial in one indeterminate decomposes into linear factors; he thereby gave the rational equivalent of the fundamental theorem of algebra.

[2] *On the arithmetic theory of algebraic quantities*. Gött. Nachr. 1919, p. 279 (lemma on p. 296).—For the case of fields consisting of ordinary numbers, Ostrowski, as I know, has also arrived at the main theorem above; he will shortly publish his investigations concerning it. That in my arrangement of the proof the main theorem holds for arbitrary abstractly defined fields rests on the fact that the reducibility form constructed for indeterminates has *numerical coefficients independent of the particular underlying field.*

[3] D. Hilbert, *Mathematical Problems.* Gött. Nachr. 1900, p. 253, Problem 14.

[4)] For, in the terminology of 2, the indeterminates Z are not zeros of $\mathfrak{P}$.

2. The totality of these polynomials $\Phi(Z)$ which vanish identically in A, B upon the substitution $Z = C(A, B)$ forms an *ideal of polynomials*[5], more precisely a *prime ideal* $\mathfrak{P}$; for if a product $\Phi_1\Phi_2$ vanishes by virtue of the substitution, then at least one factor vanishes. Since (2) is satisfied identically in A, B, it remains valid for every particular system of values A, B, where A, B, and consequently also $\Gamma = C(A, B)$, denote elements of an arbitrary field. *The coefficients* Γ *of every polynomial reducible in an extension field therefore satisfy the conditions* $\Phi(\Gamma) = 0$*; they are zeros of* $\mathfrak{P}$, or equivalently of the finitely many basis polynomials of $\mathfrak{P}$. It remains to *prove the converse.*

For this purpose it should be noted that all relations among A, B, C remain valid if, by introducing a new indeterminate y, one transforms the polynomials (1) into homogeneous forms $F(x, y)$, $G(x, y)$, $H(x, y)$ of degrees $l, m, l + m$. Thus coefficient systems Γ for which, for example, $\bar{F}(x, y)$[6] becomes a power of y are also zeros of $\mathfrak{P}$; on passing to inhomogeneous polynomials, these correspond to a lowering of the degree of $\bar{H}(x)$ and not to a factorization. It will be shown that, apart from this lowering of degree, the converse always holds; in particular, *for homogeneous forms the converse holds without exception as soon as not all* Γ *vanish; in other words, every zero of* $\mathfrak{P}$ *is supplied by the parametric representation* $\Gamma = C(A, B)$ *with elements* A, B *of an extension field*[7].

I establish this result by directly constructing finitely many functions $\Phi(Z)$. By means of the Kronecker substitution

$$x_\lambda = \xi^{d^{n-\lambda}}\text{[8]}$$

I associate with the polynomials (1) polynomials in *one* indeterminate; I show that gaps occur in their exponents and, by forming the norm of the corresponding coefficients, obtain the functions $\Phi(Z)$ and the desired criterion.

3. Put

$$\begin{aligned} &d = l + m + 1; && i = i_1 d^{n-1} + i_2 d^{n-2} + \cdots + i_n; \\ &j = j_1 d^{n-1} + \cdots + j_n; && k = k_1 d^{n-1} + \cdots + k_n. \end{aligned} \tag{4}$$

Under the Kronecker substitution, the polynomials F, G, H in (1) correspond respectively to the polynomials

$$\begin{aligned} f(\xi) &= \sum A_{i_1 \ldots i_n} \xi^i && (i_1 + \cdots + i_n \le l), \\ g(\xi) &= \sum B_{j_1 \ldots j_n} \xi^j && (j_1 + \cdots + j_n \le m), \\ h(\xi) &= \sum C_{k_1 \ldots k_n}(A, B) \xi^k && (k_1 + \cdots + k_n \le l + m). \end{aligned} \tag{5}$$

This correspondence is, as is well known, *one-to-one*: for all the *induced* exponents occurring in (5), $k = 0$ implies $k_1 = 0, \ldots, k_n = 0$; and consequently $i + j = i' + j'$ implies $i_1 + j_1 = i'_1 + j'_1, \ldots, i_n + j_n = i'_n + j'_n$. Thus distinct products $\xi^i\xi^j$ can yield the same exponent ξ^k only when the corresponding products $x_1^{i_1} \cdots x_n^{i_n} x_1^{j_1} \cdots x_n^{j_n}$ also yield the same exponent. Hence

$$h(\xi) = f(\xi)g(\xi), \tag{6}$$

and conversely, from the satisfaction of a relation (6) in which no exponents other than the induced exponents occur in $f(\xi)$ and $g(\xi)$, there follows

$$H(x) = F(x)G(x). \tag{7}$$

Moreover, *gaps actually occur among the induced exponents in* $f(\xi)$ *and* $g(\xi)$. For the highest exponent of $f(\xi)$ is ld^{n-1} and the second highest is $(l-1)d^{n-1} + d^{n-2}$; their difference is $d^{n-2}(d-1) > 1$, since $d = l + m + 1 \ge 3$ and $n \ge 2$; the same holds for $g(\xi)$.

The relations (6) and (7), which hold for the indeterminates A, B, remain valid for every particular system of values A, B. To preserve the degrees in doing so, I homogenize (6) and (7) by means of the indeterminates η and y. *A homogeneous form* $H(x, y)$ *therefore decomposes in an algebraic extension field if and only if the*

[5] These totalities are usually called modules; in fact, however, the property characterizing them—that together with Φ_1 and Φ_2 they contain $\Phi_1 - \Phi_2$, and together with Φ they contain $\Psi\Phi$, where Ψ denotes an arbitrary polynomial with integer coefficients in Z—is the ideal property.

[6] Polynomials and forms obtained by replacing the indeterminates in $F, G, \ldots, f, g, \ldots$ by particular systems of values will throughout be denoted by bars: $\bar{F}, \bar{G}, \ldots, \bar{f}, \bar{g}, \ldots$.

[7] That "in general" the zeros of $\mathfrak{P}$ are supplied by the parametric representation follows from the property of the prime ideal $\mathfrak{P}$ of defining an irreducible algebraic variety. But, as is well known, this does not imply—as I originally overlooked, and as A. Ostrowski pointed out to me some time ago—that the parametric representation fails for no particular system of values. The proof given here is based on more elementary concepts.

[8] *Festschrift*, p. 11.

corresponding binary form $h(\xi,\eta)$ can there be split into two factors in such a way that no exponents other than the induced exponents occur in the factors.

4. To carry out the formation of the norm mentioned at the end of 2, let

$$a_1, b_1; \ldots; a_p, b_p; \quad a_{p+1}, b_{p+1}; \ldots; a_{p+q}, b_{p+q}$$

denote new indeterminates. Put

(8)
$$\begin{aligned}\varphi(\xi,\eta) &= (a_1\xi + b_1\eta)\cdots(a_p\xi + b_p\eta) = r_p\xi^p + r_{p-1}\xi^{p-1}\eta + \cdots + r_0\eta^p,\\ \psi(\xi,\eta) &= (a_{p+1}\xi + b_{p+1}\eta)\cdots(a_{p+q}\xi + b_{p+q}\eta) = s_q\xi^q + s_{q-1}\xi^{q-1}\eta + \cdots + s_0\eta^q,\\ \chi(\xi,\eta) &= \varphi(\xi,\eta)\psi(\xi,\eta) = t_{p+q}\xi^{p+q} + t_{p+q-1}\xi^{p+q-1}\eta + \cdots + t_0\eta^{p+q};\end{aligned}$$

thus r, s, t are respectively the homogenized elementary symmetric functions, that is, the symmetric functions of the pairs a, b which are linear in each individual pair and from which all integral symmetric functions homogeneous and of the same degree in every individual pair can be expressed integrally and with integer coefficients—and in only one way.

With further indeterminates $u_{\mu\nu}$ I now form the linear form

(9)
$$\zeta(u,a,b) = \sum u_{\mu\nu} r_\mu s_\nu,$$

where the summation extends over prescribed indices μ and ν. The product of $\zeta(u)$ with all its mutually distinct conjugates, distinct also from $\zeta(u)$ itself, arising from permutation of the pairs a, b—the norm $N(\zeta(u))$ of $\zeta(u)$ with respect to the field of the $t(a,b)$, when $\zeta(u)$ is regarded as a function in the field of the $r_\mu(a,b)$ and $s_\nu(a,b)$—is then an integral symmetric function of all the pairs a, b, homogeneous and of the same degree in every pair. By the preceding discussion it is therefore a uniquely determined polynomial with integer coefficients in the $t(a,b)$ and $u_{\mu\nu}$:

(10)
$$N(\zeta(u,a,b)) = T(t(a,b),u) \qquad [\text{identically in } a,b,u].$$

The same argument shows that

$$N(z-\zeta(u)) = z^\delta + T_{\delta-1}(t,u)z^{\delta-1} + \cdots + T(t,u) \qquad [\text{identically in } a,b,u,z],$$

where all the T are polynomials with integer coefficients in t and u. Both sides of this identity vanish for $z = \zeta(u)$; and, because the elementary symmetric functions $r(a,b)$ and $s(a,b)$ are algebraically independent, they do so identically in r, s if one puts $t(a,b)$, according to (8), equal to the integral bilinear combination $w(r,s)$ of r and s and regards $\zeta(u)$ as a function of r and s. Thus

(11)
$$\zeta(u)^\delta + T_{\delta-1}(w(r,s),u)\zeta(u)^{\delta-1} + \cdots + T(w(r,s),u) = 0 \quad [\text{identically in } r,s,u].^{9)}$$

The identities (10) and (11) remain valid for all particular systems of values α, β of a, b, respectively ϱ, σ of r, s. If ϱ, σ are chosen in particular so that all products $\varrho_\mu\sigma_\nu$ vanish—where μ, ν denote the indices occurring in (9)—and hence $\zeta(u)$ vanishes under the substitution, then, on putting $w(\varrho,\sigma) = \tau$, (11) gives

(12)
$$T(\tau,u) = 0 \qquad [\text{identically in } u].$$

Conversely, let $\tau_0, \ldots, \tau_{p+q}$ be *systems of values, not all zero, for which (12) is satisfied.* Since in an algebraic extension field there exists a decomposition

(12)
$$\bar\chi(\xi,\eta) = \tau_{p+q}\xi^{p+q} + \cdots + \tau_0\eta^{p+q} = (\alpha_1\xi + \beta_1\eta)\cdots(\alpha_{p+q}\xi + \beta_{p+q}\eta),$$

in which α and β do not vanish simultaneously in any factor[10)], although some of the α or β may vanish, we have $\tau = t(\alpha,\beta)$. Substitution of these values in (10) shows, by virtue of (12), that $\zeta(u,\alpha,\beta)$ or one of its conjugate factors vanishes identically in u. Thus, after a suitable numbering of α, β, put $r(\alpha,\beta) = \varrho$ and $s(\alpha,\beta) = \sigma$. This means that $\bar\chi(\xi,\eta)$ *admits at least one decomposition*

(13)
$$\bar\chi(\xi,\eta) = \bar\varphi(\xi,\eta)\bar\psi(\xi,\eta) = \sum \varrho_\kappa\xi^\kappa\eta^{p-\kappa} \cdot \sum \sigma_\lambda\xi^\lambda\eta^{q-\lambda},$$

such that all products $\varrho_\mu\sigma_\nu$ occurring in $\zeta(u)$ vanish, but not all ϱ or all σ vanish.

---

9) When the summation in (9) is extended over all indices, (11) represents Kronecker's extension of Gauss's theorem, essentially in Kronecker's arrangement of the proof (*On the theory of forms of higher degree*, Berliner Ber. 1883, Works, vol. 2, p. 417).

10) This (rational) "fundamental theorem of algebra" is the existence theorem on which the unrestricted validity of the converse stated at the end of 2 is based.

5. Let the degrees p, q in (8) now be equal to ld^{n-1} and md^{n-1}, that is, to the degrees of $f(\xi)$ and $g(\xi)$ in (5). Split the indices μ, ν into $\mu^{(1)}, \nu^{(1)}, \mu^{(2)}, \nu^{(2)}$ as follows: $\mu^{(1)}$ runs through all exponents missing from $f(\xi)$, and $\nu^{(1)}$ through all exponents of ξ in $\psi(\xi, \eta)$; correspondingly, $\nu^{(2)}$ runs through all exponents missing from $g(\xi)$, and $\mu^{(2)}$ through all exponents of ξ in $\varphi(\xi, \eta)$. Further, let

$$e(\xi) = \sum Z_{k_1 \dots k_n} \xi^k \qquad (k_1 + \cdots + k_n \leq l + m)$$

denote the polynomial in one indeterminate corresponding to the polynomial (3), and let

$$S(Z, u)$$

denote the polynomial with integer coefficients in Z and u obtained from $T(t, u)$—the uniquely determined right-hand side of (10), where the summation in (9) is extended over the indicated indices $\mu^{(1)}, \nu^{(1)}, \mu^{(2)}, \nu^{(2)}$— by replacing the t by the coefficients Z and the corresponding zero coefficients of $e(\xi)$.

If the r, s are now replaced by the coefficients A, B and the corresponding zero coefficients of $f(\xi)$ and $g(\xi)$, then $\zeta(u)$ *vanishes* under this substitution for the indicated summation. Further, $t = w(r, s)$ goes over into the coefficients $C(A, B)$ and the corresponding zero coefficients of $h(\xi)$; hence $T(t, u)$ goes over into $S(C(A, B), u)$. The identity (11) therefore gives

$$S(C(A, B), u) = 0. \qquad [\text{identically in } A, B, u]. \tag{14}$$

Since (14) remains valid for every particular system of values, the coefficients $\Gamma = C(A, B)$ of those particular $\bar{H}(x)$, or general $\bar{H}(x, y)$, which *decompose into two factors in an extension field* satisfy the condition

$$S(\Gamma, u) = 0 \qquad [\text{identically in } u]. \tag{15}$$

Conversely, suppose that condition (15) is satisfied for the coefficients Γ, not all zero, of a polynomial $\bar{H}(x)$, respectively a form $\bar{H}(x, y)$. By the preceding discussion this is equivalent to $T(\tau, u) = 0$, where τ denotes all the coefficients of $\bar{h}(\xi, \eta)$. By (13) there consequently exists, in an extension field of the Γ, a decomposition

$$\bar{h}(\xi, \eta) = \bar{f}(\xi, \eta) \cdot \bar{g}(\xi, \eta),$$

in which, by the choice of summation, no exponents other than the induced exponents occur in $\bar{f}$ and $\bar{g}$; consequently there is a relation

$$\bar{H}(x, y) = \bar{F}(x, y) \cdot \bar{G}(x, y).$$

As soon as neither factor becomes of degree zero for $y = 1$, and hence in particular when the Γ entail no lowering of the degree of $\bar{H}(x)$, there follows the further relation

$$\bar{H}(x) = \bar{F}(x) \cdot \bar{G}(x).$$

Condition (15) is therefore necessary and sufficient for $\bar{H}(x, y)$, and, when a lowering of degree is excluded, also $\bar{H}(x)$, to decompose into two factors in an extension field.

It also follows that $S(Z, u)$ cannot vanish identically in Z and u, since it was shown in 1 that for $n \geq 2$ the polynomials with indeterminates as coefficients, and hence also the corresponding homogeneous forms in one more indeterminate, are absolutely irreducible. Thus, with U denoting power products of the u,

$$S(Z, u) = \sum \Phi_\lambda(Z) U_\lambda,$$

where by (14) the $\Phi_\lambda(Z)$ are polynomials belonging to $\mathfrak{P}$. *It has thereby been shown that $\mathfrak{P}$ has no zeros other than those given by the parametric representation $\Gamma = C(A, B)$, where A and B belong to an algebraic extension field of the Γ.* The converse stated at the end of 2 is thus proved.

6. *The condition for absolute irreducibility can now be formulated directly.* One need only split the degree of $E(x)$ in (3), in all possible ways, into two positive summands $l + m$ and form the expression $S(Z, u)$ for each splitting. The product of these forms,

$$R(Z, u) = \prod S(Z, u), \tag{16}$$

is then the *reducibility form of $E(x)$*; for, by the preceding argument, every *factorization* of $\bar{E}(x)$, respectively $\bar{E}(x, y)$, corresponds to the vanishing of one factor of (16), and conversely. This proves the *main*

theorem stated in the introduction and shows at the same time how the reducibility form can actually be constructed in finitely many steps.

7. The *existence of the reducibility form* (16) immediately yields *Ostrowski's theorem* mentioned in the introduction. Let

$$\bar{E}(x) = \sum \Gamma_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n} \qquad (k_1 + \cdots + k_n \leq v)$$

be an absolutely irreducible polynomial whose coefficients Γ are algebraic integers; let $\mathfrak{K}$ denote a finite algebraic number field containing all the Γ, and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{K}$.

Then the reducibility form $R(Z, u)$ of $\bar{E}(x)$, constructed for the exact degree of $\bar{E}(x)$, remains *nonzero* after the substitution $Z = \Gamma$; thus

$$R(\Gamma, u) = \sum P_\lambda U_\lambda \neq 0 \qquad [\text{identically in } u].$$

The ideal $\mathfrak{r} = (P_1, P_2, \dots)$ is therefore divisible by only a *finite number* of prime ideals of $\mathfrak{K}$. If $\mathfrak{p}$ is distinct from these finitely many prime ideals, then $R(\Gamma, u)$ does not vanish identically modulo $\mathfrak{p}$; and since the residue classes modulo $\mathfrak{p}$ again form a field, it follows that $\bar{E}(x)$ is *irreducible modulo* $\mathfrak{p}$, more precisely absolutely irreducible. The same holds for $\bar{E}(x, y)$, so that no lowering of degree occurs modulo $\mathfrak{p}$ either.

If the coefficients of $\bar{E}(x)$ are algebraic fractions, $\mathfrak{p}$ must also be chosen distinct from the finitely many prime ideals dividing the common denominator Δ; modulo all the remaining prime ideals, $\bar{E}(x)$ may be replaced by $\Delta \cdot \bar{E}(x)$, so that the preceding hypotheses are satisfied. This proves the theorem.

Erlangen, August 1921.

(Received 28 August 1921.)

21. Formal Calculus of Variations and Differential Invariants

Encyclopedia of Mathematical Sciences II, 3 (1922), pp. 68–71 (in: R. Weitzenböck, *Differential Invariants*)

28. Formal Calculus of Variations and Differential Invariants.[149)]

The construction of all differential invariants and the derivation of the principal theorems can be carried out most uniformly by the formal methods of the calculus of variations. This principle goes back to Riemann[78)] and received its principal development in invariant theory from Lipschitz[73)].

Begin with the variational problem belonging to a homogeneous form $f(dx)$—where

$$\left| \frac{\partial^2 f}{\partial dx_i \, \partial dx_k} \right| \neq 0$$

is assumed—namely,

$$\delta \int_{t_0}^{t_1} f(x') \, dt = 0, \qquad \left(x_i' = \frac{dx_i}{dt} \right). \tag{140}$$

Integration by parts leads to the invariant system of equations

$$2\psi_i = \frac{d}{dt} \frac{\partial f}{\partial x_i'} - \frac{\partial f}{\partial x_i} = 0,$$

where the Lagrangian expressions ψ_i are contragredient to the dx. Formally, this is seen most simply by defining the ψ_i through the integral-free formal identity corresponding to integration by parts (Lagrange's central equation[150)])

$$\delta f' - df_\delta = -2 \sum \psi_i(d, d) \, \delta x_i, \qquad \left(f_\delta = \sum \frac{\partial f}{\partial dx_i} \, \delta x_i \right),$$

where both f and df_δ are invariants and hence so is the right-hand side. In particular, for a quadratic form one obtains

$$\delta \sum g_{ik} dx_i dx_k - 2d \sum g_{ik} dx_i \delta x_k = -2 \sum \psi_\mu(d, d) \, \delta x_\mu.$$

If d is here replaced by the cogredient operator $(d + \lambda\delta)$ and powers of λ are compared, the corresponding system of identities is obtained:

$$\begin{cases} D \sum g_{ik} dx_i dx_k - 2d \sum g_{ik} dx_i Dx_k = -2 \sum \psi_\mu(d, d) \, Dx_\mu, \\ D \sum g_{ik} dx_i \delta x_k - \delta \sum g_{ik} dx_i Dx_k \quad - d \sum g_{ik} \delta x_i Dx_k \\ \qquad\qquad = -2 \sum \psi_\mu(d, \delta) \, Dx_\mu, \\ D \sum g_{ik} \delta x_i \delta x_k - 2\delta \sum g_{ik} \delta x_i Dx_k = -2 \sum \psi_\mu(\delta, \delta) \, Dx_\mu, \end{cases} \tag{141}$$

from which $\psi_\mu(d, \delta)$, and therefore in particular also $\psi_\mu(d, d)$ and $\psi_\mu(\delta, \delta)$, are seen to be contragredient vectors. From (141), $\psi_\mu(d, \delta)$ is calculated as

$$\psi_\mu(d, \delta) = \sum g_{i\mu} \, d\delta x_i + \sum \left[\begin{smallmatrix} ik \\ \mu \end{smallmatrix} \right] dx_i \delta x_k,$$

and this gives the cogredient vector

$$p^\sigma(d, \delta) = \sum g^{\sigma\mu} \psi_\mu = d\delta x_\sigma + \sum \left\{ \begin{smallmatrix} ik \\ \sigma \end{smallmatrix} \right\} dx_i \delta x_k. \tag{142}$$

The equations $p^\nu(d, d) = 0$ evidently represent the equations of geodesic lines.

Knowledge of the cogredient vector $p^\sigma(d, \delta)$ leads directly to covariant differentiation (cf. No. 19). If, for example, $h(d, \delta)$ is a form in the two sets dx and δx, then the expression

$$h^{(1)}(dx, \delta x) = \delta h - \sum \frac{\partial h}{\partial dx_\sigma} p^\sigma(d, \delta) - \sum \frac{\partial h}{\partial \delta x_\sigma} p^\sigma(\delta, \delta) \tag{143}$$

[149)] This section is by E. Noether.

[150)] For a particular f, this designation is due to Heun; cf. his article IV, 1 II, p. 447.

is itself an invariant, as a difference of invariants, and is constructed so that the second differentials cancel. Thus $h^{(1)}(dx, \delta x)$ is a form involving only first differentials: the covariant derivative of h. The same applies when h contains several sets $d^{(1)}x, \ldots, d^{(\lambda)}x$.[151)]

Riemann's and Lipschitz's construction of the curvature form is based on the same principle. From $\delta^2 f$ one passes to the "normal form of the second variation"

$$\Omega = \delta^2 \sum g_{ik} dx_i dx_k - 2d\delta \sum g_{ik} dx_i \delta x_k + d^2 \sum g_{ik} \delta x_i \delta x_k, \tag{144}$$

which, being a sum of invariants, is itself again an invariant and in which, as a generalization of Lagrange's central equation, the third differentials have now been eliminated. The second differentials are eliminated, analogously to covariant differentiation, by forming the difference

$$K = \Omega - 2 \sum \{p^\sigma(d, \delta)\psi_\sigma(d, \delta) - p^\sigma(\delta, \delta)\psi_\sigma(d, d)\}, \tag{145}$$

which may also be written as[152)]

$$\begin{aligned} \frac{1}{2}K = {} & d \sum \psi_\sigma(d, \delta)\delta x_\sigma - \delta \sum \psi_\sigma(d, d)\delta x_\sigma \\ & - \sum \{p^\sigma(d, \delta)\psi_\sigma(d, \delta) - p^\sigma(\delta, \delta)\psi_\sigma(d, d)\}. \end{aligned} \tag{146}$$

The rule for forming K may also be expressed by saying that the second differentials in Ω are eliminated by setting $p(d, \delta)$ and $p(\delta, \delta)$—respectively, the right-hand sides of (141)—equal to zero. This is Riemann's definition of the curvature form (cf. No. 21). It must, however, be expressly noted—as (146) makes particularly clear—that this setting equal to zero may be performed only after differentiation has taken place; Lipschitz's formal method avoids this difficulty. Correspondingly, the covariant derivative $h^{(1)}$ in (143) could also be defined by eliminating the second differentials from δh through setting $p(d, \delta), \ldots$ equal to zero.

Successive formation of covariant derivatives from the curvature form gives a sequence of forms [$\Phi_4, \Phi_5, \ldots$ in Christoffel's notation]. According to Christoffel and Ricci, their projective invariants, together with f, exhaust the totality of the differential invariants of the quadratic form; and their equivalence under linear transformations, without any further integrability condition, expresses the equivalence of two quadratic differential forms (cf. No. 22). The underlying reason for this reduction theorem rests on the existence of the Riemannian normal coordinates arising from the variational problem (140) (cf. No. 20). These transform the geodesic lines passing through a point into straight lines and consequently transform linearly under an arbitrary transformation of the x. The construction of all invariants and the equivalence problem are thus reduced to the corresponding problem for the individual homogeneous components in the expansion of f in normal coordinates, and one shows that these components are linear combinations of $f, \Phi_4, \Phi_5, \ldots$. For quadratic forms this is carried out in detail by Vermeil[92)], following a note by E. Noether[93)]. According to that note, the theorems and methods remain valid when an arbitrary differential expression is taken as basis (cf. Nos. 22 and 23); this demonstrates the scope of the methods of the formal calculus of variations as compared with those of pure elimination theory.[153)]

Levi-Civita[134)] interpreted the setting of $p(d, \delta)$ equal to zero geometrically as the "parallel displacement of a vector" (cf. also Hessenberg[133)]). This concept, axiomatized by Weyl, is essentially restricted to quadratic forms, but admits a generalization of another kind. It is preserved under enlargement of the group (multiplication of the g_{ik} by an arbitrary function), provided that a linear form is taken as basis in addition to the quadratic form. Then $p(d, \delta)$ is uniquely determined, and invariant constructions corresponding to those above can be carried out and geodesic coordinates defined; but $p(d, d) = 0$ no longer arises from a variational problem![154)] Questions concerning a reduction theorem and equivalence have not yet been treated here in general; R. Weitzenböck has given a reduction theorem only for invariants of lowest order.[155)]

Finally, mention should be made of the general "invariant variational problems," that is, those in which the (simple or multiple) integral J is invariant under some group in Lie's sense. Papers by Hamel[156)], Her-

[151)] Lipschitz, J. f. Math. 72 (1870), p. 17.

[152)] Lipschitz, J. f. Math. 82 (1876), § 1.

[153)] For these remarks and further geometric interpretations, cf. the seminar lectures of F. Klein listed under "Literature."

[154)] H. Weyl, *Pure Infinitesimal Geometry*, Math. Ztschr. 2 (1918), pp. 384–411, and *Space, Time, Matter* (3rd and 4th eds.).

[155)] Wien. Ber. 129 (1920), pp. 683 and 697.

[156)] Math. Ann. 59 (1904), pp. 416–434; Ztschr. Math. Phys. 50 (1904), pp. 1–54.

glotz[157], Lorentz[158], Fokker[159], Weyl[160], and Klein[161] deal with particular cases of physical interest. E. Noether's general formulation[162] shows that invariance of J under a G_ϱ (a finite group with ϱ essential parameters) corresponds to ϱ linearly independent divergences; invariance under an infinite group involving ϱ arbitrary functions and their derivatives through order σ corresponds to ϱ dependencies among the Lagrangian expressions and their derivatives through order σ. In both cases the converse holds. Since the Lagrangian expressions become (relative) invariants of the group, this also gives a process for generating invariants.

(Completed in March 1921.)

[157] Ann. d. Phys. (4) 36 (1911), p. 511, especially § 9.
[158] Verslag der Amsterd. Akad., April and September 1916, October 1916, May 1917.
[159] Ibid., January 1917.
[160] Ann. d. Phys. (4) 54 (1917), p. 117, § 2.
[161] Gött. Nachr. 1917, pp. 469–482; ibid. 1918, pp. 171–189.
[162] Gött. Nachr. 1918, pp. 235–257.

22. On the Theory of Polynomial Ideals and Resultants

Math. Ann. 88 (1923), pp. 53–79

On the Theory of Polynomial Ideals and Resultants.

By

Kurt Hentzelt †.

Edited by Emmy Noether in Göttingen.

In what follows the question is the *general problem of elimination theory, namely to determine the common zeros of all polynomials of an ideal of polynomials*; or, what is identical with this, the zeros of any finite number of polynomials that form a basis of the ideal. At the same time a conceptual interpretation of the multiplicities that occur will emerge. The coefficients of the polynomials may be assigned to any field; the zeros then belong to the algebraically closed field derived from it. Moreover, the ideal may be assumed, without restriction of generality, to be transformed (ğ 3). Then the essential result is the following:

To every ideal $\mathfrak{m}$ *of polynomials one can assign a resultant form:*

$$R_{\mathfrak{m}} = R^{(1)}(x_1, \ldots, x_n) \cdots R^{(i)}(x_i, \ldots, x_n) \cdots R^{(n)}(x_n) \equiv 0(\mathfrak{m}),$$

in such a way that $R_{\mathfrak{m}}$ *vanishes for all zeros of* $\mathfrak{m}$ *and only for these. If* $\mathfrak{n}$ *is a divisor of* $\mathfrak{m}$*, and if the resultant forms* $R_{\mathfrak{n}}$ *and* $R_{\mathfrak{m}}$ *agree, then the ideals* $\mathfrak{n}$ *and* $\mathfrak{m}$ *also agree.*[1]

The second part of the main theorem shows that the resultant form supplies the zeros in characteristic multiplicity. This second part is analogous to the fact that two ideals of an algebraic number field, one of which is a divisor of the other, agree if and only if their *norms* agree; the inner reason for the two theorems is also the same.

Namely, $\mathfrak{m}$ may be conceived as a module of linear forms $\mathfrak{M}_{i-1}$, by regarding each polynomial as a linear form in the power products of $x_1, \ldots, x_{i-1}$ and adjoining $x_{i+1}, \ldots, x_n$ to the coefficient domain. The resultant factor $R^{(i)}$ then becomes equal to the *norm* of the corresponding fundamental module (ğ 1) $\mathfrak{G}_{i-1}$ with respect to $\mathfrak{M}_{i-1}$; this also immediately gives an *interpretation of the multiplicity – product of degree and exponent of a factor of* $R^{(i)}$ *– by the number of linearly independent residue classes*[2], a fact that until now was known only in the special case in which the resultant can be defined for indeterminate coefficients[3].

For the derivation of these results, ğğ 1 and 2 give theorems on modules of linear forms whose coefficients are rational integers or polynomials in one indeterminate. The connection with the ideals of polynomials introduced in ğ 3 is supplied by the isomorphism theorem of ğ 4. Section 5 gives the above-mentioned second part of the main theorem; ğ 7 gives the theorem on the zeros, preceded in ğ 6 by a general elimination theory. There, at the same time, when new indeterminates are introduced, the decomposition of the resolvent into linear forms in these indeterminates is proved; and thus, for the elimination given here, an unobjectionable proof is supplied for an assertion of Kronecker[4].

---

[1] Kurt Hentzelt has been missing before Dixmuiden since October 1914 and must be counted among the dead. The present article is a completely free reworking of the most essential part of his dissertation "Zur Theorie der Formenmoduln und Resultanten," with which he received his doctorate under E. Fischer in Erlangen in the summer of 1914. This dissertation, composed entirely on the basis of his own ideas, is built up without gaps; but lemma follows lemma, all concepts are paraphrased by formulas with four and five indices, and the text is almost wholly absent, so that the greatest difficulties are presented to understanding. He did not himself get to the planned reworking. I give the work again in a purely conceptual form, by which a great simplification is obtained of proofs whose fundamental ideas throughout go back to Hentzelt, and by which, as I hope, the beauty of the work becomes evident. – The parts of the dissertation that – for a given basis – concern the question of forming the functions that occur by finitely many steps are to remain reserved for a separate publication. (E. N.)

[2] These latter results show their true significance when the decomposition of ideals into primary ideals is brought in; the multiplicity corresponding to a primary ideal is then defined as the number of linearly independent residue classes of the complement modulo this ideal. This is to be taken up elsewhere. (E. N.)

[3] Cf. Macaulay, *The algebraic theory of modular systems*, Cambridge Tracts 19 (Cambridge University Press, 1916), No. 67; also Lasker, Zur Theorie der Moduln und Ideale, Math. Ann. 60 (1905), pp. 20–116; p. 98. That in this case the resultant and the resultant form coincide is shown in the still unpublished theorems of Hentzelt mentioned under 1). (E. N.)

[4] The attempted proof in König, *Algebraische GröSSen* (Leipzig 1903, Teubner), V, ğ 4 – for Kronecker's elimination theory – is known not to have succeeded. That even for the multiplicities introduced by König into Kronecker's elimination theory the second part of Hentzelt's main theorem does not hold is shown by Macaulay, loc. cit., p. 23; there it is further shown that Kronecker's elimination theory does not correspond to decomposition into primary ideals. (E. N.)

ğ 1. Modules of Linear Forms.

By integral quantities $a, b, c, \ldots$ in the first two sections we shall mean rational integers or polynomials in one indeterminate with coefficients from an arbitrary, abstractly defined field P; by linear forms $a(\xi), b(\xi), \ldots$ we shall mean such forms in finitely many indeterminates $\xi_1, \ldots, \xi_k$ with integral quantities as coefficients.

A *module* $\mathfrak{A}$ *of linear forms* is defined by the conditions: together with $a(\xi)$ and $b(\xi)$, $\mathfrak{A}$ contains the difference $a(\xi) - b(\xi)$; together with $a(\xi)$ it contains $c \cdot a(\xi)$, where c denotes an arbitrary integral quantity.

By the *rank of* $\mathfrak{A}$ we mean, as usual, the maximal number of linearly independent linear forms from $\mathfrak{A}$; by the λ-th *determinantal divisor* d_λ of $\mathfrak{A}$, the greatest common divisor of all determinants of order λ from $\mathfrak{A}$ (that is, all determinants of order λ formed from the coefficient matrix of any λ linear forms from $\mathfrak{A}$). If ρ is the rank of $\mathfrak{A}$, so that $d_1, \ldots, d_\rho$ are the non-zero determinantal divisors, then the *elementary divisors* of $\mathfrak{A}$ are defined by $e_1 = d_1$, $e_2 = d_2/d_1, \ldots, e_\rho = d_\rho/d_{\rho-1}$, $e_{\rho+i} = 0$. It is known that $\mathfrak{A}$ is a finite module having a module basis of exactly ρ linear forms $a_1(\xi), \ldots, a_\rho(\xi)$, by which every linear form from $\mathfrak{A}$ can be represented linearly, with integral quantities as coefficients: $\mathfrak{A} = (a_1(\xi), \ldots, a_\rho(\xi))$. If A denotes the coefficient matrix of these linear forms, then the determinantal and elementary divisors of $\mathfrak{A}$ agree with those of A; hence first it follows that *each elementary divisor* e_i *divides the following one* e_{i+1}. The matrix equation furnished by the elementary-divisor theory,

$$PAQ = \begin{pmatrix} e_1 & & & 0 \\ & e_2 & & \\ & & \ddots & \\ 0 & & & e_\rho \end{pmatrix},$$

further shows – if new indeterminates $\eta_1, \ldots, \eta_k$ are introduced by the unimodular transformation $\xi = Q(\eta)$ – that the module equation holds:

$$\mathfrak{A} = (e_1\eta_1, e_2\eta_2, \ldots, e_\rho\eta_\rho). \tag{1}$$

The concept most essential for what follows is that of the fundamental module[5], according to

Definition I. *A module* $\mathfrak{G}$ *is called a fundamental module if it has no proper divisor of the same rank*[6].

Thus $\mathfrak{G}$ is a fundamental module if and only if from

$$c \cdot g(\xi) \equiv 0(\mathfrak{G}); \quad c \neq 0 \quad \text{there always follows:} \quad g(\xi) \equiv 0(\mathfrak{G}). \tag{2}$$

The connection between an arbitrary module and a fundamental module is given by

Theorem I. *Every module* $\mathfrak{A}$ *is divisible by one and only one fundamental module* $\mathfrak{G}$ *of the same rank;* $\mathfrak{G}$ *is defined as the smallest divisor of* $\mathfrak{A}$ *having the same rank, and is represented by*

$$\mathfrak{G} = (\eta_1, \ldots, \eta_\rho); \tag{3}$$

$\mathfrak{G}$ *shall be called the fundamental module of* $\mathfrak{A}$.

The condition that $\mathfrak{G}$ is to be the smallest divisor of the same rank is expressed as follows: $\mathfrak{G}$ contains all and only the linear forms $g(\xi)$ that satisfy a relation

$$b \cdot g(\xi) \equiv 0(\mathfrak{A}); \quad b \neq 0. \tag{4}$$

It follows first that $\mathfrak{G}$ is a module, since together with

$$b_1 g_1(\xi) \equiv 0(\mathfrak{A}); \quad b_1 \neq 0; \qquad b_2 g_2(\xi) \equiv 0(\mathfrak{A}); \quad b_2 \neq 0$$

also

$$b_1 b_2 (g_1(\xi) - g_2(\xi)) \equiv 0(\mathfrak{A}); \quad b_1 b_2 \neq 0$$

is fulfilled; and of course also $b_1 \cdot c g_1(\xi) \equiv 0(\mathfrak{A})$. But $\mathfrak{G}$ is also a fundamental module; for from

$$c \cdot g(\xi) \equiv 0(\mathfrak{G}); \quad c \neq 0$$

[5] Cf. Steinitz, Rechteckige Systeme und Moduln in algebraischen Zahlkörpern II. Math. Ann. 72 (1912), pp. 297–345, No. 36. Hentzelt seems in any case, independently of Steinitz – with whom points of contact are also found elsewhere – to have reached, for his simpler case, the concept in the form of formula (4). (E. N.)

[6] Divisor understood in the module sense: $\mathfrak{A}$ is divisible by $\mathfrak{B}$, $\mathfrak{A} \equiv 0(\mathfrak{B})$, if every element of $\mathfrak{A}$ is contained in $\mathfrak{B}$; $\mathfrak{B}$ is called a proper divisor if it contains elements different from those of $\mathfrak{A}$.

there follows, by (4),

$$bcg(\xi) \equiv 0(\mathfrak{A}); \quad bc \neq 0,$$

and hence again by (4) also $g(\xi) \equiv 0(\mathfrak{G})$.

There is moreover no fundamental module $\mathfrak{G}_1$ different from the smallest divisor $\mathfrak{G}$ of the same rank that satisfies the conditions. For $\mathfrak{G}_1$ would have to be divisible by $\mathfrak{G}$, but as a fundamental module it has no proper divisor of the same rank, and hence is identical with $\mathfrak{G}$. Finally, the module represented by the right hand side of (3) is a fundamental module, since every proper divisor must contain a further indeterminate η, and so has higher rank. Thus (3) gives the uniquely defined fundamental module of $\mathfrak{A}$, and *Theorem I is proved in all its parts.*

A further concept essential for what follows is Dedekind's concept of the quotient of two modules[7]:

Definition II. *The quotient* $\mathfrak{c} = \mathfrak{A}/\mathfrak{B}$ *of two modules of linear forms is defined as the totality of the integral quantities* c *satisfying the condition*

$$c \cdot \mathfrak{B} \equiv 0(\mathfrak{A}).$$

$\mathfrak{c}$ *is an ideal of integral quantities, hence a principal ideal. Correspondingly, the quotient* $\mathfrak{C} = \mathfrak{A}/\mathfrak{b}$ *of a module* $\mathfrak{A}$ *of linear forms by an ideal* $\mathfrak{b}$ *of integral quantities is defined as the totality of the linear forms* $c(\xi)$ *satisfying the condition*

$$c(\xi) \cdot \mathfrak{b} \equiv 0(\mathfrak{A}).$$

$\mathfrak{C}$ *is again a module of linear forms, and indeed, as soon as* $\mathfrak{b}$ *is different from the zero ideal, a module of the same rank as* $\mathfrak{A}$.

One need only remark that by definition it is clear that the module property belongs to the quotient in each case; systems of integral quantities with the module property, however, are ideals.

The quotient concept leads to a connection between the fundamental module and the highest elementary divisor, namely:

Theorem II. *Between the fundamental module and the highest elementary divisor of* $\mathfrak{A}$ *there is the reciprocal relation*

$$(e_\rho) = \mathfrak{A}/\mathfrak{G}; \qquad \mathfrak{G} = \mathfrak{A}/(e_\rho), \tag{5}$$

where (e_ρ) *denotes the principal ideal derived from* e_ρ.

For since every elementary divisor divides e_ρ, from (1) and (3) we have

$$e_\rho \mathfrak{G} \equiv 0(\mathfrak{A}) \quad \text{and consequently} \quad (e_\rho) \cdot \mathfrak{G} \equiv 0(\mathfrak{A}); \tag{6}$$

hence (e_ρ) is divisible by the quotient $\mathfrak{A}/\mathfrak{G}$. But the converse also holds; for from

$$b\mathfrak{G} \equiv 0(\mathfrak{A}) \quad \text{there follows} \quad b\eta_\rho \equiv 0(\mathfrak{A}) \quad \text{and hence} \quad b \equiv 0((e_\rho)),$$

which proves the first formula (5)[8]. Formula (6) further shows that $\mathfrak{G}$ is divisible by the quotient $\mathfrak{A}/(e_\rho)$; this quotient is a divisor of $\mathfrak{A}$ of the same rank, hence, by the definition of the fundamental module of $\mathfrak{A}$, conversely divisible by $\mathfrak{G}$. Thus the second formula (5) is also proved.

If d denotes any determinant of order ρ from $\mathfrak{A}$ which does not vanish identically, then d is divisible by the ρ-th determinantal divisor d_ρ, and hence by e_ρ; consequently $d\mathfrak{G} \equiv 0(\mathfrak{A})$, and by the preceding conclusion $\mathfrak{G} = \mathfrak{A}/(d)$. For what follows, however, it is essential that this latter quotient representation for $\mathfrak{G}$ can be proved without going back to the elementary divisors, and hence has a more general validity, according to

[7] In Dedekind the matter concerns modules of numbers, for which multiplication is also defined, so that Dedekind's quotient does not agree with the quotient defined here. (E. N.)

[8] Set $\mathfrak{A}_0 = \mathfrak{A}, \ldots, \mathfrak{A}_\lambda = (\mathfrak{A}, \eta_\rho, \ldots, \eta_{\rho-\lambda+1})$, where in each case $\mathfrak{A}_i$ has highest elementary divisor $e_{\rho-i}$. Then by the same conclusions one obtains

$$(e_\rho) = \mathfrak{A}_0/\mathfrak{A}_1, \ldots, (e_{\rho-\lambda}) = \mathfrak{A}_\lambda/\mathfrak{A}_{\lambda+1}, \ldots, (e_1) = \mathfrak{A}_{\rho-1}/\mathfrak{A}_\rho.$$

More generally, set $\zeta_\lambda = b_{\lambda 1}\eta_1 + \cdots + b_{\lambda\lambda}\eta_\lambda$, assume $(b_{\lambda\lambda}, e_\lambda) = 1$, and let

$$\mathfrak{B}_0 = \mathfrak{A}, \ldots, \mathfrak{B}_\lambda = (\mathfrak{A}, \zeta_\rho, \ldots, \zeta_{\rho-\lambda+1}).$$

Then $\mathfrak{B}_\lambda$ also has highest elementary divisor $e_{\rho-\lambda}$, and hence

$$(e_{\rho-\lambda}) = \mathfrak{B}_\lambda/\mathfrak{B}_{\lambda+1}.$$

Theorem III. *If by integral quantities one understands polynomials in several indeterminates*[9], *then the quotient representation still holds*

$$\mathfrak{G} = \mathfrak{A}/(d), \tag{7}$$

where d denotes any determinant of order ρ from $\mathfrak{A}$ which does not vanish identically.

First it is clear that the notions of rank, fundamental module and module quotient – which now is just no longer a principal ideal – are preserved under this extension, and so is Theorem I, with the exception of the basis representation.

Let now

$$a_1(\xi) = a_{11}\xi_1 + \cdots + a_{1k}\xi_k, \ldots, a_\rho(\xi) = a_{\rho 1}\xi_1 + \cdots + a_{\rho k}\xi_k$$

be ρ linearly independent linear forms from $\mathfrak{A}$, which in general will not form a module basis. Let the indeterminates ξ be so designated that

$$d = |a_{ij}| \neq 0; \qquad i, j = 1, 2, \ldots, \rho.$$

It follows that ρ linear forms of special shape belong to $\mathfrak{A}$:

$$d\xi_\lambda + b_{\lambda,\rho+1}\xi_{\rho+1} + \cdots + b_{\lambda,k}\xi_k \equiv 0(\mathfrak{A}) \quad (\lambda = 1, 2, \ldots, \rho). \tag{8}$$

But $\mathfrak{A}$ can contain no linear form depending only on $\xi_{\rho+1}, \ldots, \xi_k$, say $c_{\rho+1}\xi_{\rho+1} + \cdots + c_k\xi_k$, since otherwise at least one determinant of order $\rho + 1$, namely $d \cdot c_\alpha$, would be non-zero.

Now the quotient $\mathfrak{A}/(d)$, as a divisor of $\mathfrak{A}$ of the same rank, is divisible by $\mathfrak{G}$; but the converse also holds. For every $g(\xi) \equiv 0(\mathfrak{G})$ satisfies, by definition,

$$c \cdot g(\xi) \equiv 0(\mathfrak{A}); \quad c \neq 0 \quad \text{and consequently} \quad d \cdot c \cdot g(\xi) \equiv 0(\mathfrak{A}).$$

By (8), however,

$$d \cdot g(\xi) = g_{\rho+1}\xi_{\rho+1} + \cdots + g_k\xi_k \equiv 0(\mathfrak{A}),$$

and consequently

$$cg_{\rho+1}\xi_{\rho+1} + \cdots + cg_k\xi_k \equiv 0(\mathfrak{A}).$$

By what has just been observed this implies $c \cdot g_{\rho+1} = 0, \ldots, c \cdot g_k = 0$, and because $c \neq 0$, also $g_{\rho+1} = 0, \ldots, g_k = 0$; hence $d \cdot g(\xi) \equiv 0(\mathfrak{A})$, proving (7).

It should be noted that $d \cdot g(\xi) \equiv 0(\mathfrak{A})$ also follows directly from the fact that the two modules $(a_1(\xi), \ldots, a_\rho(\xi))$ and $(g(\xi), a_1(\xi), \ldots, a_\rho(\xi))$ have the same rank ρ, so that – putting $g(\xi) = c_1\xi_1 + \cdots + c_k\xi_k$ – the determinant of order $\rho + 1$

$$\begin{vmatrix} a_1(\xi) & a_{11} & \cdots & a_{1\rho} \\ \vdots & \vdots & & \vdots \\ a_\rho(\xi) & a_{\rho 1} & \cdots & a_{\rho\rho} \\ g(\xi) & c_1 & \cdots & c_\rho \end{vmatrix}$$

vanishes. The proof given above, however, recurs in ğ 4 following formula (30).

ğ 2. Decomposition Theorems for Norms and Modules.

We now return to modules of linear forms with respect to rational integers or polynomials in one indeterminate with coefficients from P.

Definition III. *If, as usual, all linear forms in ξ that are congruent to one another modulo $\mathfrak{A}$ are collected into one residue class, then the symbol $\mathfrak{G} \mid \mathfrak{A}$ shall denote the system of residue classes of $\mathfrak{G}$ modulo $\mathfrak{A}$, that is, the system of all residue classes modulo $\mathfrak{A}$ that consist of elements of $\mathfrak{G}$. The norm of $\mathfrak{G}$ with respect to $\mathfrak{A}$ – in symbols $N(\mathfrak{G} \mid \mathfrak{A})$ – is defined as the determinant of the transition substitution from $\mathfrak{G}$ to $\mathfrak{A}$, that is, as the determinant of the substitution which expresses any linearly independent module basis of $\mathfrak{A}$ by such a basis of the fundamental module $\mathfrak{G}$ of $\mathfrak{A}$.*

[9] In fact only this is used: that the integral quantities reproduce themselves under addition, subtraction and multiplication, with the usual rules of calculation holding, so that they form a ring; and further, that in this ring a product vanishes only when one factor vanishes, so that the ring may be extended to a field by quotient formation (adjunction of pairs of elements). On the other hand no basis representation of the module is used; thus (7) holds for example also for the domain of all algebraic integers as coefficients. (E. N.)

From (1) and (3), respectively from the remark to Theorem II, one obtains:

$$N(\mathfrak{G} \mid \mathfrak{A}) = e_1 e_2 \cdots e_\rho = d_\rho; \qquad \mathfrak{G} = \mathfrak{A}/(N(\mathfrak{G} \mid \mathfrak{A})). \tag{9}$$

From (1), (3) and (9) it follows in the familiar way that, in the case of rational integers, $N(\mathfrak{G} \mid \mathfrak{A})$ represents the number of residue classes of $\mathfrak{G}$ modulo $\mathfrak{A}$, whereas in the case of polynomials in one indeterminate – where the number of residue classes is in general infinite – the degree of $N(\mathfrak{G} \mid \mathfrak{A})$ becomes equal to the *number of residue classes linearly independent with respect to* P. If $\mathfrak{B}$ is a divisor of $\mathfrak{A}$ of the same rank, then, together with a representative of any such residue class, $\mathfrak{B}$ also contains all elements of the residue class; hence $\mathfrak{B}$ arises from $\mathfrak{A}$ by adjoining finitely many residue classes, or their linear combinations. It follows at once that:

Theorem IV. *If $\mathfrak{B}$ is a divisor of $\mathfrak{A}$ of the same rank, so that the fundamental modules agree, and if moreover $N(\mathfrak{G} \mid \mathfrak{B}) = N(\mathfrak{G} \mid \mathfrak{A})$, then also $\mathfrak{B} = \mathfrak{A}$.*

On the connection between the decomposition of norms and modules one has

Theorem V. *Let*

$$N(\mathfrak{G} \mid \mathfrak{A}) = r \cdot s, \qquad (r, s) = 1; \tag{10}$$

then there exists one and only one module $\mathfrak{R}$, and likewise one and only one module $\mathfrak{S}$, both divisors of $\mathfrak{A}$ of the same rank, such that

$$r = N(\mathfrak{G} \mid \mathfrak{R}), \qquad s = N(\mathfrak{G} \mid \mathfrak{S})$$

holds. $\mathfrak{R}$ and $\mathfrak{S}$ are defined by

$$\mathfrak{R} = \mathfrak{A}/(s); \qquad \mathfrak{S} = \mathfrak{A}/(r),$$

and $\mathfrak{A}$ is equal to the least common multiple of $\mathfrak{R}$ and $\mathfrak{S}$.[10] *If one sets $r_\rho = (r, e_\rho)$, $s_\rho = (s, e_\rho)$, then the reciprocities hold*

$$(s_\rho) = \mathfrak{A}/\mathfrak{R}; \quad \mathfrak{R} = \mathfrak{A}/(s_\rho); \qquad (r_\rho) = \mathfrak{A}/\mathfrak{S}; \quad \mathfrak{S} = \mathfrak{A}/(r_\rho). \tag{11}$$

Indeed, setting generally $r_i = (r, e_i)$, $s_i = (s, e_i)$, one obtains from (9) and (10):

$$(r_i, s_i) = 1; \qquad e_i = r_i s_i; \qquad r = r_1 \cdots r_\rho; \qquad s = s_1 \cdots s_\rho,$$

and each r_i respectively s_i divides the following r_{i+1} respectively s_{i+1}. Thus, if one sets

$$\mathfrak{R} = (r_1\eta_1, \ldots, r_\rho\eta_\rho); \qquad \mathfrak{S} = (s_1\eta_1, \ldots, s_\rho\eta_\rho),$$

then $\mathfrak{R}$ and $\mathfrak{S}$ are divisors of $\mathfrak{A}$ of the same rank; owing to the relative primeness of r_i and s_i, $\mathfrak{A}$ becomes the least common multiple of $\mathfrak{R}$ and $\mathfrak{S}$, and moreover

$$N(\mathfrak{G} \mid \mathfrak{R}) = r_1 \cdots r_\rho = r; \qquad N(\mathfrak{G} \mid \mathfrak{S}) = s_1 \cdots s_\rho = s.$$

Furthermore

$$s_\rho \mathfrak{R} \equiv 0(\mathfrak{A}); \qquad r_\rho \mathfrak{S} \equiv 0(\mathfrak{A});$$

and from $c\mathfrak{R} \equiv 0(\mathfrak{A})$ follows $cr_\rho\eta_\rho \equiv 0(\mathfrak{A})$, hence $c \equiv 0((s_\rho))$, proving $(s_\rho) = \mathfrak{A}/\mathfrak{R}$, and similarly $(r_\rho) = \mathfrak{A}/\mathfrak{S}$. From

$$b(\eta) = b_1\eta_1 + \cdots + b_\rho\eta_\rho \equiv 0(\mathfrak{A}/(s_\rho))$$

it further follows, because all r_i are relatively prime to s_ρ, that $b_i \equiv 0((r_i))$; hence $\mathfrak{R} = \mathfrak{A}/(s_\rho)$ and similarly $\mathfrak{S} = \mathfrak{A}/(r_\rho)$. Thus the reciprocities (11) are proved; in the special case $r = 1$ they pass into (5).

It remains to show the *unique determination* of $\mathfrak{R}$ and $\mathfrak{S}$. Let $\overline{\mathfrak{R}}$ and $\overline{\mathfrak{S}}$ be modules satisfying the conditions of Theorem V, and let $\bar{r}_i$ and $\bar{s}_i$ be their elementary divisors. Since $\bar{r}_i$ and $\bar{s}_i$ are divisors of e_i, it follows, because

$$r = \bar{r}_1 \cdots \bar{r}_\rho, \qquad s = \bar{s}_1 \cdots \bar{s}_\rho, \qquad (\bar{r}_i, \bar{s}_i) = 1,$$

that also

$$e_i = \bar{r}_i\bar{s}_i, \qquad \bar{r}_i = (r, e_i) = r_i, \qquad \bar{s}_i = (s, e_i) = s_i.$$

[10] Least common multiple $[\mathfrak{R}, \mathfrak{S}]$ understood in the module sense: the totality of linear forms that are divisible both by $\mathfrak{R}$ and by $\mathfrak{S}$. Correspondingly, the greatest common divisor $(\mathfrak{R}, \mathfrak{S})$ in the module sense is to be understood as the totality of linear forms that can be represented as the sum of an element from $\mathfrak{R}$ and an element from $\mathfrak{S}$.

Thus $\overline{\mathfrak{R}}$ and $\overline{\mathfrak{S}}$ agree with $\mathfrak{R}$ and $\mathfrak{S}$ in elementary divisors and in fundamental module. If therefore, by a unimodular substitution $\eta = Q(\xi)$, new indeterminates ξ are introduced, then

$$\overline{\mathfrak{R}} = (r_1\xi_1, \ldots, r_\rho\xi_\rho);$$

$$\mathfrak{A} = (r_1 s_1(q_{11}\xi_1 + \cdots + q_{1\rho}\xi_\rho), \ldots, r_\rho s_\rho(q_{\rho 1}\xi_1 + \cdots + q_{\rho\rho}\xi_\rho)).$$

From $\mathfrak{A} \equiv 0(\mathfrak{R})$ one thus obtains

$$r_i s_i(q_{i1}\xi_1 + \cdots + q_{i\rho}\xi_\rho) \equiv 0(\mathfrak{R});$$

therefore $r_i s_i q_{ij} \equiv 0((r_i))$. Since $(r, s) = 1$, this gives $r_i q_{ij} \equiv 0((r_i))$, or $\overline{\mathfrak{R}} \equiv 0(\mathfrak{R})$. But since $N(\mathfrak{G} \mid \mathfrak{R}) = N(\mathfrak{G} \mid \overline{\mathfrak{R}})$, Theorem IV gives $\mathfrak{R} = \overline{\mathfrak{R}}$, and correspondingly $\mathfrak{S} = \overline{\mathfrak{S}}$. Theorem V is thereby proved in all its parts.

ğ 3. Ideals of Polynomials.

Let $\mathfrak{m}$ be an *ideal of polynomials* in the n indeterminates $y_1, \ldots, y_n$, with coefficients from an arbitrary, abstractly defined field P; that is, together with $\Phi_1(y)$ and $\Phi_2(y)$, $\mathfrak{m}$ also contains the difference $\Phi_1(y) - \Phi_2(y)$, and together with $\Phi(y)$ it also contains $A(y) \cdot \Phi(y)$, where $A(y)$ denotes an arbitrary polynomial with coefficients from P[11].

Let the y be subjected to a transformation with indeterminates as coefficients,

$$y = U(x); \quad \text{for instance} \quad \begin{cases} y_1 = x_1, \\ y_2 = u_{21}x_1 + x_2, \\ \cdots \\ y_n = u_{n1}x_1 + \cdots + u_{n,n-1}x_{n-1} + x_n, \end{cases} \tag{12}$$

and adjoin the indeterminates $u_{\mu\nu}$ to the coefficient domain of the polynomials, which thereby passes into a field $P(u)$. By this adjunction let $\mathfrak{m}$ pass into $\mathfrak{m}_{(u)}$; hence $\mathfrak{m}_{(u)}$ contains, besides the polynomials $\Phi_\lambda(y)$ from $\mathfrak{m}$, all linear combinations $\sum \alpha_\lambda(u)\Phi_\lambda(y)$ of finitely many Φ_λ, where $\alpha_\lambda(u)$ denotes rational functions of the $u_{\mu\nu}$ with coefficients from P. By multiplication with a suitable polynomial in u, the $\alpha_\lambda(u)$ may, without restriction of generality, be assumed to be power products in u. Thus one has

$$\sum \alpha_\lambda(u)\Phi_\lambda(y) \equiv 0(\mathfrak{m}_{(u)}); \qquad \Phi_\lambda(y) \equiv 0(\mathfrak{m}) \quad \text{and conversely.} \tag{13}$$

By means of (12), $\mathfrak{m}_{(u)}$ passes into an ideal $\mathfrak{m}$ of polynomials in $x_1, \ldots, x_n$ with coefficients from $P(u)$:

$$\mathfrak{m}_{(u)} = \mathfrak{m} \quad \text{by means of} \quad y = U(x). \tag{14}$$

The combination of the relations (14) and (13) says the following:

$$\text{From } F(x) \equiv 0(\mathfrak{m}); \quad F(x) = \Phi(y) = \sum \alpha_\lambda(u)\Phi_\lambda(y) = \sum \alpha_\lambda(u)F_\lambda(x) \text{ follows } F_\lambda(x) \equiv 0(\mathfrak{m}); \tag{15}$$

whereas (14) and (15) conversely yield (13) again.

Definition IV. *Ideals $\mathfrak{m}$ of polynomials in $x_1, \ldots, x_n$ with coefficients from $P(u)$ which satisfy the relations (15), and hence arise from $\mathfrak{m}_{(u)}$ by means of $y = U(x)$, shall be called transformed ideals.*

Transformed ideals are distinguished by the existence of regular polynomials; *a polynomial of degree r is called regular with respect to x_i if it contains the term x_i^r with non-zero coefficient.* One sees that the polynomials $F_i(x)$ are regular with respect to x_1. In what follows the main point will be to regard these transformed ideals as modules of linear forms in certain power products of the x. For this the concept of the fundamental ideal must be fixed; later it will pass into the fundamental module. We first give a notation that will be maintained throughout from now on:

Notation. *By $F^{(i)}, f^{(i)}, a^{(i)}, \ldots$ we shall always mean polynomials in the x that are free of $x_1, \ldots, x_{i-1}$.*

Definition V. *To every ideal $\mathfrak{m}$ there are defined n fundamental ideals $\mathfrak{g}_0, \mathfrak{g}_1, \ldots, \mathfrak{g}_{n-1}$ by the following stipulation: the fundamental ideal of stage $(i-1)$, $\mathfrak{g}_{i-1}$, contains all and only the polynomials $G(x)$ for which there is a polynomial $b^{(i)}$ – in general varying with $G(x)$ – such that*

$$b^{(i)}G(x) \equiv 0(\mathfrak{m}); \qquad b^{(i)} \neq 0. \tag{16}$$

[11] The conceptually resulting designation "ideal" instead of the formerly generally customary "module" or "module of forms" already proves necessary here in order to distinguish these from the modules of linear forms. (E. N.)

That the $\mathfrak{g}$ are in fact ideals corresponds exactly to the proof of the module property for $\mathfrak{G}$ following formula (4), with (16) playing the analogous role. The ideal $\mathfrak{g}_i$ is divisible by $\mathfrak{g}_{i-1}$, since every polynomial $b^{(i+1)}$ is at the same time a $b^{(i)}$.

For the fundamental ideals one has:

Theorem VI. *The fundamental ideals of transformed ideals are transformed ideals*[12].

The proof rests on a known theorem of Dedekind–Mertens[13]: let a and b be indeterminates, and set

$$\sum a_{i_1,\dots,i_s} z_1^{i_1} \cdots z_s^{i_s} \cdot \sum b_{j_1,\dots,j_s} z_1^{j_1} \cdots z_s^{j_s} = \sum c_{k_1,\dots,k_s} z_1^{k_1} \cdots z_s^{k_s},$$

$$\sum i \leq \nu, \qquad \sum j \leq \mu, \qquad \sum k \leq \nu + \mu.$$

If $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ denote the modules derived respectively from the a, b, c by means of rational integers, then there exists an exponent q such that the identity holds:

$$\mathfrak{A}^q \mathfrak{B} = \mathfrak{A}^{q-1} \mathfrak{C}. \tag{17}$$

Here $\mathfrak{A}^q$ consists of the power products of q-th dimension in the a and their integral linear combinations.

For the proof of Theorem VI, now put

$$\begin{cases} G(x) = \Gamma(y) = \sum \alpha_\lambda(u) \Gamma_\lambda(y) = \sum \alpha_\lambda(u) G_\lambda(x), \\ b^{(i)}(x) = \varphi(y) = \sum \beta_\mu(u) \varphi_\mu(y), \end{cases} \tag{18}$$

where $\alpha_\lambda(u)$ and $\beta_\mu(u)$ are power products in the u. Then, by (16), (14) and (18),

$$\sum \beta_\mu(u) \varphi_\mu(y) \cdot \sum \alpha_\lambda(u) \Gamma_\lambda(y) \equiv 0 (\overline{\mathfrak{m}}_{(u)}); \qquad \sum \beta_\mu(u) \varphi_\mu(y) \neq 0. \tag{19}$$

On the left stands the product of two polynomials in u whose coefficients are the polynomials $\varphi_\mu(y)$ and $\Gamma_\lambda(y)$; the coefficients of the product polynomial in u are, by the right hand side of (19), polynomials from $\overline{\mathfrak{m}}$. If, therefore, in (17) one replaces the a, b, c by these polynomials in y, one obtains

$$\Big\{ \sum \beta_\mu(u) \varphi_\mu(y) \Big\}^q \cdot \Gamma_\lambda(y) \equiv 0 (\overline{\mathfrak{m}}_{(u)}),$$

which by (18) is equivalent to:

$$b^{(i)}(x)^q \cdot G_\lambda(x) \equiv 0 (\mathfrak{m}); \qquad G_\lambda(x) \equiv 0 (\mathfrak{g}_{i-1}). \tag{20}$$

The relations (16), (18) and (20) show that the *fundamental ideals* $\mathfrak{g}_{i-1}$ *are indeed transformed ideals.*

ğ 4. Connection between ideals of polynomials and modules of linear forms.

To regard an ideal $\mathfrak{m}$ of polynomials, which is always assumed transformed, as a module $\mathfrak{M}_{i-1}$ $(i = 1, \dots, n)$ of linear forms, the individual polynomials $F(x)$ are to be considered as linear forms in the power products ξ_λ of $x_1 \dots x_{i-1}$:

$$F(x) = \sum a_\lambda^{(i)} \xi_\lambda,$$

where, according to the notation of ğ 3, the $a_\lambda^{(i)}$ are polynomials in $x_i \dots x_n$. From the definition of the ideal it follows at once that $\mathfrak{M}_{i-1}$ has the module property with respect to these integral quantities $a^{(i)}, b^{(i)}, \dots$; and since the infinitely many power products ξ of $x_1 \dots x_{i-1}$ occur only linearly, by reason of their linear independence they play for $\mathfrak{M}_{i-1}$ the role of indeterminates. Each module $\mathfrak{M}_{i-1}$ contains infinitely many indeterminates ξ, but in each individual linear form only finitely many indeterminates occur. Likewise each fundamental ideal $\mathfrak{g}_{i-1}$ is to be regarded as a module $\mathfrak{G}_{i-1}$ of linear forms, where the indeterminates are again the power products of $x_1 \dots x_{i-1}$. For $i = 1$ there is only one indeterminate ξ_0, corresponding to the unit.

[12] Theorem VI is used only in ğ 7.

[13] Dedekind: Über einen arithmetischen Satz von GauSS, Mitt. d. deutsch. math. Ges. zu Prag 1892. F. Mertens: Über einen algebraischen Satz, Ber. d. Ak. d. Wissensch. Wien 101 (1892), pp. 1560–1566. – Kronecker's extension of Gauss's theorem to polynomials with indeterminate coefficients is an immediate consequence of this theorem.

One can now, and this is the basis of everything that follows, restrict oneself, despite these infinitely many indeterminates ξ, to modules of linear forms in finitely many indeterminates, according to the following theorem.

Theorem VII. *The residue-class system $\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}$ is isomorphic to a residue-class system $\mathfrak{G}^*_{i-1} \mid \mathfrak{M}^*_{i-1}$, where $\mathfrak{M}^*_{i-1}$ is a module in finitely many indeterminates and $\mathfrak{G}^*_{i-1}$ is its fundamental module. The module $\mathfrak{M}_{i-1}$ has – after adjoining $x_{i+1} \dots x_n$ to $P(u)$ – only finitely many elementary divisors different from 1, namely the elementary divisors of $\mathfrak{M}^*_{i-1}$ that are different from 1.*

The elementary divisors of $\mathfrak{M}_{i-1}$ are to be defined as in note 8). The isomorphism occurring in Theorem VII rests on the following definition.

Definition V. *Two residue-class systems are called isomorphic if they can be put in one-to-one correspondence in such a way that the difference of two classes is assigned to the difference of the corresponding classes, and the product of a class by an integral quantity to the product of the corresponding class by the same integral quantity.*

The proof of Theorem VII is obtained by complete induction. For $i = 1$ the theorem is evident: $\mathfrak{M}_0$ is a module of linear forms in one indeterminate ξ_0, corresponding to the power product of dimension zero of the x, that is, to the unit; the integral quantities are all polynomials in $x_1 \dots x_n$. The fundamental ideal $\mathfrak{g}_0$ is the unit ideal consisting of all polynomials in $x_1 \dots x_n$, and hence $\mathfrak{G}_0$ is the module (ξ_0), the fundamental module of $\mathfrak{M}_0$; thus here $\mathfrak{G}^*_0 \mid \mathfrak{M}^*_0$ coincides with $\mathfrak{G}_0 \mid \mathfrak{M}_0$. Finally, since $\mathfrak{M}_0$ has rank 1, it can have at most one elementary divisor different from 1.

We first pass from $i = 1$ to $i = 2$, in order to use the insight thereby obtained into the structure of $\mathfrak{G}_1 \mid \mathfrak{M}_1$ for the general induction step. For this purpose we first show that for $\mathfrak{G}_0 \mid \mathfrak{M}_0$ an x_1-bounded system of representatives may be chosen; because of the divisibility of $\mathfrak{g}_1$ by $\mathfrak{g}_0$, this will then lead to the finitely many indeterminates of $\mathfrak{G}^*_1$.

As a transformed ideal, $\mathfrak{m}$ possesses by ğ 3 at least one polynomial $C^{(1)}(x)$ regular in x_1, say of dimension k; hence $\mathfrak{M}_0$ contains the linear form $C^{(1)}\xi_0$. By the regularity of $C^{(1)}(x)$, every polynomial $H(x)$ admits a representation

$$H(x) = b_0^{(2)} + b_1^{(2)} x_1 + \dots + b_{k-1}^{(2)} x_1^{k-1} \quad (C^{(1)}(x)); \tag{21}$$

therefore, since $C^{(1)}\xi_0$ belongs to $\mathfrak{M}_0$, one can indeed choose for $\mathfrak{G}_0 \mid \mathfrak{M}_0$ a system of representatives that does not reach the k-th dimension in x_1.

If now, in particular, for the polynomials $G(x)$ from $\mathfrak{g}_1$ and $F(x)$ from $\mathfrak{m}$ one writes

$$\begin{cases} G(x) = g_0^{(2)} + g_1^{(2)} x_1 + \dots + g_{k-1}^{(2)} x_1^{k-1} & (C^{(1)}(x)), \\ F(x) = a_0^{(2)} + a_1^{(2)} x_1 + \dots + a_{k-1}^{(2)} x_1^{k-1} & (C^{(1)}(x)), \end{cases} \tag{22}$$

and if $\mathfrak{G}^*_1$ denotes the system of all linear forms $g(\xi) = g_0^{(2)}\xi_0 + \dots + g_{k-1}^{(2)}\xi_{k-1}$, and correspondingly $\mathfrak{M}^*_1$ the system of the linear forms $a(\xi) = a_0^{(2)}\xi_0 + \dots + a_{k-1}^{(2)}\xi_{k-1}$, then the ideal property of $\mathfrak{g}_1$ and $\mathfrak{m}$ shows that $\mathfrak{G}^*_1$ and $\mathfrak{M}^*_1$ are modules of linear forms in $\xi_0 \dots \xi_{k-1}$ with respect to the integral quantities $b^{(2)}, c^{(2)}, \dots$. Likewise the principal ideal derived from $C^{(1)}(x)$ gives a module with respect to these integral quantities,

$$\mathfrak{G}_1 = (\xi_0, \xi_1, \dots, \xi_r, \dots),$$

where $\xi_r = x_1^r C^{(1)}(x)$. The ξ_r are linearly independent with respect to these integral quantities $b^{(2)}, c^{(2)}, \dots$, both among themselves and from the finitely many ξ. From the divisibility of $\mathfrak{G}_1$ by $\mathfrak{M}_1$, and hence by $\mathfrak{G}_1$, it follows that $\mathfrak{G}^*_1$ is divisible by $\mathfrak{G}_1$ and $\mathfrak{M}^*_1$ by $\mathfrak{M}_1$. Taking (22) into account, one obtains

$$\mathfrak{G}_1 = (\mathfrak{G}^*_1, \mathfrak{G}_1), \qquad \mathfrak{M}_1 = (\mathfrak{M}^*_1, \mathfrak{G}_1). \tag{23}$$

From (23) and from the linear independence of the ξ and ξ, Theorem VII for $i = 2$ follows as follows. Because $\mathfrak{G}_1$ is divisible by $\mathfrak{M}_1$, one first has $\mathfrak{G}_1 \mid \mathfrak{M}_1 = \mathfrak{G}^*_1 \mid \mathfrak{M}_1$. To prove the isomorphism with $\mathfrak{G}^*_1 \mid \mathfrak{M}^*_1$, let certain linear forms $g^*(\xi)$ from $\mathfrak{G}^*_1$ give a system of representatives of $\mathfrak{G}^*_1 \mid \mathfrak{M}^*_1$. Because of the linear independence of the ξ and ξ, from $g^*(\xi) \equiv 0(\mathfrak{M}_1)$ it follows also that $g^*(\xi) \equiv 0(\mathfrak{M}^*_1)$; the $g^*(\xi)$ are therefore also incongruent modulo $\mathfrak{M}_1$, form a system of representatives of $\mathfrak{G}_1 \mid \mathfrak{M}_1$, and the correspondence from $\mathfrak{G}_1 \mid \mathfrak{M}_1$ to $\mathfrak{G}^*_1 \mid \mathfrak{M}^*_1$ mediated by this system of representatives is isomorphic in the sense of Definition V.

In exactly the same way one obtains: from $b^{(2)}g(\xi) \equiv 0(\mathfrak{M}_1)$, $b^{(2)} \neq 0$, follows $b^{(2)}g(\xi) \equiv 0(\mathfrak{M}^*_1)$, $b^{(2)} \neq 0$. Since this is satisfied for all $g(\xi)$ from $\mathfrak{G}^*_1$, and only for these – for by (23) $\mathfrak{G}^*_1$ consists of all polynomials of

the fundamental ideal $\mathfrak{g}_1$ that are at the same time linear forms in ξ – $\mathfrak{G}_1^*$ is thereby characterized as the fundamental module of $\mathfrak{M}_1^*$.

Adjoining finally $x_3 \dots x_n$ to $P(u)$, one gets

$$\begin{cases} \mathfrak{G}_1^* = (\eta_1, \dots, \eta_\rho), & \mathfrak{M}_1^* = (e_1\eta_1, \dots, e_\rho\eta_\rho), \\ \mathfrak{G}_1 = (\eta_\rho, \dots, \eta_1, \xi_0, \dots, \xi_r, \dots), & \mathfrak{M}_1 = (e_\rho\eta_\rho, \dots, e_1\eta_1, \xi_0, \dots, \xi_r, \dots), \end{cases} \tag{24}$$

and hence

$$(e_\rho) = \mathfrak{M}_1/\mathfrak{G}_1 = \mathfrak{M}_1/(\mathfrak{M}_1, \eta_\rho), \qquad (e_{\rho-1}) = (\mathfrak{M}_1, \eta_\rho)/\mathfrak{G}_1 \quad \text{etc.}$$

Thus, taking note 8) into account, $e_\rho, e_{\rho-1}, \dots, e_1, 1, \dots, 1, \dots$ are recognized as the elementary divisors of $\mathfrak{M}_1$. This proves all parts of Theorem VII for $i = 2$.

It should be noted that (22) and (23) use only that $C^{(1)}(x)$ is regular in x_1. These formulae, and the arguments attached to them leading to Theorem VII, therefore remain valid if, in place of (12), the special transformation

$$y_1 = x_1; \quad y_2 = u_{21}x_1 + z_2; \quad \dots; \quad y_n = u_{n1}x_1 + z_n \tag{25}$$

is taken as the basis; by composition with

$$\begin{cases} z = U_1(x) \quad \text{or} \\ z_2 = x_2; \quad z_3 = u_{32}x_2 + x_3; \quad \dots; \quad z_n = u_{n2}x_2 + \dots + u_{n,n-1}x_{n-1} + x_n, \end{cases} \tag{26}$$

this again gives (12). If $\tilde{\mathfrak{m}}_{(u)}$ passes by means of (25) into $\tilde{\mathfrak{m}}$, and if $\tilde{\mathfrak{g}}_1, \tilde{\mathfrak{G}}_1, \dots$ have for $\tilde{\mathfrak{m}}$ the same meaning as $\mathfrak{g}_1, \mathfrak{G}_1, \dots$ have for $\mathfrak{m}$, then

$$\tilde{\mathfrak{G}}_1 = (\tilde{\mathfrak{G}}_1^*, \tilde{\mathfrak{G}}_1), \qquad \tilde{\mathfrak{M}}_1 = (\tilde{\mathfrak{M}}_1^*, \tilde{\mathfrak{G}}_1). \tag{27}$$

Here (27) arises from (23) simply by inversion of (26). This is evident for $\mathfrak{m}$ and $C^{(1)}(x)$, and hence also for $\mathfrak{G}_1$ and $\mathfrak{M}_1$. It is also true for $\mathfrak{g}_1$, since

$$b^{(2)}(x)G(x) \equiv 0(\mathfrak{m}), \quad b^{(2)} \neq 0, \qquad \tilde{b}^{(2)}(z)\tilde{G}(x,z) \equiv 0(\tilde{\mathfrak{m}}), \quad \tilde{b}^{(2)} \neq 0$$

mutually condition one another through $z = U_1(x)$. Thus $\tilde{\mathfrak{g}}_1 = \mathfrak{g}_1$ by means of (26); hence also $\tilde{\mathfrak{G}}_1 = \mathfrak{G}_1$. Consequently, by the definition given through (22), the same holds for $\mathfrak{G}_1^*$ and $\mathfrak{M}_1^*$ as for $\tilde{\mathfrak{G}}_1^*$ and $\tilde{\mathfrak{M}}_1^*$, and so for the whole representation (27).

For the general induction step, suppose the following hypotheses hold:

$$\begin{cases} \mathfrak{G}_{i-1} = (\mathfrak{G}_{i-1}^*, \mathfrak{G}_{i-1}), & \mathfrak{M}_{i-1} = (\mathfrak{M}_{i-1}^*, \mathfrak{G}_{i-1}), \\ \mathfrak{G}_{i-1} = (\xi_0, \xi_1, \dots, \xi_r, \dots), \end{cases} \tag{28}$$

where $\mathfrak{G}_{i-1}^*$ and $\mathfrak{M}_{i-1}^*$ are modules, with respect to the integral quantities $b^{(i)}, c^{(i)}, \dots$, of linear forms in finitely many indeterminates ξ, certain power products of $x_1, \dots, x_{i-1}$; and where the ξ are linearly independent, both among themselves and from the ξ, with respect to these integral quantities. A representation corresponding to (28), and the linear independence of the ξ and ξ, is also to hold when, instead of (12), one uses the special transformation

$$\begin{aligned} &y_1 = x_1; \quad \dots; \quad y_{i-1} = u_{i-1,1}x_1 + \dots + x_{i-1}; \\ &y_i = u_{i,1}x_1 + \dots + u_{i,i-1}x_{i-1} + z_i; \quad \dots; \quad y_n = u_{n,1}x_1 + \dots + u_{n,i-1}x_{i-1} + z_n, \end{aligned} \tag{29}$$

which can be composed to give (12) by means of

$$z = U_{i-1}(x) \quad \text{or} \quad z_i = x_i; \quad z_{i+1} = u_{i+1,i}x_i + x_{i+1}; \quad \dots; \quad z_n = u_{n,i}x_i + \dots + u_{n,n-1}x_{n-1} + x_n.$$

Moreover this special representation is to arise from (28) simply by inversion of $z = U_{i-1}(x)$.

From the hypotheses (28) and the linear independence of the ξ and ξ, the isomorphism of $\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}$ with $\mathfrak{G}_{i-1}^* \mid \mathfrak{M}_{i-1}^*$ follows by assignment to the same system of representatives, by exactly the same arguments as those attached above to (23). Likewise it follows that $\mathfrak{G}_{i-1}^*$ becomes the fundamental module of $\mathfrak{M}_{i-1}^*$, and that $\mathfrak{M}_{i-1}$ has only finitely many elementary divisors different from 1, namely those elementary divisors of $\mathfrak{M}_{i-1}^*$ that are different from 1.

To carry out the induction step it remains first to show again that for $\mathfrak{G}^*_{i-1} \mid \mathfrak{M}^*_{i-1}$, and hence also for $\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}$, an x_i-bounded system of representatives may be chosen. This follows from the quotient representation proved in (7), Theorem III:

$$\mathfrak{G}^*_{i-1} = \mathfrak{M}^*_{i-1}/(C^{(i)}), \tag{30}$$

where $C^{(i)}$ means any non-identically vanishing determinant of degree ρ from $\mathfrak{M}^*_{i-1}$, ρ being the rank of $\mathfrak{M}^*_{i-1}$. From the part of the hypotheses referring to the special transformation (29), it follows that $C^{(i)}$ may always be assumed regular with respect to x_i. For the module $\widetilde{\mathfrak{M}}^*_{i-1}$ corresponding to $\mathfrak{M}^*_{i-1}$ has the same rank; if $\widetilde{C}^{(i)}$ denotes any non-identically vanishing determinant of degree ρ from $\widetilde{\mathfrak{M}}^*_{i-1}$ which passes by $z = U_{i-1}(x)$ into a regular $C^{(i)}$, then by hypothesis $C^{(i)}$ is a determinant of degree ρ from $\mathfrak{M}^*_{i-1}$.

From the existence of $C^{(i)}$ it follows, as in (8), with a suitable numbering of the ξ, that ρ linear forms of the special shape

$$L_\lambda(\xi) = C^{(i)}\xi_\lambda + c^{(i)}_{\lambda,1}\xi_{\rho+1} + \cdots + c^{(i)}_{\lambda,s-\rho}\xi_s \qquad (\lambda = 1 \ldots \rho)$$

belong to $\mathfrak{M}^*_{i-1}$. Every linear form in ξ can now be brought into the form

$$H(\xi) = a^{(i)}_1\xi_1 + \cdots + a^{(i)}_\rho\xi_\rho + b^{(i)}_1\xi_{\rho+1} + \cdots + b^{(i)}_{s-\rho}\xi_s \quad (L_1(\xi), \ldots, L_\rho(\xi)), \tag{31}$$

where $a^{(i)}_1 \ldots a^{(i)}_\rho$ are bounded in x_i and do not reach the degree k of $C^{(i)}$. This representation is unique; for from

$$a^{(i)}_1\xi_1 + \cdots + a^{(i)}_\rho\xi_\rho + b^{(i)}_1\xi_{\rho+1} + \cdots + b^{(i)}_{s-\rho}\xi_s \equiv 0 \quad (L_1(\xi), \ldots, L_\rho(\xi))$$

it follows, by comparing coefficients in $\xi_1 \ldots \xi_\rho$ and considering the degrees in x_i, that all $a^{(i)}$ and $b^{(i)}$ vanish identically.

Let now in particular

$$H(\xi) \equiv 0(\mathfrak{G}^*_{i-1}); \qquad \text{hence} \qquad C^{(i)}H(\xi) \equiv 0(\mathfrak{M}^*_{i-1}) \quad \text{by (30).}$$

As in the proof of Theorem III one obtains

$$C^{(i)}H(\xi) - \sum_{\tau=1}^{s-\rho}\{C^{(i)}b^{(i)}_\tau - \sum_\lambda a^{(i)}_\lambda c^{(i)}_{\lambda,\tau}\}\xi_{\rho+\tau} \equiv 0(\mathfrak{M}^*_{i-1}),$$

and therefore, since as in Theorem III the coefficients of $\xi_{\rho+1} \ldots \xi_s$ must vanish,

$$C^{(i)}b^{(i)}_\tau = \sum_\lambda a^{(i)}_\lambda c^{(i)}_{\lambda,\tau} \qquad (\tau = 1 \ldots s-\rho).$$

Thus the $b^{(i)}_\tau$ are also bounded and do not reach the maximal degree of the $c^{(i)}_{\lambda,\tau}$. The existence of an x_i-bounded system of representatives for $\mathfrak{G}^*_{i-1} \mid \mathfrak{M}^*_{i-1}$, that is for $\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}$, not reaching a certain fixed degree r, is thereby proved.

Let $\vartheta_1 \ldots \vartheta_t$ denote the finitely many power products

$$x_i^\alpha\xi_\lambda \quad (\alpha = 0, 1, \ldots, k-1;\ \lambda = 1, 2, \ldots, \rho), \qquad x_i^\beta\xi_{\rho+\tau} \quad (\beta = 0, 1, \ldots, r-1;\ \tau = 1, 2, \ldots, s-\rho)$$

and arrange the countably infinite expressions

$$x_i^\gamma L_\lambda \quad (\gamma = 0, 1, \ldots \text{ in inf.};\ \lambda = 1, 2, \ldots, \rho), \qquad x_i^\gamma\xi_\nu \quad (\gamma, \nu = 0, 1, \ldots \text{ in inf.})$$

in a simply infinite sequence $\omega_0, \omega_1, \ldots, \omega_\mu, \ldots$. Then the ϑ and ω are linearly independent, both each among themselves and from one another, with respect to the integral quantities $b^{(i+1)}, c^{(i+1)}, \ldots$. For from

$$\sum c^{(i+1)}_\alpha x_i^\alpha\xi_\lambda + \sum c^{(i+1)}_\beta x_i^\beta\xi_{\rho+\tau} + \sum d^{(i+1)}_\gamma x_i^\gamma L_\lambda(\xi) + \sum e^{(i+1)}_{\gamma\nu} x_i^\gamma\xi_\nu = 0,$$

each sum extending over finitely many terms, the assumed linear independence of the ξ and ξ, and of the ξ among themselves with respect to the integral quantities $b^{(i)}$, gives the vanishing of all $e^{(i+1)}_{\gamma\nu}$. The uniqueness of the representation (31) further gives the vanishing of the $c^{(i+1)}_\alpha$ and $c^{(i+1)}_\beta$, and finally, because of the linear independence of the $L_\lambda(\xi)$, the vanishing of the $d^{(i+1)}_\gamma$.

If the module $(\mathfrak{G}_{i-1}, L_1(\xi), \ldots, L_\rho(\xi))$ is now regarded as a module $\mathfrak{G}_i$ with respect to the integral quantities $b^{(i+1)}$, then $\mathfrak{G}_i$ is divisible by $\mathfrak{M}_i$, because $\mathfrak{G}_{i-1}, L_1(\xi), \ldots, L_\rho(\xi)$ are divisible by $\mathfrak{M}_{i-1}$, and

$$\mathfrak{G}_i = (\omega_0, \omega_1, \ldots, \omega_\mu, \ldots).$$

For each $H(x) \equiv 0(\mathfrak{g}_{i-1})$, (28), (31), and what has just been proved give

$$H(x) = b_1^{(i+1)}\vartheta_1 + \cdots + b_t^{(i+1)}\vartheta_t \quad (\mathfrak{G}_i)$$

as a module equation with respect to the integral quantities $b^{(i+1)}, c^{(i+1)}$. Since $\mathfrak{g}_i$ is divisible by $\mathfrak{g}_{i-1}$ and $\mathfrak{m}$ is divisible by $\mathfrak{g}_i$, if one now sets, in particular, for every $G(x)$ from $\mathfrak{G}_i$ and every $F(x)$ from $\mathfrak{M}_i$,

$$G(x) = g_1^{(i+1)}\vartheta_1 + \cdots + g_t^{(i+1)}\vartheta_t \quad (\mathfrak{G}_i), \qquad F(x) = a_1^{(i+1)}\vartheta_1 + \cdots + a_t^{(i+1)}\vartheta_t \quad (\mathfrak{G}_i),$$

and denotes by $\mathfrak{G}_i^*$ the module consisting of all $g(\vartheta)$, and by $\mathfrak{M}_i^*$ the module consisting of all $a(\vartheta)$, then exactly the arguments leading to (23) give

$$\mathfrak{G}_i = (\mathfrak{G}_i^*, \mathfrak{G}_i), \qquad \mathfrak{M}_i = (\mathfrak{M}_i^*, \mathfrak{G}_i), \qquad \mathfrak{G}_i = (\omega_0, \omega_1, \ldots, \omega_\mu, \ldots). \tag{32}$$

In deriving (32), again only the regularity of $C^{(i)}$ in x_i was used, so the whole argument remains valid if the special transformation (29) is taken with the index increased by one. The same considerations as those attached to (27) then show that this special representation arises from (32) simply by the inversion of $z = U_i(x)$.

Thus all hypotheses (28), etc., of the general induction step have been proved for the next index; and since, as shown there, Theorem VII follows directly from these hypotheses, Theorem VII is proved in general. At the same time it has been shown that the arbitrariness in $(\mathfrak{G}_{i-1}^*, \mathfrak{M}_{i-1}^*)$ caused by the arbitrary choice of $C^{(i)}$ is again removed by the isomorphism of the residue-class system $\mathfrak{G}_{i-1}^* \mid \mathfrak{M}_{i-1}^*$.

In particular, if the field P used in ğ 3 as coefficient domain has characteristic zero – that is, if the prime field contained in P and derived from the unit is of the type of the rational numbers – then the indeterminates $u_{\mu\nu}$ can be specialized to quantities $\bar{u}_{\mu\nu}$ from P in such a way that for $i = 1 \ldots n$ each $C^{(i)}$ remains regular in x_i. The above arguments show that Theorem VII remains valid under this specialization as well.[14] The fundamental module and elementary divisors need not, however, arise necessarily from the general case by the specialization $u_{\mu\nu} = \bar{u}_{\mu\nu}$.[15]

ğ 5. Resultant form and elementary-divisor form of an ideal of polynomials.

Let $x_{i+1} \ldots x_n$ be adjoined to $P(u)$, so that $\mathfrak{G}_{i-1}$ and $\mathfrak{M}_{i-1}$, and therefore also $\mathfrak{G}_{i-1}^*$ and $\mathfrak{M}_{i-1}^*$, pass into modules of linear forms in which the integral quantities can be regarded as polynomials in one indeterminate x_i. By Theorem VII, in this case the elementary divisors different from 1 of $\mathfrak{M}_{i-1}$, together with at most finitely many elementary divisors equal to 1, agree with those of $\mathfrak{M}_{i-1}^*$. The product of these elementary divisors, the ρ-th determinantal divisor of $\mathfrak{M}_{i-1}^*$, was equal to the determinant of the transition substitution from $\mathfrak{G}_{i-1}^*$ to $\mathfrak{M}_{i-1}^*$, hence to $N(\mathfrak{G}_{i-1}^* \mid \mathfrak{M}_{i-1}^*)$ by Definition III. Formula (24), or the analogous formula following from (28) for general i, shows that the product of these elementary divisors is also equal to the determinant of the transition substitution from $\mathfrak{G}_{i-1}$ to $\mathfrak{M}_{i-1}$, and is therefore to be denoted by $N(\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1})$. Thus

$$N(\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}) = N(\mathfrak{G}_{i-1}^* \mid \mathfrak{M}_{i-1}^*) = R^{(i)}(x),$$

where the polynomial $R^{(i)}(x)$, that is, the greatest common divisor, in the polynomial sense, of all ρ-rowed determinants from $\mathfrak{M}_{i-1}^*$, may be assumed integral and primitive in $x_{i+1} \ldots x_n$, and consequently, as a divisor of $C^{(i)}$, becomes regular in x_i. Likewise the highest elementary divisor $E^{(i)}(x)$ of $\mathfrak{M}_{i-1}$, respectively of $\mathfrak{M}_{i-1}^*$,

[14] Hentzelt takes, instead of an arbitrary P, only the field of all complex numbers and treats chiefly this latter case, whereas he uses indeterminates only in the actual elimination theory. Hentzelt then further shows, essentially by the arguments given here, that in order to form the resultant form it suffices to go, in each $\mathfrak{M}_{i-1}$, only up to some finite degree in the x that exceeds a fixed bound. What is missing is the isomorphism of $\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}$ with $\mathfrak{G}_{i-1}^* \mid \mathfrak{M}_{i-1}^*$ given in Theorem VII, which explains the independence from the degree numbers. (E. N.)

[15] For $\mathfrak{m} = (x^2, ux + y)$ one has $\mathfrak{g}_0 = (1)$, $\mathfrak{g}_1 = (1)$. If $C^{(1)} = x^2$ is chosen, then $\mathfrak{G}_1^* = (1, x)$, $\mathfrak{M}_1^* = (ux + y, xy)$; this $\mathfrak{M}_1^*$ has elementary divisors y^2 and 1, and $C^{(2)} = y^2$ can be chosen. For $u = 0$, $C^{(1)}$ and $C^{(2)}$ remain regular in x and y respectively; but $\mathfrak{M}_1^* = (y, xy)$ has elementary divisors y, y. Thus $\mathfrak{G}_1 \mid \mathfrak{M}_1$ is still isomorphic to the residue-class system of a finite module, but is not isomorphic to $\mathfrak{G}_1 \mid \mathfrak{M}_1$. If instead one had chosen $C^{(1)} = ux + y$ and specialized so that $C^{(1)}$ remained regular, the isomorphism would also have been preserved. (E. N.)

may be assumed integral and primitive in $x_{i+1}\dots x_n$ and hence regular in x_i. This leads to the following definition.

Definition VI. *The polynomial $R^{(i)}(x)$ is called the resultant of the i-th stage of $\mathfrak{m}$, and $E^{(i)}(x)$ the elementary divisor of the i-th stage. Thus the resultant of the i-th stage is the norm of the fundamental ideal $\mathfrak{g}_{i-1}$ with respect to $\mathfrak{m}$, interpreted as the norm of the module $\mathfrak{G}_{i-1}$ with respect to $\mathfrak{M}_{i-1}$, where $x_{i+1}\dots x_n$ are adjoined to $P(u)$; likewise $E^{(i)}(x)$, under the same adjunction, becomes equal to the quotient $\mathfrak{M}_{i-1}/\mathfrak{G}_{i-1}$. The resultant form and elementary-divisor form of $\mathfrak{m}$ are the products*

$$R_{\mathfrak{m}} = R^{(1)}R^{(2)}\cdots R^{(n)}, \qquad E_{\mathfrak{m}} = E^{(1)}E^{(2)}\cdots E^{(n)}.$$

For resultant form and elementary-divisor form one has:

Theorem VIII. *The resultant form is divisible by the elementary form; conversely, a power of $E_{\mathfrak{m}}$ is divisible by $R_{\mathfrak{m}}$. The forms $E_{\mathfrak{m}}$ and $R_{\mathfrak{m}}$ are divisible by $\mathfrak{m}$; more generally, $E^{(i)}\cdots E^{(n)}\mathfrak{g}_{i-1} \equiv 0(\mathfrak{m})$ and consequently $R^{(i)}\cdots R^{(n)}\mathfrak{g}_{i-1} \equiv 0(\mathfrak{m})$.*

Indeed, since the norm is divisible by the highest elementary divisor and conversely a power of this highest elementary divisor is divisible by the norm, this divisibility follows for $R^{(i)}(x)$ and $E^{(i)}(x)$ after adjoining $x_{i+1}\dots x_n$. But $R^{(i)}(x)$ and $E^{(i)}(x)$ are assumed primitive polynomials with respect to $x_{i+1}\dots x_n$; hence the divisibility holds with respect to all indeterminates $x_i, x_{i+1}, \dots, x_n$. Thus $R_{\mathfrak{m}}$ is divisible by $E_{\mathfrak{m}}$, and some power of $E_{\mathfrak{m}}$ by $R_{\mathfrak{m}}$, according to the definition of these expressions in all indeterminates x.

Furthermore, by Theorems VII and II, after adjoining $x_{i+1}\dots x_n$, the highest elementary divisor $E^{(i)}(x)$ is defined as the quotient $\mathfrak{M}_{i-1}/\mathfrak{G}_{i-1}$. Thus, returning to polynomials in all indeterminates x, for every

$$G(x) \equiv 0(\mathfrak{g}_{i-1}) \quad \text{there is a} \quad b^{(i+1)} \neq 0 \quad \text{such that} \quad b^{(i+1)}E^{(i)}(x)G(x) \equiv 0(\mathfrak{m}). \tag{33}$$

In particular $\mathfrak{g}_0$ is the unit ideal, whence

$$b^{(2)}E^{(1)}(x) \equiv 0(\mathfrak{m}), \quad b^{(2)} \neq 0, \qquad \text{and thus} \qquad E^{(1)}(x) \equiv 0(\mathfrak{g}_1).$$

In general, from (33), applied to

$$E^{(1)}(x)\cdots E^{(i-1)}(x) \equiv 0(\mathfrak{g}_{i-1}),$$

there exists $b^{(i+1)} \neq 0$ such that $b^{(i+1)}E^{(1)}\cdots E^{(i)} \equiv 0(\mathfrak{m})$; hence $E^{(1)}\cdots E^{(i)} \equiv 0(\mathfrak{g}_i)$. Since $\mathfrak{g}_n = \mathfrak{m}$, one obtains

$$E_{\mathfrak{m}} = E^{(1)}\cdots E^{(n)} \equiv 0(\mathfrak{m}) \quad \text{and consequently} \quad R_{\mathfrak{m}} = R^{(1)}\cdots R^{(n)} \equiv 0(\mathfrak{m}). \tag{34}$$

If in (33) $G(x)$ runs through the finitely many polynomials of an ideal basis of $\mathfrak{g}_{i-1}$, and if $c^{(i+1)}(x)$ denotes the product of the corresponding $b^{(i+1)}(x)$, then

$$c^{(i+1)}E^{(i)}(x)\mathfrak{g}_{i-1} \equiv 0(\mathfrak{m}); \qquad c^{(i+1)} \neq 0, \quad \text{and hence} \quad E^{(i)}(x)\mathfrak{g}_{i-1} \equiv 0(\mathfrak{g}_i),$$

and from this, as above, by finite repetition,

$$E^{(n)}(x)\cdots E^{(i)}(x)\mathfrak{g}_{i-1} \equiv 0(\mathfrak{m})$$

and consequently also

$$R^{(n)}(x)\cdots R^{(i)}(x)\mathfrak{g}_{i-1} \equiv 0(\mathfrak{m}).$$

This proves all parts of Theorem VIII.

Theorem VIII depends essentially on properties of the elementary-divisor form; the characteristic significance of the resultant form for $\mathfrak{m}$ is shown by

Theorem IX. *If $\mathfrak{n}$ is a divisor of $\mathfrak{m}$ – divisor understood in the ideal sense – and if the resultant forms $R_{\mathfrak{n}}$ and $R_{\mathfrak{m}}$ agree, then the ideals $\mathfrak{n}$ and $\mathfrak{m}$ agree.*

Let $\mathfrak{g}_0 \dots \mathfrak{g}_{n-1}, \mathfrak{g}_n = \mathfrak{m}$ and $\mathfrak{h}_0 \dots \mathfrak{h}_{n-1}, \mathfrak{h}_n = \mathfrak{n}$ denote the fundamental ideals of $\mathfrak{m}$ and $\mathfrak{n}$. First $\mathfrak{g}_0$ and $\mathfrak{h}_0$ are both the unit ideal, hence $\mathfrak{g}_0 = \mathfrak{h}_0$. Assume now that $\mathfrak{g}_{i-1} = \mathfrak{h}_{i-1}$, so that $\mathfrak{M}_{i-1}$ and $\mathfrak{N}_{i-1}$ have the same fundamental module $\mathfrak{G}_{i-1}$. The hypothesis $R_{\mathfrak{n}} = R_{\mathfrak{m}}$, after adjoining $x_{i+1}\dots x_n$, may be written as

$$N(\mathfrak{G}_{i-1} \mid \mathfrak{N}_{i-1}) = N(\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}) \quad \text{or} \quad N(\mathfrak{G}^*_{i-1} \mid \mathfrak{N}^*_{i-1}) = N(\mathfrak{G}^*_{i-1} \mid \mathfrak{M}^*_{i-1}).$$

Here, in accordance with (32), $\mathfrak{N}_{i-1} = (\mathfrak{N}^*_{i-1}, \mathfrak{G}_{i-1})$, so that $\mathfrak{N}^*_{i-1}$ is likewise a module of linear forms in ξ, with $\mathfrak{G}^*_{i-1}$ as its fundamental module. Since $\mathfrak{M}_{i-1}$ is divisible by $\mathfrak{N}_{i-1}$, which entails the divisibility of

$\mathfrak{M}^*_{i-1}$ by $\mathfrak{N}^*_{i-1}$, Theorem IV shows that, under this adjunction, the two modules $\mathfrak{M}^*_{i-1}$ and $\mathfrak{N}^*_{i-1}$ agree, and consequently so do $\mathfrak{N}_{i-1}$ and $\mathfrak{M}_{i-1}$. But adjoining $x_{i+1}\dots x_n$ means that one adds to $\mathfrak{M}_{i-1}$, respectively to $\mathfrak{m}$, all polynomials $G(x)$ for which

$$b^{(i+1)}(x)G(x) \equiv 0(\mathfrak{m}), \qquad b^{(i+1)} \neq 0.$$

Thus, by the adjunction, $\mathfrak{M}_{i-1}$, respectively $\mathfrak{m}$, passes into $\mathfrak{g}_i$, and correspondingly $\mathfrak{n}$ into $\mathfrak{h}_i$; therefore $\mathfrak{g}_i = \mathfrak{h}_i$. Hence finally $\mathfrak{g}_n = \mathfrak{h}_n$, i.e. $\mathfrak{m} = \mathfrak{n}$.

Finally the same transfer principle, applied to Theorem V, gives the following.

Theorem X. *Let $R^{(i)} = S^{(i)}T^{(i)}$ be a decomposition of $R^{(i)}$ into relatively prime polynomials $S^{(i)}$ and $T^{(i)}$ in the polynomial sense. Then there exists one and only one ideal $\mathfrak{j}$, and likewise one and only one ideal $\mathfrak{t}$, both divisors of $\mathfrak{m}$ with the same fundamental ideal of the $(i-1)$-st stage, $\mathfrak{g}_{i-1}$, such that $S^{(i)} = N(\mathfrak{G}_{i-1} \mid \mathfrak{S}_{i-1})$ and $T^{(i)} = N(\mathfrak{G}_{i-1} \mid \mathfrak{T}_{i-1})$. The ideals $\mathfrak{j}$ and $\mathfrak{t}$ are defined as the totality of polynomials $S(x)$ and $T(x)$, respectively, such that*

$$s^{(i+1)}(x)T^{(i)}(x)S(x) \equiv 0(\mathfrak{m}), \quad s^{(i+1)} \neq 0,$$
$$t^{(i+1)}(x)S^{(i)}(x)T(x) \equiv 0(\mathfrak{m}), \quad t^{(i+1)} \neq 0,$$

and $\mathfrak{g}_i$ becomes the least common multiple of $\mathfrak{j}$ and $\mathfrak{t}$,

$$\mathfrak{g}_i = [\mathfrak{j}, \mathfrak{t}].$$

It remains only to note that $s^{(i+1)}$ and $t^{(i+1)}$ can be chosen fixed for $\mathfrak{j}$ and $\mathfrak{t}$, as the product of the $s^{(i+1)}$ and $t^{(i+1)}$ corresponding to the basis elements of $\mathfrak{j}$ and $\mathfrak{t}$, and that, as remarked above, by adjoining $x_{i+1}\dots x_n$ the ideal $\mathfrak{m}$ is transformed into $\mathfrak{g}_i$. In particular, the decomposition of $R^{(i)}$ can be continued up to powers of irreducible polynomials – primary factors – which entails a corresponding representation of $\mathfrak{g}_i$ as a least common multiple.

ğ 6. Proper elimination theory.

By Theorem VIII, respectively formula (34), the resultant form and the elementary-divisor form are divisible by $\mathfrak{m}$, and therefore vanish at all zeros of $\mathfrak{m}$. Here by "zeros of $\mathfrak{m}$" are meant value systems of $x_1\dots x_i$ belonging to the algebraically closed field derived from $P(u; x_{i+1}\dots x_n)$[16], such that every polynomial from $\mathfrak{m}$ vanishes at these value systems, while $x_{i+1}\dots x_n$ are thought of as adjoined to the coefficient field $(i = 1, \dots, n)$. These adjoined $x_{i+1}\dots x_n$ can, as will be shown, also be replaced by quantities from $P(u)$. The content of elimination theory, conversely, is the derivation of the zeros of $\mathfrak{m}$ from those of the resultant form. This converse rests on the successive elimination to be developed in this section; since in the next section the divisibility of the form $D^{(i)}(x)$ occurring in it by $E^{(i)}(x)$ will be proved, the desired converse follows from the divisibility of a power of $E^{(i)}(x)$ by $R^{(i)}(x)$.

The theory of successive elimination to be given here rests on the following result.

Theorem XI. *Let $\mathfrak{b}$ be an ideal of polynomials in one indeterminate t with coefficients in P, hence a principal ideal; let $h(t)$ be a polynomial from $\mathfrak{b}$ of degree k, and let $\mathfrak{B}$ be the module of linear forms in $1, t, \dots, t^{k-1}$ into which $\mathfrak{b}$ passes modulo $h(t)$. Then $\mathfrak{B}$ has rank $k-p$, where p is the degree of the basis polynomial $f(t)$ of $\mathfrak{b}$.*

By hypothesis $h(t) = h_1(t)f(t)$, where $h_1(t)$ has degree $k-p$. The residue classes of $\mathfrak{b}$ modulo $h(t)$ represented by $f(t), tf(t), \dots, t^{k-p-1}f(t)$ are therefore linearly independent; and every residue class of $\mathfrak{b}$ modulo $h(t)$ can be represented linearly by these $k-p$ special classes, with coefficients in P. But modulo $h(t)$ the ideal $\mathfrak{b}$ passes into a module of linear forms in $1, t, \dots, t^{k-1}$, whose rank is therefore exactly $k-p$.

Now let $\mathfrak{a} = \mathfrak{a}_1$ be a transformed ideal of polynomials, and let $A^{(1)}(x)$ be a polynomial from $\mathfrak{a}_1$, regular in x_1, of degree k_1. Let $\mathfrak{A}_1$ be the module of linear forms in $1, x_1, \dots, x_1^{k_1-1}$, with polynomials $a^{(2)}(x)$ as coefficients, into which $\mathfrak{a}_1$ passes modulo $A^{(1)}(x)$. Let $\mathfrak{a}_2$ denote the ideal in $x_2\dots x_n$ derived from all k_1-rowed determinants from $\mathfrak{A}_1$. By Theorem XI, $\mathfrak{a}_2$ is the zero ideal if and only if the polynomials from $\mathfrak{a}_1$ have a common divisor, in the polynomial sense, of degree $p_1 > 0$ in x_1. If $\mathfrak{a}_2$ is different from the zero ideal, then, since $\mathfrak{a}$ is assumed transformed, it contains a polynomial $A^{(2)}(x)$ regular in x_2, of degree k_2, as is seen

[16] Steinitz showed, in his Algebraische Theorie der Körper (J. f. M. 137 (1910), pp. 167–309), that every field can be extended, essentially uniquely, to an algebraically closed one, thus giving the rational equivalent of the fundamental theorem of algebra. In fact, for each $i = 1, \dots, n$ one is dealing with a finite extension field of $P(u, x_{i+1}, \dots, x_n)$. (E. N.)

directly by composing the transformation (12) from the special transformations (25) and (26). Let $\mathfrak{A}_2$ again denote the module of linear forms in $1, x_2, \ldots, x_2^{k_2-1}$ into which $\mathfrak{a}_2$ passes modulo $A^{(2)}(x)$, and $\mathfrak{a}_3$ the ideal in $x_3 \ldots x_n$ derived from all k_2-rowed determinants from $\mathfrak{A}_2$; this ideal must contain a polynomial $A^{(3)}(x)$ regular in x_3.

In this way one continues the process until one reaches a zero ideal, or until $\mathfrak{a}_{n+1}$ becomes the unit ideal; for since $\mathfrak{a}_{n+1}$ is free of the x, it can only be the zero ideal or the unit ideal. It is seen that the ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ are uniquely determined by $\mathfrak{a}$, independently of the chosen polynomials $A^{(\lambda)}(x)$. This is clear for $\mathfrak{a}_1 = \mathfrak{a}$, and can therefore be assumed for $\mathfrak{a}_1, \ldots, \mathfrak{a}_i$. If $\mathfrak{a}_i$ passes modulo $A^{(i)}(x)$ into the module of linear forms $\mathfrak{A}_i$, then $\mathfrak{A}_i$ can also be characterized as the totality of the polynomials from $\mathfrak{a}_i$ that do not reach degree k_i in x_i; thus $\mathfrak{A}_i$ depends only on the degree k_i of $A^{(i)}(x)$. Let $\bar{A}^{(i)}(x)$ be a polynomial from $\mathfrak{a}_i$, regular in x_i, of degree $\bar{k}_i > k_i$, let $\overline{\mathfrak{A}}_i$ be the corresponding module of linear forms, and let $\bar{\mathfrak{a}}_{i+1}$ be the ideal derived from the $\bar{k}_i$-rowed determinants from $\overline{\mathfrak{A}}_i$. Then the module equation holds:

$$\overline{\mathfrak{A}}_i = (\mathfrak{A}_i, A^{(i)}, x_i A^{(i)}, \ldots, x_i^{\bar{k}_i - k_i - 1} A^{(i)}).$$

Since, by the regularity of $A^{(i)}(x)$ in x_i, the polynomials $A^{(i)}, x_i A^{(i)}, \ldots$ can be introduced as new indeterminates of the linear forms, it follows that the k_i-rowed determinants from $\mathfrak{A}_i$ agree with the $\bar{k}_i$-rowed determinants from $\overline{\mathfrak{A}}_i$, and therefore $\bar{\mathfrak{a}}_{i+1} = \mathfrak{a}_{i+1}$.[17]

Furthermore $\mathfrak{a}_{i+1}$ is always divisible by $\mathfrak{a}_i$. This is clear if $\mathfrak{a}_{i+1}$ is the zero ideal; in the opposite case $\mathfrak{A}_i$ has rank k_i, so that $\mathfrak{a}_{i+1}$ is the ideal which by definition consists of the k_i-rowed determinants from $\mathfrak{A}_i$, and is divisible by $\mathfrak{A}_i$ and hence by $\mathfrak{a}_i$. Thus every $\mathfrak{a}_{i+1}$ is divisible by $\mathfrak{a}$; if therefore $\mathfrak{a}_{n+1}$ becomes the unit ideal, then $\mathfrak{a}$ itself is the unit ideal.

Let now $\mathfrak{a}$ be different from the unit ideal, with $\mathfrak{a}_1 \neq 0, \ldots, \mathfrak{a}_i \neq 0$, and $\mathfrak{a}_{i+1} = 0$. Let $D^{(i)}(x)$ be the greatest common divisor, existing by Theorem XI, of all polynomials from $\mathfrak{a}_i$, where divisor is understood in the polynomial sense; as a divisor of $A^{(i)}(x)$, $D^{(i)}(x)$ is itself regular in x_i of degree $p_i > 0$. Adjoin $x_{i+1} \ldots x_n$ to $P(u)$; then $D^{(i)}(x)$ has, in an algebraic extension field of $P(u; x_{i+1} \ldots x_n)$, a decomposition into p_i linear factors. Let $x_i - \bar{x}_i$ be one such linear factor, so that all polynomials from $\mathfrak{a}_i$ vanish for $x_i = \bar{x}_i$; then, by Theorem XI, the polynomials from $\mathfrak{a}_{i-1}$ acquire for this specialization a greatest common divisor $D^{(i-1)}(x)$. As a divisor of $A^{(i-1)}(x)$, $D^{(i-1)}(x)$ is again regular in x_{i-1} of degree $p_{i-1} > 0$; in particular it cannot vanish identically, and in an extension field of $P(u, \bar{x}_i, x_{i+1}, \ldots, x_n)$ it decomposes into p_{i-1} linear factors. If $x_{i-1} - \bar{x}_{i-1}$ is such a linear factor, there corresponds to it a greatest common divisor from $\mathfrak{a}_{i-2}$. Continuing in this way, one reaches finitely many common zeros of $\mathfrak{a}$ lying in an algebraic extension field of $P(u; x_{i+1} \ldots x_n)$. Conversely, because $\mathfrak{a}_i$ is divisible by $\mathfrak{a}$, every zero of $\mathfrak{a}$ is also a zero of $\mathfrak{a}_i$. If, in particular, $x_1 = \bar{x}_1, \ldots, x_i = \bar{x}_i, x_{i+1} = x_{i+1}, \ldots, x_n = x_n$ is a zero of $\mathfrak{a}$, then $\mathfrak{a}_{i+1} = 0$ follows, and the polynomials from $\mathfrak{a}_i$ acquire a greatest common divisor with the linear factor $x_i - \bar{x}_i$. Summarizing:

Theorem XII. *Let $\mathfrak{a}$ be different from the unit ideal, with $\mathfrak{a}_1 \neq 0, \ldots, \mathfrak{a}_i \neq 0$ and $\mathfrak{a}_{i+1} = 0$. Then, after adjoining $x_{i+1} \ldots x_n$ to $P(u)$, there exist finitely many associated value systems $\bar{x}_1 \ldots \bar{x}_i$, lying in an algebraic extension field of $P(u, x_{i+1}, \ldots, x_n)$, such that all polynomials from $\mathfrak{a}$ vanish for $x_1 = \bar{x}_1, \ldots, x_i = \bar{x}_i, x_{i+1} = x_{i+1}, \ldots, x_n = x_n$. Conversely, if such a zero of $\mathfrak{a}$ is present, then $\mathfrak{a}_{i+1} = 0$ follows, as does the occurrence of a common divisor $D^{(i)}(x)$ of all polynomials from $\mathfrak{a}_i$ that has the linear factor $x_i - \bar{x}_i$.*

Theorem XII shows in particular that every ideal $\mathfrak{a}$ having no zero is the unit ideal.

To carry out a decomposition that also explicitly exhibits the association of the value systems, introduce new indeterminates v, which may be adjoined to $P(u, x_{i+1}, \ldots, x_n)$. Put

$$z_i = -v_1 x_1 - \cdots - v_{i-1} x_{i-1} + x_i. \tag{35}$$

Then the composition of (12) with (35) is again a substitution of type (12), in which now only the u_{ik} are replaced by $w_{ik} = u_{ik} - v_k$, and more generally $u_{i+h,k}$ by $w_{i+h,k} = u_{i+h,k} - u_{i+h,i} v_k$. If the substitution (35) carries the, by hypothesis transformed, ideal $\mathfrak{a}$ into $\mathfrak{b}$, then $\mathfrak{b}$ is obtained from $\mathfrak{a}$ simply by replacing the $u_{\mu\nu}$ by $w_{\mu\nu}$ and adjoining the v; and by the same process the ideals $\mathfrak{b}_1, \mathfrak{b}_2, \ldots$ defined by $\mathfrak{b}$ arise from $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$. Conversely $\mathfrak{a}_i$ is obtained from $\mathfrak{b}_i$ by $v = 0$; therefore the ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ are simultaneously zero ideals or simultaneously different from the zero ideal.

Now again let $\mathfrak{a}_1 \neq 0; \ldots; \mathfrak{a}_i \neq 0; \mathfrak{a}_{i+1} = 0$, and hence also $\mathfrak{b}_1 \neq 0; \ldots; \mathfrak{b}_i \neq 0; \mathfrak{b}_{i+1} = 0$. Let $\bar{x}_1 \ldots \bar{x}_i, x_{i+1} \ldots x_n$ be an associated zero-system of $\mathfrak{a}$. Define $\bar{z}_i = \bar{x}_i + v_1 \bar{x}_1 + \cdots + v_{i-1} \bar{x}_{i-1}$. Then

[17] This is in principle the same inference on which the isomorphism of $\mathfrak{G}^*_{i-1} \mid \mathfrak{M}^*_{i-1}$ with $\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}$ rested.

$\bar{x}_1 \dots \bar{x}_{i-1}, \bar{z}_i, x_{i+1} \dots x_n$ is, by (35), a zero of $\mathfrak{b}$. Hence if $H^{(i)}(z,x)$ denotes the greatest common divisor of all polynomials from $\mathfrak{b}_i$, which may be assumed integral and primitive in the v, then by the last part of Theorem XII, $H^{(i)}(z,x)$ has the factor

$$z_i - \bar{z}_i = z_i - (\bar{x}_i + v_1\bar{x}_1 + \cdots + v_{i-1}\bar{x}_{i-1}),$$

and to every zero of $\mathfrak{a}$ occurring after adjoining $x_{i+1} \dots x_n$ there corresponds such a factor. It must be shown that this exhausts the factorization of $H^{(i)}(z,x)$, i.e. that no factor $H_1^{(i)}$ can be separated from $H^{(i)}$ which does not decompose into linear factors in z and v. If this were the case, then because of the assumed primitivity in v, $H^{(i)}$ would contain at least one linear factor $z_i - \bar{z}_i$, where $\bar{z}_i$ belongs to an algebraic extension field of $P(u, v, x_{i+1}, \dots, x_n)$. If $\bar{x}_1 \dots \bar{x}_{i-1}, \bar{z}_i, x_{i+1} \dots x_n$ is the corresponding zero of $\mathfrak{b}$, then it must coincide with one of the finitely many zeros of $\mathfrak{a}$ that occur after adjoining $x_{i+1} \dots x_n$, and so it must be independent of v. Hence $\bar{z}_i$ necessarily contains the v linearly, not algebraically or rationally non-linearly; contrary to the assumption, another linear factor $z_i - (\bar{x}_i + v_1\bar{x}_1 + \cdots + v_{i-1}\bar{x}_{i-1})$ in z and v can be split from $H_1^{(i)}$. Thus the explicit decomposition is

$$H^{(i)}(z,x) = \prod \{z_i - (\bar{x}_i + v_1\bar{x}_1 + \cdots + v_{i-1}\bar{x}_{i-1})\}^{\alpha_\lambda}.$$

Since the degree of $H^{(i)}$ and the individual exponents α_λ must agree with the corresponding ones for $D^{(i)}(x)$ – for $H^{(i)}$ arises from $D^{(i)}$ by the specialization $u_{\mu\nu} = w_{\mu\nu}$, and $D^{(i)}$ from $H^{(i)}$ by the specialization $v = 0$ – this decomposition also shows that, because the indeterminates $u_{\mu\nu}$ are adjoined to P, every zero $\bar{x}_i$ of $D^{(i)}$ occurring in the elimination starting from $\mathfrak{a}$ corresponds to a greatest common divisor from $\mathfrak{a}_{i-1} \dots \mathfrak{a}_1$ that is respectively linear, or to a power of such; hence in each case only one associated zero-system $\bar{x}_1 \dots \bar{x}_i, x_{i+1} \dots x_n$ of $\mathfrak{a}$ is obtained.[18]

ğ 7. Resultant form and elimination theory.

To establish the connection between the resultant form and elimination theory, apply the successive elimination of ğ 6 specifically to the quotient $\mathfrak{a} = \mathfrak{m}/\mathfrak{g}_{i-1}$ of ideal by fundamental ideal of the $(i-1)$-st stage. It must first be shown that this quotient is a transformed ideal. Now $\mathfrak{m}$ is transformed and hence, by Theorem VI of ğ 3, so is $\mathfrak{g}_{i-1}$. From

$$H(x) \equiv 0(\mathfrak{m}/\mathfrak{g}_{i-1}); \qquad H(x) = \overline{H}(y) = \sum \alpha_i(u)\overline{H}_i(y) = \sum \alpha_i(u) H_i(x)$$

one obtains

$$\overline{H}(y)\overline{\mathfrak{g}}_{i-1,(u)} \equiv 0(\overline{\mathfrak{m}}_{(u)}), \quad \text{hence also} \quad \overline{H}(y)\overline{\mathfrak{g}}_{i-1} \equiv 0(\overline{\mathfrak{m}}_{(u)}),$$

or

$$\overline{H}_i(y)\overline{\mathfrak{g}}_{i-1} \equiv 0(\overline{\mathfrak{m}}), \quad \text{hence} \quad H_i(x)\mathfrak{g}_{i-1} \equiv 0(\mathfrak{m}).$$

This proves the divisibility of $H_i(x)$ by $\mathfrak{m}/\mathfrak{g}_{i-1}$ and hence that this ideal is transformed, so that the elimination method of ğ 6 applies.

But (30), taking account of (28) – ğ 4 – shows that $C^{(i)}(x)$ is divisible by $\mathfrak{m}/\mathfrak{g}_{i-1}$, where $C^{(i)}(x)$ denotes any non-identically vanishing determinant of degree ρ from $\mathfrak{M}_{i-1}^*$. Since for $i > 1$ this $C^{(i)}$ has degree zero in x_1, the module $\mathfrak{A}_1$ corresponding to the ideal $\mathfrak{a} = \mathfrak{a}_1$ contains the polynomials $C^{(i)}, x_1C^{(i)}, \dots, x_1^{k_1-1}C^{(i)}$, and therefore $(C^{(i)})^{k_1}$ is divisible by $\mathfrak{a}_2$; similarly $(C^{(i)})^{k_1k_2}$ is divisible by $\mathfrak{a}_3$, and finally $(C^{(i)})^{k_1k_2\cdots k_{i-1}}$ by $\mathfrak{a}_i$. Thus $\mathfrak{a}_1, \dots, \mathfrak{a}_i$ are different from the zero ideal, as also holds for $i = 1$. Let $D^{(i)}(x)$ now be the greatest common divisor of all polynomials from $\mathfrak{a}_i$, which has degree $p_i > 0$ only when $\mathfrak{a}_{i+1}$ is the zero ideal. By the definition of $D^{(i)}(x)$, and taking into account the divisibility of $\mathfrak{a}_i$ by $\mathfrak{a}$, one obtains

$$d^{(i+1)}D^{(i)}(x) \equiv 0(\mathfrak{m}/\mathfrak{g}_{i-1}); \qquad d^{(i+1)} \neq 0.$$

Thus $d^{(i+1)}D^{(i)}$ is a polynomial, free of $x_1 \dots x_{i-1}$, belonging to $\mathfrak{m}/\mathfrak{g}_{i-1}$. But $E^{(i)}(x)$ was defined (Theorem II and ğ 4), as the highest elementary divisor of $\mathfrak{M}_{i-1}$ or $\mathfrak{M}_{i-1}^*$, to be the greatest common divisor, in the polynomial sense, of all polynomials from $\mathfrak{m}/\mathfrak{g}_{i-1}$ that are free of $x_1 \dots x_{i-1}$. Therefore $d^{(i+1)}D^{(i)}$, and because of the regularity of $E^{(i)}(x)$ in x_i also $D^{(i)}(x)$, is divisible by $E^{(i)}(x)$.

[18] It should be pointed out that the successive elimination given here, in contrast to Kronecker's method, depends only on the given ideal $\mathfrak{a}$ and is independent of every ideal basis; in particular this also holds for the exponents α_λ. A complete execution of the elimination by this method would, according to Hentzelt, require the continuation of the procedure on the quotient $\mathfrak{a}/D^{(i)}$, which may be omitted in view of the next section. (E. N.)

The same argument can be carried out if the transformation (12) had from the beginning been composed with (35), that is, if the indeterminates $u_{\mu\nu}$ had been replaced by $w_{\mu\nu}$; this gives the divisibility of $H^{(i)}(z,x)$ by the corresponding $\bar{E}^{(i)}(z,x)$. Since, just as $D^{(i)}(x)$ and $H^{(i)}(z,x)$ pass into one another by specialization, so too do $E^{(i)}(x)$ and $\bar{E}^{(i)}(z,x)$, and also $R^{(i)}(x)$ and $\bar{R}^{(i)}(z,x)$, the multiplicity numbers in the decomposition into linear factors must also agree mutually. Taking into account, furthermore, that a power of $E^{(i)}(x)$ is divisible by $R^{(i)}(x)$, one obtains the following summary.

Theorem XIII. *If $R^{(i)}(x)$ is decomposed in an algebraic extension field of $P(u, x_{i+1}, \ldots, x_n)$ into linear factors $x_i - \bar{x}_i$, then $\bar{x}_i$ can be completed in one and only one way to an associated value system $\bar{x}_1 \ldots \bar{x}_i, x_{i+1} \ldots x_n$ that is a zero of $\mathfrak{m}/\mathfrak{g}_{i-1}$ and consequently of $\mathfrak{m}$. The finitely many zeros of $\mathfrak{m}$ arising in this way from the linear factors of $R^{(i)}$ – finitely many after adjoining $x_{i+1} \ldots x_n$ – are collected by the explicit decomposition*

$$\bar{R}^{(i)}(z,x) = \prod\{z_i - (\bar{x}_i + v_1\bar{x}_1 + \cdots + v_{i-1}\bar{x}_{i-1})\}^{\alpha_\lambda}. \tag{36}$$

Because of the regularity of $\bar{R}^{(i)}(z,x)$ in z_i, this decomposition is preserved if the $x_{i+1} \ldots x_n$ adjoined to $P(u)$ are replaced by arbitrary special value systems $\bar{x}_{i+1} \ldots \bar{x}_n$ from $P(u)$ or from the algebraically closed field derived from it.

This also accomplishes a separation of the zeros of $\mathfrak{m}$ according to the individual factors of the resultant form; the number of indeterminates x adjoined to $P(u)$ is also called the dimension of the corresponding algebraic object.

If, in the decomposition of $\bar{R}^{(i)}(z,x)$ or of the corresponding $R^{(i)}(x)$, the factors conjugate over $P(u, x_{i+1} \ldots x_n)$ are collected together – factors that for general P may be wholly or partially identical – one obtains a decomposition of $R^{(i)}(x)$ into powers of polynomials irreducible over $P(u, x_{i+1} \ldots x_n)$:

$$R^{(i)}(x) = S_1^{(i)}(x)^{\beta_1} \cdots S_\nu^{(i)}(x)^{\beta_\nu}.$$

By Theorem X, this decomposition corresponds to a representation $\mathfrak{g}_i = [\mathfrak{j}_1 \ldots \mathfrak{j}_\nu]$ such that $S_\mu^{(i)}(x)^{\beta_\mu}$ is equal to the norm of $\mathfrak{g}_{i-1}$ with respect to the ideal $\mathfrak{j}_\mu$, respectively to the norm of the module $\mathfrak{G}_{i-1}$ with respect to the module corresponding to $\mathfrak{j}_\mu$. This clarifies the meaning of the exponents β_μ: in particular, if γ_μ is the degree of $S_\mu^{(i)}$, then the multiplicity $\beta_\mu\gamma_\mu$ is equal to the number of residue classes of $\mathfrak{g}_{i-1}$ modulo $\mathfrak{j}_\mu$ that are linearly independent over $P(u, x_{i+1} \ldots x_n)$.

Finally consider briefly the special case where P has characteristic zero. If the $u_{\mu\nu}$ are specialized to quantities $\bar{u}_{\mu\nu}$ from P in such a way that the n determinants $C^{(i)}(x)$ $(i = 1, 2, \ldots, n)$ remain regular in x_i,[19] then the regularity of $R^{(i)}$ is also preserved. Under this specialization, $R^{(i)}$ and likewise $\bar{R}^{(i)}(z,x)$ become a common divisor of all ρ-rowed determinants from $\mathfrak{M}_{i-1}^*$, though not necessarily the greatest common divisor. But the specialization can always be chosen so that this latter property also remains true. For, as the existence of the module basis shows, $R^{(i)}(z,x)$ can also be characterized as the greatest common divisor of finitely many ρ-rowed determinants from $\mathfrak{M}_{i-1}^*$. The decomposition of the so specialized $\bar{R}^{(i)}(z,x)$ is then obtained simply by replacing the $u_{\mu\nu}$ by $\bar{u}_{\mu\nu}$ in (36), so that the whole elimination theory is preserved.

(Received March 17, 1922.)

23. Algebraic and Differential Invariants

Jahresber. d. Deutschen Mathematiker-Vereinigung 32 (1923), pp. 177–184

Algebraic and Differential Invariants.

Report following the lecture, Leipzig, September 18, 1922.

By Emmy Noether in Göttingen.

[19] Hentzelt assumes this specialization of the $u_{\mu\nu}$ from the start and therefore has to call upon much more complicated considerations to prove the decomposability of $H^{(i)}(z,x)$ and $\bar{R}^{(i)}(z,x)$ into linear factors in z and v. The exponents that occur there need not necessarily agree with the ones above. (E. N.)

If I am to report on the development of algebraic and differential invariants, then in both areas I should like to restrict myself to the critical period which, according to a remark of HILBERT, follows the naive and formal period. This critical period is characterized, for the algebraic invariants, by the name of HILBERT himself; for the differential invariants, by the name of RIEMANN — or, in substantive terms: for the algebraic invariants by the arithmetical methods of algebra, which essentially developed around these questions and were able here to show their full sharpness; for the differential invariants by the methods of the formal calculus of variations. Thus I should like to report on the arithmetical methods with their significance beyond the special subject, while in the second part I can restrict myself to the subordination of the differential invariants to the algebraic ones, which is accomplished precisely in connection with the methods of the calculus of variations.

1. The *algebraic invariants* are, as is well known, based on the *general linear group* in $x_1, \ldots, x_n$:

$$x_i = \sum_k s_{ik} x'_k \qquad \text{or briefly:} \qquad x = S(x'), \tag{1}$$

where the s_{ik} denote indeterminates, so that $\Delta = |s_{ik}|$ is non-zero. If now $f(a,x)$, $g(b,x), \ldots$ are forms in x, of dimensions $\alpha, \beta, \ldots$, with indeterminates $a, b, \ldots$ as coefficients, then by means of (1) the *induced transformation* of the $a, b, \ldots$ arises; for from

$$f(a,x) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum {}' a'_{j_1 \ldots j_n} {x'_1}^{j_1} \cdots {x'_n}^{j_n} = f(a', x'),$$
$$g(b,x) = \sum b_{r_1 \ldots r_n} x_1^{r_1} \cdots x_n^{r_n} = \sum {}' b'_{s_1 \ldots s_n} {x'_1}^{s_1} \cdots {x'_n}^{s_n} = g(b', x')$$

it follows that the $a', b', \ldots$ become linear homogeneous functions of the $a, b, \ldots$, whose coefficients are of degrees $\alpha, \beta, \ldots$ in the s_{ik}:

$$a' = A_\alpha(a); \qquad b' = B_\beta(b) \ldots . \tag{2}$$

By an *invariant* one now understands an invariant with respect to the transformations (1) and (2); that is, an integral rational function of the indeterminates $a, b, \ldots, x, y, \ldots$ — where also $y = S(y')$ — which, under application of the transformations, reproduces itself up to a factor, a power of the substitution determinant:

$$I(a', b', \ldots, x', y', \ldots) = \Delta^\rho I(a, b, \ldots, x, y, \ldots). \tag{3}$$

The coefficients of I may be assumed to be rational, or even rational integers, since every invariant with coefficients in an arbitrary number field P can be expressed linearly, with coefficients from P, by finitely many such special ones. Likewise it is no restriction to assume I separately homogeneous in each series, since here again every invariant can be assembled as a sum of finitely many such special ones.

It should be noted that conversely (1) and (2) are again determined by the requirement (3). As OSTROWSKI and SCHUR have recently shown,[1)] the induced transformations can also be characterized as the totality of the linear transformations, separated in each individual series, which — apart from certain specifiable exceptions — allow an arbitrary invariant I free of the $x, y, \ldots$.

The product of two invariants is again an invariant, but the sum is one if and only if the weight — the exponent ρ in (3) — agrees. If, however, one restricts oneself to transformations of determinant one, then any sum is again an invariant and also exhausts all invariants with respect to the so restricted group. One therefore obtains an integral domain, indeed a *homogeneous integral domain*, that is, a domain for which membership of a polynomial implies membership of its homogeneous components separately — which here again amounts to the separately homogeneous invariants according to (3).

Here arises the fundamental problem around which invariant theory, and arithmetical algebra in general, has developed: *Is this integral domain finite, that is, does it possess a finite integral basis $I_1, \ldots, I_k$ such that every invariant can be represented integrally and rationally through $I_1, \ldots, I_k$, $I = G(I_1, \ldots, I_k)$.* HILBERT's solution of the problem — GORDAN's proof for the binary case does not admit an extension because of its unmanageable symbolic computations, and the MERTENS-HILBERT proof does not do so because of its use of the decomposition of a binary form into linear forms — rests on reducing the question of the integral basis to that of the ideal basis. I should like to sketch the train of thought here, emphasizing the arithmetical fundamental ideas, and then to go on to three connected circles of questions: actual construction of the basis by finitely many steps; finiteness questions for subgroups; finiteness questions taking integrality into account.

2. I recall the *definition of an ideal* for finite algebraic number fields. A system $\mathfrak{a}$ of numbers of the field is called an ideal if

[1)] A. OSTROWSKI and I. SCHUR, Über eine fundamentale Eigenschaft der Invarianten einer binären Form, Math. Zeitschr. 15 (1922), and related, not yet published work of OSTROWSKI.

1. $\mathfrak{a}$ belongs to the domain $\mathfrak{o}$ of all integers of the field,
2. together with α and β, the difference $\alpha - \beta$ also belongs to $\mathfrak{a}$,
3. together with α, $\lambda\alpha$ also belongs to $\mathfrak{a}$, where λ is understood to be any element of $\mathfrak{o}$.

And, as is well known, the theorem holds that every ideal has an *ideal basis*: $\mathfrak{a} = (\alpha_1, \ldots, \alpha_k)$; that is, there are finitely many elements $\alpha_1, \ldots, \alpha_k$ from $\mathfrak{a}$ such that, by means of 2. and 3., $\mathfrak{a}$ is derivable from $\alpha_1, \ldots, \alpha_k$; thus $\alpha = \lambda_1\alpha_1 + \cdots + \lambda_k\alpha_k$ exhausts all elements from $\mathfrak{a}$.[2)]

This definition of an ideal rests only on the fact that $\mathfrak{o}$ forms an integral domain; the concept of ideal, and likewise that of ideal basis, therefore remains literally the same when $\mathfrak{o}$ is replaced by an arbitrary integral domain.

HILBERT's finiteness proof now decomposes into the following three theorems:

1. In the domain of all polynomials in n indeterminates with coefficients in a field of rationality, the ideal-basis theorem holds for every ideal — and consequently also for every arbitrary system $\mathfrak{S}$.
2. A homogeneous integral domain $\mathfrak{J}$ of polynomials is finite if and only if the ideal-basis theorem holds in $\mathfrak{J}$.
3. For the domain of invariants $\mathfrak{J}$, the ideal-basis theorem holds in the sharpened form that every ideal basis formed with respect to the domain of all polynomials is at the same time an ideal basis in $\mathfrak{J}$, so that beside

$$I = A_1 I_1 + \cdots + A_k I_k \qquad \text{one always has} \qquad I = i_1 I_1 + \cdots + i_k I_k$$

where the A denote polynomials in the $a, b, \ldots, x, y, \ldots$, and the i denote invariants.

The proof of 1. rests, in principle, on the same arguments as in the algebraic number field; in both cases the existence of the ideal basis follows directly from a general theorem on modules of linear forms.[3)] From 1. the existence of the ideal basis follows directly for every finite integral domain of polynomials; for homogeneous domains, the converse is also easy to see. Only in 3. are special properties of invariants used; namely, in HILBERT, 3. follows from a known theorem on the Ω-process, whereas recently E. FISCHER has shown that 3. can — on the basis of other general theorems — already be obtained from the property of the general linear group that, along with every transformation, it also contains the contragredient one, respectively its conjugate-complex one.[4)]

3. The *actual construction of the basis* rests on a further arithmetical transformation of the notion of finiteness by drawing on the theory of *function fields*. The following holds:

4. An integral domain $\mathfrak{J}$ of polynomials is finite if and only if there is contained in $\mathfrak{J}$ a finite subdomain $\mathfrak{J}'$ such that $\mathfrak{J}$ depends algebraically integrally on $\mathfrak{J}'$; every integral basis of $\mathfrak{J}'$ is then supplemented by a fundamental system of these algebraically integral quantities to a basis of $\mathfrak{J}$.[5)]

If, specifically, as in the case of the invariants, one deals with homogeneous domains $\mathfrak{J}$ for which the ideal-basis theorem holds in the sharper form 3., then such a domain $\mathfrak{J}'$ is derivable from some always-existing finitely many polynomials $I_1, \ldots, I_s$ as an integral basis, from whose vanishing the vanishing of all polynomials from $\mathfrak{J}$ follows. This fact is again based on a general theorem of ideal theory:

5. To every ideal $\mathfrak{a}$ of polynomials there belongs an ordinary rational integer r such that for every ideal $\mathfrak{b}$ which vanishes at all zeros of $\mathfrak{a}$, $\mathfrak{b}^r$ is divisible by $\mathfrak{a}$.

In the case of invariants, one can determine an *upper bound for the degrees* of $I_1, \ldots, I_s$, and thus also for their number s, depending only on the degrees of the basic forms under consideration. At this point, again, special properties of invariants are used; the relevant theorem says that a numerically specialized system of basic forms has a non-zero invariant if and only if $\Delta = |s_{ik}|$ depends algebraically integrally on the transformed coefficients.

From this upper bound K. HENTZELT[6)] has determined an *upper bound for the degrees of the invariants of the integral basis*, again depending only on the degrees of the basic forms. He succeeds in doing this by giving, for the exponent r in 5., an upper bound depending only on the number and the highest degree of the polynomials of an ideal basis of $\mathfrak{a}$, independent of the coefficients of these polynomials, and computable from the given numbers in finitely many steps. In principle the problem posed is thereby completely settled; admittedly the bound given is quite high. Thus, for a ternary quadratic form, where the discriminant — that

[2)] That k can be reduced to two is irrelevant for what follows.

[3)] Compare my comparative report on the arithmetical theory of algebraic functions. Jahresber. 28 (1920), p. 187 and note 2), p. 188.

[4)] E. FISCHER, Über die Endlichkeit der Invarianten. Göttinger Nachrichten 1915, and Leipzig lecture.

[5)] HILBERT shows (Über die vollen Invariantensysteme, Math. Annalen 42 (1893), ğ 1 and 2) that these facts follow from the assumed finiteness; conversely, that finiteness follows from algebraically integral dependence follows from the existence of the rational basis (E. Noether, Körper und Systeme rationaler Funktionen, Math. Annalen 76 (1915), ğ 12).

[6)] I shall shortly publish the work from the estate.

is, an invariant of degree 3 — already forms the basis of all invariants free of the x, according to HILBERT and HENTZELT one reaches high into the millions.

4. In the finiteness question for invariants of *subgroups* of the general linear group, only partial results have so far been reached. The method rests almost exclusively on reducing the invariants of subgroups to simultaneous invariants of the general linear group, according to the procedure used by STUDY for the orthogonal group. This has been carried out by WEITZENBÖCK for motion invariants and affine invariants, and by DERUYTS for semi-invariants and shear invariants;[7] the question of the reach of this method is still undecided. FISCHER's remark mentioned at the end of 2. likewise solves the finiteness problem for a series of subgroups; in particular, it thereby gives the simplest proof for the orthogonal group. But the example of semi-invariants shows — as FISCHER has recently pointed out[8] — that for subgroups, despite finiteness, the sharper form 3. for the ideal basis need not be fulfilled.

Interpreted in the sense of field theory, the finiteness question present here leads to HILBERT's problem of *relatively integral functions*, that is, to the question whether such integral domains as consist of the totality of the polynomials of a field of rational functions are always finite. In this direction lies the elementary provable fact that for the invariants of finite groups a distinguished integral basis can be given directly — the system of coefficients of the Galois resolvent.[9]

5. The question whether the finiteness theorem for invariants can be sharpened with respect to *integrality* is also not yet settled in general. To be sure, as HILBERT showed, the ideal-basis theorem also holds for the domain of all integral polynomials; and likewise the connection 2. between ideal basis and integral basis remains valid;[10] but the proof for the — unnecessary — sharpened version 3. fails. For the case of binary invariants, integral finiteness can be proved;[11] the proof, which represents an integrality sharpening of the binary MERTENS-HILBERT finiteness proof, uses, besides the theorem on the integral ideal basis, also the decomposition of binary forms into linear forms, and therefore does not permit transfer to more indeterminates. On similar foundations, by contrast, integral finiteness for the invariants of finite groups follows, as a sharpening of the proof mentioned above, although now again only an existence proof and no actual specification of the basis results.[12] Here too, only a further development of the theory of function fields and of general ideal theory will presumably lead to the goal.

6. I now pass to the *differential invariants* and to the question raised in the introduction concerning their reduction to the theory of algebraic invariants. The underlying group is, as is well known, defined by means of $x_i = x_i(y)$ as:

$$dx_i = \sum_k \frac{\partial x_i}{\partial y_k} dy_k; \qquad d\delta x_i = \sum_k \frac{\partial x_i}{\partial y_k} d\delta y_k + \sum_{k,l} \frac{\partial^2 x_i}{\partial y_k \partial y_l} dy_k\, \delta y_l; \ \ldots. \tag{4}$$

To pass to the transformations induced by (4), one may begin with an arbitrary function $f(x, dx) = g(y, dy)$; by requiring the invariance of $\delta f, \delta^2 f, \ldots$ with respect to (4), one obtains the transformations for the derivatives of f with respect to x and dx. If one restricts oneself, for instance, to forms homogeneous in the dx:

$$f(x, dx) = \sum a_{i_1 \ldots i_n}(x) dx_1^{i_1} \cdots dx_n^{i_n} = \sum {}' a'_{j_1 \ldots j_n}(y) dy_1^{j_1} \cdots dy_n^{j_n} = g(y, dy),$$

then the a' are linear in the a, the $\frac{\partial a'}{\partial y}$ are linear in the a and $\frac{\partial a}{\partial x}$, and so on:

$$a' = A_0(a), \qquad \frac{\partial a'}{\partial y} = A_1\left(a, \frac{\partial a}{\partial x}\right), \qquad \frac{\partial^2 a'}{\partial y^2} = A_2\left(a, \frac{\partial a}{\partial x}, \frac{\partial^2 a}{\partial x^2}\right), \ldots \tag{5}$$

and the question is one of invariance with respect to the transformations (4) and (5). Here all the quantities occurring,

$$a, \ \frac{\partial a}{\partial x}, \ldots, \ dx, \ \delta x, \ d\delta x, \ldots, \ \frac{\partial x}{\partial y}, \ \frac{\partial^2 x}{\partial y^2}, \ldots$$

are to be regarded as indeterminates, so the determinant of each individual transformation is certainly non-zero. Only when the formally completed theory is applied to special functions does the question arise of restriction to such functions that the transformations remain uniquely reversible in a certain domain and

[7] For literature references, compare WEITZENBÖCK's encyclopedia article on invariant theory; III E 1.

[8] Leipzig lecture and Math. Zeitschrift.

[9] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann. 77 (1916).

[10] From this connection it follows in particular that the decomposition theorems of general ideal theory hold for all finite integral domains, as I developed them in Math. Ann. 83 (1921).

[11] E. Noether, Die Endlichkeit des Systems der ganzzahligen Invarianten binärer Formen. Göttinger Nachrichten 1919.

[12] ğ 4 of the work cited under 11).

that a sufficient number of differential quotients exist, exactly as in the algebraic case, under numerical specialization, the determinant $|s_{ik}|$ must be assumed non-zero.

Under this treatment of all arguments occurring as indeterminates, one is thus dealing with a special linear group, not directly accessible to the ordinary algebraic methods, in which the transformations of dx and $a' = A_0(a)$ agree with (1) and the induced (2). The question arises whether, perhaps quite generally, by the *introduction of new arguments*, the transformations (4) and (5) can be reduced to the general linear group (1) and the transformations (2) thereby *induced*.

This is in fact the case. The higher differentials $d^2x, \delta dx, \ldots$ are to be replaced by the Lagrange derivatives arising from the variational problem belonging to $f(x, dx)$, and by further combinations formed from them by polar formation (transmissions in the sense of WEYL and SCHOUTEN), all of which are cogredient to the dx, so that their transformation is given by the general linear group (1). The quantities $\frac{\partial a}{\partial x}, \frac{\partial^2 a}{\partial x^2}, \ldots$ (or, more generally, the derivatives of the homogeneously assumed f with respect to x and dx), however, are to be replaced by the coefficients of certain forms arising from the „normal forms of the higher variations“ by the above elimination of the $d^2x, \delta dx, \ldots$, and of their „covariant derivatives“

$$[\Omega_i], \quad [\Omega_i^{(1)}], \quad [\Omega_i^{(2)}], \ldots \qquad (i = 1, 2, \ldots);$$

and since the $[\Omega_i^{(k)}]$ are invariants with respect to (4) and (5) which depend only on the dx and δx, these coefficients satisfy the algebraically induced transformations (2).[13] Through this *reduction theorem*, the theory of differential invariants is subordinated to algebraic invariant theory.

The series of the $[\Omega_i]$ breaks off with $[\Omega_\alpha]$ if $f(x, dx)$ is a homogeneous form of α-th dimension in the dx. For quadratic forms, $[\Omega_2]$ becomes identical with RIEMANN's curvature form, and the formation process indicated here is exactly the one given by RIEMANN in the Latin prize essay, which LIPSCHITZ, independently of this and in connection with RIEMANN's habilitation lecture, also developed.[14] The proof of the reduction theorem, which CHRISTOFFEL and RICCI had carried out computationally for quadratic differential forms, rests on the introduction of „RIEMANN normal coordinates“, which transform the extremals emanating from a point into straight lines; since thereby to an arbitrary transformation of the x there corresponds a linear transformation of the normal coordinates, these determine the passage to the general linear group.

The question arises whether such a reduction theorem also exists when, following WEYL and SCHOUTEN, the group is defined not by a variational problem but only by a transmission; that is, when, corresponding to the Lagrange derivatives, expressions $\psi_i(d\delta x, dx, \delta x)$ are set up through which the elimination of the higher differentials is achieved, with the restriction, unnecessary in itself, that the ψ_i should be linear in the dx being added in analogy with quadratic differential forms (for arbitrary homogeneous $f(x, dx)$, the polarized Lagrange derivatives become homogeneous of first order only in dx). By the requirement of cogredience of ψ to the dx, the transformation of their coefficients is induced, and thus, in analogy with (5), the group is fixed. For invariants of the lowest orders, WEITZENBÖCK has confirmed the reduction theorem computationally in the WEYL case; a general Ansatz is still lacking.[15]

(Received October 26, 1922.)

[13] E. Noether, Invarianten beliebiger Differentialausdrücke. Göttinger Nachrichten. 1918.

[14] Compare also my account of RIEMANN and LIPSCHITZ in no. 28 of the second part of WEITZENBÖCK's encyclopedia article mentioned under 7).

[15] Compare: WEYL, Raum, Zeit, Materie; SCHOUTEN, Math. Zeitschr. 13 (1922); WEITZENBÖCK, Sitzungsber. d. Wiener Akademie, 1920 and 1921.

24. Elimination Theory and General Ideal Theory

Math. Ann. 90 (1923), pp. 229–261

Elimination Theory and General Ideal Theory.

By

Emmy Noether in Göttingen.

In what follows the question is the placement of elimination theory – in the arithmetical form that I gave to Hentzelt's presentation[1] and that may be described as an ideal theory in the polynomial domain – within general ideal theory,[2] and, at the same time, a new foundation of the parts referring to zeroes. The basic concepts of both theories are briefly assembled in ğ 1, as are those of field theory,[3] so that I can refer to them here.

The classification and the new foundation group themselves around four questions: the arithmetical formulation of the concept of dimension; the theory of zeroes; the connection between the decomposition theorems for norms and elementary divisors and those of general ideal theory; the characterization of prime ideals and primary ideals by norm and elementary-divisor form.

The arithmetical formulation of the *concept of dimension* (ğ 4) is given by chains of prime ideals, the arithmetical equivalent of the fact that on surfaces there are curves, and on curves there are points. This arithmetical formulation, which is proved identical with the parameter definition of elimination theory, can be transferred with a slight modification to arbitrary ring domains and, together with the transfer of certain parts of the other questions, gives there an exact insight into the structure of ideals, as I shall show elsewhere.

In H.-N. the question of *zeroes* is, as usual, attacked directly for the given ideal, namely by going back to successive elimination, whereby the character of verification is not entirely avoided. In contrast stands the route always taken for polynomials in one variable: one represents the given polynomial as a product of powers of prime functions (primary functions) and constructs, for each individual prime function, the field of zeroes as a field isomorphic to the residue-class field. The degree of the prime function gives the degree of this field; the degree of the primary function, however, whose zeroes coincide with those of the prime function, gives the degree of the ring of residue classes modulo this primary function. If, for each prime function, one passes to the Galois field, one obtains the decomposition into linear factors; and with this, for the originally given polynomial, the question of zeroes, decomposition into linear factors, and multiplicity is settled. Quite correspondingly, here (ğ 3) the system of residue classes modulo a prime ideal is extended, by forming quotients, to the residue-class field, and a field of zeroes is constructed that is isomorphic to it. This field of zeroes contains a subfield generated by adjoining indeterminates – say $x_{i+1}, \ldots, x_n$; the degree of the norm gives the degree with respect to this subfield; at the same time, by passage to the Galois field, the decomposition of the elementary-divisor form and hence of the norm into linear factors is obtained. For the corresponding primary ideal, however, the zeroes are the same; the decomposition is also given along with it, since the norm becomes a power of the elementary-divisor form of the prime ideal (ğ 2); the degree of the norm gives the degree of the ring of residue classes modulo the primary ideal with respect to the subfield derived from the indeterminates.

Thus the question of zeroes of an arbitrary ideal is reduced to the connection between the decomposition theorems for norms and elementary divisors and those of general ideal theory (ğ 5). The fact that the zeroes of the ideal are composed from those of its individual associated prime ideals corresponds to the decomposition of the norm into greatest primary factors, which become equal to powers of the elementary-divisor form of the individual associated prime ideals;[4] thereby the decomposition into linear factors is accomplished for the norm in general. Multiplicity, however, receives its interpretation in H.-N. by means of the fundamental ideals and their components; the degree of a greatest primary factor of the norm is made equal to the number of linearly independent residue classes – after adjoining $x_{i+1}, \ldots, x_n$ – of the fundamental ideal of $(i-1)$-st stage modulo a component of the fundamental ideal of i-th stage. Now the fundamental ideal of $(i-1)$-st stage is proved identical with the isolated component of the decomposition that is uniquely defined by all

[1] Kurt Hentzelt, Zur Theorie der Polynomideale und Resultanten. Edited by E. Noether. Math. Ann. 88 (1922), pp. 53–79; cited H.-N.

[2] E. Noether, Idealtheorie in Ringbereichen, Math. Ann. 83 (1921), pp. 24–66; cited Ideal Theory.

[3] E. Steinitz, Algebraische Theorie der Körper, J. f. M. 137 (1910), pp. 167–309; cited Steinitz.

[4] This parallelism between elimination theory and general ideal theory is not fulfilled in Kronecker's elimination theory; compare H.-N., note 4).

prime ideals of dimension higher than the $(n-i)$-th; and a component of the fundamental ideal of i-th stage is proved identical with the isolated component of the decomposition defined by the prime ideal corresponding to the factor of the norm and by all prime ideals of higher dimension. The degree of the corresponding factor of the norm becomes – after adjoining $x_{i+1}, \ldots, x_n$ – equal to the degree of that subring of the residue classes of this component that consists only of classes of the fundamental ideal of $(i-1)$-st stage.

The characterization of the prime ideals and proper primary ideals (ğ 6) results as a direct consequence of the consideration of the residue-class fields. If the original coefficient domain is a perfect field, then prime functions correspond to the prime ideals as norm and elementary-divisor form, proper primary functions to the proper primary ideals, and conversely. For an imperfect field as coefficient domain only conditions can be given that are either necessary or sufficient; as examples show, the norm of a prime ideal can become properly primary, and the elementary-divisor form of a proper primary ideal can become a prime function. More precisely, in characteristic p the norm of a prime ideal becomes the p^g-th power ($g \geqq 0$) of its elementary-divisor form; whereas, for proper primary ideals whose elementary-divisor form is a prime function, the norm can become an arbitrary power, as examples again show. Finally, absolute prime ideals are considered (ğ 7), that is, those that remain prime ideals when the coefficient domain is extended to an algebraically closed field. For absolute prime ideals with coefficients from a (finite) algebraic number field, the characterization leads to the transfer of a theorem first stated by A. Ostrowski for absolute prime functions: the property of being a prime ideal is preserved modulo every prime ideal of the number field, with at most finitely many exceptions.

Let the analogy of the last question with ideal theory in algebraic number fields also be pointed out. As the elementary-divisor form of such an ideal one has to regard the least integral rational number divisible by the ideal (note 10), which for a prime ideal therefore always becomes a prime number, whereas conversely an ideal becomes a prime ideal as soon as its norm is a prime number; the proofs also run quite in parallel. The examples mentioned above thus show that, over an imperfect field, the analogue of prime ideals of higher degree and ramification ideals occurs, whereas over a perfect field there are only prime ideals of first degree and no ramification ideals.

ğ 1. Basic Concepts of Elimination Theory, General Ideal Theory, and Field Theory

1. The domain. Let $\bar{\mathfrak{S}}$ denote the integral domain of all polynomials in $y_1, \ldots, y_n$ with coefficients from an abstractly defined field P. Let the y be subjected to a transformation with indeterminates $u_{\mu\nu}$ as coefficients:[5]

$$y_1 = u_{11}x_1 + \cdots + u_{1n}x_n;\ \ldots;\ y_n = u_{n1}x_1 + \cdots + u_{nn}x_n \tag{1}$$

with inverse

$$x_1 = t_{11}y_1 + \cdots + t_{n1}y_n;\ \ldots;\ x_n = t_{1n}y_1 + \cdots + t_{nn}y_n, \tag{1'}$$

and the $u_{\mu\nu}$, or – what is equivalent because of mutual rational expressibility – the $t_{\mu\nu}$, are adjoined to P, so that the coefficient domain $P(u) = P(t)$ arises; let $\mathfrak{S}$ denote the integral domain of all polynomials in $x_1, \ldots, x_n$ with coefficients from $P(u)$. The domains $\mathfrak{S}$ and $\bar{\mathfrak{S}}$ underlie elimination theory; ideals $\mathfrak{a}, \mathfrak{b}, \ldots$ in $\mathfrak{S}$ and $\bar{\mathfrak{a}}, \bar{\mathfrak{b}}, \ldots$ in $\bar{\mathfrak{S}}$ are considered. An ideal in an arbitrary ring is here defined in the usual way by the requirement that, together with α and β, it also contain $\alpha - \beta$, and, together with α, also $\lambda\alpha$, where λ is an arbitrary ring element; $\mathfrak{o}$ will always denote the unit ideal consisting of all elements.

2. Transformed ideals. An ideal $\mathfrak{m}$ in $\mathfrak{S}$ is called transformed if it arises from an ideal $\overline{\mathfrak{m}}$ in $\bar{\mathfrak{S}}$ by means of (1) after adjoining the $u_{\mu\nu}$, or the $t_{\mu\nu}$. Thus $\mathfrak{m}$ consists, when $\bar{f}(y)$ or $\bar{g}(y)$ runs through all polynomials in $\overline{\mathfrak{m}}$, of all linear combinations

$$f(x) = \sum U_i(u)\bar{f}_i(y) = \sum U_i(u)f_i(x)$$

or also

$$g(x) = \sum T_i(t)\bar{g}_i(y) = \sum T_i(t)g_i(x);$$

in particular all $f_i(x) = \bar{f}_i(y)$ are contained, or, what amounts to the same thing, all $g_i(x) = \bar{g}_i(y)$. Since $f(x)$ respectively $g(x)$ are fixed only up to quantities from $P(u) = P(t)$, the U_i, T_i may, without loss of generality, be assumed to be power products of the u, respectively the t. The polynomials $f(x), g(x)$ again pass into polynomials of $\mathfrak{m}$ if U, T are replaced by arbitrary other power products, in particular by interchanging the columns of (1), respectively the rows of (1'); hence $\mathfrak{m}$ contains, together with any polynomial, all those

[5] The transformation is, with a view to ğ 3 and so on, somewhat more general than in H.-N.; all results there are thereby retained all the more.

arising from it by interchanging the x, provided only that the corresponding interchanges are carried out in the coefficients depending on u, respectively t. All ideals occurring in what follows are to be assumed transformed unless the contrary is expressly stated. Non-transformed ideals pass, by composing (1) with $x_i = v_{i1}z_1 + \cdots + v_{in}z_n$, into transformed ideals in the polynomial domain of the z with coefficients from $P(u, v)$, whereas for transformed ideals this composition amounts merely to replacing the $u_{\mu\nu}$ by bilinear combinations of the u, v.

3. Notation. By $f^{(i)}, g^{(i)}, \ldots, a^{(i)}, b^{(i)}, \ldots$ we shall throughout understand polynomials in $\mathfrak{S}$ that are free of $x_1, \ldots, x_{i-1}$.

4. Fundamental ideals. To every ideal $\mathfrak{m}$ there are assigned n fundamental ideals $\mathfrak{g}_0, \mathfrak{g}_1, \ldots, \mathfrak{g}_{n-1}$ by the following stipulation: the fundamental ideal of $(i-1)$-st stage, $\mathfrak{g}_{i-1}$, contains all and only those polynomials $G(x)$ for which there exists a polynomial $b^{(i)} \neq 0$ – in general varying with $G(x)$ – such that $b^{(i)}G(x) \equiv 0(\mathfrak{m})$. From the existence of the ideal basis follows also the existence of at least one $B^{(i)}$, fixed for all $G(x)$, so that

$$B^{(i)}\mathfrak{g}_{i-1} \equiv 0(\mathfrak{m}), \qquad B^{(i)} \neq 0. \tag{2}$$

The fundamental ideals of transformed ideals themselves become transformed ideals (H.-N., Theorem VI). The fundamental ideal of i-th stage $\mathfrak{g}_i$ is also defined as the ideal into which $\mathfrak{m}$ passes when $x_{i+1}, \ldots, x_n$ are adjoined to $P(u)$, provided one restricts oneself – which then means no loss of generality – to polynomials integral in $x_{i+1}, \ldots, x_n$; $\mathfrak{g}_0$ is always equal to the unit ideal $\mathfrak{o}$.

5. Module representation of ideals, elementary divisors and individual norms. If every polynomial $f(x)$ is regarded as a linear form in the power products ξ of $x_1, \ldots, x_{i-1}$, with polynomials $a^{(i)}$ as coefficients, then the ideal $\mathfrak{m}$ passes into a module $\mathfrak{M}_{i-1}$ of linear forms with respect to the domain of the $a^{(i)}$; that is, $\mathfrak{M}_{i-1}$ contains, together with any two linear forms, also their difference, and, together with a linear form $l(\xi)$, also $a^{(i)}l(\xi)$ for arbitrary $a^{(i)}$. As fundamental module of such a module $\mathfrak{M}$ one denotes the totality of linear forms $g(\xi)$ for which $b^{(i)}g(\xi) = 0(\mathfrak{M})$, $b^{(i)} \neq 0$; hence the fundamental ideal $\mathfrak{g}_{i-1}$ passes, under the module representation, into the fundamental module $\mathfrak{G}_{i-1}$ of $\mathfrak{M}_{i-1}$. $\mathfrak{M}_{i-1}$ and $\mathfrak{G}_{i-1}$ depend on infinitely many indeterminates ξ, in such a way that in each individual linear form only finitely many of these indeterminates occur. $\mathfrak{M}_{i-1}$ has the characteristic property that, after adjoining $x_{i+1}, \ldots, x_n$ to $P(u)$, it has only finitely many elementary divisors different from unity; that is, after this adjunction $\mathfrak{G}_{i-1}$ and $\mathfrak{M}_{i-1}$ admit a basis representation – with ζ denoting new indeterminates, connected with the ξ by invertible linear transformations integral in x_i, in such a way that in $\zeta_i = r_i(\xi)$ only finitely many of these indeterminates occur at a time –

$$\begin{aligned} \mathfrak{G}_{i-1} &= (\zeta_0, \zeta_1, \ldots, \zeta_\sigma, \zeta_{\sigma+1}, \ldots, \zeta_{\sigma+\nu}, \ldots), \\ \mathfrak{M}_{i-1} &= (E^{(i)}\zeta_0, E_1^{(i)}\zeta_1, \ldots, E_\sigma^{(i)}\zeta_\sigma, \zeta_{\sigma+1}, \ldots, \zeta_{\sigma+\nu}, \ldots), \end{aligned} \tag{3}$$

where each $E_\mu^{(i)}$ divides the preceding one (H.-N. (24) and (28)).

The highest elementary divisor $E^{(i)}$ is also defined as the greatest common divisor – in the polynomial sense – of all $B^{(i)}$ occurring in (2); it can be assumed integral and primitive in $x_{i+1}, \ldots, x_n$, and is then regular in x_i, that is, $E^{(i)}$ contains the term x_i^λ with non-zero coefficient, if it is of degree λ in the x.

The product $R^{(i)}$ of all elementary divisors occurring in (3) is called the norm of $\mathfrak{G}_{i-1}$ with respect to $\mathfrak{M}_{i-1}$, or also the individual norm of the ideal $\mathfrak{m}$; in symbols, taking account of the fact that $\mathfrak{m}$ passes into $\mathfrak{g}_i$ when $x_{i+1}, \ldots, x_n$ are adjoined:

$$R^{(i)} = E^{(i)}E_1^{(i)} \cdots E_\sigma^{(i)} = N(\mathfrak{G}_{i-1} \mid \mathfrak{M}_{i-1}) = N(\mathfrak{g}_{i-1} \mid \mathfrak{g}_i). \tag{5}$$

As (3) shows, after adjoining $x_{i+1}, \ldots, x_n$, $R^{(i)}$ becomes equal to the determinant of the transition substitution from $\mathfrak{G}_{i-1}$ to $\mathfrak{M}_{i-1}$, and the degree of $R^{(i)}$ gives the number of residue classes, linearly independent over $P(u, x_{i+1}, \ldots, x_n)$, of $\mathfrak{G}_{i-1}$ modulo $\mathfrak{M}_{i-1}$, hence of $\mathfrak{g}_{i-1}$ modulo $\mathfrak{g}_i$; $R^{(i)}$ can be assumed integral and primitive in $x_{i+1}, \ldots, x_n$, and is then regular in x_i. $R^{(i)}$ can be computed as the greatest common divisor – in the polynomial sense – of all ϱ-rowed determinants of a module $\mathfrak{M}_{i-1}^*$, always existing, of rank ϱ, having the property that the residue-class system $\mathfrak{G}_{i-1}^*/\mathfrak{M}_{i-1}^*$ is isomorphic to $\mathfrak{G}_{i-1}/\mathfrak{M}_{i-1}$, where $\mathfrak{G}_{i-1}^*$ is understood as the fundamental module of $\mathfrak{M}_{i-1}^*$ (H.-N., Theorem VII and ğ 5).

6. Elementary-divisor form and norm (resultant form) of ideals. The product $E_\mathfrak{m} = E^{(1)}E^{(2)} \cdots E^{(n)}$ of all highest elementary divisors is called the elementary-divisor form, and the product $R_\mathfrak{m} = R^{(1)}R^{(2)} \cdots R^{(n)}$ of all individual norms the norm (resultant form)[6] of $\mathfrak{m}$. The elementary-divisor form

[6] In H.-N. only the term resultant form is used; the term norm corresponds to the arithmetical properties.

and the norm are divisible by the ideal; the norm is divisible by the elementary-divisor form, and a power of the latter by the norm. More generally one still has:

$$(4)\qquad \begin{aligned} &E^{(i)}\mathfrak{g}_{i-1} = 0(\mathfrak{g}_i), && E^{(n)}\cdots E^{(i)}\mathfrak{g}_{i-1} = 0(\mathfrak{m}), \quad \text{and consequently}\\ &R^{(i)}\mathfrak{g}_{i-1} = 0(\mathfrak{g}_i), && R^{(n)}\cdots R^{(i)}\mathfrak{g}_{i-1} = 0(\mathfrak{m}), \quad \text{(H.-N., Theorem VIII)}, \end{aligned}$$

and further: if $\mathfrak{m}$ is divisible by $\mathfrak{n}$, and the norms $R_\mathfrak{m}$ and $R_\mathfrak{n}$ agree, then *the ideals* $\mathfrak{m}$ *and* $\mathfrak{n}$ *also agree* (H.-N., Theorem IX). Taking into account that, for a divisor of $\mathfrak{m}$, agreement of $R^{(1)}, R^{(2)}, \ldots$ entails agreement of the fundamental ideals $\mathfrak{g}_1, \mathfrak{g}_2, \ldots$, and that always $\mathfrak{g}_0 = \mathfrak{o}$, one obtains correspondingly: if $\mathfrak{n}$ is a *proper divisor* of $\mathfrak{m}$, then the first individual norm of $\mathfrak{n}$ that differs from the corresponding one of $\mathfrak{m}$ becomes a *proper divisor*.[7] *If* $\mathfrak{m}$ *contains a polynomial* $G^{(i)} \neq 0$, then by definition $\mathfrak{g}_0, \mathfrak{g}_1, \ldots, \mathfrak{g}_{i-1}$ are equal to the unit ideal; consequently, by the property of individual norms stated in 5, namely to determine the number of linearly independent residue classes, $R^{(1)}, \ldots, R^{(i-1)}$ become equal to *unity*; hence also $E^{(1)}, \ldots, E^{(i-1)}$ become equal to *unity*.

7. Decomposition of the individual norms and elementary divisors; components of the fundamental ideals. By a prime function one understands a polynomial irreducible with respect to $P(u)$; by a primary function, the power of a prime function. A proper primary function is one that is not at the same time a prime function, where therefore powers higher than the first are involved. A decomposition of a polynomial into greatest primary factors is one in which every factor is a primary function, but the product of any two factors is no longer primary.[8] To the decomposition of the individual norm $R^{(i)} = N(\mathfrak{g}_{i-1} \mid \mathfrak{g}_i)$ into greatest primary factors $Q_\lambda^{(i)}$ there corresponds a representation of $\mathfrak{g}_i$ as a least common multiple

$$\mathfrak{g}_i = [\mathfrak{r}_1, \mathfrak{r}_2, \ldots, \mathfrak{r}_s],$$

such that $Q_\lambda^{(i)} = N(\mathfrak{g}_{i-1} \mid \mathfrak{r}_\lambda)$; here $\mathfrak{r}_\lambda$ possesses $\mathfrak{g}_{i-1}$ as its fundamental ideal of $(i-1)$-st stage, and agrees with its fundamental ideal of i-th stage; the $\mathfrak{r}_\lambda$ are called the components of the fundamental ideals. The highest elementary divisor of $\mathfrak{r}_\lambda$ becomes equal to the greatest common divisor – in the polynomial sense – of $Q_\lambda^{(i)}$ and $E^{(i)}$, hence equal to a greatest primary factor of $E^{(i)}$. The $\mathfrak{r}_\lambda$ are uniquely determined by their behavior, stated above, with respect to the fundamental ideals and by the requirement that either the individual norm or the highest elementary divisor should be a greatest primary factor of $R^{(i)}$ respectively $E^{(i)}$ (H.-N., Theorem X).

8. Concept of dimension. To the ideal $\mathfrak{m}$ the highest dimension $n-i$ is assigned if $R^{(i)}$ is the first individual norm different from unity – or, what by 6 is equivalent, if $\mathfrak{g}_i$ is the first fundamental ideal different from the unit ideal; the dimension -1 is assigned to the unit ideal $\mathfrak{o}$. If there is only one individual norm $R^{(i)}$ different from unity, so that $\mathfrak{g}_i = \mathfrak{g}_{i+1} = \cdots = \mathfrak{m}$, then the highest dimension is also called simply the dimension of $\mathfrak{m}$. If $\mathfrak{m}$ contains a polynomial $G^{(i)} \neq 0$, then it is of highest dimension at most $n-i$, as the remark at the end of 6 shows. If $\mathfrak{m}$ has highest dimension $n-i$ and $\mathfrak{n}$ is a divisor of $\mathfrak{m}$, then $\mathfrak{n}$ also has highest dimension at most $n-i$.

9. Norm (resultant form) and zeroes. By zeroes of an ideal $\mathfrak{m}$ one understands all systems of values of $x_1, \ldots, x_i$ belonging to a suitable algebraic extension field of $P(u; x_{i+1}, \ldots, x_n)$ $(i = 1, 2, \ldots, n)$ for which – after adjoining $x_{i+1}, \ldots, x_n$ to the coefficient domain – all polynomials from $\mathfrak{m}$ vanish. To each factor $R^{(i)}$ of the norm (resultant form), under this adjunction, there correspond as many zeroes of $\mathfrak{m}$ as the degree of $R^{(i)}$ indicates; and $R^{(i)}$, written in bilinear combinations $w_{\mu\nu}$ of the $u_{\mu\nu}$ and further indeterminates v, admits the explicit decomposition:

$$R^{(i)} = \prod\{z - (v_1\bar{x}_{1\nu} + \cdots + v_{i-1}\bar{x}_{i-1,\nu} + v_i\bar{x}_{i,\nu})\}^{\lambda_\nu},$$

where $\bar{x}_{1\nu}, \ldots, \bar{x}_{i,\nu}$ denotes a system of associated zeroes (H.-N., Theorem XIII; a new foundation will be given in ğ 3). Thus among the zeroes of an ideal of highest dimension $n-i$ there are zeroes depending on $(n-i)$ parameters, but none depending on more parameters; this proves the agreement of the concept of dimension given in 8 with the usual formulation.

10. The ring domain of general ideal theory. The underlying domain is to be a commutative ring in which the *theorem of the finite chain* holds: every chain of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k, \ldots$, where each $\mathfrak{a}_i$ is a proper divisor – divisor in the ideal sense – of the immediately preceding one, breaks off after finitely many

[7] On the other hand, later factors of $R_\mathfrak{n}$ can become multiples of the corresponding factors of $R_\mathfrak{m}$; for instance always when $\mathfrak{m}$ is a prime ideal and $\mathfrak{n}$ is not the unit ideal.

[8] The definition of prime function and primary function could also be formulated in exact analogy with 11 by replacing only the word ideal by polynomial. The greatest primary factors are the analogue of the greatest primary components of the decomposition in 12.

terms. This requirement is equivalent to the other, that every ideal possesses an ideal basis (Ideal Theory, Theorem I), and is therefore fulfilled in particular for the polynomial domain. In the following numbers 11, 12, 13, this general ring domain is assumed.

11. Prime ideals and primary ideals. An ideal $\mathfrak{p}$ is called a prime ideal if from the divisibility of a product by $\mathfrak{p}$ follows the divisibility of at least one factor; $\mathfrak{q}$ is called a primary ideal – or primary – if from the divisibility of a product by $\mathfrak{q}$ follows the divisibility of one factor or of a power of every factor. In symbols:

$$a \not\equiv 0(\mathfrak{p}), \quad b \not\equiv 0(\mathfrak{p}) \quad \text{implies} \quad ab \not\equiv 0(\mathfrak{p});$$

$$a \not\equiv 0(\mathfrak{q}), \quad b^x \not\equiv 0(\mathfrak{q}) \text{ for every power } x \quad \text{implies} \quad ab \not\equiv 0(\mathfrak{q}).$$

To every primary ideal $\mathfrak{q}$ there is one and only one associated prime ideal $\mathfrak{p}$, which is a divisor of $\mathfrak{q}$ and a power of which is divisible by $\mathfrak{q}$, $\mathfrak{q} \equiv 0(\mathfrak{p})$, $\mathfrak{p}^\rho \equiv 0(\mathfrak{q})$; here $\mathfrak{p}$ consists of all ring elements of which a power is divisible by $\mathfrak{q}$. As the definition shows, every prime ideal is at the same time a primary ideal; proper primary ideals mean those that are not at the same time prime ideals, so that $\rho > 1$.

12. The decomposition theorem. A representation $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$ of an ideal as a least common multiple is called shortest if no $\mathfrak{q}$ is contained in the least common multiple of the others – in its complement; it is called a representation by greatest primary components if every $\mathfrak{q}$ is primary, but the least common multiple of any two $\mathfrak{q}$'s is not primary. Every ideal admits a shortest representation by *finitely many greatest primary components*; for two different such representations, *the number of components and the associated prime ideals, all of which are mutually distinct, agree.* The prime ideals thus uniquely determined are to be called the prime ideals, or associated prime ideals, of the ideal (Ideal Theory, Theorem IX).

13. Isolated components of the decomposition. An ideal $\mathfrak{r} = [\mathfrak{q}_{i_1}, \ldots, \mathfrak{q}_{i_\lambda}]$ is called an isolated component of the decomposition of $\mathfrak{a}$ if the $\mathfrak{q}_{i_j}$ occur in at least one shortest representation of $\mathfrak{a}$ by greatest primary components and satisfy the condition that none of their associated prime ideals is contained in one of the other prime ideals of $\mathfrak{a}$. The *isolated components* of the decomposition are *uniquely determined by their prime ideals*; in particular the isolated greatest primary components are uniquely determined (Ideal Theory, Theorem XIII).

14. Characteristic, perfect and imperfect fields, extension of the first kind. A field Ω is said to have characteristic zero if the prime field contained in Ω and derived from the unit is of the type of the field of rational numbers; it has characteristic p if this prime field is of the type of the residue-class system modulo a prime number p. A field Ω is called perfect if every prime function with coefficients from Ω decomposes in a suitable extension field into distinct linear factors; otherwise it is called imperfect. Every field of characteristic zero is perfect; a field of characteristic p is perfect if and only if, together with every element, it also contains its p-th root. A prime function in an imperfect field is an integral function of degree r in x^{p^f}, and decomposes in a suitable extension field into p^f-th powers of r distinct linear factors; f is called the exponent. A prime function is said to be of the first kind if it decomposes in a suitable extension field into distinct linear factors, so that the exponent f is zero; an extension is called of the first kind if every element is of the first kind, that is, is a zero of a prime function of the first kind. Every extension that arises by adjoining an element of the first kind is of the first kind; over perfect fields there are only extensions of the first kind (Steinitz, ǧ 11 and ǧ 13).

15. Reduced degree and exponent of a finite extension. If $\mathfrak{K}$ is a finite extension of an imperfect field Ω, then $\mathfrak{K}$ contains a subfield $\mathfrak{K}_0$ of degree r that is of the first kind with respect to Ω and consists of all and only the elements of the first kind in $\mathfrak{K}$. The p^f-th power of every element of $\mathfrak{K}$ belongs to $\mathfrak{K}_0$, and there are elements in $\mathfrak{K}$ that are exactly of degree rp^f. r is called the reduced degree, f the exponent of the finite extension (Steinitz, ǧ 14, 1 and ǧ 14, 5).

ǧ 2. Elementary-Divisor Form and Norm of the Prime Ideals and Primary Ideals. Divisors of the Prime Ideals

From now on we shall throughout be concerned with the polynomial domain defined in ǧ 1, 1. First it is to be shown that, also for prime ideals and primary ideals, one may restrict oneself to transformed ideals, according to

Lemma I. *The transformed ideal* $\mathfrak{p}$ *of a prime ideal* $\bar{\mathfrak{p}}$ *in* $\bar{\mathfrak{S}}$ *becomes a prime ideal; the transformed* $\mathfrak{q}$ *of a primary ideal* $\bar{\mathfrak{q}}$ *in* $\bar{\mathfrak{S}}$ *becomes a primary ideal. In other words, the property of being a prime ideal or a primary ideal is preserved when the* $u_{\mu\nu}$ *are adjoined to* P.

Indeed suppose that $\mathfrak{a} \not\equiv 0(\mathfrak{p})$, $\mathfrak{b} \not\equiv 0(\mathfrak{p})$, where $\mathfrak{a}$ and $\mathfrak{b}$ need not be transformed ideals; say $a(x) \not\equiv 0(\mathfrak{p})$ and $b(x) \not\equiv 0(\mathfrak{p})$, with $a(x)$ and $b(x)$ polynomials from $\mathfrak{a}$ and $\mathfrak{b}$. By inversion of (1) according to (1') one

obtains – with T understood, without loss of generality, as power products of the $t_{\mu\nu}$ –

$$a(x) = \sum T_j \bar{a}_j(y), \qquad b(x) = \sum T_j \bar{b}_j(y),$$

and at least one $\bar{a}_j(y)$ and one $\bar{b}_j(y)$ must fail to be divisible by $\bar{\mathfrak{p}}$. Let, for example, $\bar{a}_r(y) \not\equiv 0(\bar{\mathfrak{p}})$ and $\bar{b}_s(y) \not\equiv 0(\bar{\mathfrak{p}})$ be the respective highest terms under some lexicographic ordering of the T's; then also $\bar{a}_r(y)\bar{b}_s(y) \not\equiv 0(\bar{\mathfrak{p}})$, and consequently $a(x)b(x) \not\equiv 0(\mathfrak{p})$ and hence $\mathfrak{ab} \not\equiv 0(\mathfrak{p})$, proving that $\mathfrak{p}$ is prime. The proof evidently rests on the fact that the residue-class system modulo a prime ideal forms a ring without zero divisors, a property preserved by adjoining indeterminates.

Correspondingly suppose that $\mathfrak{a} \not\equiv 0(\mathfrak{q})$ and $\mathfrak{b}^z \not\equiv 0(\mathfrak{q})$ for every power z; then from the existence of the ideal basis it follows that there must exist an $a(x)$ from $\mathfrak{a}$ and a $b(x)$ from $\mathfrak{b}$ such that $a(x) \not\equiv 0(\mathfrak{q})$ and $b(x)^z \not\equiv 0(\mathfrak{q})$ for every power z; for under the contrary assumption, a power of $\mathfrak{b}$ would be divisible by $\mathfrak{q}$.

Putting $a(x)b(x) = c(x)$, let $\mathfrak{a}^*, \mathfrak{b}^*, \mathfrak{c}^*$ denote the ideals respectively derived from the coefficients $\bar{a}_j(y), \bar{b}_j(y), \bar{c}_j(y)$ of $a(x), b(x), c(x)$. Then $\mathfrak{b}^{*z} \not\equiv 0(\bar{\mathfrak{q}})$ for every power z, since otherwise $b(x)^z$ would be divisible by $\mathfrak{q}$; because $\mathfrak{a}^* \not\equiv 0(\bar{\mathfrak{q}})$, one must also have $\mathfrak{a}^*\mathfrak{b}^{*\lambda} \not\equiv 0(\bar{\mathfrak{q}})$ for every power λ. But by the Dedekind-Mertens theorem[9] there exists an exponent h such that $\mathfrak{a}^*\mathfrak{b}^{*h} = \mathfrak{b}^{*h-1}\mathfrak{c}^*$; hence $\mathfrak{c}^* \not\equiv 0(\bar{\mathfrak{q}})$. This gives $c(x) \not\equiv 0(\mathfrak{q})$ and consequently $\mathfrak{ab} \not\equiv 0(\mathfrak{q})$, proving that $\mathfrak{q}$ is primary.

Also in representing an ideal as a least common multiple one may restrict oneself to transformed ideals, according to

Lemma II. *From a representation $\overline{\mathfrak{m}} = [\bar{\mathfrak{c}}_1, \ldots, \bar{\mathfrak{c}}_\alpha]$ in $\bar{\mathfrak{S}}$ follows a representation $\mathfrak{m} = [\mathfrak{c}_1, \ldots, \mathfrak{c}_\alpha]$ in $\mathfrak{S}$, where $\mathfrak{c}_i$ denotes the transformed ideal of $\bar{\mathfrak{c}}_i$. In particular, therefore, in every shortest representation by greatest primary components (ǧ 1, 12.) these may be assumed transformed.*

Indeed $\mathfrak{m}$ is divisible by $[\mathfrak{c}_1, \ldots, \mathfrak{c}_\alpha]$, since every polynomial $f(x)$ from $\mathfrak{m}$ – after multiplication, if necessary, by a suitable power of $u_{\mu\nu}$ – is of the form $\sum U_i \bar{f}_i(y)$, where each $\bar{f}_i(y)$, as a polynomial from $\overline{\mathfrak{m}}$, is by assumption divisible by all the $\bar{\mathfrak{c}}_i$. Conversely, if $f(x)$ is divisible by every $\mathfrak{c}_i$, then it has the above form and is therefore divisible by $\mathfrak{m}$. Thus if one starts from a decomposition into greatest primary components in $\bar{\mathfrak{S}}$, one obtains a decomposition $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_\alpha]$ in $\mathfrak{S}$; here the $\mathfrak{q}$, as transformed ideals of primary ideals, are primary by Lemma I, and they are greatest primary components, since distinct associated prime ideals $\bar{\mathfrak{p}}$ in $\bar{\mathfrak{S}}$ correspond to distinct $\mathfrak{p}$ in $\mathfrak{S}$.

We now need a first characterization of prime ideals and primary ideals by elementary-divisor form and norm, still without complete separation of prime and primary. In exact analogy with ideal theory in algebraic number fields,[10]

Theorem I. *The elementary-divisor form of a prime ideal becomes equal to a prime function, and the norm to a power of this prime function. For primary ideals, elementary-divisor form and norm become primary functions, namely powers of the same prime function, which itself is the elementary-divisor form of the associated prime ideal. For prime ideals and primary ideals, highest dimension coincides with dimension simpliciter; this dimension agrees for a primary ideal and its associated prime ideal.*

Theorem I is evidently fulfilled for the unit ideal, whose elementary-divisor form and norm become unity. Now let the prime ideal $\mathfrak{p}$ have highest dimension $(n-i)$; by (4), ǧ 1, 6, one obtains

$$E^{(n)} \cdots E^{(i+1)}\mathfrak{g}_i \equiv 0(\mathfrak{p}), \quad \text{but} \quad E^{(n)} \cdots E^{(i+1)} \not\equiv 0(\mathfrak{p}),$$

since otherwise $\mathfrak{p}$ would, by ǧ 1, 8, have highest dimension at most $n-i-1$. Hence $\mathfrak{g}_i \equiv 0(\mathfrak{p})$, so that $\mathfrak{p}$ is identical with its fundamental ideal of i-th stage and consequently also with $\mathfrak{g}_{i+1}, \mathfrak{g}_{i+2}, \ldots$. Thus $R^{(i+1)} = N(\mathfrak{g}_i \mid \mathfrak{g}_{i+1})$, $R^{(i+2)}, \ldots$ become equal to unity, and hence also $E^{(i+1)}, E^{(i+2)}, \ldots$, as divisors of $R^{(i+1)}, R^{(i+2)}, \ldots$; therefore the elementary-divisor form becomes equal to $E^{(i)}$, which must be equal to a prime function $P^{(i)}$. For by ǧ 1, 5 and taking into account that $\mathfrak{g}_{i-1}$ becomes the unit ideal, $E^{(i)}$ is defined as the greatest common divisor – in the polynomial sense – of all $B^{(i)}$ divisible by $\mathfrak{p}$; from $E^{(i)} = C_1^{(i)}C_2^{(i)} \equiv 0(\mathfrak{p})$ it would follow that $E^{(i)}$ must be contained in one of its factors $C_1^{(i)}$ or $C_2^{(i)}$. Since, however, a power of $E^{(i)}$ is divisible by $R^{(i)}$, $R^{(i)}$ becomes a power – possibly the first power – of this prime function $P^{(i)}$; at the same time $R^{(i)}$ becomes the norm of $\mathfrak{p}$. Since only one individual norm different from unity occurs, the highest dimension of $\mathfrak{p}$ finally agrees with its dimension simpliciter.

[9] Compare H.-N., p. 63 and note 13).

[10] As the highest elementary divisor of ideals in algebraic number fields one has to regard the least integral rational number divisible by the ideal, hence in particular the prime number divisible by a prime ideal or the prime-power divisible by a primary ideal (a power of a prime ideal). In fact every ideal $\mathfrak{a}^*$ is also a module A^* of linear forms in the elements $\omega_1, \ldots, \omega_n$ of a field basis, with $(\omega_1, \ldots, \omega_n)$ the fundamental module of A^*; the least integral rational number divisible by $\mathfrak{a}^*$ therefore becomes the highest elementary divisor of this module A^*, whereas the norm of $\mathfrak{a}^*$ becomes the product of all elementary divisors of A^*.

Correspondingly, let the primary ideal $\mathfrak{q}$ have highest dimension $n-i$; then, as above,

$$E^{(n)} \cdots E^{(i+1)} \mathfrak{g}_i \equiv 0(\mathfrak{q}), \quad (E^{(n)} \cdots E^{(i+1)})^z \not\equiv 0(\mathfrak{q})$$

for every power z; and consequently, as above, $\mathfrak{q} = \mathfrak{g}_i$, its elementary-divisor form is $E^{(i)}$, its norm is $R^{(i)}$, and its highest dimension is its dimension simpliciter. This dimension agrees with that of the associated prime ideal; for from $\mathfrak{p}^\rho \equiv 0(\mathfrak{q})$, $\mathfrak{q} \equiv 0(\mathfrak{p})$ it follows that the dimension $(n-i)$ of $\mathfrak{p}$ is at most equal to that of $\mathfrak{q}$, and that of $\mathfrak{q}$ at most equal to that of $\mathfrak{p}^\rho$; from $(P^{(i)})^\rho \equiv 0(\mathfrak{p}^\rho)$, where $P^{(i)}$ denotes the elementary-divisor form of $\mathfrak{p}$, the latter highest dimension is found to be at most $n-i$, and thus $n-i$ is the dimension of $\mathfrak{p}$ and $\mathfrak{q}$. From $(P^{(i)})^\rho \equiv 0(\mathfrak{q})$ it follows further that $E^{(i)}$ – as the greatest common divisor of all $B^{(i)}$ from $\mathfrak{q}$ – becomes a power of $P^{(i)}$, which may also be the first power, and that the same holds for $R^{(i)}$. This proves Theorem I in all its parts.

A characterization of prime ideals by means of the concept of dimension is given by

Theorem II. *A prime ideal has no proper divisor of the same highest dimension; conversely, every ideal with this property is prime.*

The proof rests on

Lemma III. *If a prime ideal $\mathfrak{p}$ of polynomials with coefficients from a field Ω has only finitely many residue classes linearly independent over Ω, then $\mathfrak{p}$ has no proper divisor different from the unit ideal; in other words, the residue-class system modulo $\mathfrak{p}$ forms a field.*

The hypothesis says that there is a finite number k such that among any $(k+1)$ residue classes there is a linear dependence with coefficients from Ω – more precisely, with coefficients from the residue-class field (Ω) represented by all elements of Ω – but that at least one system of k residue classes linearly independent over (Ω) exists. It follows immediately that all residue classes can be expressed linearly by any chosen system of k linearly independent ones. Now let $\mathfrak{a}$ be a proper divisor of $\mathfrak{p}$, and let $a(z) \not\equiv 0(\mathfrak{p})$ be a polynomial from $\mathfrak{a}$; from $c_1 f_1(z) + \cdots + c_k f_k(z) \not\equiv 0(\mathfrak{p})$ it follows that

$$c_1 a(z) f_1(z) + \cdots + c_k a(z) f_k(z) \not\equiv 0(\mathfrak{p});$$

that means that, together with the residue classes of $f_1, \ldots, f_k$, the residue classes of $af_1, \ldots, af_k$ also form a system of k linearly independent ones, through which in particular the unit class can be linearly represented. Hence $\mathfrak{a}$ is the unit ideal; expressed differently, the residue-class system forms a field, since for $a(z) \not\equiv 0(\mathfrak{p})$ there is always an $f(z)$ such that $1 \equiv a(z)f(z)(\mathfrak{p})$.

For the proof of the first part of Theorem II it remains only to observe that every prime ideal of dimension $(n-i)$ – more generally every ideal of highest dimension $(n-i)$ – has only finitely many residue classes linearly independent over $P(u; x_{i+1}, \ldots, x_n)$, namely, by ğ 1, 5, as many as the degree of $R^{(i)}$ indicates, since here $\mathfrak{g}_{i-1}$ becomes the unit ideal. Every proper divisor $\mathfrak{a}$ of $\mathfrak{p}$ therefore becomes the unit ideal when $x_{i+1}, \ldots, x_n$ are adjoined to $P(u)$; expressed differently, the fundamental ideal of i-th stage of $\mathfrak{a}$ becomes the unit ideal, which means that the highest dimension of $\mathfrak{a}$ is at most $n-i-1$. In order that the assertion also hold for a non-transformed ideal $\mathfrak{a}$ as divisor, one has only to pass, according to ğ 1, 2, to a new transformed domain.

Conversely suppose now that $\mathfrak{p}$ has no proper divisor of the same highest dimension $n-i$, and let $\mathfrak{a} \not\equiv 0(\mathfrak{p})$ and $\mathfrak{b} \not\equiv 0(\mathfrak{p})$, with $\mathfrak{a}$ and $\mathfrak{b}$ again assumed to be transformed ideals. Then, by hypothesis, since $(\mathfrak{a}, \mathfrak{p})$ and $(\mathfrak{b}, \mathfrak{p})$, as greatest common divisors – in the ideal sense – become proper divisors of $\mathfrak{p}$, one has

$$G^{(i+1)} \equiv 0(\mathfrak{a}, \mathfrak{p}), \qquad H^{(i+1)} \equiv 0(\mathfrak{b}, \mathfrak{p}), \qquad G^{(i+1)} \not\equiv 0, \qquad H^{(i+1)} \not\equiv 0.$$

This gives

$$G^{(i+1)} H^{(i+1)} \equiv 0(\mathfrak{ab}, \mathfrak{p}), \qquad G^{(i+1)} H^{(i+1)} \not\equiv 0;$$

and consequently necessarily $\mathfrak{ab} \not\equiv 0(\mathfrak{p})$, since otherwise $\mathfrak{p}$ would have smaller highest dimension than $n-i$. Since $\mathfrak{a}, \mathfrak{b}$ are transformed ideals, $\bar{\mathfrak{p}}$, and by Lemma I also $\mathfrak{p}$, are prime ideals. This proves Theorem II.

ğ 3. Zeroes of the Prime Ideals and Primary Ideals

The passage to a direct foundation of the theory of zeroes (ğ 1, 9.), at first for prime ideals, is formed by the following lemma, which extends Lemma III and is valid for prime ideals in arbitrary rings:

Lemma IV. *The residue-class system modulo every prime ideal different from the unit ideal can be extended by quotient formation to a field, the residue-class field of the prime ideal.*

The residue-class system modulo an arbitrary ideal forms a ring, since sum, difference and product again belong to the system, and the associative, commutative and distributive laws are preserved on passage to

residue classes. If the ideal is specifically prime, this ring has no zero divisors; for the definition of prime ideals (ğ 1, 11.) says that the product of non-vanishing residue classes likewise does not vanish. If the prime ideal is different from the unit ideal, then this ring contains at least one element different from the zero element, and can therefore be extended to a field by quotient formation – adjunction of pairs of elements;[11] thus the residue-class field is defined.

We first fix the notation that will be kept throughout what follows:

Notation: Residue classes shall generally be denoted by putting any representative of the class in parentheses, $(x), \ldots, (a(x)), \ldots$; similarly, fields of residue classes shall be denoted by parentheses. In particular, (P), $(P(u))$, $(P(u, x_{i+1}, \ldots, x_n))$ denote the residue-class fields consisting of all and only those residue classes that can be represented by elements from P, $P(u)$, $P(u, x_{i+1}, \ldots, x_n)$.

We also recall the following: A field $\mathfrak{R}$ is said to have *algebraic rank (transcendence degree) k* with respect to a base field Ω if $\mathfrak{R}$ contains at least one system of k quantities algebraically independent over Ω – transcendental quantities – but every $k+1$ quantities from $\mathfrak{R}$ are algebraically dependent over Ω. If $\mathfrak{R}$ can be represented as an algebraic extension field of a subfield $\Omega(z_1, \ldots, z_s)$, where the z are algebraically independent – transcendental – over Ω, then necessarily $s = k$;[12] likewise the algebraic rank of $\mathfrak{R}(u)$ over $\Omega(u)$ is equal to k when u denotes indeterminates not contained in $\mathfrak{R}$.

The construction of the field of zeroes now proceeds in complete analogy with the usual route for prime functions of one indeterminate,[13] according to

Theorem III. *To the residue-class field $(\mathfrak{R})$ of a prime ideal $\mathfrak{p}$ of dimension $n-i$ there can be assigned, isomorphically, a field of zeroes R of $\mathfrak{p}$, which has algebraic rank $n-i$ – depends on $n-i$ parameters – and in particular can be regarded as a finite extension field of $P(u, x_{i+1}, \ldots, x_n)$. The isomorphism between $(\mathfrak{R})$ and R includes that between (P) and P, $(P(u))$ and $P(u)$, and, when $x_{i+1}, \ldots, x_n$ are taken as parameters, also that between $(P(u, x_{i+1}, \ldots, x_n))$ and $P(u, x_{i+1}, \ldots, x_n)$. Conversely, every field of zeroes of algebraic rank $n-i$ – depending on $n-i$ parameters – is isomorphic to the residue-class field $(\mathfrak{R})$.*

Theorem III yields as a corollary the familiar theorem: *If an ideal $\mathfrak{a}$ vanishes in all zeroes of a prime ideal $\mathfrak{p}$, then $\mathfrak{a}$ is divisible by $\mathfrak{p}$.*

For the proof, first note that the residue-class field $(\mathfrak{R})$ has algebraic rank $n-i$ with respect to $(P(u))$. Indeed, the classes $(x_{i+1}), \ldots, (x_n)$ are algebraically independent with respect to $(P(u))$, since $\mathfrak{p}$, being of dimension $n-i$, contains no polynomial free of $x_1, \ldots, x_i$; every further class, however, is dependent on these. For from the membership of the elementary-divisor form $P^{(i)}$ in $\mathfrak{p}$ it follows, by ğ 1, 2., also for $\lambda = 1, 2, \ldots, i$ that polynomials belong to $\mathfrak{p}$ which depend respectively on $x_\lambda, x_{i+1}, \ldots, x_n$. Thus $(\mathfrak{R})$ becomes a finite extension field of $(P(u, x_{i+1}, \ldots, x_n))$; by ğ 1, 5. – taking into account that $\mathfrak{g}_{i-1}$ is equal to the unit ideal and $\mathfrak{g}_i$, by Theorem I, to $\mathfrak{p}$ – the degree over this subfield is equal to the degree of the norm.

To pass to an isomorphic field of zeroes, one further observes that $P(u, x_{i+1}, \ldots, x_n)$ and $(P(u, x_{i+1}, \ldots, x_n))$ are related isomorphically by assigning to each element of $P(u, x_{i+1}, \ldots, x_n)$ the residue class represented by that element. First, under this assignment, the integral domains consisting of polynomials in $u, x_{i+1}, \ldots, x_n$ and respectively in $(u), (x_{i+1}), \ldots, (x_n)$ correspond isomorphically, since $\mathfrak{p}$ contains no polynomial free of $x_1, \ldots, x_i$, and therefore distinct polynomials from $P(u, x_{i+1}, \ldots, x_n)$ correspond to distinct classes; from isomorphic integral domains, however, isomorphic fields arise by quotient formation. The isomorphic relation between $P(u, x_{i+1}, \ldots, x_n)$ and $(P(u, x_{i+1}, \ldots, x_n))$ includes that between P and (P), $P(u)$ and $(P(u))$. To extend this isomorphism to one between $(\mathfrak{R})$ and a field of zeroes R, let certain new elements $\bar{x}_1, \ldots, \bar{x}_i$ be assigned isomorphically to the classes $(x_1), \ldots, (x_i)$; that is, to each polynomial $(a(x))$ there corresponds a polynomial $a(\bar{x}_1, \ldots, \bar{x}_i, x_{i+1}, \ldots, x_n)$, and sums and products correspond to sums and products. By quotient formation – where one may restrict oneself to denominators from the subfield $(P(u, x_{i+1}, \ldots, x_n))$ respectively $P(u, x_{i+1}, \ldots, x_n)$ – to the residue-class field $(\mathfrak{R})$ there then corresponds a field R, a finite extension of $P(u, x_{i+1}, \ldots, x_n)$ of the degree of the norm; it can be called the field of zeroes. For the assignment says that $f(\bar{x}_1, \ldots, \bar{x}_i, x_{i+1}, \ldots, x_n)$ vanishes as soon as $f(x) \equiv 0(\mathfrak{p})$. In place of $(P(u, x_{i+1}, \ldots, x_n))$, any other subfield of $(\mathfrak{R})$ arising by adjoining $n-i$ algebraically independent quantities could occur throughout the argument.

Conversely it is easy to show that every field of zeroes R of algebraic rank $n-i$ is isomorphic to the residue-

[11] Steinitz, ğ 3. The assumption of *one* non-zero element in the original integral domain suffices, since then the existence of the unit is secured by quotient formation, and hence the original domain becomes a subdomain of the field; Steinitz assumes the existence of the unit in the integral domain.

[12] For a proof of this familiar fact valid in arbitrary characteristic, compare Steinitz, ğ 22, 9. – On adjoining the u, the algebraic rank cannot increase, since only rational combinations of the original elements with coefficients from $\Omega(u)$ are involved; nor can it decrease, since every relation between elements of $\mathfrak{R}$ with coefficients from $\Omega(u)$ decomposes into finitely many relations with coefficients from Ω.

[13] Steinitz, ğ 6.

class field. Since R can be derived rationally, with coefficients from $P(u)$, from the quantities $\bar{x}_1, \ldots, \bar{x}_n$, among these quantities there must be $n-i$ algebraically independent, hence transcendental, elements with respect to $P(u)$. In particular this must hold for $\bar{x}_{i+1}, \ldots, \bar{x}_n$, since, because $P^{(i)} \equiv 0(\mathfrak{p})$, it follows as above that R is an algebraic extension field of $P(u, \bar{x}_{i+1}, \ldots, \bar{x}_n)$. Since by hypothesis $f(\bar{x})$ vanishes for every polynomial $f(x)$ in $\mathfrak{p}$, to every class of the polynomial domain of the (x) contained in $(\mathfrak{R})$ there corresponds one and only one element of R which is a polynomial in the $\bar{x}$; and sums and products correspond to sums and products. But different classes correspond to different elements of R; otherwise a non-zero class, and hence after suitable multiplication also a class represented by a polynomial from $(P(u, x_{i+1}, \ldots, x_n))$, would correspond to the element zero in R, and contrary to the hypothesis the quantities $\bar{x}_{i+1}, \ldots, \bar{x}_n$ would satisfy an algebraic dependence. This assignment exhausts all polynomials in the $\bar{x}$ contained in R; by quotient formation – where one may again restrict oneself to denominators from $(P(u, x_{i+1}, \ldots, x_n))$ respectively $P(u, \bar{x}_{i+1}, \ldots, \bar{x}_n)$ – isomorphic fields arise from these isomorphic integral domains.

Now let the ideal $\mathfrak{a}$ vanish in all zeroes of $\mathfrak{p}$, in particular also in all zeroes depending on $n-i$ parameters. If $a(x)$ is any polynomial from $\mathfrak{a}$, then $a(\bar{x})$ vanishes; because of the isomorphism between R and $(\mathfrak{R})$, the class $(a(x))$ is thus the zero class, and $a(x)$, hence $\mathfrak{a}$, is divisible by $\mathfrak{p}$. This proves Theorem III and its corollary.

To pass from Theorem III to the decomposition given in ğ 1, 9., first for prime ideals, and in order to be able to make more precise statements about the exponents, a further investigation of the elementary-divisor form is needed, according to

Lemma V. *If in characteristic p the elementary-divisor form $E^{(i)}$ of a prime ideal or primary ideal – more generally, of an ideal $\mathfrak{a}$ for which highest dimension and dimension simpliciter coincide – has exponent f with respect to x_i, hence is an integral function of $x_i^{p^f}$, then it also has exponent f with respect to $x_{i+1}, \ldots, x_n$ and with respect to the indeterminates $u_{\mu r}$ respectively $t_{\mu r}$ occurring in $E^{(i)}$. In particular, if the coefficient domain is a perfect field, the elementary-divisor form $P^{(i)}$ of a prime ideal always has exponent zero with respect to x_i, hence is a prime function of the first kind.*

For this it is to be observed that $P(u, x_{i+1}, \ldots, x_n)$ becomes imperfect as soon as P is a perfect field of characteristic p, so that it does not follow directly from ğ 1, 14. that $P^{(i)}$ is of the first kind. Let $E^{(i)}$ have exponent f with respect to x_i, but let it contain another indeterminate $x_{i+\lambda}$ with exponent f'. Then – by interchanging the $u_{\mu r}$ respectively $t_{\mu r}$ – there also exists, by ğ 1, 2., a non-zero polynomial $G^{(i)}$, divisible by the ideal, that is an integral function of $x_i^{p^{f'}}$, and which, by definition of the elementary-divisor form, is divisible by $E^{(i)}$. But since $G^{(i)}$ has the same degree as $E^{(i)}$, it must agree with $E^{(i)}$ up to a factor from $P(u)$; hence necessarily $f' = f$. Thus $E^{(i)}$ – which may be assumed integral and primitive in the $t_{\mu r}$ – is of the form

$$E^{(i)} = \sum c_\lambda(t)\, x_i^{\lambda_i p^f} \cdots x_n^{\lambda_n p^f} = \sum c_i(t)\, g_i(y^{p^f}, t^{p^f}) = \sum T_\mu(t)\, \bar{h}_\mu(y^{p^f}),$$

where the T_μ are power products of the t, and the $\bar{h}$ are divisible by $\bar{\mathfrak{a}}$. Therefore one obtains a polynomial again belonging to $\mathfrak{a}$ if in the T_μ every exponent of the individual t is replaced by the greatest multiple of p^f contained in it; as the displayed representation shows, this amounts to replacing, in $c_\lambda(t)$, every exponent of the t by the greatest multiple of p^f contained in it. By this substitution $E^{(i)}$ passes into a polynomial in $t, x_i, \ldots, x_n$ which, by definition, is divisible by $E^{(i)}$, and, because of the assumed primitivity, also with respect to the t; hence it must be identical with $E^{(i)}$, since the degree has increased in no argument. In particular, if P is perfect, then $E^{(i)}$, as an integral function of x^{p^f}, t^{p^f}, is a p^f-th power; hence, if a prime ideal is involved, necessarily $f = 0$, and the elementary-divisor form $P^{(i)}$ becomes a prime function of the first kind.

The decomposition is now given by

Theorem IV. *The elementary-divisor form $P^{(i)}$ of a prime ideal admits, in the Galois field derived from the field of zeroes, the explicit decomposition:*

$$P^{(i)} = \prod (x_i - t_{1i}\bar{y}_{1\nu} - \cdots - t_{ni}\bar{y}_{n\nu})^\delta = \prod (t_{1i}(y_1 - \bar{y}_{1\nu}) + \cdots + t_{ni}(y_n - \bar{y}_{n\nu}))^\delta,$$

where $\bar{y}_{1\nu}, \ldots, \bar{y}_{n\nu}$ denotes in each case an associated system of zeroes of the original indeterminates y, independent of $t_{1i}, \ldots, t_{ni}$; distinct ν correspond to distinct linear factors; and the exponent δ has the value one when P is perfect and the value p^f ($f \geq 0$) when it is imperfect. Thereby, after adjoining new indeterminates v, the decomposition of the elementary-divisor form written in bilinear combinations of the u and v in place of the $u_{\mu\nu}$ is also determined:

$$P^{(i)}(u, v) = \prod (z - v_1\bar{x}_{1\nu} - \cdots - v_i\bar{x}_{i\nu})^\delta,$$

where δ has the same meaning as above. Likewise the decomposition of the norm of a prime ideal, or of a primary ideal with $\mathfrak{p}$ as associated prime ideal – as a power of $P^{(i)}$ – is also given.

As a corollary of Theorem IV one also obtains: *If two prime ideals agree in their elementary-divisor form $P^{(i)}$, then they are identical.*

The proof of Theorem IV will amount to proving that the elementary-divisor form $P^{(i)}$ is identical with the fundamental equation of the extension field $(P(u, x_i, x_{i+1}, \ldots, x_n))$ over $(P(u, x_{i+1}, \ldots, x_n))$. First, to gain insight into the dependence on the indeterminates $u_{\mu r}$ respectively $t_{\mu r}$, pass to the residue-class field $(\bar{\mathfrak{R}})$ of $\bar{\mathfrak{p}}$, which, by what was said in the definition of algebraic rank, must have algebraic rank $n-i$ with respect to $(\bar{P})$, where $(\bar{P})$ denotes the subfield represented by elements of P. For $(\bar{\mathfrak{R}})$ arises by adjoining the indeterminates u respectively t to a subfield isomorphic to $(\mathfrak{R})$, obtained by quotient formation from all and only those classes representable by polynomials from $\bar{\mathfrak{S}}$, with $(\bar{P})$ and (P) corresponding to one another. The algebraic rank of $(\bar{\mathfrak{R}})$ with respect to $(P(u))$ is therefore equal to that of this subfield with respect to $(\bar{P})$, and hence, by the isomorphism, to that of $(\mathfrak{R})$ with respect to (P). Since $(\bar{\mathfrak{R}})$ can be derived rationally, with coefficients from $(\bar{P})$, from the classes $(y_1), \ldots, (y_n)$, there must be among these classes $n-i$ algebraically independent ones, and $(\bar{\mathfrak{R}})$ arises as a finite algebraic extension field of the subfield generated by adjoining these $n-i$ classes to $(\bar{P})$.[14]

If one adjoins only the indeterminates $t_{\sigma\tau}$ occurring in $x_{i+1}, \ldots, x_n$, then again a residue-class field arises which contains the classes $(y_1), \ldots, (y_n)$ and $(x_{i+1}), \ldots, (x_n)$ and becomes a finite algebraic extension field of $(P(t_{\sigma\tau}, x_{i+1}, \ldots, x_n))$; these are fields isomorphic to subfields of $(\bar{\mathfrak{R}})$, not identical with them, since for different indeterminates the residue classes are represented by the same elements but are not identical, because they do not contain the same elements. Thus in the dependence of the classes (y) on $(P(t_{\sigma\tau}, x_{i+1}, \ldots, x_n))$ only the indeterminates $t_{\sigma\tau}$ enter. Now form, by adjoining $t_{1i}, \ldots, t_{ni}$, the class $(x_i) = (t_{1i}y_1 + \cdots + t_{ni}y_n)$; let $(x_{i\nu}) = (t_{1i}y_{1\nu} + \cdots + t_{ni}y_{n\nu})$ be the r distinct conjugate values lying in the Galois field with respect to $(P(t_{\sigma\tau}, t_{1i}, \ldots, t_{ni}, x_{i+1}, \ldots, x_n))$. Then – according as one is dealing with extensions of the first kind or not – the product over the factors $t-(x_{i\nu})$, or over their p^f-th powers, is a prime function (G) with respect to $(P(t, x_{i+1}, \ldots, x_n))$; for, since there are elements of degree $r \cdot p^f$ (ğ 1, 15.), (x_i) must necessarily be one such element, since every element arises by specializing the $t_{1i}, \ldots, t_{ni}$; but (x_i) is a zero of (G). Passing to the isomorphic field of zeroes of $\mathfrak{p}$ and to the Galois field derived from it, G therefore admits a decomposition into linear factors $t-t_{1i}\bar{y}_{1\nu}-\cdots-t_{ni}\bar{y}_{n\nu}$ respectively their p^f-th powers. Now, since (G) vanishes for $t=(x_i)$, $G(x_i)$ is divisible by $\mathfrak{p}$ and hence by $P^{(i)}$; and, as a prime function with respect to $P(u, x_{i+1}, \ldots, x_n)$ and as primitive in $x_{i+1}, \ldots, x_n$, G must become identical with $P^{(i)}$. Thus the first decomposition of Theorem IV is proved.

To pass to the second decomposition, note that the property of being, or not being, an extension of the first kind is preserved when indeterminates are adjoined. Therefore, after adjoining $v_1, \ldots, v_i$ and all the $t_{\mu\nu}$, form the class $(z) = (v_1x_1 + \cdots + v_ix_i)$ and the conjugate classes $(z_\nu) = (v_1x_{1\nu} + \cdots + v_ix_{i\nu})$. Then the product over all $t-(z_\nu)$, or over their p^f-th powers, is again a prime function (H) that vanishes for $t=(z)$. Hence H is representable as a product of linear factors, as above, and is identical with the elementary-divisor form of the prime ideal derived from $\mathfrak{p}$ by composing the transformation (1) with $z = v_1x_1 + \cdots + v_ix_i$; this elementary-divisor form, however – because of the mutual specialization – is obtained from $P^{(i)}$ by replacing the $u_{\mu\nu}$ by certain bilinear combinations of the u and v.[15] With these decompositions, the decomposition of the norm as a power of $P^{(i)}$ is also given,[16] and likewise that of the norm and elementary-divisor form of a primary ideal with $\mathfrak{p}$ as associated prime ideal.

Finally, if two prime ideals agree in their elementary-divisor form $P^{(i)}$, then, as a consequence of the above decomposition, they agree in their zeroes; hence they are mutually divisible by one another and are therefore identical.

ğ 4. Arithmetical Formulation of the Concept of Dimension.

A first formulation of the concept of dimension that is independent of the introduction of transformed ideals is given by

Theorem V. *The dimension of a prime ideal is given by the algebraic rank of its residue-class field. The*

[14] This remark shows that Theorem III with its corollary could have been stated and proved directly for the field of zeroes $\bar{R}$ of $\bar{\mathfrak{p}}$. Only by passing to the transformed ideal is it achieved that in the greatest primary components of equal dimension of an arbitrary ideal the same parameters occur among the zeroes; and only thereby does the connection with norm and elementary-divisor form of an arbitrary ideal result.

[15] Compare H.-N., ğ 7.

[16] For extensions of the first kind, hence in particular over perfect fields, the first power is involved; over imperfect fields the p^g-th power is involved, as will be shown in ğ 6, Theorems XIII and XIV.

highest dimension of an ideal is equal to the highest of the dimension numbers of its associated prime ideals.

The first part of Theorem V was proved in the first remark to Theorem IV, where it was shown that the algebraic rank of the residue-class field $(\bar{\mathfrak{R}})$ of $\bar{\mathfrak{p}}$ is equal to that of the residue-class field $(\mathfrak{R})$ of $\mathfrak{p}$, hence equal to the dimension of $\mathfrak{p}$, in agreement with ğ 1, 8. For the proof of the second part, let $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_a]$ be a shortest representation by greatest primary components. Then, first of all, no $\mathfrak{q}$ as a divisor of $\mathfrak{m}$ can possess higher dimension than $\mathfrak{m}$. But the product of all $\mathfrak{q}$ is divisible by $\mathfrak{m}$, and therefore so is the product of all elementary-divisor forms of the individual $\mathfrak{q}$'s. If, then, $n-i$ is the highest of the dimension numbers of the $\mathfrak{q}$, then $\mathfrak{m}$ contains a polynomial $G^{(i)} \neq 0$ and can therefore not have dimension higher than $n-i$. The dimension numbers of the $\mathfrak{q}$ agree, by Theorem I, with those of their associated prime ideals. Thus if, without introducing transformed ideals, one defines the dimension of a prime ideal by the algebraic rank of its residue-class field, then the second part of Theorem V gives the definition of the highest dimension of an arbitrary ideal.

In order, on the other hand, to grasp the concept of dimension by chains of prime ideals – again independently of the introduction of transformed ideals – one has, supplementing Theorem II, to show:

Theorem VI. *Every prime ideal different from the unit ideal possesses – after possible adjunction of indeterminates – at least one prime ideal as divisor whose dimension has decreased by exactly one unit.*

Indeed, if $\mathfrak{p}$ has dimension $(n-i) > 0$ and v denotes a new indeterminate, then

$$\mathfrak{c} = (\mathfrak{p}, x_i - v)$$

is an ideal with the required property. This follows from an isomorphic correspondence. One has $\mathfrak{c} = (\mathfrak{p}^*, x_i - v)$, where $\mathfrak{p}^*$ arises from $\mathfrak{p}$ by replacing x_i by the indeterminate v and adjoining v to the coefficient domain; the residue classes are likewise obtained by replacing the class (x_i) by (v). But $\mathfrak{p}$ passes into itself when x_i is adjoined to $P(u)$; for from

$$h(x_i) f(x) \equiv 0(\mathfrak{p}), \qquad h(x_i) \neq 0$$

one necessarily obtains $f(x) \equiv 0(\mathfrak{p})$. Otherwise $\mathfrak{p}$ would contain a polynomial depending only on x_i, and therefore also one depending only on x_n, contrary to the supposition it would have dimension at most zero. Under the assignment $v \sim x_i$, therefore, the zero class modulo $\mathfrak{c}$ necessarily corresponds to the zero class modulo $\mathfrak{p}$, and of course conversely as well. Hence there is an isomorphism between the residue-class system modulo $\mathfrak{p}$ and that modulo $\mathfrak{c}$; the latter has no zero divisors, so $\mathfrak{c}$ is a prime ideal. Under this isomorphism the algebraic dependence between (x_i) and $(P(u, x_{i+1}, \ldots, x_n))$ corresponds to a relation between $(x_{i+1}), \ldots, (x_n)$ with respect to $(P(u, v))$, whereas for $\lambda = 1, \ldots, i-1$ the dependences between (x_λ) and $(P(u, x_{i+1}, \ldots, x_n))$ remain as such, and hence do not further lower the algebraic rank. The algebraic rank has decreased by exactly one unit. If $\mathfrak{p}$ was of dimension zero, $\mathfrak{c}$ becomes the unit ideal; the above result therefore remains valid. In the original domain $\bar{\mathfrak{S}}$, consequently,

$$\bar{\mathfrak{a}} = (\bar{\mathfrak{p}}, v + v_1 y_1 + \cdots + v_n y_n),$$

where v_λ is put for $-t_{\lambda i}$, is an ideal of the required kind. If, in particular, P contains infinitely many elements, then $v, v_1, \ldots, v_n$ can always be specialized to elements of P in such a way that norm and elementary-divisor form, and hence the dimension of $\bar{\mathfrak{a}}$, become equal to those of the specialized ideal $\mathfrak{b}$;[17] the elementary-divisor form need not, however, remain a prime function. By Theorem V, $\mathfrak{b}$ nevertheless possesses at least one associated prime ideal of the desired dimension; passing back again to $\bar{\mathfrak{S}}$, Theorem VI therefore holds there without adjoining any indeterminates.

Theorem II and Theorem VI immediately give the desired formulation according to

Theorem VII. *A prime ideal $\mathfrak{p}$ has dimension $n-i$ if – after possible adjunction of indeterminates – there exists at least one chain of $1 + (n-i) + 1$ prime ideals*

$$\mathfrak{p}_0 = \mathfrak{p}; \quad \mathfrak{p}_1, \ldots, \mathfrak{p}_{n-i}; \quad \mathfrak{p}_{n-i+1},$$

each of which is a proper divisor of the immediately preceding one, whereas no such chain with a larger number of members exists. This definition also holds in the original domain, and without introducing any indeterminates, when P contains infinitely many elements.[18]

[17] Compare H.-N., the last paragraph of ğ 7.

[18] This chain definition of dimension gives, in the case of an algebraic number field, dimension zero for the ordinary prime ideals, dimension -1 for the unit ideal, and dimension 1 for the zero ideal. Indeed the latter also satisfies the definition of prime ideals: in a field a product of non-vanishing quantities is always different from zero. Theorem II remains valid, with this definition of dimension, in algebraic number fields.

First it is clear that the last member of the chain must be equal to the unit ideal – which satisfies the definition of a prime ideal – since otherwise the chain could be lengthened by adjoining $\mathfrak{o}$; for $\mathfrak{o}$ itself Theorem VII gives dimension -1, in agreement with ğ 1, 8. Now let $\mathfrak{p}$ be different from $\mathfrak{o}$ and of dimension $n-i$. Then the number of members of the chain can be at most $1+(n-i)+1$, since by Theorem II two prime ideals of the same dimension cannot occur. Conversely, by Theorem VI, after possible adjunction of new indeterminates, there exists at least one chain of this length, since the dimension has decreased by exactly one unit at every member of the chain. If one takes Theorem VII as the definition of dimension – a definition which plainly can be stated in exactly the same way in the original domain, and for which, by Theorem VI, the introduction of indeterminates becomes unnecessary when P contains infinitely many elements – then the definition of the highest dimension of an arbitrary ideal is again given by the second part of Theorem V.

ğ 5. Classification of the Fundamental Ideals and of Their Components in General Ideal Theory. Zeroes of Ideals.

The question is the characterization of the fundamental ideals and their components (ğ 1, 7.) by isolated components of the decomposition (ğ 1, 13.) in the sense of general ideal theory. This characterization will show the parallelism between the decomposition theorems for norms and those of general ideal theory, and will make it possible to state, for arbitrary ideals, the theory of zeroes given in ğ 3 for prime ideals and primary ideals. For the fundamental ideals one has

Theorem VIII. *The fundamental ideals $\mathfrak{g}_i$ of i-th stage are the isolated components of the decomposition that are uniquely determined by the totality of the associated prime ideals of dimensions $n-1, n-2, \ldots, n-i$. If all associated prime ideals have the same dimension, then the ideal also has this dimension; that is, only one factor $R^{(i)}$ of the norm occurs. In general the norm has as many factors $R^{(i)}, R^{(i+\sigma)}, R^{(i+\tau)}, \ldots$ different from unity as different dimension numbers occur among the associated prime ideals.*

Precede the proof by

Lemma VI. *If an ideal is represented as a least common multiple, $\mathfrak{m} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_\alpha]$, then its fundamental ideal $\mathfrak{g}_i$ is the least common multiple of the fundamental ideals $\mathfrak{h}_i$ of i-th stage of the $\mathfrak{a}$.*

For from

$$b^{(i+1)} f \equiv 0(\mathfrak{m}), \qquad b^{(i+1)} \neq 0$$

one obtains

$$b^{(i+1)} f \equiv 0(\mathfrak{a}_\lambda), \qquad b^{(i+1)} \neq 0;$$

therefore $\mathfrak{g}_i$ is divisible by $[\mathfrak{h}_{i1}, \ldots, \mathfrak{h}_{i\alpha}]$. Conversely, from

$$c_\lambda^{(i+1)} f \equiv 0(\mathfrak{a}_\lambda), \qquad c_\lambda^{(i+1)} \neq 0$$

one obtains

$$c_1^{(i+1)} \cdots c_\alpha^{(i+1)} f \equiv 0(\mathfrak{m}), \qquad c_1^{(i+1)} \cdots c_\alpha^{(i+1)} \neq 0,$$

and hence the converse divisibility, proving the lemma.

Now let the associated prime ideals of $\mathfrak{m}$ be ordered by dimension (some dimensions may of course be absent, $j_\lambda = 0$):

$$\mathfrak{p}_{1,1}, \ldots, \mathfrak{p}_{1,j_1}; \quad \mathfrak{p}_{2,1}, \ldots, \mathfrak{p}_{2,j_2}; \quad \ldots; \quad \mathfrak{p}_{n,1}, \ldots, \mathfrak{p}_{n,j_n},$$

where in general $\mathfrak{p}_{\lambda,\kappa}$ denotes a prime ideal of dimension $n-\lambda$; let $\mathfrak{q}_{\lambda,\kappa}$ be the corresponding primary ideal occurring in a fixed given decomposition of $\mathfrak{m}$. Then by definition the fundamental ideal of i-th stage is equal to the unit ideal for all $\mathfrak{q}_{\lambda,\kappa}$ for which $\lambda > i$, whereas for $\lambda \leq i$ it is, by Theorem I, equal to $\mathfrak{q}_{\lambda,\kappa}$. Therefore, by Lemma VI:

$$\mathfrak{g}_i = [\mathfrak{q}_{1,1}, \ldots, \mathfrak{q}_{1,j_1}; \ldots; \mathfrak{q}_{i,1}, \ldots, \mathfrak{q}_{i,j_i}], \tag{5}$$

and this representation recognizes $\mathfrak{g}_i$ as an isolated component of the decomposition, since none of the prime ideals belonging to $\mathfrak{g}_i$ can be contained in one of the remaining prime ideals, all of which have lower dimension.

If, in particular, only associated prime ideals of dimension $n-i$ occur, then by (5) one has $\mathfrak{g}_0, \ldots, \mathfrak{g}_{i-1}$ equal to the unit ideal, while $\mathfrak{g}_i = \mathfrak{g}_{i+1} = \cdots = \mathfrak{m}$; hence $R_\mathfrak{m} = R^{(i)}$. If, however, prime ideals of different dimensions occur, say $j_i, j_{i+\sigma}, j_{i+\tau}, \ldots$ are non-zero, then by (5):

$$\mathfrak{g}_0 \neq \mathfrak{g}_i \neq \mathfrak{g}_{i+\sigma} \neq \mathfrak{g}_{i+\tau} \neq \cdots,$$

whereas

$$\mathfrak{g}_0 = \mathfrak{g}_1 = \cdots = \mathfrak{g}_{i-1} = \mathfrak{o}, \qquad \mathfrak{g}_i = \mathfrak{g}_{i+1} = \cdots = \mathfrak{g}_{i+\sigma-1}, \ldots,$$

therefore the factors $R^{(i)}, R^{(i+\sigma)}, R^{(i+\tau)}$, and only these, are different from unity.[19]

By means of Theorem VIII, Theorem I sharpens to

Theorem IX. *An ideal is primary if and only if its elementary-divisor form – and therefore its norm – is a primary function.*

That the condition is fulfilled for primary ideals was shown in Theorem I. Conversely, let the elementary-divisor form of $\mathfrak{m}$ be given by $Q^{(i)} = (P^{(i)})^\rho$, where $P^{(i)}$ denotes a prime function. By Theorem VIII all prime ideals of $\mathfrak{m}$ then have the same dimension $n-i$. From $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_a]$ one obtains:

$$Q^{(i)} \equiv 0(\mathfrak{q}_\lambda); \quad \text{hence} \quad (P^{(i)})^\rho \equiv 0(\mathfrak{p}_\lambda) \quad \text{and therefore} \quad P^{(i)} \equiv 0(\mathfrak{p}_\lambda).$$

Since all $\mathfrak{p}_\lambda$ have dimension $n-i$ and $P^{(i)}$ is a prime function, $P^{(i)}$ becomes the elementary-divisor form of each $\mathfrak{p}_\lambda$. Thus, by the corollary to Theorem IV, all $\mathfrak{p}_\lambda$ coincide. Hence, since greatest primary components are involved, only one $\mathfrak{p}$ can occur; $\mathfrak{m}$ is primary, the special prime case for $\rho = 1$ not being excluded. Theorems VIII and IX lead to the classification of the components of the fundamental ideals as follows:

Theorem X. *The component $\mathfrak{r}_\lambda$ of the fundamental ideal $\mathfrak{g}_i$ corresponding to the greatest primary factor $Q_\lambda^{(i)} = (P_\lambda^{(i)})^{\rho_\lambda}$ of $R^{(i)}$ is given by the isolated component of the decomposition which is uniquely determined by the associated prime ideals of dimensions $n-1, \ldots, n-i+1$ and by that prime ideal of dimension $n-i$ whose elementary-divisor form becomes equal to $P_\lambda^{(i)}$. Associated prime ideals and greatest primary factors of the norm correspond one-to-one.*

By ğ 1, 7. the $\mathfrak{r}_\lambda$ agree with their fundamental ideal of i-th stage and possess $\mathfrak{g}_{i-1}$ as fundamental ideal of $(i-1)$-st stage. Hence, by Theorem VIII respectively (5), they admit a shortest representation:

$$\mathfrak{r}_\lambda = [\mathfrak{g}_{i-1}, \mathfrak{q}_{\lambda,1}, \ldots, \mathfrak{q}_{\lambda,t_\lambda}],$$

where all $\mathfrak{q}$ have dimension $n-i$ and belong to distinct prime ideals. By the definition of $Q_\lambda^{(i)}$ – taking into account that $\mathfrak{r}_\lambda$ agrees with its fundamental ideal of i-th stage – one has:

$$Q_\lambda^{(i)} \mathfrak{g}_{i-1} \equiv 0(\mathfrak{q}_{\lambda,\kappa}), \quad (\kappa = 1, \ldots, t_\lambda)$$

and consequently

$$(Q_\lambda^{(i)})^{\sigma_\lambda} \equiv 0(\mathfrak{q}_{\lambda,\kappa}); \quad \text{hence} \quad (P_\lambda^{(i)})^{\rho_\lambda \sigma_\lambda} \equiv 0(\mathfrak{p}_{\lambda,\kappa}),$$
$$\text{and therefore} \quad P_\lambda^{(i)} \equiv 0(\mathfrak{p}_{\lambda,\kappa}),$$

from which, as in the proof of Theorem IX, it follows that in the representation of $\mathfrak{r}_\lambda$ only one $\mathfrak{q}_\lambda$ and associated $\mathfrak{p}_\lambda$ of dimension $n-i$ can occur, and that the elementary-divisor form of $\mathfrak{p}_\lambda$ is given by $P_\lambda^{(i)}$. It remains to prove that $\mathfrak{p}_\lambda$ is an associated prime ideal of $\mathfrak{m}$ and that $\mathfrak{q}_\lambda$ actually occurs in at least one representation of $\mathfrak{m}$ by greatest primary components. Then $\mathfrak{r}_\lambda$ is also recognized as the isolated component of the decomposition, since no prime ideal can be absorbed in one of equal or lower dimension, namely as the component determined by $\mathfrak{p}_\lambda$ and by all associated prime ideals of higher dimension. For this proof it suffices to show that $\mathfrak{q}_\lambda$ occurs in a shortest representation of $\mathfrak{g}_i$, since such a representation can always, by Theorem VIII, be completed to a shortest representation of $\mathfrak{m}$. Thus it is enough to show that the representation

$$\mathfrak{g}_i = [\mathfrak{r}_1, \ldots, \mathfrak{r}_\alpha] = [\mathfrak{g}_{i-1}, \mathfrak{q}_1, \ldots, \mathfrak{q}_\alpha]$$

becomes a shortest one. If, for instance, $\mathfrak{q}_\lambda$ were absorbed by its complement, so that $\mathfrak{g}_{i-1}\mathfrak{q}_1 \cdots \mathfrak{q}_{\lambda-1}\mathfrak{q}_{\lambda+1} \cdots \mathfrak{q}_\alpha$ were divisible by $\mathfrak{q}_\lambda$, then, because $\mathfrak{g}_{i-1} \not\equiv 0(\mathfrak{q}_\lambda)$, it would follow that a power of some $\mathfrak{q}_\mu$ is divisible by $\mathfrak{q}_\lambda$ for $\mu \neq \lambda$. Thus the associated prime ideals $\mathfrak{p}_\mu$ and $\mathfrak{p}_\lambda$, both of the same dimension, would have to coincide by Theorem II; but this is impossible, since their elementary-divisor forms $P_\mu^{(i)}$ and $P_\lambda^{(i)}$ are distinct by definition. The representation of $\mathfrak{g}_i$, to which by Theorem VIII all associated prime ideals of dimension $n-i$ correspond, further shows that to every such prime ideal there really corresponds a greatest primary factor of the norm. The one-to-one correspondence is therefore proved.

Theorem X immediately gives the transfer of Theorem IV according to

[19] Taking Lemma II into account, Theorem VIII again implies that the fundamental ideals – as least common multiples of transformed ideals – become transformed ideals. Since Theorem VIII rests only on theorems from H.-N. where this fact is not used, this gives at the same time a new proof which reveals the internal reason. In H.-N. the theorem is used only in the theory of zeroes, which is newly developed here.

Theorem XI. *The individual greatest primary factors* $Q_\lambda^{(i)} = (P_\lambda^{(i)})^{\rho_\lambda}$ *of the norm admit a product representation:*

$$Q_\lambda^{(i)} = \prod(x_i - t_{1i}\bar{y}_{1\nu} - \cdots - t_{ni}\bar{y}_{n\nu})^{\delta_\lambda\rho_\lambda} = \prod(t_{1i}(y_1 - \bar{y}_{1\nu}) + \cdots + t_{ni}(y_n - \bar{y}_{n\nu}))^{\delta_\lambda\rho_\lambda},$$

where $\bar{y}_{1\nu}, \ldots, \bar{y}_{n\nu}$ *represents in each case an associated system of zeroes of the associated prime ideal* $\mathfrak{p}_\lambda$*, in the original indeterminates* y*, independent of* $t_{1i}, \ldots, t_{ni}$*, and* δ_λ *has the value one or* p^{f_λ}*. Thus the decomposition of the norm into linear factors is completely given. The degree of* $Q_\lambda^{(i)}$ *gives the degree, over the residue-class subfield* $(P(u, x_{i+1}, \ldots, x_n))$ *obtained by quotient formation, of the subring of residue classes, represented by residue classes from* $\mathfrak{g}_{i-1}$*, modulo the isolated component* $\mathfrak{r}_\lambda$*; for primary ideals this is therefore the ring of all residue classes. When new indeterminates* v *are adjoined, one further obtains the decomposition:*

$$Q_\lambda^{(i)}(u, v) = \prod(z - v_1\bar{x}_{1\nu} - \cdots - v_i\bar{x}_{i\nu})^{\delta_\lambda\rho_\lambda}.$$

Since $P_\lambda^{(i)}$ has been recognized by Theorem X as the elementary-divisor form of $\mathfrak{p}_\lambda$, this is in fact only the substitution of the decomposition of Theorem IV. The remark on the degree is only another formulation of what was said in ğ 1, 5. and 7.[20]

ğ 6. Characterization of Prime Ideals and Proper Primary Ideals by Elementary-Divisor Form and Norm.

In Theorem IX primary ideals were characterized by elementary-divisor form and norm, but only in such a way that the prime case was to be regarded as a special case of primary. We now need to separate prime ideals from proper primary ideals; the considerations will run parallel to those of ğ 3. Conditions that are either necessary or sufficient are easily stated according to

Theorem XII. *A necessary condition for a prime ideal is that its elementary-divisor form be a prime function; a sufficient condition is that its norm be a prime function. In other words, the elementary-divisor form of a prime ideal is always a prime function, and the norm of a proper primary ideal is always a proper primary function.*

That the elementary-divisor form of a prime ideal is a prime function was already shown in Theorem I. Suppose now that the norm $R_\mathfrak{q}$ is equal to a prime function. It is to be shown that, under this hypothesis, every proper divisor $\mathfrak{a}$ of $\mathfrak{q}$ has lower highest dimension; then $\mathfrak{q}$ is recognized as a prime ideal by Theorem II. Indeed, by ğ 1, 6. the first factor of the norm $R_\mathfrak{a}$ that differs from the corresponding one of $R_\mathfrak{q}$ is a proper divisor. Since $R_\mathfrak{q} = P^{(i)}$, the factor $R^{(i)}$ of $R_\mathfrak{a}$ must therefore be equal to a proper divisor of $P^{(i)}$, hence to unity; $\mathfrak{a}$ has lower highest dimension.

A second simple proof rests on the following lemma, on which the next theorem also rests:

Lemma VII. *The system of residue classes represented by polynomials* $H^{(i)}$ *modulo the elementary-divisor form* $E^{(i)}$ *of a primary ideal – more generally, of an ideal that has only associated prime ideals of dimension* $n - i$ *– is isomorphic to a subsystem of the residue classes modulo this ideal. The degree of the elementary-divisor form gives the degree of this residue-class system with respect to the quotient field* $(P(u, x_{i+1}, \ldots, x_n))$*.*

Indeed, one defines a correspondence by assigning to one another the classes represented by the same polynomials $H^{(i)}$; sums and products correspond to sums and products. The assignment is also one-to-one. For all polynomials $H^{(i)}$ belonging to the zero class modulo the ideal are, by definition, divisible by $E^{(i)}$; hence the zero class corresponds to the zero class modulo $E^{(i)}$, and conversely as well.

Now let the norm of an ideal be a prime function $P^{(i)}$, hence identical with the elementary-divisor form. The degrees of the residue-class systems modulo the elementary-divisor form $P^{(i)}$ and modulo $\mathfrak{q}$ therefore agree with respect to $(P(u, x_{i+1}, \ldots, x_n))$; the subsystem isomorphic to the residue-class system modulo $P^{(i)}$ therefore exhausts the residue classes modulo $\mathfrak{q}$, and since this system can have no zero divisors, $\mathfrak{q}$ is a prime ideal.

In general Theorem XII cannot be sharpened to necessary and sufficient conditions, as will be shown below by examples. This is possible, however, when the coefficient domain P is a perfect field (ğ 1, 14.), according to

[20] Likewise the formulation of multiplicity mentioned in note 2) of H.-N. is an immediate consequence of Theorem X. For, after adjoining $x_{i+1}, \ldots, x_n$, the residue-class system $\mathfrak{g}_{i-1} \mid \mathfrak{r}_\lambda$ is isomorphic to $\mathfrak{t}_\lambda \mid \mathfrak{r}_\lambda$, where $\mathfrak{t}_\lambda = [\mathfrak{g}_{i-1}, \mathfrak{r}_1, \ldots, \mathfrak{r}_{\lambda-1}, \mathfrak{r}_{\lambda+1}, \ldots, \mathfrak{r}_a]$ is put, as follows from passing back to modules of linear forms (H.-N., Theorem V) in view of the relative primality of the factors $Q_\mu^{(i)}$. Directly it is shown that $\mathfrak{t}_\lambda \mid \mathfrak{r}_\lambda$ is isomorphic to $\mathfrak{t}_\lambda \mid \mathfrak{q}_\lambda$; here $\mathfrak{t}_\lambda$ arises from the complement of $\mathfrak{q}_\lambda$ after adjoining $x_{i+1}, \ldots, x_n$.

Theorem XIII. *If the coefficient domain P is a perfect field, then norm and elementary-divisor form of a prime ideal become prime functions and consequently identical; norm and elementary-divisor form of a proper primary ideal become proper primary functions. Thus, over a perfect field, the condition that the elementary-divisor form be a prime function is necessary and sufficient for a prime ideal; in the condition the norm may also stand in place of the elementary-divisor form.*

Taking Theorem XII into account, Theorem XIII will be proved once it is shown that over a perfect field the ideal becomes prime as soon as its elementary-divisor form is a prime function, and that then the norm is equal to this prime function. In Lemma V, ğ 3, it was shown that, over a perfect field, the elementary-divisor form becomes a prime function of the first kind as soon as it is a prime function at all. Therefore let $(\mathfrak{R})$ denote the residue-class field obtained by adjoining (x_i) to $(P(u, x_{i+1}, \ldots, x_n))$, that is, $(P(u, x_i, x_{i+1}, \ldots, x_n))$ modulo $P^{(i)}$. Then (x_i) is a zero of the prime function of the first kind $(P^{(i)})$, and hence, as for example Lagrange's formula shows, $(y_1), \ldots, (y_n)$ are contained in $(\mathfrak{R})$. The subsystem of the residue classes modulo the ideal $\mathfrak{q}$ under consideration that is isomorphic, by Lemma VII, to $(\mathfrak{R})$ – where only denominators from $(P(u, x_{i+1}, \ldots, x_n))$ occur – therefore contains the residue classes $(y_1), \ldots, (y_n)$ and hence exhausts the residue-class system modulo $\mathfrak{q}$. Since, being isomorphic to $(\mathfrak{R})$, it can have no zero divisors, $\mathfrak{q}$ is a prime ideal. The degree of this residue-class field $(\mathfrak{R})$ of $\mathfrak{q}$ with respect to $(P(u, x_{i+1}, \ldots, x_n))$ is equal to the degree of the norm of $\mathfrak{q}$; on the other hand, by the isomorphism with $(\mathfrak{R})$, it is equal to the degree of the elementary-divisor form $P^{(i)}$. Thus norm and elementary-divisor form must agree.

For imperfect coefficient domains Theorem XII still allows the following sharpening:

Theorem XIV. *If the coefficient domain P is an imperfect field of characteristic p, then the norm of a prime ideal is the p^g-th power of the elementary-divisor form; one has $0 \leq g \leq (i-1)f$, where f denotes the exponent of the elementary-divisor form and $n-i$ the dimension of the prime ideal.*

Theorem XIV amounts to the assertion that the residue-class field $(\mathfrak{R})$ of $\mathfrak{p}$ has degree p^g $(g \geq 0)$ with respect to the subfield $(\mathfrak{R}') = (P(u, x_i, x_{i+1}, \ldots, x_n))$ isomorphic to $(\mathfrak{R})$. This follows directly from the Steinitz theorems stated in ğ 1, 15., more precisely from

Lemma VIII. *Let Λ be a finite extension of the imperfect field Ω of reduced degree r and exponent f; let Λ_0 be the field of the first kind contained in Λ, and let M be an intermediate field between Λ_0 and Λ. Then the degree of every element of Λ with respect to M is a power of p, where p denotes the characteristic of Ω.*

For the $p^{f'}$-th power $(f' \leq f)$ of every element z of Λ belongs to Λ_0; hence z is a zero of a prime function $G(t) = (t-z)^{p^{f'}}$ with coefficients in Λ_0. Let $H(t) = (t-z)^{\delta}$ be the prime function in M with zero z. Then $H(t)$ also has coefficients in $\Lambda_0(z)$, and therefore the coefficients of $H(t)$ belong to the intersection field of M and $\Lambda_0(z)$, hence to an intermediate field between Λ_0 and $\Lambda_0(z)$. The degree of z with respect to M is therefore equal to the degree with respect to this intermediate field, and hence, as a divisor of $p^{f'}$, is a power of p.

For the proof of Theorem XIV it remains only to observe that the field $(\mathfrak{R}') = (P(u, x_i, x_{i+1}, \ldots, x_n))$ must have degree $r \cdot p^f$ with respect to $(P(u, x_{i+1}, \ldots, x_n))$, if r denotes the reduced degree and f the exponent of $(\mathfrak{R})$; and consequently the field of the first kind $(\mathfrak{R}_0)$ contained in $(\mathfrak{R})$ must be a subfield of $(\mathfrak{R}')$. Since there are elements of degree $r \cdot p^f$ in $(\mathfrak{R})$ (ğ 1, 15.), (x_i) must necessarily be of this degree, since all elements of $(\mathfrak{R})$ arise by specializing the $t_{\mu\nu}$ in (x_i). The exponent of $(\mathfrak{R})$ agrees with the exponent of the elementary-divisor form, and $(x_i)^{p^f}$ has degree r and is an element of $(\mathfrak{R}_0)$, hence a primitive element of $(\mathfrak{R}_0)$. Since $(\mathfrak{R})$ arises by adjoining finitely many elements – say $(x_1), \ldots, (x_{i-1})$ – to $(\mathfrak{R}')$, repeated finite application of Lemma VIII gives the desired proof and at the same time the estimate for g.[21]

We now add the examples which show that Theorem XII cannot in general be sharpened beyond Theorem XIV. They concern a prime ideal whose norm is equal to the square of the elementary-divisor form $(g > 0)$, and proper primary ideals whose elementary-divisor forms are prime functions. The latter example also shows that no analogue of Theorem XIV exists here, but that the norm can become an arbitrary power of the elementary-divisor form.

Let the coefficient domain P arise by adjoining two indeterminates λ, μ to the field of residue classes modulo 2, and therefore let P be an imperfect field of characteristic two. Consider the ideal

$$\bar{\mathfrak{p}} = (y_1^2 + \lambda,\ y_2^2 + \mu),$$

which must be a prime ideal, since the residue-class system $(\overline{\mathfrak{R}})$ is isomorphic to the field $P(\sqrt{\lambda}, \sqrt{\mu})$. The field $(\overline{\mathfrak{R}})$ has degree four with respect to (P), reduced degree $r = 1$, and exponent $f = 2$. Therefore the

[21] Compare the parallel considerations in A. Ostrowski, Zur arithmetischen Theorie der algebraischen GröSSen, Gött. Nachr. 1919, pp. 279–298, especially p. 288, where the corresponding theorem is stated without proof.

elementary-divisor form $P^{(2)}$ is of the second degree, and the norm is of the fourth degree and consequently the square of $P^{(2)}$, as can also be checked directly from the module representation (3), ğ 1, 5. One obtains

$$P^{(2)} = (u_{11}u_{22} + u_{12}u_{21})^2 x_2^2 + (u_{11}^2\mu + u_{21}^2\lambda)$$

or, after a suitable multiplication:

$$x_2^2 + (t_{12}^2\lambda + t_{22}^2\mu).$$

Let P now arise by adjoining the one indeterminate λ to the field of residue classes modulo 2, and take as basis the ideal

$$\bar{\mathfrak{q}} = (y_1^2 + \lambda,\, y_2^2 + \lambda) = (y_1^2 + \lambda, (y_1 + y_2)^2)$$

As elementary-divisor form, by specializing $\mu = \lambda$ in the one just given, one obtains:

$$P^{(2)} = x_2^2 + \lambda(t_{12}^2 + t_{22}^2),$$

hence a prime function, since $t_{12} = (0)$, $t_{22} = (1)$ leads to the prime function $x_2^2 + \lambda$. But $\bar{\mathfrak{q}}$ is proper primary, since it contains $(y_1 + y_2)^2$ but not $(y_1 + y_2)$. The norm must be equal to the square, hence to the p-th power, of $P^{(2)}$, since the number of residue classes of $\bar{\mathfrak{q}}$ linearly independent over P is four.

That this last analogue of Theorem XIV is not always fulfilled is shown by the following example. Let P arise by adjoining the indeterminate λ to the residue-class field modulo 3, and take as basis

$$\bar{\mathfrak{q}} = (y_1^3 + \lambda, (y_1 - y_2)^2)$$

so that, as above, $\bar{\mathfrak{q}}$ is a proper primary ideal. The elementary-divisor form becomes – taking into account that $y_2^3 + \lambda$ is also divisible by $\bar{\mathfrak{q}}$ –

$$P^{(2)} = x_2^3 + \lambda(t_{12} + t_{22})^3,$$

a prime function; but the norm is equal to the square of $P^{(2)}$, since there are six linearly independent residue classes modulo $\bar{\mathfrak{q}}$. Thus the p^g-th power of the elementary-divisor form does not occur here.

The first example shows that, over an imperfect field as coefficient domain, just as in algebraic number fields, prime ideals of degree higher than the first may occur, where p^g is to be called the degree of the prime ideal. The further examples are to be understood as analogues of ramification ideals: a prime number may be divisible by a higher power of a prime ideal, by a primary ideal. For, as shown in note 10), the elementary-divisor form corresponds to the least integral rational number divisible by an ideal in an algebraic number field.

ğ 7. Absolute Prime Ideals.

A prime ideal with coefficients in P is called an *absolute prime ideal* if it remains a prime ideal in the algebraically closed field A to which P can be extended.[22] Correspondingly, a prime function P with coefficients in P is called an *absolute prime function* – absolutely irreducible polynomial – if P remains a prime function in A. The characterization of absolute prime ideals is given by

Theorem XV. *A necessary and sufficient condition for an absolute prime ideal is that its elementary-divisor form – which may be assumed integral and primitive in the u – become an absolute prime function as a polynomial in the x and u. The elementary-divisor form becomes identical with the norm, so that the condition may also be stated for the norm.*

For the proof, observe first that in general norm and elementary-divisor form are preserved under algebraic extension of the coefficient domain. Indeed the individual factors $R^{(i)}$ respectively $E^{(i)}$ are defined as greatest common divisors in the polynomial sense, a property preserved by algebraic extension of the coefficient domain. Thus $P^{(i)}$ remains the elementary-divisor form of $\mathfrak{p}$ when passing from P to A, hence when passing to a perfect field as coefficient domain, since every algebraically closed field is perfect, as the definition immediately shows. By Theorem XIII, a necessary and sufficient condition for $\mathfrak{p}$ to be an absolute prime ideal is that $P^{(i)}$ become a prime function with respect to $A(u)$; that is, an absolute prime function as a polynomial in the x and u, if $P^{(i)}$ is assumed integral and primitive in the u. At the same time, by Theorem XIII, $P^{(i)}$ becomes identical with the norm of $\mathfrak{p}$ as soon as A is taken as coefficient domain. Hence, by what was just noted, the same holds over P. This proves Theorem XV.

[22] An algebraically closed field is, as is well known, a field in which every polynomial in one indeterminate decomposes into linear factors. For the existence and essential uniqueness of the algebraically closed field belonging to an arbitrary field, see Steinitz.

For absolute prime functions P with coefficients in a (finite) algebraic number field $\mathfrak{K}$, one now has the theorem[23] that P remains a prime function, more precisely an absolute prime function, modulo every prime ideal of $\mathfrak{K}$, with at most finitely many prime ideals of $\mathfrak{K}$ excepted. The transfer of this theorem to absolute prime ideals rests on

Theorem XVI. *If, as coefficient domain, one takes, in place of a field, the ring $\mathfrak{o}^*$ of all algebraic integers of a (finite) algebraic number field $\mathfrak{K}$, then norm and elementary-divisor form of a polynomial ideal are preserved as norm and elementary-divisor form modulo every prime ideal of $\mathfrak{K}$, with at most finitely many prime ideals of $\mathfrak{K}$ excepted.*

For the proof the polynomial domain on which everything is based is to be modified relative to ğ 1, 1. Let $\bar{\mathfrak{S}}$ consist of all polynomials in $y_1, \ldots, y_n$ with coefficients in $\mathfrak{o}^*$, hence algebraic integers of $\mathfrak{K}$; let the coefficient domain of $\mathfrak{S}$ be $\mathfrak{o}^*[u]$, that is, all polynomials in u with coefficients in $\mathfrak{o}^*$. If $\bar{\mathfrak{m}}$ is an ideal in $\bar{\mathfrak{S}}$, it passes by (1) into a transformed ideal $\mathfrak{m}$ in $\mathfrak{S}$. It is to be shown that only finitely many polynomials from $\mathfrak{o}^*[u]$ occur in the denominators in forming the norm; then Theorem XVI follows directly.

First note that the module representation (3) in ğ 1, 5. for the formation of the individual norm amounts to reducing powers of x_{i-1} modulo a polynomial regular in x_{i-1}, $C^{(i-1)} = U_{i-1}(u)x_{i-1}^k + \text{lower terms}$[24]; here all coefficients of $C^{(i-1)}$, in particular U_{i-1}, may be assumed to be elements of $\mathfrak{o}^*[u]$. Since this is a matter of successive reduction of $x_1, \ldots, x_{i-1}$, the module representation integral in the x is also integral in $\mathfrak{o}^*[u]$ except for power products $U_1^{\lambda_1} \cdots U_{i-1}^{\lambda_{i-1}}$ in the denominator. The product $U_1 U_2 \cdots U_n$, considered as a polynomial in the u, defines by its coefficients an ideal $\mathfrak{r}^*$ of $\mathfrak{K}$, which is therefore divisible by only finitely many prime ideals of $\mathfrak{K}$. If $\mathfrak{p}^*$ is chosen different from these finitely many, and if the residue-class field modulo $\mathfrak{p}^*$ is used as coefficient domain, the original module representation is preserved by replacing each number of $\mathfrak{o}^*$ by its residue class modulo $\mathfrak{p}^*$.

Furthermore, since norm and elementary-divisor form are determined only up to factors from $\mathfrak{o}^*[u]$, they may also be assumed divisible by $\mathfrak{m}$ with respect to $\mathfrak{o}^*[u]$. Suppose, under this convention, that for instance $R^{(i)} = V_i(u)x_i^l + \text{lower terms}$, so that, in the divisibility of all ρ-rowed determinants of the module $\mathfrak{M}_{i-1}^*$ of rank ρ determined by $C^{(i-1)}$, only powers of V_i occur in the denominator besides the $U_1^{\lambda_1} \cdots U_{i-1}^{\lambda_{i-1}}$. Choose $\mathfrak{p}^*$ further distinct from the finitely many prime ideals of $\mathfrak{K}$ that occur in the ideal determined by $V_1 V_2 \cdots V_n$. Then $R^{(i)}$ remains a common divisor of these determinants when the residue-class field modulo $\mathfrak{p}^*$ is taken as coefficient domain, and the rank of $\mathfrak{M}_{i-1}^*$ is preserved, since $C^{(i)}$ was a ρ-rowed determinant from $\mathfrak{M}_{i-1}^*$.

Finally $\mathfrak{p}^*$ is to be chosen so that $R^{(i)}$ remains the greatest common divisor in each case. Let $D^{(i)}$ run through all ρ-rowed determinants from $\mathfrak{M}_{i-1}^*$, so that by hypothesis $U_1^{\lambda_1} \cdots U_{i-1}^{\lambda_{i-1}} V_i^\sigma D^{(i)} = R^{(i)} T^{(i)}$, with the $T^{(i)}$ having no common divisor containing x in the polynomial sense. Consequently the ideal derived from all $T^{(i)}$ contains a polynomial $G^{(i+1)} = W_i(u)x_{i+1}^m + \text{lower terms}$, $W_i \neq 0$; that $G^{(i+1)}$ may be assumed regular in x_{i+1} follows from composing the transformation (1) with one of $x_{i+1}, \ldots, x_n$ having new indeterminates as coefficients. If, then, $\mathfrak{p}^*$ is also chosen distinct from the finitely many prime ideals contained in the ideal determined by $W_1 W_2 \cdots W_n$, then when the residue-class field modulo $\mathfrak{p}^*$ is used as coefficient domain, $R_\mathfrak{m}$ is in fact preserved as norm. Quite correspondingly $\mathfrak{p}^*$ can be chosen still further so that $E_\mathfrak{m}$ also remains the elementary-divisor form. This proves Theorem XVI.

From Theorems XV and XVI, as a generalization of the theorem on absolute prime functions and using that theorem, one obtains

Theorem XVII. *If $\mathfrak{p}$ is an absolute prime ideal with algebraic integers from a (finite) algebraic number field $\mathfrak{K}$ as coefficients, then $\mathfrak{p}$ remains a prime ideal, more precisely an absolute prime ideal, modulo every prime ideal of $\mathfrak{K}$, with at most finitely many prime ideals of $\mathfrak{K}$ excepted.*

For the proof, let the norm $R_\mathfrak{p}$ of $\mathfrak{p}$ be chosen, as in Theorem XVI, so that it is divisible by $\mathfrak{p}$ also with respect to $\mathfrak{o}^*[u]$. Then $R_\mathfrak{p} = T(u)P^{(i)}(x)$, where $P^{(i)}(x)$ may be assumed integral and primitive in the u. By Theorem XV, $P^{(i)}$, regarded as a polynomial in u and x with coefficients in $\mathfrak{K}$, is an absolute prime function. By the theorem on absolute prime functions it retains this property modulo every prime ideal of $\mathfrak{K}$, with at most finitely many prime ideals of $\mathfrak{K}$ excepted. Thus choose $\mathfrak{p}^*$ different from these finitely many prime ideals and, by Theorem XVI, also different from finitely many further prime ideals of $\mathfrak{K}$. Then $P^{(i)}$ – its coefficients from $\mathfrak{o}^*$ being replaced by the corresponding residue classes modulo $\mathfrak{p}^*$ – becomes the norm of $\mathfrak{p}$ when the residue-class field modulo $\mathfrak{p}^*$ is taken as coefficient domain P, and this norm is an absolute prime function. Taking P as coefficient domain, $\mathfrak{p}$ therefore remains an absolute prime ideal by Theorem XV. This

[23] A. Ostrowski, loc. cit. (note 21)); lemma p. 296. – A simpler proof is in E. Noether, Ein algebraisches Kriterium für absolute Irreduzibilität, Math. Ann. 85 (1922), pp. 26–33, no. 7.

[24] Compare H.-N. ğ 4.

proves Theorem XVII.

Göttingen, May 8, 1923.

(Received March 9, 1923.)

25. Elimination Theory and Ideal Theory.

Jahresber. d. Deutschen Mathematiker-Vereinigung 33 (1924), pp. 116–120

Lecture delivered in Marburg on September 25, 1923.[1)]

By Emmy Noether in Göttingen.

In what follows I would like to show how elimination theory can be built up in exact parallel with the theory of zeros for polynomials in one indeterminate. This construction rests on a connection between Hentzelt's elimination theory and the methods of field theory, as developed by Steinitz, and ideal theory, as I myself have developed it.

I first want to sketch the question in the case of polynomials in one indeterminate. As coefficient domain let a fixed field P be taken once for all, to which the concepts prime function, etc., refer. Here P may be assumed to be abstractly defined in the sense of Steinitz, but in the special case it may naturally coincide with the field of rational numbers or the field of all complex numbers – according to the assumption formerly usual in elimination theory. The theory of zeros for polynomials in one indeterminate now splits into four steps:

1. *The decomposition theorem*, which permits the reduction of the question to one for prime functions – polynomials irreducible in P. For from

$$a(x) = p_1(x)^{\varrho_1} \cdots p_r(x)^{\varrho_r} = q_1(x) \cdots q_r(x)$$

– where the $p(x)$ denote distinct prime functions and the $q(x)$ therefore denote "largest primary functions" – it follows that $a(x)$ vanishes at all and only the zeros of the prime functions $p(x)$.

2. *The construction of the zero field for a prime function $p(x)$.* Such a zero field $\mathfrak{R} = P(\alpha)$ – where α denotes a zero of $p(x)$ – can always, by Steinitz, be constructed as an extension field of P isomorphic to the residue-class field ($\mathfrak{R}$) of $p(x)$. Conversely, every zero field lying in an extension field of P is isomorphic to the residue-class field ($\mathfrak{R}$); zero field and residue-class field are thus abstractly identical.

3. *The decomposition of $p(x)$ into linear factors in the Galois field determined by $p(x)$.* By repeating the construction given under 2. one arrives at the essentially uniquely determined Galois field $P(\alpha_1, \ldots, \alpha_m)$, which is precisely sufficient for $p(x)$ to split into linear factors.

4. *The meaning of multiplicity for the original polynomial $a(x)$.* By 1., 2., 3., the question of the zeros, and the corresponding decomposition into linear factors, is settled for an arbitrary polynomial $a(x)$. The multiplicity may be regarded as the degree of the individual primary function $q(x)$ – that is, the number of residue classes modulo $q(x)$ linearly independent with respect to P; for in the case of the algebraically closed coefficient domain P, where the $p(x)$ become linear, this number is precisely the multiplicity of the zeros.

I now pass to general elimination theory, and therefore take as basis the domain $\mathfrak{S}$ of all polynomials in $x_1, \ldots, x_n$ with coefficients from P; elimination theory can then be defined as the *theory of the zeros of an ideal* from this polynomial domain. By an ideal $\mathfrak{a}$ I understand, as usual, a system of polynomials such that together with f and g also $f - g$, and together with f also Af, belongs to $\mathfrak{a}$, where A is understood to be an arbitrary polynomial from $\mathfrak{S}$. By a zero of $\mathfrak{a}$ I understand every value system $\alpha_1, \ldots, \alpha_n$, belonging to an extension field of P, such that $f(\alpha)$ vanishes for every polynomial f belonging to the ideal. If $f_1, \ldots, f_t$ denotes an always existing ideal basis of $\mathfrak{a}$ – so that $f = A_1 f_1 + \cdots + A_t f_t$ holds for every f from $\mathfrak{a}$ – then the zeros of $\mathfrak{a}$ are plainly identical with the zeros of $f_1, \ldots, f_t$. Since, conversely, every system of finitely many polynomials can be regarded as a basis of the ideal derived from it, the definition of zeros just given for elimination theory is identical with the customary one, but avoids the difficulty lying in the arbitrary singling out of a basis. For polynomials in one indeterminate, where only principal ideals are involved, this difficulty does not arise, since the basis polynomial is uniquely determined up to a unit – a quantity from P as factor – but even there the ideal-theoretic conception will give a more exact insight.

Elimination theory now splits, correspondingly to the case of one indeterminate, into four steps:

I. *The decomposition theorem* – the representation of an ideal by largest primary components – which permits the reduction of the question to one for prime ideals. Here an ideal is called a prime ideal if it divides a product only when it divides at least one factor; it is called a primary ideal if it divides at least one factor or a power of each factor. To every primary ideal $\mathfrak{q}$ there belongs one and only one associated prime ideal $\mathfrak{p}$, which is a divisor of $\mathfrak{q}$ and a power of which is divisible by $\mathfrak{q}$. One has the representation as least

[1)] Detailed presentation and literature references are in Math. Ann. 90 and in a forthcoming paper.

common multiple:

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]; \qquad \mathfrak{p}_1^{\sigma_1} \cdots \mathfrak{p}_r^{\sigma_r} \equiv 0\,(\mathfrak{a}).$$

Here the $\mathfrak{q}$ are largest primary components; that is, each $\mathfrak{q}$ is primary, but the least common multiple of any two $\mathfrak{q}$'s is not primary. Moreover, without loss of generality it may be assumed that no $\mathfrak{q}$ divides the least common multiple of the remaining ones, so that no $\mathfrak{q}$ can simply be omitted; the $\mathfrak{p}$ are the associated prime ideals of the $\mathfrak{q}$. Now it is not the $\mathfrak{q}$, but – and herein lies the analogue to the case of one indeterminate – their associated prime ideals $\mathfrak{p}$ that are uniquely determined by $\mathfrak{a}$; and since each $\mathfrak{p}$ is a divisor of $\mathfrak{a}$, and conversely a product of powers of the $\mathfrak{p}$ is divisible by $\mathfrak{a}$, the zeros of the ideal therefore coincide with those of its associated prime ideals.

II. *The construction of the zero field for a prime ideal* $\mathfrak{p}$. By definition the residue classes modulo a prime ideal form a ring without zero divisors, containing at least one element distinct from the zero element as soon as $\mathfrak{p}$ is different from the unit ideal; by forming quotients this ring can therefore be extended to the residue-class field $(\mathfrak{R})$ of $\mathfrak{p}$. One can always construct an extension field $\mathfrak{R}$ of P isomorphic to $(\mathfrak{R})$ which becomes the zero field of $\mathfrak{p}$; that is, $\mathfrak{R} = P(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ denotes a zero of $\mathfrak{p}$. Here $\mathfrak{R}$ has transcendence degree k $(0 \leq k < n)$ over P, hence contains k elements algebraically independent over P, whereas any $(k+1)$ elements become algebraically dependent over P. Conversely, every zero field of transcendence degree k lying in an extension field of P is isomorphic to the residue-class field $(\mathfrak{R})$; zero field of transcendence degree k and residue-class field are therefore abstractly identical.

III. *Decomposition of the norm of* $\mathfrak{p}$ *into linear factors in the Galois field determined by* $\mathfrak{p}$. If the indeterminates $x_1, \ldots, x_n$ are regarded as generated from original indeterminates $y_1, \ldots, y_n$ by a linear transformation with indeterminates as coefficients, then the zero field $\mathfrak{R}$ of transcendence degree k can be regarded as a finite algebraic extension field of $P(x_{i+1}, \ldots, x_n)$ $(k = n - i)$. One can therefore pass to the Galois field $\overline{\mathfrak{R}}$ over $P(x_{i+1}, \ldots, x_n)$, in which the prime function $P^{(i)}(x_i, x_{i+1}, \ldots, x_n)$ with the zero α_i splits into linear factors. This prime function $P^{(i)}$, when one returns to the original indeterminates y, plays the role of the fundamental equation; for α_i becomes equal to the fundamental form $u_1\beta_1 + \cdots + u_n\beta_n$, where β denotes a zero system in the y algebraically dependent on the parameters $x_{i+1}, \ldots, x_n$. The decomposition into linear factors thus gives the product over all zeros. But the prime function $P^{(i)}$, or a power of it, may also be regarded as the norm $N(\mathfrak{p})$ of $\mathfrak{p}$, by considering $\mathfrak{p}$ as a module of linear forms in the power products of $x_1, \ldots, x_{i-1}$, taking $P(x_{i+1}, \ldots, x_n)$ instead of P as coefficient domain, and defining the norm as the product over all elementary divisors – of which only finitely many are distinct from the unit. For a perfect field P as coefficient domain one always obtains $N(\mathfrak{p}) = P^{(i)}$; for an imperfect field a power of $P^{(i)}$ may occur as the norm.

IV. *The norm of the original ideal and the meaning of multiplicity.* If correspondingly one regards the ideal $\mathfrak{a}$ successively as a module of linear forms in the power products of $x_1, \ldots, x_{i-1}$ $(i = 1, 2, \ldots, n)$, then it can be shown that, on taking $P(x_{i+1}, \ldots, x_n)$ as basis, this module has in each case only finitely many elementary divisors distinct from the unit; this is a finiteness condition following from the existence of an ideal basis. The product over these finitely many elementary divisors gives the individual norms; the norm $N(\mathfrak{a})$ is defined as the product of all individual norms. The largest primary factors $Q^{(i)}(x_i, x_{i+1}, \ldots, x_n)$ of $N(\mathfrak{a})$ correspond one-to-one to the associated prime ideals $\mathfrak{p}$ of $\mathfrak{a}$, in such a way that $Q^{(i)}$ becomes a power of $P^{(i)}$, where $P^{(i)}$ (or, if necessary, a power of $P^{(i)}$) denotes the norm $N(\mathfrak{p})$ of $\mathfrak{p}$. Thus there arises a decomposition

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{\varrho_1} \cdots N(\mathfrak{p}_r)^{\varrho_r} = Q_1 \cdots Q_r,$$

– where if necessary $N(\mathfrak{p})$ is to be replaced by the highest elementary divisor $E(\mathfrak{p}) = P^{(i)}$ – and thus, by I, II, III, the decomposition of the norm into linear factors has been effected for all zeros of $\mathfrak{a}$. The multiplicity of the zeros corresponding to the individual prime ideal $\mathfrak{p}$ of $\mathfrak{a}$ can be regarded as the degree of $Q^{(i)}$, which can be interpreted as the number of residue classes linearly independent over $P(x_{i+1}, \ldots, x_n)$. More precisely, these are the residue classes of certain isolated components of the decomposition uniquely determined by $\mathfrak{p}$ and by the prime ideals of higher dimension, namely the residue classes of the ground ideal of the $(i-1)$-st stage modulo the component, determined by $\mathfrak{p}$, of the ground ideal of the i-th stage; the latter component has $\mathfrak{p}$ and all prime ideals of higher dimension as associated prime ideals, while the former has only the prime ideals of higher dimension.

A complete *insertion of the case of one indeterminate* is obtained when one passes here too to the principal ideal. The decomposition given under 1. then splits – according to whether $a(x)$ is regarded as basis polynomial or norm – into two separate decompositions: into the representation of the principal ideal as the least common multiple of largest primary components according to I, which here amounts to a representation as a product of powers of prime ideals; or into the decomposition of the norm as a product

of powers of the norms of the individual prime ideals according to IV. In the construction of the zero field according to 2., what is in question in reality is the zero field of the prime ideal defined by $p(x)$, while in 3. the norm is decomposed into linear factors. The definition of multiplicity according to 4. is subordinated to that given in IV, since the ground ideal of the zeroth stage is equal to the unit ideal, while for one indeterminate the ground ideal of the first stage already equals the ideal itself.

The *insertion into the usual elimination theory* is given by the fact that the norm of the ideal has the meaning of a resultant. In this interpretation, the old problem of elimination theory thus becomes a part of the ideal theory of the polynomial domain, namely that part which, beside the decomposition theorems for ideals, also treats the decomposition of their norms and the connection between the two decompositions.

(Received 19 October 1923.)

26. Abstract Construction of Ideal Theory in the Algebraic Number Field

J. Ber. d. DMV 33 (1924), p. 102

4. E. Noether, Göttingen: Abstract construction of ideal theory in the algebraic number field.

The abstract properties were stated that are completely equivalent to ideal theory in the algebraic number field, and that therefore characterize all rings which possess such an ideal theory. They are the rings with identity element and without zero divisors in which the double chain condition holds—every divisor chain of ideals terminates after finitely many steps, and likewise every multiple chain modulo every ideal different from the zero ideal—and which are integrally closed with respect to their quotient field. If the latter assumption is dropped, one obtains theorems concerning ideal theory in a finite order, some of which are already found without proof in Dedekind (3rd edition).

A detailed presentation will appear in the Mathematische Annalen.

27. Hilbert Numbers in Ideal Theory

J. Ber. d. DMV 34 (1925), p. 101

— E. NOETHER: Hilbert numbers in ideal theory. By Hilbert numbers one generally understands numbers that refer to the enumeration of residue classes of ideals. Hilbert himself, in his "characteristic function," gave a function which, for the ideals of the polynomial domain, gives from a certain bound onward the exact number of linearly independent residue classes. For the lower degree numbers Macaulay supplemented this function by a generating function, which Ostrowski was able to evaluate explicitly. But Macaulay also gave numbers of another kind, which have proved to be the essential ones for general ideal theory, since they can be formulated abstractly. In accordance with the general decomposition theorems, it is enough to give the definition for primary ideals $\mathfrak{q}$. What is involved is the number of residue classes linearly independent over the residue field of the associated prime ideal $\mathfrak{p}$. These numbers split into partial systems, each given by the number of irreducible components of $\mathfrak{q}, \mathfrak{q}/\mathfrak{p}, \mathfrak{q}/\mathfrak{p}^2, \ldots$. The number of the i-th partial system is also characterized by the number of terms in a composition series running from $\mathfrak{q}/\mathfrak{p}^i$ to $\mathfrak{q}/\mathfrak{p}^{i-1}$. The total composition series and its Hilbert numbers form the equivalent of the representation of primary ideals as powers of prime ideals, which is no longer valid in the general case—for instance, in finite orders of an algebraic number field.

28. Group Characters and Ideal Theory

J. Ber. d. DMV 34 (1925), p. 144

3. E. Noether, Göttingen: Group characters and ideal theory.

The Frobenius theory of group characters—that is, of representations of finite groups—is conceived as the ideal theory of a completely reducible ring, the group ring. Therefore the isomorphism theorems for the additive decomposition of a completely reducible ring are developed in general: the representation as a direct sum of directly indecomposable simple ideals is unique up to isomorphism, and the indecomposable one-sided ideals belonging to the same two-sided ideal are mutually isomorphic. Thus, if isomorphic ideals are combined into one class, there are as many distinct indecomposable ideal classes as there are two-sided indecomposable ideals.

Upon specialization to completely reducible systems of hypercomplex quantities—in particular, to the group ring—indecomposable ideal classes and irreducible representation classes correspond uniquely to one another. Furthermore, two-sided indecomposable ideals correspond to characters, and the number of additively indecomposable components of a two-sided ideal equals the rank of the indecomposable ideals. The Frobenius theory is thereby placed within this framework.

A detailed presentation is to appear in the Math. Ann.

29. The Finiteness Theorem for the Invariants of Finite Linear Groups of Characteristic p.

Nachr. v. d. Ges. d. Wiss. zu Göttingen 1926, pp. 28–35

By Emmy Noether in Göttingen.

Presented by R. Courant in the session of 30 July 1926.

I show in what follows that the well-known finiteness theorem for the invariants of finite groups of linear substitutions[1] remains valid when, as coefficient domain, instead of an ordinary number field one takes an arbitrary field – hence in particular one of characteristic p.[2] However, the known proofs of finiteness fail as soon as the order of the group is divisible by p; deeper arithmetical facts must be brought in, namely the following criterion, previously known only for characteristic zero:

Finiteness criterion[3]: An integral domain $\mathfrak{S}$ of polynomials – more generally of rational functions – with coefficients from a field is finite if and only if $\mathfrak{S}$ contains a finite subring $\mathfrak{R}$ such that $\mathfrak{S}$ depends algebraically and integrally on $\mathfrak{R}$. Each integral basis of $\mathfrak{R}$ is then completed, by a module basis of $\mathfrak{S}$ with respect to a certain subring of $\mathfrak{R}$, to an integral basis of $\mathfrak{S}$.

This criterion – which is of independent interest in itself – rests on the existence of the rational basis and on the fact that the divisor-chain theorem is preserved in passing to the integral quantities of a finite extension. This second theorem was proved in the preceding note of Artin and van der Waerden for arbitrary characteristic, only under a certain finiteness assumption on the original domain, an assumption fulfilled in the case of finite groups (the root ring represents a finite extension). For the existence of the rational basis I give a proof valid for arbitrary fields as coefficient domain; hence I can prove the finiteness criterion under the above restriction.

That, for invariants of finite groups, the finiteness criterion is fulfilled rests on the principle of symmetric functions. Whereas in characteristic zero the coefficients of the Galois resolvent already furnish the integral basis, in the general case they generate only the finite subring required in the finiteness criterion. From the existence of this finite subring the finiteness of the "relative" invariants and of the "modular" invariants follows by the same arguments.

The invariants considered here include, as special cases, the "projective invariants mod p" treated by Dickson and his school.[4] Here the finiteness theorem was known for modular invariants, but not for general "formal" invariants.

ğ 1. The Finiteness Criterion

1. **Theorem on the existence of the rational basis.** First formulation: Every system S of rational functions of n indeterminates, with coefficients from a field P, possesses a finite rational basis; that is, there are finitely many functions of the system such that every function of the system can be expressed rationally, with coefficients from P, through these finitely many.

Second formulation: Let $\mathfrak{K}$ be an intermediate field between P and $P(x_1, \ldots, x_n)$ – where $x_1, \ldots, x_n$ denote indeterminates – of transcendence degree $t \leq n$; let $y_1, \ldots, y_t$ be an irreducible system[5] from $\mathfrak{K}$. Then $\mathfrak{K}$ becomes a finite algebraic extension of $P(y_1, \ldots, y_t)$.

The two formulations are in fact equivalent. It is enough to prove the existence of the rational basis for all intermediate fields; for the field derived from a system S becomes such an intermediate field $\mathfrak{K}$, whose rational basis immediately gives a rational basis of S, since every element of $\mathfrak{K}$ becomes a rational combination of finitely many functions from S. From the second formulation it follows, however, that an arbitrary irreducible system $y_1, \ldots, y_t$ from $\mathfrak{K}$, enlarged by the finitely many functions that characterize $\mathfrak{K}$ as a finite extension of $P(y_1, \ldots, y_t)$, gives such a rational basis. Conversely, if according to the first formulation a rational basis of

[1] For an elementary proof of finiteness see E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann. 77 (1916), pp. 89–92.

[2] For the concepts of field theory see E. Steinitz, Algebraische Theorie der Körper. J. f. M., 137 (1910), pp. 167–309. Characteristic in ğ 4, root field in ğ 12, quotient field in ğ 3.

[3] Compare E. Noether, Algebraische und Differentialinvarianten. Jahresber. d. d. Math.-Ver. 32 (1923), pp. 177–184, no. 3, Theorem 4, and the literature cited there. In the last sentence of the criterion there it incorrectly says "module basis with respect to $\mathfrak{R}$" (fundamental system of integral quantities) instead of "with respect to a certain subring of $\mathfrak{R}$".

[4] Compare Dickson, On Invariants and the theory of Numbers. The Madison Colloquium 1913. More recent literature is in the volumes of the Transactions of the American Mathematical Society that have appeared since then.

[5] A system is called irreducible, according to Steinitz, if it consists of algebraically independent functions. A system is said to have transcendence degree t if it contains at least one irreducible system of t elements, but none of more elements. For the simple theorems on irreducible systems used below, see Steinitz, ğ 22.

$\mathfrak{K}$ is given, then by the definition of transcendence degree each basis element must be algebraically dependent on $P(y_1, \ldots, y_t)$; hence $\mathfrak{K}$ is thereby characterized as a finite algebraic extension of $P(y_1, \ldots, y_t)$.

The theorem will be proved in the second formulation. First let $\mathfrak{K}$ have the same transcendence degree n as $P(x_1, \ldots, x_n)$; let $y_1, \ldots, y_n$ be an irreducible system from $\mathfrak{K}$ and consequently from $P(x_1, \ldots, x_n)$. Because the transcendence degree of $y_1, \ldots, y_n$ is n, each x_i becomes algebraic over $P(y_1, \ldots, y_n)$; thus $P(x_1, \ldots, x_n)$, and hence $\mathfrak{K}$ as an intermediate field, becomes a finite algebraic extension of $P(y_1, \ldots, y_n)$.

Now let $t < n$; let the numbering of the x be chosen so that $y_1, \ldots, y_t, x_{t+1}, \ldots, x_n$ form an irreducible system from $P(x_1, \ldots, x_n)$. Then $x_{t+1}, \ldots, x_n$ are irreducible with respect to $P(y_1, \ldots, y_t)$ and hence, by the transitive law of algebraic dependence, also irreducible with respect to $\mathfrak{K}$ and to every intermediate field $\mathfrak{M}$ between $P(y_1, \ldots, y_t)$ and $\mathfrak{K}$. This means that $\overline{\mathfrak{K}} = \mathfrak{K}(x_{t+1}, \ldots, x_n)$, respectively $\overline{\mathfrak{M}} = \mathfrak{M}(x_{t+1}, \ldots, x_n)$, becomes a purely transcendental extension of $\mathfrak{K}$, respectively $\mathfrak{M}$; hence every element of $\overline{\mathfrak{K}}$ not belonging to $\mathfrak{K}$ is transcendental with respect to $\mathfrak{K}$, and similarly every element of $\overline{\mathfrak{M}}$ not belonging to $\mathfrak{M}$ is transcendental with respect to $\mathfrak{M}$. Likewise let $\overline{P}$ be set equal to the purely transcendental extension $P(x_{t+1}, \ldots, x_n)$; then $y_1, \ldots, y_t$ are irreducible with respect to $\overline{P}$.

The proof can now be reduced to the case already settled by taking $\overline{P}$ as coefficient domain. From $P < \mathfrak{K} < P(x_1, \ldots, x_t;\ x_{t+1}, \ldots, x_n)$[6] it follows that $\overline{P} < \overline{\mathfrak{K}} < \overline{P}(x_1, \ldots, x_t)$, where $\overline{\mathfrak{K}}$ has the same transcendence degree t over $\overline{P}$ as $\overline{P}(x_1, \ldots, x_t)$. Hence $\overline{\mathfrak{K}}$ has a finite rational basis with respect to $\overline{P}$ as coefficient domain, say $y_1, \ldots, y_t; z_1, \ldots, z_s$. Here the z can be chosen from $\mathfrak{K}$, since $\overline{\mathfrak{K}}$ is the union field of $\mathfrak{K}$ and $\overline{P}$. It remains to show that $\mathfrak{K}$ equals $\mathfrak{M} = P(y_1, \ldots, y_t; z_1, \ldots, z_s)$. Now $\mathfrak{M}$ is an intermediate field between $P(y_1, \ldots, y_t)$ and $\mathfrak{K}$; hence every element of $\mathfrak{K}$ is algebraic with respect to $\mathfrak{M}$. On the other hand, $\overline{\mathfrak{M}}$ equals $\overline{\mathfrak{K}}$, and hence $\mathfrak{K}$ is contained in $\overline{\mathfrak{M}}$. Thus $\mathfrak{K}$ is an intermediate field between $\mathfrak{M}$ and $\overline{\mathfrak{M}}$; since every element of $\overline{\mathfrak{M}}$ not belonging to $\mathfrak{M}$ is transcendental with respect to $\mathfrak{M}$, it necessarily follows that $\mathfrak{K}$ is identical with $\mathfrak{M}$.

Corollary: If $P < \mathfrak{K} < \mathfrak{L} < P(x_1, \ldots, x_n)$ and $\mathfrak{L}$ is algebraic with respect to $\mathfrak{K}$, then $\mathfrak{L}$ is a finite algebraic extension of $\mathfrak{K}$. For every element of a rational basis of $\mathfrak{L}$ is then algebraic with respect to $\mathfrak{K}$; hence $\mathfrak{L}$ is characterized as a finite extension of $\mathfrak{K}$.

2. **Proof of the finiteness criterion.** The condition is plainly necessary; for if $\mathfrak{S}$ is a finite integral domain, then $\mathfrak{S}$ itself can be regarded as the finite subring $\mathfrak{R}$ occurring in the criterion.

The condition is sufficient under the assumption that the root field $P^{1/p}$ is a finite extension of the coefficient field[7] whenever the latter has characteristic p; for characteristic zero no restrictive assumption is needed. To prove this one has to show that $\mathfrak{S}$ has a finite module basis with respect to a subring of $\mathfrak{R}$.

Let $\mathfrak{K}$ denote the quotient field[8] of $\mathfrak{R}$, and let $\mathfrak{L}$ denote the quotient field of $\mathfrak{S}$. These quotient fields exist since the rings involved have no zero divisors; and one has $P < \mathfrak{K} < \mathfrak{L} < P(x_1, \ldots, x_n)$. Hence by the corollary under 1., $\mathfrak{L}$ becomes a finite algebraic extension field of $\mathfrak{K}$. Moreover, by hypothesis every element of $\mathfrak{S}$ is integral with respect to $\mathfrak{R}$, and thus $\mathfrak{S}$ becomes a subring of the ring $\mathfrak{S}'$ consisting of all elements of $\mathfrak{L}$ integral over $\mathfrak{R}$. But since nothing is assumed about the integral closedness of $\mathfrak{R}$ in $\mathfrak{K}$, the fact that the divisor-chain theorem is preserved under finite extension cannot be applied directly. Rather, one must first pass to a likewise finite subring $\mathfrak{T}$ of $\mathfrak{R}$ for which this integral closedness is fulfilled.

First suppose that the coefficient domain P contains infinitely many elements. Then one can select from $\mathfrak{R}$ an irreducible system $g_1(x), \ldots, g_t(x)$ in such a way that $\mathfrak{R}$, and hence $\mathfrak{S}$, is integral over $\mathfrak{T} = P[g_1(x), \ldots, g_t(x)]$. Namely, let $f_1(x), \ldots, f_k(x)$ be the integral basis of $\mathfrak{R}$ existing by hypothesis; if this does not form an irreducible system, then – after a possible renumbering of the indices – let $F(f_k; f_1, \ldots, f_{k-1}) = 0$ be a relation satisfied by f_k. If one replaces $f_1, \ldots, f_{k-1}$ by

$$f_1 + t_1 f_k, \ldots, f_{k-1} + t_{k-1} f_k;$$

then f_k, and hence also $f_1, \ldots, f_{k-1}$, is integral over these new functions when the t_i are chosen as indeterminates. Since P has infinitely many elements, the t_i can be specialized to elements of P in such a way that this integral dependence is preserved. After finitely many steps, using the transitive law of integral dependence, one therefore arrives at the required ring $\mathfrak{T} = P[g_1(x), \ldots, g_t(x)]$[9]. Then $\mathfrak{L}$ is a finite extension field of the quotient field $P(g_1(x), \ldots, g_t(x))$ of $\mathfrak{T}$, and the ring $\mathfrak{S}'$ of all elements of $\mathfrak{L}$ integral over $\mathfrak{R}$ is identical with the ring of all elements of $\mathfrak{L}$ integral over $\mathfrak{T}$.

In $\mathfrak{T}$ the divisor-chain theorem holds for the system of all ideals, and $\mathfrak{T}$ is integrally closed in its quotient field, both because $\mathfrak{T}$ is isomorphic to the polynomial domain in t indeterminates. From the assumption that

[6] $P < \mathfrak{K}$ means: P is contained in $\mathfrak{K}$, hence is a subfield of $\mathfrak{K}$.

[7] See p. 28, note 2.

[8] See p. 28, note 2.

[9] Compare Hilbert, Über die vollen Invariantensysteme, ğ 1. Math. Ann. 42 (1893), pp. 313–373.

$P^{1/p}$ is finite over P it follows further that $\mathfrak{T}^{1/p}$ is finite over $\mathfrak{T}$.[10] Hence in $\mathfrak{S}'$ the divisor-chain theorem holds for the system of all $\mathfrak{T}$-modules; in particular, $\mathfrak{S}$, as a subring of $\mathfrak{S}'$ containing $\mathfrak{T}$, has a finite $\mathfrak{T}$-module basis[10]. The existence of the finite $\mathfrak{T}$-module basis for $\mathfrak{S}$ continues to hold without any restrictive assumption on the coefficient domain P if $\mathfrak{L}$ is an extension of the first kind of $P(g_1(x), \ldots, g_t(x))$, hence in particular always when P has characteristic zero.[11]

Let $h_1(x), \ldots, h_s(x)$ be a $\mathfrak{T}$-module basis of $\mathfrak{S}$. Then the representation

$$f(x) = A_1(g)h_1(x) + \cdots + A_s(g)h_s(x)$$

for an arbitrary $f(x)$ from $\mathfrak{S}$ – where the A, as elements of $\mathfrak{T}$, denote polynomials in the g – shows that $g_1(x), \ldots, g_t(x), h_1(x), \ldots, h_s(x)$ form the required integral basis.

If the field P contains only finitely many elements, then the field $P(u)$ obtained by adjoining an indeterminate u – that is, an element transcendental over $\mathfrak{S}$ – contains infinitely many elements. Thus the ring $\mathfrak{S}(u)$ has a finite integral basis with respect to $P(u)$ as coefficient domain; and since $\mathfrak{S}(u)$ is the union ring of $\mathfrak{S}$ and $P(u)$, this basis can be chosen from $\mathfrak{S}$ by splitting according to powers of u, although the basis elements g_i of $\mathfrak{S}$ will now no longer form an irreducible system. Accordingly every polynomial $f(x)$ from $\mathfrak{S}$ admits a representation $C(u)f(x) = G(u, g_i, h_i)$, where $C(u)$ denotes a nonzero polynomial from $P[u]$ and G becomes integral in u, g_i, h_i. Comparing the coefficients of a suitable power of u shows that $g_i(x)$ and $h_i(x)$ give an integral basis of $\mathfrak{S}$. Hence the **finiteness criterion is proved in full generality**.

ğ 2. Finiteness of the Invariants

1. By a **finite linear group of characteristic** p is meant a group $\mathfrak{H}$ of h linear substitutions $A_1, \ldots, A_h$ (of nonzero determinant) with coefficients from a field P of characteristic p. Here A_k is the linear substitution

$$x_1^{(k)} = a_{11}^{(k)}x_1 + \cdots + a_{1n}^{(k)}x_n, \ldots, \quad x_n^{(k)} = a_{n1}^{(k)}x_1 + \cdots + a_{nn}^{(k)}x_n,$$

or, in abbreviated form, $(x^{(k)}) = A_k(x)$. Thus the group $\mathfrak{H}$ carries the row (x) with elements $x_1, \ldots, x_n$ into the rows $(x^{(k)})$ with elements $x_1^{(k)}, \ldots, x_n^{(k)}$. Since the identity must be contained among $A_1, \ldots, A_h$, the row (x) is also contained among the rows $(x^{(k)})$.

By an **integral rational (absolute) invariant of the group** is meant such an integral rational function of $x_1, \ldots, x_n$ – with coefficients from P[12] – that remains identically unchanged under application of $A_1, \ldots, A_h$. Thus all symmetric functions, with coefficients from P, of the rows $(x^{(k)})$ belong to these invariants. Conversely, for every such invariant one has

$$f(x) = f(x^{(1)}) = \cdots = f(x^{(h)}) \quad \text{or} \quad h \cdot f(x) = f(x^{(1)}) + \cdots + f(x^{(h)}).$$

It follows that in the case where the order h of the group is not divisible by the characteristic – in particular in characteristic zero – the symmetric functions of the rows $(x^{(k)})$, with coefficients from P, exhaust the totality of invariants. Since these symmetric functions possess a finite integral basis, the proof of finiteness is accomplished in this case; at the same time the integral basis is obtained as the system $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ of coefficients of the Galois resolvent:[13]

$$\begin{aligned}\Phi(z, u) &= \prod(z - u_1x_1^{(k)} - \cdots - u_nx_n^{(k)}) \\ &= z^h + \sum G_{\alpha\alpha_1\ldots\alpha_n}(x)z^\alpha u_1^{\alpha_1} \cdots u_n^{\alpha_n} \quad (\alpha \neq h;\ \alpha + \alpha_1 + \cdots + \alpha_n = h).\end{aligned}$$

2. In the case where h is divisible by p, it is not necessary that every invariant of the group be a symmetric function of the rows $(x^{(k)})$, since one can no longer conclude from $h \cdot f(x)$ to $f(x)$. But the ring $\mathfrak{R}$ derived from the finitely many invariants $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ – the coefficients of the Galois resolvent – forms a finite subring of the system $\mathfrak{S}$ of all invariants, and it remains to show that $\mathfrak{S}$, with respect to $\mathfrak{R}$, satisfies the hypotheses of the finiteness criterion.

[10] Compare the note of Artin and van der Waerden cited in the introduction.

[11] Compare, for example, E. Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, ğ 3. Math. Ann. 96 (1926), pp. 26–61.

[12] This is not a restriction of generality inasmuch as every invariant with coefficients from a field of characteristic p – which must possess a common overfield with P in order for the invariants to be defined – can be linearly decomposed into finitely many invariants with coefficients from P. In the general case one need only express the coefficients through ones that are linearly independent over P; then the property of invariance is satisfied identically in these independent coefficients.

[13] See p. 28, note 1.

First, without loss of generality,[14] the subfield $\overline{P}$ of P derived from all substitution coefficients $a_{\mu\nu}^{(k)}$ may be taken as coefficient domain. This field, derived from finitely many elements, is thus obtained by adjoining finitely many algebraic or transcendental elements to the prime field; and since the prime field is perfect, it follows that $\overline{P}^{1/p}$ is finite with respect to $\overline{P}$.[15]

It remains to show that $\mathfrak{S}$ depends algebraically and integrally on $\mathfrak{R}$. By 1., among the h rows $x^{(k)}$ there also occurs the original $x_1, \ldots, x_n$; hence the Galois resolvent $\Phi(z, u)$ vanishes identically in u for $z = u_1 x_1 + \cdots + u_n x_n$. If one specializes in each case all u to zero except u_i, which is set equal to one, one obtains a relation

$$x_i^h + \sum x_i^\alpha G_{\alpha 0 \ldots \alpha_i \ldots 0}(x) = 0 \quad (\alpha \neq h;\ \alpha + \alpha_i = h),$$

which shows that each x_i depends algebraically and integrally on $\mathfrak{R}$. But then the same holds for every polynomial in x; in particular $\mathfrak{S}$ is integral over $\mathfrak{R}$. Thus the hypotheses of the finiteness criterion are fulfilled, and the **finiteness of the invariants is proved**.

3. It should be noted that the same arguments give the **finiteness of the relative and modular invariants**. A polynomial $f(x)$ is called a **relative invariant** of the group if all $f(x^{(k)})$ differ from $f(x)$ only by a nonzero factor from $\overline{P}$. The system of absolute invariants – in particular the ring $\mathfrak{R}$ derived from the $G_{\alpha\alpha_1 \ldots \alpha_n}(x)$ – therefore forms a finite subring of the ring derived from all relative invariants; and, as above, the hypotheses of the finiteness criterion with respect to $\mathfrak{R}$ are fulfilled.

A polynomial $f(x)$ is called a **modular invariant** of the group if $f(x)$ becomes equal to $f(x^{(k)})$ for every special value system $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ from $\overline{P}$. Every absolute invariant is at the same time a modular invariant; if, however, $\overline{P}$ contains only finitely many elements, the converse need not hold. Here too the hypotheses of the finiteness criterion are fulfilled with respect to the subring $\mathfrak{R}$ derived from the $G_{\alpha\alpha_1 \ldots \alpha_n}(x)$.

[14] See p. 33, note.

[15] See p. 32, note 2.

30. Abstract Construction of Ideal Theory in Algebraic Number and Function Fields.

Math. Ann. 96 (1927), pp. 26–61.

By

Emmy Noether in Göttingen.

In what follows an abstract characterization is given of all those rings whose ideal theory agrees with the ideal theory of all integers of an algebraic number field: that is, whose ideals can be represented uniquely as products of powers of prime ideals. Among the best-known examples of such rings are also the ring of all integers of an algebraic function field in one indeterminate, and, more generally, in several indeterminates as soon as, following Kronecker, one restricts to ideals of highest dimension, i.e. passes to a certain quotient ring, the functional domain.

For the underlying commutative ring, the axioms completely equivalent to this ideal theory are the following:[1]

I. Divisor-chain condition: Every chain of ideals in which each ideal is a proper divisor of the preceding one terminates after finitely many steps; in other words, in every divisor chain of ideals there is an index from which on all ideals are equal.

II. Multiple-chain condition modulo every nonzero ideal. Every chain of ideals — all of which are divisors of a fixed ideal different from the zero ideal — in which each ideal is a proper multiple of the preceding one terminates after finitely many steps.

III. Existence of the identity element for multiplication.

IV. Ring without zero divisors.

V. Integral closedness in the quotient field: Every element of the quotient field that is integral with respect to the ring belongs to the ring.

From these axioms I develop, step by step, an increasingly restricted ideal theory up to the desired one; conversely, I show that all these axioms are in fact satisfied there.

From the divisor-chain condition I it follows, as I showed in *Ideal Theory* §4, that an ideal is representable as the least common multiple of finitely many primary ideals belonging to distinct prime ideals. I recall this proof briefly here (§6), both because it can be simplified by using the concept of the ideal quotient, and because I want to correct an oversight: the original proof uses, at one point, the not-assumed existence of the identity element of multiplication.[2]

The assumption of the multiple-chain condition has the effect (§7) that, in the residue class ring modulo every ideal different from the zero ideal, a prime ideal cannot have a proper divisor, except for the unit ideal containing all elements. Consequently the primary components of these ideals are determined uniquely, except for those belonging to the unit ideal. In a somewhat less sharp form this result is already found in Masazo Sono;[3] his assumption of the existence of a composition series in the residue class ring is equivalent to the "double chain condition" in this ring, as I show briefly at the end (§10). By double chain condition I mean the validity of both the divisor-chain and multiple-chain conditions without restriction to ideals different from the zero ideal.

If axiom III — existence of the identity element — is also satisfied, the unit ideal does not occur as an associated prime ideal. The primary components are therefore uniquely determined; they are pairwise coprime, and their least common multiple equals their product. Axioms I, II, III hold for all finite orders of an algebraic number field; already Dedekind (Dirichlet–Dedekind, *Zahlentheorie*, 3rd ed., 11th supplement,

[1] For the definition of the basic concepts of ideal theory, compare for instance E. Noether, *Idealtheorie in Ringbereichen*, Math. Ann. 83 (1921), pp. 24–66 (cited below as *Ideal Theory*). Incidentally, the most essential concepts are also formulated briefly in the present paper, especially in §§1, 4, and 5. For completeness, some material is included that is not needed for the immediate purposes of this paper.

[2] P. Urysohn called my attention to this oversight; my own alteration of the proof was somewhat more cumbersome than the one given here, which is due to E. Artin. He had already filled the gap for himself earlier, and, independently of me, had also observed the simplification with the ideal quotient. — I take a further simplification, which avoids the introduction of the "reduced representation," from a related question in W. Krull, *Algebraische Theorie der Ringe III*, Math. Ann. 92 (1924), pp. 181–213, Theorem I.

[3] Masazo Sono, *On the Reduction of Ideals*, Memoirs of the College of Science, Kyoto University, Series A, 7 (1924), pp. 191–204.

ğ172), without giving the proof in full detail, stated here the unique representation of an ideal as a product of pairwise coprime one-kind ideals (primary components).

From assumption IV — absence of zero divisors — it follows that the different powers of an ideal distinct from both the zero ideal and the unit ideal are all distinct, and that the quotient field exists. If finally axiom V of integral closedness in the quotient field is also satisfied, the primary ideals — uniquely determined because of IV — become powers of prime ideals, and the usual factorization theorem is obtained (ğ8). This latter proof rests on a consequence of integral closedness already drawn by Dedekind (3rd ed., ğ172) in the case of number fields: a genuinely fractional element can be represented as a quotient of integers in such a way that even the square of the numerator is not divisible by the denominator. In later presentations this consequence is replaced — likewise as a consequence of integral closedness — by the much less transparent generalized Gaussian theorem or by corresponding module theorems that say somewhat more; all of these are theorems whose application presupposes basis elements, whereas here one works directly with the ideals themselves.

In the converse direction §9, the axioms distinct from axiom V follow almost directly; V follows from the proof that a genuinely fractional element can always be represented so that no power of the numerator is divisible by the denominator, which is therefore a strengthening of the consequence originally derived from V. This proof succeeds only after one draws from the ideal representation the usual conclusions: representation by principal ideals modulo a fixed ideal, and the theory of fractional ideals, i.e. of ideal quotients in the field. The fact that integral closedness follows from the representation by powers of prime ideals was also already known to Dedekind, as is shown by a remark in the 3rd edition, ğ172, p. 522, bottom.

Axioms I through V imply that the four decompositions which are generally distinct — into least pairwise coprime ideals, into mutually prime ideals, into largest primary components, and into irreducible ideals — coincide; conversely, from this coincidence and axioms I–IV, integral closedness follows. For rings with zero divisors, fulfillment of the remaining axioms — with V defined as integral closedness in the quotient ring — does not necessarily imply that the decompositions coincide, as the example of the residue class ring modulo certain ideals of a finite order shows §9.

In ğ1 I sketch the theory of quantities integral with respect to a ring, up to Dedekind's consequence from integral closedness. In ğ2 I show how the chain conditions are transferred from the ring to modules consisting of linear forms, with this ring as coefficient and multiplier domain.[4] From this I draw (ğ3) the conclusion that, on passing to the integral elements of an algebraic extension field of the first kind, axioms I to IV remain valid for every order, while for the order consisting of all integral elements, V is also valid. This fact — of course familiar for the algebraic number field — permits the subordination of the function fields mentioned at the beginning; in particular, by the simple proof that the functional domain derived from integral polynomials in several indeterminates satisfies the axioms, Kronecker's ideal theory is fully subsumed.[5]

The ideal theory subsequently developed does not presuppose these ğğ2 and 3, which serve only for classification. In ğ4 and ğ5 the foundations independent of axioms I through V are given; this brings out more sharply than in the original foundation which parts of the theory are independent of finiteness assumptions.

ğ 1.
Theory of Integral Quantities.

Let there be given a commutative ring[6] $\mathfrak{T}$ without zero divisors, with identity element e for multiplication (axioms III and IV); in $\mathfrak{T}$ a fixed subring $\mathfrak{R}$ containing the identity element is distinguished. The concepts module, order, integral are throughout to refer to this fixed ring $\mathfrak{R}$, which later will be omitted from the notation for brevity.[7] (Elements of $\mathfrak{R}$ will be denoted by Latin letters, elements of $\mathfrak{T}$ in general by Greek

[4]This form of the module theorems is due to Prüfer (Neue Begründung der algebraischen Zahlentheorie, ğ2, Math. Ann. 94 (1924), pp. 198–243) and is more transparent than the customary transfer of the basis theorems.

[5]The difference appears only in the discriminant theorems, because the residue class ring of the functional domain modulo a prime number becomes an imperfect field, and hence extensions of the second kind can occur.

[6]As is known, a ring is defined once an equality relation is given in a set, and in addition two operations, addition and multiplication, are given satisfying the usual laws: addition is associative, commutative, and uniquely reversible; multiplication is associative — commutative when the ring is commutative — and distributive with respect to addition. If the underlying definition of equality is not set-theoretic identity, then, so that the same definition of equality is retained in every subsystem, such a subsystem (subring, module, ideal) must contain with any element all elements equal to it. Likewise, in every extension it must be assumed that the new definition of equality includes the old one. All concepts such as "finitely many elements," "unique assignment," etc. are meant in the sense of the equality definition; for example, "there is one and only one element" means that there is only one element up to equality. Incidentally, one can always pass from equality to set-theoretic identity by collecting equal elements into a class and introducing these classes as the new elements. The remarks given here on the definition of equality are due to R. Hölzer.

[7]The theory of integral quantities remains valid if zero divisors are admitted, provided that in their place one assumes the divisor-chain condition

letters.)

1. A system $\mathfrak{M}$ of elements of $\mathfrak{T}$ is called, as usual, an $\mathfrak{R}$-module — briefly, a module — if, together with two elements α and β, it also contains their difference, and with α also $r\alpha$, where r is any element of $\mathfrak{R}$. $\mathfrak{M}$ is said to be divisible by $\mathfrak{N}$,

$$\mathfrak{M} \equiv 0(\mathfrak{N}),$$

and $\mathfrak{M}$ is called a multiple, $\mathfrak{N}$ a divisor, if every element of $\mathfrak{M}$ is also contained in $\mathfrak{N}$. $\mathfrak{R}$-modules all of whose elements belong to $\mathfrak{R}$ are called ideals in $\mathfrak{R}$.

Clearly the intersection — the least common multiple $[\ldots, \mathfrak{M}_i, \ldots]$ — of any number of modules from $\mathfrak{T}$ is again a module; likewise $\mathfrak{T}$ itself is a module. Thus the module derived from any system Σ of elements of $\mathfrak{T}$ exists uniquely as the intersection of all modules containing Σ. The sum — the greatest common divisor $(\ldots, \mathfrak{M}_i, \ldots)$ — of any system of modules is the module derived from their union. The product $\mathfrak{MN}$ of two modules is defined as the module derived from the elements $\mu\nu$, where μ runs through all elements of $\mathfrak{M}$ and ν through all elements of $\mathfrak{N}$. The product therefore satisfies the associative and commutative laws, since these hold for the ring elements. The distributive law in $\mathfrak{T}$ further gives, for modules, the distributive law

$$(\ldots, \mathfrak{M}_i, \ldots)\mathfrak{N} = (\ldots, \mathfrak{M}_i\mathfrak{N}, \ldots),$$

since by exactly this law in $\mathfrak{T}$ both sides are the module derived from all elements $\mu_i\nu$.

Since $\mathfrak{R}$ itself is a module, the condition that $\mathfrak{R}$ is the multiplier domain can be expressed by $\mathfrak{RM} \equiv 0(\mathfrak{M})$. Since by hypothesis $\mathfrak{R}$ contains the identity element, one also has $\mathfrak{M} \equiv 0(\mathfrak{RM})$, and hence $\mathfrak{M} = \mathfrak{RM}$.

A module $\mathfrak{M}$ is called finite if there is at least one system Σ consisting of finitely many elements from which $\mathfrak{M}$ is derived; the elements $\mu_1, \ldots, \mu_r$ of Σ are called a module basis of

$$\mathfrak{M} = (\mu_1, \ldots, \mu_r).$$

The sum and product of two — and hence of finitely many — finite modules are again finite, since they are derived from the union, respectively from the products, of the basis elements. The latter assertion follows from the representation $r_1\mu_1 + \cdots + r_k\mu_k$ of all elements μ of $\mathfrak{M}$ by the basis[8] and from the commutative law of multiplication in $\mathfrak{T}$, both of which are used here for the first time.

2. An extension ring of $\mathfrak{R}$ lying in $\mathfrak{T}$ — hence one that contains all elements of $\mathfrak{R}$ — is called an $\mathfrak{R}$-order, briefly an order. The intersection of arbitrarily many orders in $\mathfrak{T}$ is again an order, and likewise $\mathfrak{T}$ is an order; hence the order derived from any system Σ of elements of $\mathfrak{T}$ exists uniquely. Sums and products of orders are defined correspondingly as for modules; in particular $\mathfrak{O}^2 = \mathfrak{O}$ for every order.

Every order is at the same time an $\mathfrak{R}$-module; an order is called finite when it is a finite module. Since sums and products arise by forming module sums and products, sums and products of finite orders are again finite orders by 1.; further, the following transitive law holds: if $\mathfrak{A}$ is a finite $\mathfrak{R}$-order and $\mathfrak{B}$ is a finite $\mathfrak{A}$-order, then $\mathfrak{B}$ is also a finite $\mathfrak{R}$-order. For $\mathfrak{B}$ is at the same time an $\mathfrak{R}$-order, hence an $\mathfrak{R}$-module. If $\alpha_1, \ldots, \alpha_\rho$ form a module basis of $\mathfrak{A}$ with respect to $\mathfrak{R}$, and $\beta_1, \ldots, \beta_\sigma$ one of $\mathfrak{B}$ with respect to $\mathfrak{A}$, then the products $\alpha_i\beta_k$ plainly form a module basis of $\mathfrak{B}$ with respect to $\mathfrak{R}$.

3. An element α of $\mathfrak{T}$ is called integral with respect to $\mathfrak{R}$, briefly integral, if the order $\mathfrak{R}_\alpha$ derived from α is finite — equivalently, if the divisor chain of modules

$$\mathfrak{A}_\mu = (\alpha^0, \alpha, \ldots, \alpha^{\mu-1})$$

terminates after finitely many steps, $\mathfrak{A}_n = \mathfrak{A}_{n+1} = \cdots = \mathfrak{A}_{n+\nu} = \cdots$.

The definition also admits a second formulation, to be used in 4.: an element α of $\mathfrak{T}$ is called integral if there is at least one principal module $\mathfrak{C}$ different from the zero module — i.e. $\mathfrak{C}$ is derived from an element $\gamma \neq 0$ — such that the product of the order $\mathfrak{R}_\alpha$ with $\mathfrak{C}$ is a finite module; in other words, such that the chain of modules $\mathfrak{CA}_\mu$ terminates after finitely many steps.[9]

Finally the definition is also identical with the usual formulation: an element α of $\mathfrak{T}$ is called integral if it satisfies at least one equation

$$\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0,$$

in $\mathfrak{R}$, which by ğ2 also makes the proof of the lemma possible. Since this form of the theory of integral quantities is not used later, I only point to it in footnotes. All definitions under discussion remain valid in the presence of zero divisors; most of them require — as is known and easy to see — even weaker assumptions. What is not retained is Dedekind's formulation: "A number is integral when it has a hull." For with zero divisors present, the quotient of two finite modules need not remain finite; hence here the order is defined directly and not as a module quotient.

[8] If $\mathfrak{R}$ contains no identity element, the basis representation takes the form $r_1\mu_1 + \cdots + r_k\mu_k + n_1\mu_1 + \cdots + n_k\mu_k$, where the integers n are not ring elements but symbols for repeated addition or subtraction.

[9] If zero divisors are admitted in $\mathfrak{R}$, then the existence of a regular principal module must be required; that is, γ must be assumed to be a non-zero-divisor, a regular element, which in rings without zero divisors is simply $\gamma \neq 0$.

where the r's are elements of $\mathfrak{R}$.

These definitions are in fact identical. Since $\mathfrak{R}_\alpha$ agrees with the module derived from all powers of α, when $\mathfrak{R}_\alpha$ is finite one can always choose a module basis from these powers. If such a basis is given, for instance, by $e = \alpha^0, \alpha, \ldots, \alpha^{n-1}$, this means that the chain of the $\mathfrak{A}_\mu$ terminates at $\mathfrak{A}_n$; conversely, $\mathfrak{A}_n = \mathfrak{A}_{n+\nu} \cdots$ gives this basis. But the termination of the chain of the $\mathfrak{A}_\mu$ is also identical with the existence of the equation

$$\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0.$$

If $\mathfrak{R}_\alpha$ is finite, then $\mathfrak{CR}_\alpha$ is finite, so the chain $\mathfrak{CA}_\mu$ terminates; conversely, from the finiteness of $\mathfrak{CR}_\alpha$, hence from the termination of the $\mathfrak{CA}_\mu$, it follows that the $\mathfrak{A}_\mu$ also terminate and hence that $\mathfrak{R}_\alpha$ is finite. Indeed, since $\mathfrak{C}$ is assumed to be a principal module distinct from the zero module, $\mathfrak{CA}_n = \mathfrak{CA}_{n+\nu}$ also gives $\mathfrak{A}_n = \mathfrak{A}_{n+\nu}$.

The ring property of the integral quantities and the transitive law of integral dependence rest on the following

Lemma. Let $\mathfrak{S}$ be a finite order in $\mathfrak{T}$, and let α be any element of $\mathfrak{S}$. Then the order $\mathfrak{R}_\alpha$ derived from α is finite; in other words, all elements of a finite order are integral.

The proof follows by the usual arguments. Let $\sigma_1, \ldots, \sigma_n$ be a module basis of $\mathfrak{S}$. Since $\mathfrak{S}$ is a ring, $\alpha\sigma_i$ belongs to $\mathfrak{S}$. Thus

$$\alpha\sigma_i = r_{i1}\sigma_1 + \cdots + r_{in}\sigma_n,$$

and hence

$$|r_{ik} - \alpha e_{ik}| = 0,$$

where $e_{ik} = 0$ for $i \neq k$ and $e_{ii} = e$; this proves that α is integral. For the vanishing of the determinant one uses the hypothesis that $\mathfrak{T}$, and hence $\mathfrak{S}$, has no zero divisors.[10]

The system $\mathfrak{S}$ of all integral quantities in $\mathfrak{T}$ forms an order. It contains $\mathfrak{R}$, for the elements of $\mathfrak{R}$ are integral, since $\mathfrak{R}$ is a finite $\mathfrak{R}$-module with the identity element as basis. But $\mathfrak{S}$ also has the ring property: for the order $\mathfrak{R}_{\alpha,\beta}$ derived from two arbitrary integral quantities α, β is equal to the product $\mathfrak{R}_\alpha \cdot \mathfrak{R}_\beta$, and is therefore finite. Hence, by the lemma, $\alpha \pm \beta$ and $\alpha\beta$ are integral as elements of a finite order.

Transitive law of integral dependence. If $\mathfrak{S}$ is an order consisting of integral quantities, then every element of $\mathfrak{T}$ integral with respect to $\mathfrak{S}$ is also integral with respect to $\mathfrak{R}$. By definition α satisfies an equation

$$\alpha^m + \sigma_1\alpha^{m-1} + \cdots + \sigma_m = 0,$$

and is therefore also integral with respect to the order $\overline{\mathfrak{S}} = \mathfrak{R}_{\sigma_1,\ldots,\sigma_m}$ derived from $\sigma_1, \ldots, \sigma_m$, which is finite as the product $\mathfrak{R}_{\sigma_1} \cdot \mathfrak{R}_{\sigma_2} \cdot \ldots \cdot \mathfrak{R}_{\sigma_m}$. By the transitive law given in 2., the finite $\overline{\mathfrak{S}}$-order $\overline{\mathfrak{S}}_\alpha$ derived from α is therefore also a finite $\mathfrak{R}$-order, and α is integral by the lemma as an element of a finite order.

4. The ring $\mathfrak{R}$ is called integrally closed in $\mathfrak{T}$ if every element of $\mathfrak{T}$ integral with respect to $\mathfrak{R}$ belongs to $\mathfrak{R}$. According to the second formulation of the definition of integral quantities in 3., an element α of $\mathfrak{T}$ belongs to $\mathfrak{R}$ if and only if there is at least one principal module $\mathfrak{C}$ different from the zero module such that $\mathfrak{C} \cdot \mathfrak{R}_\alpha$ is a finite module.[11]

From the concept of an integrally closed ring Dedekind (3rd ed., ğ172) drew two important consequences, which make it possible to use this concept for ideal theory:

Dedekind consequence I. Let $\mathfrak{R}$ be integrally closed in $\mathfrak{T}$, and assume further that the divisor-chain condition for ideals (axiom I) holds in $\mathfrak{R}$. If β is a nonintegral element of $\mathfrak{T}$, and $c \neq 0$ an element of $\mathfrak{R}$, then there is an exponent $\sigma \geq 0$ such that in the sequence of elements

$$c,\ c\beta, \ldots, c\beta^r, \ldots$$

the elements $c, \ldots, c\beta^\sigma$ are integral, and all the remaining ones are nonintegral.

If all elements $c\beta^r$ were integral, then by the integral closedness of $\mathfrak{R}$ they would belong to $\mathfrak{R}$. Then the chain of modules $\mathfrak{CB}_1, \mathfrak{CB}_2, \ldots, \mathfrak{CB}_r, \ldots$ — where $\mathfrak{C}$ denotes the module derived from c, and $\mathfrak{B}_r$ the one derived from $\beta^0, \ldots, \beta^{r-1}$ — would become a chain of ideals $\mathfrak{c}_1, \ldots, \mathfrak{c}_r, \ldots$, with $\mathfrak{c}_r = (c, c\beta, \ldots, c\beta^{r-1})$, which

[10] If the divisor-chain condition is assumed in $\mathfrak{R}$ but zero divisors are admitted, then the lemma is an immediate consequence of the module theorem in ğ2, according to which the chain condition transfers to the modules from $\mathfrak{S}$. This proof too is due, for the number field, to Dedekind (4th ed., ğ173, III) and is the first application of chain conditions in the literature. In the consequences to be given under 4., Dedekind instead uses the more special fact that the number of residue classes modulo an ideal in an algebraic number field is finite.

[11] If zero divisors are admitted in $\mathfrak{R}$, $\mathfrak{C}$ must again be assumed to be a regular principal module; likewise the element c in Consequence I must be assumed regular.

terminates by hypothesis. But then, contrary to the assumption, $\mathfrak{R}_\beta$ would be finite and β integral; hence some of the elements $c\beta^r$ are nonintegral. Furthermore, with any one nonintegral element all subsequent ones are nonintegral: for if $c\beta^\tau$ is integral, hence belongs to $\mathfrak{R}$, then for $\rho < \tau$ the element $c\beta^\rho$ satisfies

$$(c\beta^\rho)^\tau - c^{\tau-\rho}(c\beta^\tau)^\rho = 0$$

and is therefore integral. Thus if $c\beta^{\sigma+1}$ is the first nonintegral element, then — since c is integral — $\sigma \geq 0$, and this is the required exponent.

Specializing the extension ring $\mathfrak{T}$ to the quotient field of $\mathfrak{R}$ — that is, to the field obtained by adjoining all pairs of elements[12] — gives the following:

Dedekind consequence II. Let $\mathfrak{R}$ be integrally closed in its quotient field $\mathfrak{K}$, and let the divisor-chain condition for ideals hold in $\mathfrak{R}$. If β is a nonintegral element of $\mathfrak{K}$, then β admits a representation as a quotient of elements of $\mathfrak{R}$,

$$\beta = m/n,$$

such that m^2/n is also nonintegral.

Put $\beta = b/c$ with $c \neq 0$. Then in the sequence $c, c\beta = b, c\beta^2, \ldots$ the first two elements are certainly integral, so $\sigma \geq 1$, where σ is the exponent of Consequence I. If one sets $m = c\beta^\sigma$, $n = c\beta^{\sigma-1}$ — because $\sigma \geq 1$, these are integral quantities of the sequence — then $m/n = \beta$, and $m^2/n = c\beta^{\sigma+1}$ is nonintegral.

The transitive law of integral closedness has the following form: if $\mathfrak{R}$ is any ring in $\mathfrak{T}$ and $\mathfrak{S}$ denotes the system of all quantities in $\mathfrak{T}$ integral with respect to $\mathfrak{R}$, then $\mathfrak{S}$ also consists of all quantities of $\mathfrak{T}$ integral with respect to $\mathfrak{S}$. For every quantity integral with respect to $\mathfrak{S}$ is also integral with respect to $\mathfrak{R}$, by the transitive law in 3., and hence belongs to $\mathfrak{S}$.

ğ2. Chain Conditions in Finite Module Domains

The module theorem by which the chain conditions are transferred occurs, in the application given here, only for modules of an extension ring. Since the proof is the same in the case of a general module domain, such a domain will be taken as the starting point.

A system M of elements $\alpha, \beta, \ldots$ is called a module domain with respect to a ring $\mathfrak{R}$ if two operations are given in M, each leading uniquely to elements of M: an additive combination of the elements and a multiplication of the elements by elements of $\mathfrak{R}$; if M is an Abelian group with respect to addition, while multiplication satisfies the associative law; and if the distributive law holds in both forms.[13]

For a module domain, all module definitions given in ğ1, 1. that do not refer to multiplication plainly remain valid. In particular, M is called a finite module domain if there are finitely many elements $\xi_1, \ldots, \xi_k$ of M such that M equals the module derived from $\xi_1, \ldots, \xi_k$, hence equals the system of all linear forms $r_1\xi_1 + \cdots + r_k\xi_k$ when $\mathfrak{R}$ has an identity element; otherwise additional terms $n_i\xi_i$ occur (compare note 8).

Module theorem. *Let M be a finite module domain with respect to a commutative ring $\mathfrak{R}$ with identity element, and suppose that in $\mathfrak{R}$ the divisor- respectively multiple-chain condition for ideals holds. Then in M the divisor- respectively multiple-chain condition for modules holds.*

The proof rests on assigning uniquely to every module in M a system of finitely many ideals from $\mathfrak{R}$ in such a way that to a proper divisor respectively proper multiple of the module there corresponds each time at least one proper divisor respectively multiple ideal.

An element of M is said to have length i if it can be written in at least one way as a linear form in $\xi_1, \ldots, \xi_i$, while it has no representation as a linear form in $\xi_1, \ldots, \xi_{i-1}$. To an arbitrary module $\mathfrak{A}$ in M assign now k ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ from $\mathfrak{R}$: let $\mathfrak{A}_i$ mean the module of all elements of $\mathfrak{A}$ of length $\leq i$, and let $\mathfrak{a}_i$ denote the system of all coefficients of ξ_i in $\mathfrak{A}_i$. First one obtains:

If $\mathfrak{B}$ is a proper divisor of $\mathfrak{A}$, and if $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$ are the ideals assigned to $\mathfrak{B}$, then among the $\mathfrak{b}_i$ there is at least one proper divisor of the corresponding $\mathfrak{a}_i$. For from $\mathfrak{A} \equiv 0 \pmod{\mathfrak{B}}$ it follows that $\mathfrak{A}_\lambda \equiv 0 \pmod{\mathfrak{B}_\lambda}$, and hence $\mathfrak{a}_\lambda \equiv 0 \pmod{\mathfrak{b}_\lambda}$ for $\lambda = 1, 2, \ldots, k$. By hypothesis there must be elements in $\mathfrak{B}$ not contained in $\mathfrak{A}$, and hence such elements of smallest length i. Then $\mathfrak{b}_i$ is a proper divisor of $\mathfrak{a}_i$; indeed $b_i \equiv 0 \pmod{\mathfrak{b}_i}$ but $\mathfrak{b}_i \not\equiv 0 \pmod{\mathfrak{a}_i}$ when

$$\beta = b_1\xi_1 + \cdots + b_i\xi_i$$

[12] In Steinitz's familiar formulation, J. f. M. 137. If zero divisors are admitted in $\mathfrak{R}$, then the quotient ring must replace the quotient field, by adjoining all quotient pairs whose denominator is a regular element of $\mathfrak{R}$. Here Dedekind consequence II is no longer valid, for n will not in general be a regular element.

[13] Compare *Ideal Theory*, ğ9.

is such an element of smallest length in $\mathfrak{B}$. If $b_i \equiv 0 \pmod{\mathfrak{a}_i}$, there exists an element

$$\alpha = a_1\xi_1 + \cdots + b_i\xi_i \equiv 0 \pmod{\mathfrak{A}},$$

and therefore an element $\beta - \alpha \equiv 0 \pmod{\mathfrak{B}}$, $\beta - \alpha \not\equiv 0 \pmod{\mathfrak{A}}$, of smaller length than β.

Now let a divisor or multiple chain

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_r, \ldots$$

be given; suppose the corresponding chain condition holds in $\mathfrak{R}$. If $\mathfrak{a}_{r1}, \ldots, \mathfrak{a}_{rk}$ are the ideals assigned to $\mathfrak{A}_r$, then the sequences

$$\mathfrak{a}_{1\lambda}, \mathfrak{a}_{2\lambda}, \ldots, \mathfrak{a}_{r\lambda}, \ldots$$

are divisor respectively multiple chains for $\lambda = 1, \ldots, k$. Hence by hypothesis there is an index μ such that the ideal $\mathfrak{a}_{\mu\lambda}$ is equal to all subsequent ideals for every λ. But then, by what was just proved, the module $\mathfrak{A}_\mu$ is equal to all subsequent modules; thus the chain conditions are transferred.

This immediately gives the following:

Consequence of the module theorem. *If in $\mathfrak{R}$ the multiple-chain condition holds modulo every ideal different from the zero ideal, then in M the multiple-chain condition holds modulo every module $\mathfrak{C}$ whose assigned ideals $\mathfrak{c}_1, \ldots, \mathfrak{c}_k$ are all different from the zero ideal.* Under these hypotheses the multiple chains $\mathfrak{a}_{1\lambda}, \ldots, \mathfrak{a}_{r\lambda}, \ldots$ terminate after finitely many steps.

Additional remark. If $\mathfrak{R}$ is a ring without identity element, then the divisor-chain condition and the multiple-chain condition modulo ideals different from the zero ideal are still transferred. Namely, instead of $\mathfrak{A}$ one considers the system $\overline{\mathfrak{A}}$ of all elements of the form

$$a_1\xi_1 + \cdots + a_k\xi_k + n_1\xi_{k+1} + \cdots + n_k\xi_{2k},$$

which again passes into $\mathfrak{A}$ when $\xi_{k+\lambda}$ is replaced by ξ_λ. To this $\overline{\mathfrak{A}}$ one can assign, correspondingly as above, $2k$ ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_k, \mathfrak{n}_1, \ldots, \mathfrak{n}_k$, where the $\mathfrak{a}_\lambda$ are ideals from $\mathfrak{R}$ and the $\mathfrak{n}_\lambda$ are ideals of the rational integers. Since for the $\mathfrak{n}_\lambda$ both the divisor-chain condition and the multiple-chain condition modulo every nonzero ideal are satisfied, the proof for the divisor-chain condition remains valid for $\overline{\mathfrak{A}}$ and hence for $\mathfrak{A}$; for the multiple-chain condition, however, one must require that the $2k$ ideals assigned to $\mathfrak{C}$ respectively $\overline{\mathfrak{C}}$ are all different from the zero ideal.

ğ3. Passage to finite extension fields

For the classification of number fields and function fields it remains to show how the axioms I through V formulated in the introduction are transferred on passing to finite extension fields.

1. *Suppose that in $\mathfrak{R}$ all axioms I through V are satisfied except axiom II – the multiple-chain condition. Let $\mathfrak{K}$ denote the quotient field of $\mathfrak{R}$, and let $\mathfrak{L}$ be a finite extension field of the first kind over $\mathfrak{K}$.*[14] *Then in the system $\mathfrak{S}$ of all elements of $\mathfrak{L}$ integral with respect to $\mathfrak{R}$ the same axioms are satisfied, and in every order from $\mathfrak{S}$ all these axioms are still satisfied with the exception of integral closedness.*

By ğ1, 3, $\mathfrak{S}$ forms a ring for which axioms III and IV – existence of the identity element and absence of zero divisors – are satisfied. By the conclusion of ğ1, 4, $\mathfrak{S}$ is integrally closed in $\mathfrak{L}$; at the same time $\mathfrak{L}$ becomes the quotient field of $\mathfrak{S}$, since every element of $\mathfrak{L}$ is carried into an element of $\mathfrak{S}$ by multiplication with a suitable element of $\mathfrak{R}$. Thus axiom V is satisfied.

The proof of I follows by familiar arguments. As an extension of the first kind, $\mathfrak{L}$ is obtained by adjoining to $\mathfrak{K}$ a single element α, which by the preceding may be assumed integral with respect to $\mathfrak{R}$. Besides α, the conjugate quantities $\alpha', \alpha'', \ldots$ contained in the Galois field of $\mathfrak{L}$ over $\mathfrak{K}$ are also integral; hence so is their product of differences, and so is the square D of this product of differences. Since $\alpha, \alpha', \ldots$ are all distinct, D is a nonzero quantity of $\mathfrak{K}$, hence, by the integral closedness of $\mathfrak{R}$ in $\mathfrak{K}$, an element of $\mathfrak{R}$. By the usual argument, because $\mathfrak{R}$ is integrally closed, $\mathfrak{S}$ is contained in the finite $\mathfrak{R}$-module domain M generated by the elements $\xi_i = \alpha^i/D$; for this one need only pass, in the representation of an element of $\mathfrak{S}$ by the ξ_i, to the conjugate elements and solve the resulting system of linear equations for the coefficients of the representation. By the module theorem of ğ2, the divisor-chain condition holds for all $\mathfrak{R}$-modules from M, hence in particular for all ideals of $\mathfrak{S}$. The divisor-chain condition likewise holds for the ideals of any order

[14] Following Steinitz, an algebraic extension field is called "of the first kind" if every element is a zero of a prime function which, in a suitable extension field, splits into pairwise distinct linear factors.

in $\mathfrak{S}$, since here too one is dealing with $\mathfrak{R}$-modules in M; for every order, moreover, axioms III and IV are satisfied.

2. *If all axioms I through V are satisfied in $\mathfrak{R}$, the same is true in $\mathfrak{S}$. In every order from $\mathfrak{S}$ all axioms still hold except integral closedness.*

In view of 1, it remains only to prove axiom II. By the corollary to the module theorem in ğ2 it is enough to prove the following. If a nonzero ideal of $\mathfrak{S}$ is regarded as an $\mathfrak{R}$-module $\mathfrak{C}$ in M, then the ideals $\mathfrak{c}_i$ of $\mathfrak{R}$ associated with $\mathfrak{C}$ are all different from the zero ideal. Now $\mathfrak{C}$ has the same finite linear rank over $\mathfrak{K}$ as M; for along with any element γ, $\mathfrak{C}$ contains also $\gamma\alpha^i$. Thus for each ξ_i there is an element $c_i \neq 0$ of $\mathfrak{R}$ such that $c_i\xi_i$ belongs to $\mathfrak{C}$; by the uniqueness of the representation by the ξ_i – where the index is to run only through the values less than the degree of the field – c_i belongs to $\mathfrak{c}_i$, and therefore $\mathfrak{c}_i$ is not the zero ideal. This argument remains valid for all orders of the same rank as M; for an order of smaller rank one passes to its quotient field, which as an intermediate field between $\mathfrak{K}$ and $\mathfrak{L}$ is also of the first kind, and whose degree over $\mathfrak{K}$ agrees with the linear rank of the order. The same argument is therefore preserved. Finally, it should be noted that an order in $\mathfrak{S}$ different from $\mathfrak{S}$ is never integrally closed: since every order also contains $\mathfrak{R}$, integral closedness would force it to contain $\mathfrak{S}$.

For the subordination of number fields and function fields, it is therefore enough to verify axioms I through V for the basic domains: the rational integers, polynomials in one indeterminate, and the functional domain of polynomials in several indeterminates.

3. *For the ring $\mathfrak{R}$ of rational integers, respectively of polynomials in one indeterminate with coefficients in a field, axioms I through V are satisfied.* Here I and II follow either from the fact that, modulo any nonzero number or any such polynomial in one indeterminate, there are only finitely many, respectively finitely many linearly independent, residue classes; or from the fact that every ideal is principal. For from this follows the unique decomposition of ideals as a product of powers of prime ideals, and hence a nonzero ideal is divisible by only finitely many ideals. Axioms III and IV are plainly satisfied, the latter as a consequence of the definition of equality. Integral closedness V follows from the fact that, by unique factorization of elements of $\mathfrak{R}$ into irreducibles up to units – divisors of one – every element of the quotient field not contained in $\mathfrak{R}$ can be written as a quotient of two relatively prime elements of $\mathfrak{R}$; hence no power of the numerator is divisible by the denominator. Such an element can therefore satisfy no equation characterizing it as integral with respect to $\mathfrak{R}$.

4. *Let $\mathfrak{R}$ now denote the ring of all polynomials in several indeterminates with coefficients in a field, or with rational integer coefficients.* Then axioms III, IV, V are satisfied as in 3, for here too the factorization of elements into irreducibles is unique up to units. The divisor-chain condition I is an immediate consequence of Hilbert's theorem on the existence of an ideal basis, whereas the multiple-chain condition II does not hold here.

However, by passing to the *functional domain*, which amounts to restricting to ideals of highest dimension, one can obtain the validity of axiom II as well; the validity of I can then be proved as in 3, without using Hilbert's theorem. Namely, adjoin to $\mathfrak{R}$ an indeterminate u and consider the ring $\mathfrak{R}^*$ of all polynomials in u with coefficients in $\mathfrak{R}$, equality being defined coefficientwise. As usual, call a polynomial in $\mathfrak{R}^*$ primitive (with respect to $\mathfrak{R}$) if the greatest common divisor of its coefficients – divisor in the sense of a polynomial in $\mathfrak{R}$, not an ideal divisor – is a unit of $\mathfrak{R}$. Then every polynomial in $\mathfrak{R}^*$ is the product of an element of $\mathfrak{R}$ and a primitive polynomial in $\mathfrak{R}^*$, and the product of primitive polynomials in $\mathfrak{R}^*$ is again primitive.

The totality of elements of the quotient field of $\mathfrak{R}^*$ whose denominators are primitive polynomials in $\mathfrak{R}^*$ therefore forms a ring, the functional domain $\mathfrak{F}$ of $\mathfrak{R}$. In this functional domain $\mathfrak{F}$, the units are exactly those elements whose numerator and denominator are primitive polynomials in $\mathfrak{R}^*$; every element of $\mathfrak{F}$ is therefore uniquely representable as the product of an element of $\mathfrak{R}$ and a unit of $\mathfrak{F}$. Hence the factorization theorem for the elements of $\mathfrak{R}$ transfers to the elements of $\mathfrak{F}$; for $\mathfrak{F}$, therefore, in addition to axioms III and IV, axiom V is also satisfied as in 3.

Moreover, in $\mathfrak{F}$ every ideal is principal. For together with any element of $\mathfrak{F}$ an ideal contains also the element of $\mathfrak{R}$ obtained from it by multiplying by a unit; and together with any two elements of $\mathfrak{R}$ it contains their greatest common divisor. Indeed, with $f(x) = t(x)\overline{f}(x)$ and $g(x) = t(x)\overline{g}(x)$ it also contains $t(x)(\overline{f}(x)+u\overline{g}(x))$, and hence $t(x)$, if $\overline{f}$ and $\overline{g}$ are relatively prime and their linear combination is consequently a unit. Thus, starting from an arbitrary element $f(x)$ of the ideal, if there is in the ideal an element $g(x)$ not divisible by it, then the greatest common divisor $t(x)$ also belongs to the ideal and is a proper divisor of $f(x)$. Repeating this finitely many times leads to a basis element of the ideal, and so the ideal is recognized as principal. Thus in $\mathfrak{F}$ the unique decomposition of ideals as products of powers of prime ideals holds, corresponding to the factorization of the elements of $\mathfrak{R}$; as in 3, it follows that axioms I and II are satisfied.

The extension fields of the quotient field of $\mathfrak{F}$ that come into consideration here are only those that can be generated by adjoining an element of $\mathfrak{S}$.[15] Taking 1 and 2 into account, this establishes the validity of axioms I through V for number fields and function fields.

ğ 4. Isomorphism theorems. Direct sums

In what follows only the ring property, respectively the module property, is assumed; no further axiom is presupposed.

1. If M and $\overline{M}$ are module domains with respect to $\mathfrak{R}$ (ğ2), M is called homomorphic to $\overline{M}$ (more precisely, module-homomorphic), $M \sim \overline{M}$, if to every element of M there corresponds one and only one element of $\overline{M}$, in such a way that $\overline{M}$ is exhausted;[16] and if, under this correspondence, difference and multiplication by the same element of $\mathfrak{R}$ correspond. Thus from $\beta \sim \overline{\beta}$ and $\gamma \sim \overline{\gamma}$ it always follows that $(\beta - \gamma) \sim (\overline{\beta} - \overline{\gamma})$ and $r\beta \sim r\overline{\beta}$.

An $\mathfrak{R}$-module $\mathfrak{B}$ in M therefore corresponds homomorphically to an $\mathfrak{R}$-module $\overline{\mathfrak{B}}$ in $\overline{M}$; and the totality $\mathfrak{C}^*$ of elements in M corresponding to elements of an $\mathfrak{R}$-module $\overline{\mathfrak{C}}$ in $\overline{M}$ forms an $\mathfrak{R}$-module in M uniquely determined by $\overline{\mathfrak{C}}$, the module $\mathfrak{C}^*$ associated with $\overline{\mathfrak{C}}$, with $\mathfrak{C}^* \sim \overline{\mathfrak{C}}$. If in particular $\mathfrak{A}$ is the module in M associated with the zero element of $\overline{M}$, then $\mathfrak{C}^*$ is a divisor of $\mathfrak{A}$ and splits into classes of elements of M congruent modulo $\mathfrak{A}$, in such a way that these classes correspond one-to-one to the elements of $\overline{\mathfrak{C}}$. If one passes from $\mathfrak{B}$ in M to $\overline{\mathfrak{B}}$ in $\overline{M}$ and then back to $\mathfrak{B}^*$, one obtains $\mathfrak{B}^* = (\mathfrak{B}, \mathfrak{A})$, the greatest common divisor of $\mathfrak{B}$ and $\mathfrak{A}$; thus $\mathfrak{B}^* = \mathfrak{B}$ if $\mathfrak{B}$ is a divisor of $\mathfrak{A}$.

If the correspondence between the elements of M and $\overline{M}$ is reversible one-to-one, the domains are called isomorphic (more precisely, module-isomorphic), $M \simeq \overline{M}$.

If $\mathfrak{A}$ is an arbitrary $\mathfrak{R}$-module in M, then a module domain $\overline{M}$ homomorphic to M arises – the residue-class module $M \mid \mathfrak{A}$ – by taking congruence modulo $\mathfrak{A}$ as the new equality relation. To every element of M there are associated all and only the elements equal to it in $\overline{M}$. Passing in $\overline{M}$ from the equality definition to identity means collecting all equal elements in $\overline{M}$ into one class – a residue class – and taking these residue classes as the new elements of $\overline{M}$.[17]

Every homomorphism is produced by passage to a residue-class module; for if $M \sim \overline{M}$ and if $\mathfrak{A}$ is the module associated with the zero element of $\overline{M}$, then, as shown above, $\overline{M}$ is isomorphic to the residue-class module $M \mid \mathfrak{A}$.

2. **First isomorphism theorem.** *Let $\overline{M}$ be the residue-class module $M \mid \mathfrak{A}$, and let $\mathfrak{C}$ be a divisor of $\mathfrak{A}$. Then there is an isomorphism $\overline{M} \mid \overline{\mathfrak{C}} \simeq M \mid \mathfrak{C}$.* Indeed, congruence modulo $\mathfrak{A}$ is at the same time congruence modulo $\mathfrak{C}$; elements equal modulo $\mathfrak{A}$ remain equal modulo $\mathfrak{C}$. Thus one may form the residue-class module $M \mid \mathfrak{C}$ – that is, equality modulo $\mathfrak{C}$ – by first identifying elements modulo $\mathfrak{A}$, passing to $\overline{M}$, and then collecting in $\overline{M}$ those elements that are equal modulo $\mathfrak{C}$; this is the same as identifying modulo $\overline{\mathfrak{C}}$ in $\overline{M}$, i.e. forming $\overline{M} \mid \overline{\mathfrak{C}}$.

Second isomorphism theorem. *If $\mathfrak{B}$ and $\mathfrak{A}$ are modules in M, then $(\mathfrak{B}, \mathfrak{A}) \mid \mathfrak{A} \simeq \mathfrak{B} \mid [\mathfrak{B}, \mathfrak{A}]$.* For by 1, $\mathfrak{B}$ becomes homomorphic to $\overline{\mathfrak{B}}$ when $(\mathfrak{B}, \mathfrak{A}) \mid \mathfrak{A}$ is put equal to $\overline{\mathfrak{B}}$; and since precisely the elements of $[\mathfrak{B}, \mathfrak{A}]$ correspond to the zero element in $\overline{\mathfrak{B}}$, the asserted isomorphism again follows from 1.

3. If $\mathfrak{R}$ and $\overline{\mathfrak{R}}$ are (commutative) rings, $\mathfrak{R}$ is called homomorphic to $\overline{\mathfrak{R}}$ (more precisely, ring-homomorphic), $\mathfrak{R} \sim \overline{\mathfrak{R}}$, if to each element of $\mathfrak{R}$ there corresponds one and only one element of $\overline{\mathfrak{R}}$ in such a way that $\overline{\mathfrak{R}}$ is exhausted, and if differences and products correspond under this assignment. If the correspondence of elements is reversible one-to-one, the rings are called isomorphic (more precisely, ring-isomorphic), $\mathfrak{R} \simeq \overline{\mathfrak{R}}$.

All the arguments in 1 and 2 remain valid when the modules are replaced by ideals in $\mathfrak{R}$,[18] and when module-homomorphism and module-isomorphism are replaced by ring-homomorphism and ring-isomorphism. In particular, if $\mathfrak{c}$ is a divisor of $\mathfrak{a}$, the residue-class ring $\mathfrak{c} \mid \mathfrak{a}$ is obtained by introducing congruence modulo $\mathfrak{a}$ as the new equality relation; here one must note that products of residue classes are now also defined.

Thus $\mathfrak{c}$ is homomorphic to $\mathfrak{c} \mid \mathfrak{a}$; every homomorphism is produced in this way, and the isomorphism theorems hold as in 2:

First isomorphism theorem. If $\overline{\mathfrak{R}}$ denotes the residue-class ring $\mathfrak{R} \mid \mathfrak{a}$, and $\mathfrak{c}$ is a divisor of $\mathfrak{a}$, then $\overline{\mathfrak{R}} \mid \overline{\mathfrak{c}} \simeq \mathfrak{R} \mid \mathfrak{c}$ in the sense of ring isomorphism.

Second isomorphism theorem. If $\mathfrak{b}$ and $\mathfrak{a}$ are ideals of $\mathfrak{R}$, then the ring-isomorphism $(\mathfrak{b}, \mathfrak{a}) \mid \mathfrak{a} \simeq \mathfrak{b} \mid$

[15] The system of quantities integral with respect to $\mathfrak{F}$ in these extension fields is also obtained by passing from $\mathfrak{S}$ to a corresponding functional domain, just as one passes from $\mathfrak{R}$ to $\mathfrak{F}$. Compare J. König, *Algebraische GröSSen*, Leipzig 1903, pp. 468/69.

[16] In the sense of the definition of equality prevailing in $\overline{M}$; compare note 9.

[17] Compare note 9.

[18] For noncommutative rings, two-sided ideals must be used.

$[\mathfrak{b}, \mathfrak{a}]$ holds.[19]

4. I now collect the calculation rules for coprime ideals[20] from which the theorems on direct sums in 5 follow. In the commutative ring $\mathfrak{R}$, assume the existence of a multiplicative identity element e. Thus $\mathfrak{a} = \mathfrak{o}\mathfrak{a}$ for every ideal of $\mathfrak{R}$, where $\mathfrak{o}$ denotes the unit ideal. Two ideals $\mathfrak{a}, \mathfrak{b}$ are called coprime if their greatest common divisor $(\mathfrak{a}, \mathfrak{b})$ is $\mathfrak{o}$.

4α. If $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$, *then* $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = (\mathfrak{a}, \mathfrak{c})$. For $(\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}, \mathfrak{b})(\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}^2, \mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c})$ is divisible by $(\mathfrak{a}, \mathfrak{b}\mathfrak{c})$ and conversely. Hence:

4β. From $\mathfrak{c}\mathfrak{b} \equiv 0 \pmod{\mathfrak{a}}$ *and* $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ *it follows that* $\mathfrak{c} \equiv 0 \pmod{\mathfrak{a}}$. Indeed, $\mathfrak{c}\mathfrak{b} \equiv 0 \pmod{\mathfrak{a}}$ is equivalent to $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{a}$; because $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$, this also gives $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{a}$, or $\mathfrak{c} \equiv 0 \pmod{\mathfrak{a}}$. Furthermore:

4γ. If each of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *is coprime to each of the ideals* $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$, *then the product of the* $\mathfrak{a}_i$ *is coprime to the product of the* $\mathfrak{b}_i$. For from $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ and $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{o}$ one obtains $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{o}$, and finite repetition gives the assertion.

From 4α and 4γ follows:

4δ. If the ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ *are pairwise coprime, i.e.* $(\mathfrak{b}_i, \mathfrak{b}_k) = \mathfrak{o}$ *for* $i \neq k$, *then their least common multiple equals their product.* Let $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ and $\mathfrak{v} = [\mathfrak{a}, \mathfrak{b}]$. Then $\mathfrak{v} = \mathfrak{o}\mathfrak{v} = (\mathfrak{a}\mathfrak{v}, \mathfrak{b}\mathfrak{v}) \equiv 0 \pmod{(\mathfrak{a}, \mathfrak{b})}$; since $\mathfrak{a}\mathfrak{b} \equiv 0 \pmod{\mathfrak{v}}$, it follows that $\mathfrak{v} = \mathfrak{a}\mathfrak{b}$. Finite repetition, using 4γ, gives the claim.

4ε. If the ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ *are pairwise coprime and* $\mathfrak{a}_i = [\mathfrak{b}_1, \ldots, \mathfrak{b}_{i-1}, \mathfrak{b}_{i+1}, \ldots, \mathfrak{b}_r] = \mathfrak{b}_1 \cdots \mathfrak{b}_{i-1}\mathfrak{b}_{i+1} \cdots \mathfrak{b}_r$, *then* $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{i-1}, \mathfrak{a}_{i+1}, \ldots, \mathfrak{a}_r) = \mathfrak{b}_i$, *and hence* $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) = \mathfrak{o}$. For by the distributive law $(\mathfrak{a}_1, \mathfrak{a}_2) = \mathfrak{b}_3 \cdots \mathfrak{b}_r(\mathfrak{b}_2, \mathfrak{b}_1) = \mathfrak{b}_3 \cdots \mathfrak{b}_r$; hence $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = \mathfrak{b}_4 \cdots \mathfrak{b}_r(\mathfrak{b}_3, \mathfrak{b}_1\mathfrak{b}_2) = \mathfrak{b}_4 \cdots \mathfrak{b}_r$, and finite repetition, after a suitable numbering, proves the assertion.

The ideal $\mathfrak{a}_i$ is called the complement of $\mathfrak{b}_i$ in the representation $\mathfrak{m} = [\mathfrak{b}_1, \ldots, \mathfrak{b}_r]$.

5. Again let the commutative ring $\mathfrak{R}$ have a multiplicative identity element. The ring $\mathfrak{R}$ is called the direct sum of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$, in symbols $\mathfrak{R} = \mathfrak{a}_1 + \mathfrak{a}_2 + \cdots + \mathfrak{a}_r$, if each element c of $\mathfrak{R}$ can be represented in one and only one way in the form $c = a_1 + a_2 + \cdots + a_r$, with a_i an element of $\mathfrak{a}_i$.

If the zero ideal is the least common multiple of the pairwise coprime ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$, *and if* $\mathfrak{a}_i$ *is the complement of* $\mathfrak{b}_i$, *then* $\mathfrak{R}$ *is the direct sum of the ideals* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$. Since $\mathfrak{o} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$, every element of $\mathfrak{R}$ admits at least one additive representation by the $\mathfrak{a}_i$. Since $[\mathfrak{a}_i, \mathfrak{b}_i] = (0)$, this representation is unique: from $0 = a_1 + a_2 + \cdots + a_r = a_i + b_i$ one obtains $a_i = 0$. By the second isomorphism theorem the $\mathfrak{a}_i$ are isomorphic to the residue-class rings $\mathfrak{R} \mid \mathfrak{b}_i$. The orthogonality relations $\mathfrak{a}_i\mathfrak{a}_k = (0)$ for $i \neq k$, and $\mathfrak{a}_i^2 = \mathfrak{a}_i$, hold; the latter because $\mathfrak{a}_i = \mathfrak{o}\mathfrak{a}_i$.

Conversely, if there is a representation of $\mathfrak{R}$ *as a direct sum,* $\mathfrak{R} = \mathfrak{a}_1 + \mathfrak{a}_2 + \cdots + \mathfrak{a}_r$, *and if one sets* $\mathfrak{b}_i = (\mathfrak{a}_1, \ldots, \mathfrak{a}_{i-1}, \mathfrak{a}_{i+1}, \ldots, \mathfrak{a}_r) = \mathfrak{a}_1 + \cdots + \mathfrak{a}_{i-1} + \mathfrak{a}_{i+1} + \cdots + \mathfrak{a}_r$, *then the* $\mathfrak{b}_i$ *are pairwise coprime and their least common multiple is the zero ideal.* For from $\mathfrak{o} = (\mathfrak{a}_i, \mathfrak{b}_i)$ follows $\mathfrak{o} = (\mathfrak{b}_k, \mathfrak{b}_i)$ for $k \neq i$, since $\mathfrak{b}_k$ is a divisor of $\mathfrak{a}_i$. If, moreover, c is divisible by all $\mathfrak{b}_i$, then

$$c = a_2^{(1)} + \cdots + a_r^{(1)} = a_1^{(2)} + a_3^{(2)} + \cdots + a_r^{(2)} = \cdots = a_1^{(r)} + \cdots + a_{r-1}^{(r)},$$

where in each case $a_i^{(\lambda)} \equiv 0 \pmod{\mathfrak{a}_i}$. By the uniqueness of the representation, since in each representation one component is zero, it follows that $0 = a_1^{(\lambda)}, \ldots, 0 = a_r^{(\lambda)}$ for every λ, and hence $c = 0$.[21]

ğ 5.
Prime Ideals and Primary Ideals.

Let $\mathfrak{R}$ again be a commutative ring for which no further axiom, not even the existence of an identity element, is assumed. We collect the basic facts about prime ideals and primary ideals.[22]

1. An ideal $\mathfrak{p}$ of $\mathfrak{R}$ is called a *weak prime ideal* if the residue-class ring $\mathfrak{R} \mid \mathfrak{p}$ is a ring without zero divisors; that is, if from $a \not\equiv 0(\mathfrak{p})$ and $b \not\equiv 0(\mathfrak{p})$ it always follows that $ab \not\equiv 0(\mathfrak{p})$. An ideal $\mathfrak{p}^*$ of $\mathfrak{R}$ is called a *strong prime ideal* if the residue-class ring $\mathfrak{R} \mid \mathfrak{p}^*$ is a ring without zero-divisor ideals; that is, if from $\mathfrak{a} \not\equiv 0(\mathfrak{p}^*)$ and $\mathfrak{b} \not\equiv 0(\mathfrak{p}^*)$ it always follows that $\mathfrak{a}\mathfrak{b} \not\equiv 0(\mathfrak{p}^*)$.

[19] These isomorphism theorems, familiar from group theory, occur for modules in a somewhat more special form first in Dedekind (compare 3rd ed., p. 484). The above form for ideals occurs in Masazo Sono, *On Congruences. I, II, III, IV*, Memoirs of the College of Science, Kyoto Imperial University, 2 (1917), 3 (1918, 1919), compare 2, p. 215. In each case only the second isomorphism theorem is stated explicitly.

[20] In the form going back to Dedekind (4th ed., ğ178, III to VIII). The calculation with the identity element that appears throughout more recent accounts is much more cumbersome.

[21] The theorems given under 5 are special cases of a general theorem on the connection between direct sum and direct intersection. Compare H. Prüfer, Theorie der Abelschen Gruppen I, Math. Zeitschr. 20 (1924), pp. 165–187, ğ6. The arguments given there remain valid also for such a general formulation of the concept of group that modules and ideals fall under it as special cases.

[22] In *Idealtheorie*, ğ4, axiom I, the divisor-chain condition, is assumed; therefore it is not made sharp there which properties of prime and primary ideals are independent of this axiom.

Every strong prime ideal is at the same time a weak prime ideal, as the specialization of $\mathfrak{a}, \mathfrak{b}$ to principal ideals shows. Conversely, *every weak prime ideal is also a strong prime ideal*; one can therefore simply speak of prime ideals. For let $\mathfrak{p}$ be a weak prime ideal; let $\mathfrak{a} \not\equiv 0(\mathfrak{p})$ and $\mathfrak{b} \not\equiv 0(\mathfrak{p})$; choose elements a and b in $\mathfrak{a}$ and $\mathfrak{b}$ such that $a \not\equiv 0(\mathfrak{p})$ and $b \not\equiv 0(\mathfrak{p})$. Then $ab \not\equiv 0(\mathfrak{p})$, hence $\mathfrak{ab} \not\equiv 0(\mathfrak{p})$, so $\mathfrak{p}$ is also a strong prime ideal.

2. An ideal $\mathfrak{q}$ of $\mathfrak{R}$ is called a *weak primary ideal* if in the residue-class ring $\mathfrak{R} \mid \mathfrak{q}$ some power of every zero divisor vanishes; equivalently, if from $a \not\equiv 0(\mathfrak{q})$ and $b^x \not\equiv 0(\mathfrak{q})$ for every x it always follows that $ab \not\equiv 0(\mathfrak{q})$. The system $\mathfrak{p}$ of all elements of $\mathfrak{R}$ that become zero divisors in $\mathfrak{R} \mid \mathfrak{q}$ forms an ideal, indeed a prime ideal; it is a divisor of $\mathfrak{q}$ and is called the associated prime ideal. For along with a, also ra is a zero divisor; along with a and b, so is $a - b$, since with a^x and b^λ the element $(a-b)^{x+\lambda}$ is always divisible by $\mathfrak{q}$. If furthermore a is not a zero divisor, then by definition no power of a is a zero divisor; from $a \not\equiv 0(\mathfrak{p})$ and $b \not\equiv 0(\mathfrak{p})$ follows $a^x b^x = (ab)^x \not\equiv 0(\mathfrak{q})$, hence $ab \not\equiv 0(\mathfrak{p})$.

An ideal $\mathfrak{q}^*$ of $\mathfrak{R}$ is called a *strong primary ideal* if in the residue-class ring $\mathfrak{R} \mid \mathfrak{q}^*$ some power of every zero-divisor ideal vanishes; that is, if from $\mathfrak{a} \not\equiv 0(\mathfrak{q}^*)$ and $\mathfrak{b}^x \not\equiv 0(\mathfrak{q}^*)$ for every x it always follows that $\mathfrak{ab} \not\equiv 0(\mathfrak{q}^*)$. As for weak primary ideals one shows: the greatest common divisor of all ideals of $\mathfrak{R}$ that become zero-divisor ideals in $\mathfrak{R} \mid \mathfrak{q}^*$ forms a prime ideal, a divisor of $\mathfrak{q}^*$, the associated prime ideal. Conversely, all primary ideals with the same associated prime ideal $\mathfrak{p}$ are said to belong to $\mathfrak{p}$.

Every strong primary ideal is at the same time a weak primary ideal, as the specialization of $\mathfrak{a}, \mathfrak{b}$ to principal ideals shows. In general, however, the converse is false.[23] *If, however, axiom I, the divisor-chain condition, is assumed in* $\mathfrak{R}$*, then every weak primary ideal is also a strong primary ideal;* one can therefore simply speak of primary ideals. Let $\mathfrak{q}$ be a weak primary ideal; suppose $\mathfrak{a} \not\equiv 0(\mathfrak{q})$ and $\mathfrak{b}^x \not\equiv 0(\mathfrak{q})$ for every x. Then there exist elements a of $\mathfrak{a}$ and b of $\mathfrak{b}$ such that $a \not\equiv 0(\mathfrak{q})$ and $b^x \not\equiv 0(\mathfrak{q})$ for every x; hence $ab \not\equiv 0(\mathfrak{q})$ and therefore $\mathfrak{ab} \not\equiv 0(\mathfrak{q})$. For if to every b in $\mathfrak{b}$ there were an exponent λ such that $b^\lambda \equiv 0(\mathfrak{q})$, then $\mathfrak{b}^{\lambda_1 + \cdots + \lambda_r} \equiv 0(\mathfrak{q})$, with $\lambda_1, \ldots, \lambda_r$ the exponents of the finitely many basis elements.[24] The same argument also shows that there is a smallest exponent ϱ such that $\mathfrak{p}^\varrho \equiv 0(\mathfrak{q})$, where $\mathfrak{p}$ is the associated prime ideal; ϱ is called the exponent of $\mathfrak{q}$.

3. In what follows the divisor-chain condition is again *not* assumed. The least common multiple $[\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$ of finitely many ideals is called a *shortest representation* if no $\mathfrak{a}_i$ is contained in the least common multiple of the remaining ideals, i.e. if no $\mathfrak{a}_i$ can be omitted.

The least common multiple of finitely many weak, respectively strong, primary ideals belonging to the same prime ideal $\mathfrak{p}$ *is again a weak primary ideal with* $\mathfrak{p}$ *as associated prime ideal. A shortest representation by finitely many weak, respectively strong, primary ideals belonging to distinct prime ideals is not a weak, respectively strong, primary ideal.* Let $\mathfrak{f} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$, and let $\mathfrak{p}$ be the associated prime ideal of the weak primary ideals $\mathfrak{q}_i$. Then $\mathfrak{p}$ also consists exactly of the elements of which some power is divisible by $\mathfrak{f}$. From $a \not\equiv 0(\mathfrak{f})$ and $b^x \not\equiv 0(\mathfrak{f})$ for every x it follows that $b \not\equiv 0(\mathfrak{p})$ and $a \not\equiv 0(\mathfrak{q}_i)$ for at least one index i; hence $ab \not\equiv 0(\mathfrak{q}_i)$, and therefore $ab \not\equiv 0(\mathfrak{f})$. If one replaces elements throughout by ideals, one can no longer infer $\mathfrak{b} \not\equiv 0(\mathfrak{p})$.

Now let $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ be a shortest representation by weak primary ideals with $\mathfrak{p}_i \neq \mathfrak{p}_k$ for $i \neq k$, and let $r \geq 2$. There is then at least one associated prime ideal, say $\mathfrak{p}_1$, which is not contained in any of the others; for every proper multiple-chain of the $\mathfrak{p}$'s must terminate after at most r steps. Hence there are elements a_i of $\mathfrak{p}_i$ such that $a_i^{\varrho_i} \equiv 0(\mathfrak{q}_i)$, while $a_2 \not\equiv 0(\mathfrak{p}_1), \ldots, a_r \not\equiv 0(\mathfrak{p}_1)$. If further $q_1 \not\equiv 0(\mathfrak{m})$ is an element of $\mathfrak{q}_1$, then $q_1 a_2^{\varrho_2} \cdots a_r^{\varrho_r} \equiv 0(\mathfrak{m})$, but no power of $a_2^{\varrho_2} \cdots a_r^{\varrho_r}$ is divisible by $\mathfrak{m}$, since otherwise divisibility by $\mathfrak{p}_1$ would follow. Thus $\mathfrak{m}$ is not a weak primary ideal. If elements are replaced throughout by ideals, that is q_1 by $\mathfrak{q}_1$ and a_i by $\mathfrak{a}_i [\not\equiv 0(\mathfrak{p}_1)$, but $\mathfrak{a}_i^{\varrho_i} \equiv 0(\mathfrak{q}_i)]$, the proof for strong primary ideals is obtained.[25]

4. *Module quotient and ideal quotient.* Let $\mathfrak{T}$ be an extension ring of $\mathfrak{R}$, and let $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ be $\mathfrak{R}$-modules in $\mathfrak{T}$. The quotient $\mathfrak{C} = \mathfrak{A} : \mathfrak{B}$ is defined as a module satisfying the conditions $\mathfrak{CB} \equiv 0(\mathfrak{A})$ and, if $\mathfrak{DB} \equiv 0(\mathfrak{A})$, then $\mathfrak{D} \equiv 0(\mathfrak{C})$; thus $\mathfrak{C}$ is the smallest module for which $\mathfrak{CB} \equiv 0(\mathfrak{A})$ holds. This determines the quotient uniquely as the greatest common divisor of all modules $\mathfrak{D}$ for which $\mathfrak{DB} \equiv 0(\mathfrak{A})$; such $\mathfrak{D}$ exist, since the zero module is certainly one of them.

From the definition it follows: if $\mathfrak{B}$ is a multiple of $\overline{\mathfrak{B}}$, then $\mathfrak{A} : \overline{\mathfrak{B}}$ is a multiple of $\mathfrak{A} : \mathfrak{B}$. If $\mathfrak{A}$ is a multiple

[23] This is shown by the following example communicated to me by R. Hölzer. Let $\mathfrak{R}$ be the polynomial domain in countably many indeterminates x_i with coefficients in a field, and let $\mathfrak{q} = (x_1^2, x_2^3, \ldots, x_\nu^{\nu+1}, \ldots, x_i x_k\, [i \neq k] \ldots)$. The zero divisors in the residue-class ring are exactly the polynomials divisible by $\mathfrak{p} = (x_1, x_2, \ldots, x_\nu, \ldots)$, and in each case a power of such a zero divisor is divisible by $\mathfrak{q}$; therefore $\mathfrak{q}$ is a weak primary ideal with associated prime ideal $\mathfrak{p}$. But $\mathfrak{q}$ is not a strong primary ideal: putting $\mathfrak{a} = (x_1, x_3, x_5, \ldots, x_{2\nu+1}, \ldots)$ and $\mathfrak{b} = (x_2, x_4, \ldots, x_{2\nu}, \ldots)$, one has $\mathfrak{ab} \equiv 0(\mathfrak{q})$, but no power of $\mathfrak{a}$ or $\mathfrak{b}$ is divisible by $\mathfrak{q}$.

[24] In order to infer the finite ideal basis from axiom I, a fixed well-ordering in $\mathfrak{R}$ must be used; compare ğ6.

[25] I owe this modification of my original proof, which makes the divisor-chain condition unnecessary, to B. L. van der Waerden.

of $\overline{\mathfrak{A}}$, then $\mathfrak{A} : \mathfrak{B}$ is a multiple of $\overline{\mathfrak{A}} : \mathfrak{B}$. Also

$$\mathfrak{A} : \mathfrak{B}\mathfrak{C} = (\mathfrak{A} : \mathfrak{B}) : \mathfrak{C} = (\mathfrak{A} : \mathfrak{C}) : \mathfrak{B}.$$

If the extension ring $\mathfrak{T}$ coincides with $\mathfrak{R}$, the module quotient becomes the ideal quotient $\mathfrak{a} : \mathfrak{b}$; hence the preceding rules also hold here. Since $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{a})$, one also has $\mathfrak{a} \equiv 0(\mathfrak{a} : \mathfrak{b})$.

5. *If* $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$, *then* $\mathfrak{b}$ *is called prime to* $\mathfrak{a}$. Thus an ideal $\mathfrak{b}$ is prime to $\mathfrak{a}$ if and only if $\mathfrak{d}\mathfrak{b} \equiv 0(\mathfrak{a})$ always implies $\mathfrak{d} \equiv 0(\mathfrak{a})$. From the calculation rules under 4 it follows: if $\mathfrak{b}$ and $\mathfrak{c}$ are prime to $\mathfrak{a}$, then so are their product and their least common multiple. If $\mathfrak{b}$ is prime to $\mathfrak{a}$ and $\mathfrak{a}$ is prime to $\mathfrak{b}$, then $\mathfrak{a}$ and $\mathfrak{b}$ are called mutually prime. From ğ4, 4β, it follows that coprime ideals are also mutually prime.

ğ 6.
Ideal theory under the assumption of the divisor-chain condition.

Let the basis be a commutative ring $\mathfrak{R}$ for which axiom I, the divisor-chain condition, is satisfied. In what follows assume also a fixed well-ordering of all elements of $\mathfrak{R}$. This also determines a well-ordering of all ideals of $\mathfrak{R}$. Indeed, the two assumptions imply at once that every ideal of $\mathfrak{R}$ possesses an ideal basis consisting of finitely many elements. Passing from the well-ordering of the elements of $\mathfrak{R}$ to a quasi-lexicographic well-ordering of all finite subsets of $\mathfrak{R}$, [26] and assigning to each ideal, as distinguished basis, the first among its possible bases in this well-ordering of finite subsets, one obtains a well-ordering of the ideals together with that of the finite subsets.

Theorem I. *Under the assumption of the divisor-chain condition, every ideal of* $\mathfrak{R}$ *admits a representation as the least common multiple of finitely many irreducible ideals, i.e. of ideals which cannot be represented as the least common multiple of two proper divisors.*

For the proof it is enough to show: if Theorem I is false for an ideal $\mathfrak{m}$, then $\mathfrak{m}$ possesses a proper divisor for which Theorem I is likewise false; from this one can construct, contrary to the divisor-chain condition, a divisor chain not terminating after finitely many steps. Indeed $\mathfrak{m}$ must be reducible, since otherwise $\mathfrak{m} = [\mathfrak{m}]$ would already give the desired representation. If $\mathfrak{m} = [\mathfrak{a}, \mathfrak{b}]$, Theorem I cannot hold for both $\mathfrak{a}$ and $\mathfrak{b}$ at the same time; otherwise the corresponding representation would follow for $\mathfrak{m}$. Hence there are proper divisors of $\mathfrak{m}$ for which Theorem I is false; let $\mathfrak{a}_1$ be the first of these in the well-ordering of ideals. Constructing in the same way, from $\mathfrak{a}_1$, a proper divisor $\mathfrak{a}_2$, and in general from $\mathfrak{a}_i$ a proper divisor $\mathfrak{a}_{i+1}$, one obtains a well-defined divisor chain which does not terminate, contradicting the assumption. [27]

Because the divisor-chain condition is assumed, ğ5, 2 permits us simply to speak of primary ideals. The connection between primary and irreducible ideals is the following.

Theorem II. *Under the assumption of the divisor-chain condition, every irreducible ideal is primary; equivalently, every non-primary ideal is reducible.*

Passing to a residue-class ring $\mathfrak{R} \mid \mathfrak{m}$ preserves the divisor-chain condition by homomorphism. The representation of $\mathfrak{m}$ as a least common multiple corresponds to the representation of the zero ideal; and by the first isomorphism theorem (ğ4, 3), primary divisors of $\mathfrak{m}$ correspond again to primary ideals in $\mathfrak{R} \mid \mathfrak{m}$ and conversely. Thus it is enough to consider the decomposition of the zero ideal in the residue-class ring. Since that ring is again a ring of the same generality, one may from the outset suppose the ideal to be decomposed to be the zero ideal of $\mathfrak{R}$.

Suppose then that the zero ideal of $\mathfrak{R}$ is not primary. There is at least one pair of ideals $\mathfrak{a}, \mathfrak{b}$ – and $\mathfrak{b}$ may be assumed principal – such that

$$\mathfrak{a} \neq (0), \qquad \mathfrak{b}^x \neq (0) \quad \text{for every } x, \qquad \text{but} \qquad \mathfrak{a}\mathfrak{b} = (0).$$

Form the chain of ideal quotients

$$\mathfrak{a}, \quad \mathfrak{a} : \mathfrak{b}, \quad \ldots, \quad \mathfrak{a} : \mathfrak{b}^\nu, \quad \ldots.$$

[26] This is to be understood as follows. Let the elements $a_1, \ldots, a_n$ of a finite subset $\mathfrak{A}_n$ be denoted so that the ordering of their indices agrees with the prescribed well-ordering in $\mathfrak{R}$. Every subset $\mathfrak{A}_n$ precedes one $\mathfrak{A}_m$ having $m > n$ elements. If $\mathfrak{A}_n$ and $\mathfrak{B}_n$ are subsets having the same number of elements, then $\mathfrak{A}_n$ is earlier than $\mathfrak{B}_n$ when the first element a_i differing from the corresponding b_i precedes b_i in the well-ordering of $\mathfrak{R}$. Thus every system of finite subsets has a first element $\mathfrak{A}_n$. Given a well-ordering of $\mathfrak{R}$, no further choice postulate is needed; in particular, if $\mathfrak{R}$ is countable, as in the case of an algebraic number field, no choice postulate is involved at all. The role of the choice postulate in ideal theory was mentioned, without further detail, in *Idealtheorie*, note 9.

[27] Theorem I plainly holds in the same way for module domains, if the divisor-chain condition is assumed for the system of all modules. Theorem I has a purely set-theoretic character—it is also the only theorem whose proof uses the well-ordering of the ideals. Independently of all operations, the following set-theoretic concepts are involved. In a set $\mathfrak{M}$, let a subset Σ of the power set—that is, a system of subsets—be distinguished. Assume Σ to be well-ordered; call its elements Σ-sets. Assume in Σ the chain condition: every chain of Σ-sets $A_1, A_2, \ldots, A_\nu, \ldots$ such that A_ν is a proper superset of $A_{\nu-1}$ terminates after finitely many steps. A Σ-set A is called reducible if it is the intersection of two Σ-sets which are both proper supersets of A, and irreducible otherwise. The preceding arguments then show that every Σ-set can be represented as the intersection of finitely many irreducible Σ-sets.

This chain terminates; let, for instance,

$$\mathfrak{t} = \mathfrak{a} : \mathfrak{b}^{m-1} = \mathfrak{a} : \mathfrak{b}^m = \cdots .$$

Thus $\mathfrak{t} = \mathfrak{t} : \mathfrak{b}$, or $\mathfrak{b}$ is prime to $\mathfrak{t}$. Further, $\mathfrak{t}$ is a divisor of $\mathfrak{a}$ different from the zero ideal, and $\mathfrak{b}^x$ is different from zero for every exponent x. It therefore suffices, for the proof of Theorem II, to establish

$$(0) = [\mathfrak{t}, \mathfrak{b}^{m+1}].$$

By definition,

$$\mathfrak{b}^{m-1}\mathfrak{t} \equiv 0 \pmod{\mathfrak{a}}, \qquad \text{hence} \qquad \mathfrak{b}^m\mathfrak{t} = (0),$$

so it remains only to show

$$\mathfrak{c} = [\mathfrak{t}, \mathfrak{b}^{m+1}] \equiv 0 \pmod{\mathfrak{b}^m\mathfrak{t}}.$$

This follows from the assumptions that $\mathfrak{b}$ is principal and prime to $\mathfrak{t}$. Every element c of $\mathfrak{c}$, because of its divisibility by $\mathfrak{b}^{m+1}$, has a representation – where n denotes an integer symbol –

$$c = kb^{m+1} + nb^{m+1} = rb^m,$$

where r is again an element of $\mathfrak{R}$. From $c \equiv 0 \pmod{\mathfrak{t}}$ follows $rb^m \equiv 0 \pmod{\mathfrak{t}}$, and hence $r \equiv 0 \pmod{\mathfrak{t}}$, since $\mathfrak{t} : \mathfrak{b} = \mathfrak{t}$. Therefore $c \equiv 0 \pmod{\mathfrak{t}\mathfrak{b}^m}$, and Theorem II is proved.

Theorem III. *Under the assumption of the divisor-chain condition, every ideal admits a shortest representation as the least common multiple of finitely many primary components belonging to distinct prime ideals, and hence greatest primary components*[28].

To obtain such a representation, replace, whenever possible, the representation by irreducible ideals furnished by Theorem I – hence, by Theorem II, by primary ideals – by a shortest representation. If the primary ideals belonging to the same prime ideal are collected together, ğ5, 3 gives the asserted representation. The primary components may be called greatest because the least common multiple of any of them is no longer primary.

ğ 7.
Ideal Theory under the Assumption of the Double-Chain Condition.

The simplifications, compared with the theory developed so far, rest on the auxiliary results given under 1 and 2.

1. *If, in a commutative ring without zero divisors, the multiple-chain condition is satisfied, then the ring is already a field.* It is to be shown that, for $a \neq 0$, the equation $ax = b$ always has a solution in the ring. That it can have at most one solution follows from the absence of zero divisors.

Let $\mathfrak{a}$ be the principal ideal generated by a. By assumption the sequence of powers terminates; let $\mathfrak{a}^m$ be equal to all following powers. If $\mathfrak{b}$ denotes the principal ideal generated by b, then

$$\mathfrak{a}^m\mathfrak{b} = \mathfrak{a}^{m+1}\mathfrak{b} \quad \text{with} \quad \mathfrak{a}^{m+1}\mathfrak{b} = (a^{m+1}b).$$

In particular the element $a^m b$ has a representation – again with n an integer symbol –

$$a^m b = ka^{m+1}b + na^{m+1}b = a^{m+1}c,$$

where c is an element of $\mathfrak{R}$. Since no zero divisors exist, this gives $b = ac$, proving that the ring is a field.

2. From 1 follows at once the auxiliary result: *If the multiple-chain condition is satisfied in a commutative ring, then a prime ideal has no proper divisor different from* $\mathfrak{o}$.

Likewise one obtains the supplement: *If only axiom II is satisfied, that is, the multiple-chain condition modulo every ideal different from the zero ideal, then every prime ideal different from the zero ideal has no proper divisor different from* $\mathfrak{o}$.

For the residue-class ring modulo a prime ideal $\mathfrak{p}$ is, by definition, a ring without zero divisors; since the multiple-chain condition is also preserved there by homomorphism, it is a field by 1. From the one-to-one

[28] The corresponding prime ideals and the isolated components are uniquely determined. Compare *Idealtheorie*, or W. Krull, "Ein neuer Beweis für die Hauptsätze der allgemeinen Idealtheorie," Math. Ann. 90 (1923), pp. 55–64. In ğ7 a direct proof of uniqueness is given for the simple special case occurring there. The primary ideals there recognized as unique are isolated components.

correspondence between the divisors of $\mathfrak{p}$ and the ideals in the residue-class ring, $\mathfrak{p}$ has no proper divisor other than $\mathfrak{o}$. [29]

Theorem IV. *If the double-chain condition is satisfied in a commutative ring, then in every shortest representation of an ideal the primary components not belonging to the unit ideal $\mathfrak{o}$ are uniquely determined.*

Supplement. Under the assumptions of axioms I and II, Theorem IV holds for every ideal different from the zero ideal.

Let

$$\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_1, \ldots, \mathfrak{q}_r] = [\overline{\mathfrak{q}}, \overline{\mathfrak{q}}_1, \ldots, \overline{\mathfrak{q}}_{\overline{r}}]$$

be shortest representations of $\mathfrak{m}$ by greatest primary components, with associated prime ideals $\mathfrak{o}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and, respectively, $\mathfrak{o}, \overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_{\overline{r}}$. The component $\mathfrak{q}$, respectively $\overline{\mathfrak{q}}$, is to be omitted when no primary ideal belonging to $\mathfrak{o}$ occurs. Since

$$\mathfrak{o}^{\varrho}\mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r} \equiv 0(\mathfrak{m}),$$

each $\overline{\mathfrak{p}}_i$ must be contained in some $\mathfrak{p}_i$ and hence, by the auxiliary result, must be identical with it. Conversely, each $\mathfrak{p}_k$ must coincide with some $\overline{\mathfrak{p}}_k$; thus the prime ideals different from $\mathfrak{o}$ agree, $\mathfrak{p}_\lambda = \overline{\mathfrak{p}}_\lambda$. Further, $\mathfrak{q}\mathfrak{q}_1 \cdots \mathfrak{q}_r \equiv 0(\overline{\mathfrak{q}}_\lambda)$, and hence $\mathfrak{q}_\lambda \equiv 0(\overline{\mathfrak{q}}_\lambda)$, because the remaining components are not divisible by $\mathfrak{p}_\lambda$ and therefore are prime to $\overline{\mathfrak{q}}_\lambda$. The converse congruence $\overline{\mathfrak{q}}_\lambda \equiv 0(\mathfrak{q}_\lambda)$ follows in the same way, proving the uniqueness of the primary components not belonging to $\mathfrak{o}$. Finally, if $\mathfrak{q}$ actually occurs, then $\overline{\mathfrak{q}}$ must also actually occur because the representations are shortest; this also proves the uniqueness of the associated prime ideals. The proof further shows that every representation containing no primary component belonging to $\mathfrak{o}$ is already shortest.

3. If to the double-chain condition one adds the existence of an identity element, Theorem IV sharpens to the following.

Theorem V. *In a commutative ring with identity in which the double-chain condition is satisfied, every ideal can be represented uniquely as a product of finitely many pairwise coprime primary ideals.*

Supplement. Under axioms I, II, III, Theorem V holds for every ideal different from the zero ideal.

Because an identity element exists, $\mathfrak{o}^2 = \mathfrak{o}$; hence every primary ideal belonging to $\mathfrak{o}$ is equal to $\mathfrak{o}$ and cannot occur in a shortest representation of an ideal different from $\mathfrak{o}$. Thus, by Theorem IV, the primary components are uniquely determined, and at the same time every representation becomes shortest after omitting $\mathfrak{o}$. By the auxiliary result under 2, two distinct prime ideals are always coprime; by the calculation rules of ğ4, 4, the same holds for their primary components. The least common multiple therefore becomes their product.

From the same assumptions there further follows the

Auxiliary result. *In a commutative ring with identity and the double-chain condition, the prime ideals prime to an ideal $\mathfrak{m}$ are exactly those, apart from the unit ideal, which are not contained in $\mathfrak{m}$. The notions prime and coprime coincide.*

Supplement. Under axioms I, II, III, the ideal $\mathfrak{m}$ must be assumed different from the zero ideal.

If $\mathfrak{p}$ is not contained in $\mathfrak{m}$, then it is different from all prime ideals belonging to $\mathfrak{m}$, and by the auxiliary result under 2 it is not divisible by any of them. Hence it is prime to each primary component and therefore to $\mathfrak{m}$; at the same time it is coprime to each component and hence to $\mathfrak{m}$.

If, however, $\mathfrak{p} \neq \mathfrak{o}$ is contained in $\mathfrak{m}$, then it must coincide with one of the associated prime ideals. Let it belong to the component $\mathfrak{q} = \mathfrak{q}_1$. Then $\mathfrak{q} : \mathfrak{p}$ is a proper divisor of $\mathfrak{q}$, since

$$\mathfrak{p}^{\varrho-1} \equiv 0(\mathfrak{q} : \mathfrak{p}), \qquad \mathfrak{p}^{\varrho-1} \not\equiv 0(\mathfrak{q}).$$

At the same time $\mathfrak{q} : \mathfrak{p}$, as a divisor of $\mathfrak{p}^{\varrho-1}$, is divisible only by the prime ideal $\mathfrak{p} \neq \mathfrak{o}$ and is therefore primary. By the uniqueness of the decomposition, the product

$$(\mathfrak{q} : \mathfrak{p})\mathfrak{q}_2 \cdots \mathfrak{q}_r,$$

which is divisible by $\mathfrak{m} : \mathfrak{p}$, is a proper divisor of $\mathfrak{m}$; hence $\mathfrak{p}$ is not prime to $\mathfrak{m}$.

Thus an ideal $\mathfrak{t} \neq \mathfrak{o}$ is prime to $\mathfrak{m}$ if and only if none of the prime ideals belonging to $\mathfrak{t}$ is contained in $\mathfrak{m}$; but in that case $\mathfrak{t}$ is also coprime to $\mathfrak{m}$. Conversely, coprime ideals are always mutually prime (ğ5, 5), so the two concepts coincide under these assumptions.

ğ 8.

Ideal theory under integral closedness in the quotient field.

[29] No identity element need exist in $\mathfrak{R}$, nor therefore in $\mathfrak{o}$, the ideal consisting of all elements of $\mathfrak{R}$, although an identity class exists in the residue-class ring by 1. The simplest example of this kind, in the weaker case of the supplement, is furnished by the system of all even integers.

The ideal theory developed so far is now to be sharpened to the usual one by adjoining the last two axioms.

1. *Auxiliary result.* Let $\mathfrak{R}$ be a commutative ring without zero divisors and with an identity element. If the divisor-chain condition is assumed in $\mathfrak{R}$ (axioms I, III, IV), then from $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$ and $\mathfrak{a} \neq (0)$ it follows that $\mathfrak{b} = \mathfrak{o}$. Hence

$$\mathfrak{c}^{\varrho} \neq \mathfrak{c}^{\varrho+1}$$

for all ideals different from the zero and unit ideals. [30] The proof is the same as for the auxiliary result ğ1, 3, since $\mathfrak{a}\mathfrak{b}$ may be regarded as a finite module over $\mathfrak{b}$. Let $\alpha_1, \ldots, \alpha_n$ be an ideal basis of $\mathfrak{a}$ existing by I. From $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$ one obtains the system

$$\alpha_i = b_{i1}\alpha_1 + \cdots + b_{in}\alpha_n, \qquad b_{ik} \equiv 0 \pmod{\mathfrak{b}}, \quad i = 1, \ldots, n.$$

Since $\mathfrak{R}$ has no zero divisors, the determinant $|b_{ik} - e_{ik}|$ vanishes; here $e_{ik} = 0$ for $i \neq k$ and $e_{ii} = e$. From the equation

$$e^n + b_1 e^{n-1} + \cdots + b_n = 0$$

with $b_i \equiv 0 \pmod{\mathfrak{b}}$ it follows that $e \equiv 0 \pmod{\mathfrak{b}}$ and therefore $\mathfrak{b} = \mathfrak{o}$.

2. It remains to show only that, after adjoining integral closedness in the quotient field (axiom V) to axioms I through IV, every primary ideal different from the zero ideal is a power of its associated prime ideal. The uniqueness of the resulting representation

$$\mathfrak{m} = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r}$$

for every ideal different from the zero ideal has already been proved by Theorem V and the auxiliary result under 1. At the same time it has been shown that these prime ideals have no proper divisor distinct from the unit ideal. The proof is first given for exponent two, using Dedekind's corollary II (ğ1, 4), and then in general by complete induction.

Auxiliary result. Under axioms I through V there are no primary ideals of exponent two other than $\mathfrak{q} = \mathfrak{p}^2$.

It is to be shown that from

$$\mathfrak{p}^2 \equiv 0 \pmod{\mathfrak{q}}, \qquad \mathfrak{q} \equiv 0 \pmod{\mathfrak{p}}, \qquad \mathfrak{q} \not\equiv 0 \pmod{\mathfrak{p}^2}$$

there necessarily follows $\mathfrak{q} = \mathfrak{p}$. Thus choose

$$c \equiv 0 \pmod{\mathfrak{q}}, \qquad \text{hence } c \equiv 0 \pmod{\mathfrak{p}}, \qquad \text{but } c \not\equiv 0 \pmod{\mathfrak{p}^2}.$$

From the auxiliary result ğ7, 3, it follows that $\mathfrak{o}c : \mathfrak{p}$ is a proper divisor of $\mathfrak{o}c$; hence there is an element b such that

$$b\mathfrak{p} \equiv 0 \pmod{\mathfrak{o}c} \equiv 0 \pmod{\mathfrak{q}}, \qquad \text{but } b \not\equiv 0 \pmod{\mathfrak{o}c}.$$

Thus $\gamma = b/c$ is not integral, that is, it belongs to the quotient field but not to $\mathfrak{R}$. We must prove $b \not\equiv 0 \pmod{\mathfrak{p}}$; then, since $\mathfrak{q}$ is primary and belongs to $\mathfrak{p}$, it follows that $\mathfrak{p} \equiv 0 \pmod{\mathfrak{q}}$.

By Dedekind's corollary II there exist elements m, n of $\mathfrak{R}$ such that

$$\gamma = b/c = m/n$$

and m^2/n is also not integral; that is,

$$bn = mc, \qquad m \not\equiv 0 \pmod{\mathfrak{o}n}, \qquad m^2 \not\equiv 0 \pmod{\mathfrak{o}n}.$$

Multiplying $b\mathfrak{p}$ by m gives

$$mb\mathfrak{p} \equiv 0 \pmod{\mathfrak{o}mc}, \qquad \text{hence} \qquad \equiv 0 \pmod{\mathfrak{o}nb}, \qquad \text{and therefore} \qquad m\mathfrak{p} \equiv 0 \pmod{\mathfrak{o}n}.$$

The last implication uses the fact that the ring has no zero divisors. Therefore $m \not\equiv 0 \pmod{\mathfrak{p}}$, because $m^2 \not\equiv 0 \pmod{\mathfrak{o}n}$ and $n \equiv 0 \pmod{\mathfrak{p}}$; the latter again follows from the auxiliary result ğ7, 3, since $\mathfrak{o}n : \mathfrak{p}$ is a proper divisor of $\mathfrak{o}n$ because $m \not\equiv 0 \pmod{\mathfrak{o}n}$. The relations

$$m \not\equiv 0 \pmod{\mathfrak{p}}, \qquad n \equiv 0 \pmod{\mathfrak{p}}, \qquad c \equiv 0 \pmod{\mathfrak{p}}, \qquad c \not\equiv 0 \pmod{\mathfrak{p}^2}, \qquad bn = mc$$

[30] On the other hand, under the same assumptions one cannot infer $\mathfrak{b} = \mathfrak{c}$ from $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. For example, let $\mathfrak{R}$ be the polynomial domain in x, y over a field, with $\mathfrak{a} = (x, y)$, $\mathfrak{b} = (x^2, xy, y^2)$, $\mathfrak{c} = (x^2, y^2)$. Then $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c} = \mathfrak{a}^3$, but $\mathfrak{b} \neq \mathfrak{c}$.

now imply $b \not\equiv 0 \pmod{\mathfrak{p}}$. For, since $\mathfrak{p}^2$ is primary, one first gets $mc \not\equiv 0 \pmod{\mathfrak{p}^2}$, and then $b \not\equiv 0 \pmod{\mathfrak{p}}$ from $bn = mc$. This proves the auxiliary result.

3. *Auxiliary result. Under axioms I through V there are no primary ideals of exponent ϱ other than $\mathfrak{q} = \mathfrak{p}^\varrho$.*

This follows from the auxiliary result under 2 without further use of the axioms.[31] First one proves:

$$\text{if } c \equiv 0 \pmod{\mathfrak{p}}, \quad c \not\equiv 0 \pmod{\mathfrak{p}^2}, \quad \text{then} \quad \mathfrak{p}^\sigma = (\mathfrak{o}c^\sigma, \mathfrak{p}^{\sigma+1})$$

for every σ. By the result under 2, $\mathfrak{p} = (\mathfrak{o}c, \mathfrak{p}^2)$. Assuming

$$\mathfrak{p}^{\sigma-1} = (\mathfrak{o}c^{\sigma-1}, \mathfrak{p}^\sigma),$$

multiplication by $\mathfrak{p}$ and the distributive law give

$$\mathfrak{p}^\sigma = (\mathfrak{p}c^{\sigma-1}, \mathfrak{p}^{\sigma+1}) = (\mathfrak{o}c^\sigma, \mathfrak{p}^2c^{\sigma-1}, \mathfrak{p}^{\sigma+1}) = (\mathfrak{o}c^\sigma, \mathfrak{p}^{\sigma+1}).$$

The desired result may be put in the following second form: if

$$\mathfrak{q} \equiv 0 \pmod{\mathfrak{p}^\sigma}, \qquad \mathfrak{q} \not\equiv 0 \pmod{\mathfrak{p}^{\sigma+1}}, \qquad \mathfrak{p}^{\sigma+\lambda} \equiv 0 \pmod{\mathfrak{q}}, \quad \lambda \geq 1,$$

then already $\mathfrak{p}^{\sigma+\lambda-1} \equiv 0 \pmod{\mathfrak{q}}$. Indeed, since $\mathfrak{q} \equiv 0 \pmod{\mathfrak{p}}$ but $\mathfrak{q} \not\equiv 0 \pmod{\mathfrak{p}^{\varrho+1}}$, such an exponent $\sigma \geq 1$ exists for every primary ideal; the latter condition follows from $\mathfrak{p}^\varrho \equiv 0 \pmod{\mathfrak{q}}$ and $\mathfrak{p}^\varrho \neq \mathfrak{p}^{\varrho+1}$ by the result under 1. Repeated application of the second form gives $\mathfrak{p}^\sigma \equiv 0 \pmod{\mathfrak{q}}$ and hence $\mathfrak{q} = \mathfrak{p}^\sigma$.

From the assumption of the second form and from the representation of $\mathfrak{p}^\sigma$, each element q of $\mathfrak{q}$ satisfies

$$q \equiv bc^\sigma \pmod{\mathfrak{p}^{\sigma+1}}, \qquad b \not\equiv 0 \pmod{\mathfrak{p}}, \quad \text{or} \quad bc^\sigma \equiv 0 \pmod{(\mathfrak{q}, \mathfrak{p}^{\sigma+1})}.$$

Since $(\mathfrak{q}, \mathfrak{p}^{\sigma+1})$ is primary, it follows that

$$c^\sigma \equiv 0 \pmod{(\mathfrak{q}, \mathfrak{p}^{\sigma+1})}, \quad \text{or} \quad c^{\sigma+\lambda-1} \equiv 0 \pmod{(\mathfrak{q}, \mathfrak{p}^{\sigma+\lambda})},$$

and hence $\mathfrak{p}^{\sigma+\lambda-1} \equiv 0 \pmod{\mathfrak{q}}$.

4. Summarizing, one obtains:

Theorem VI. *If axioms I through V hold in a commutative ring, then every ideal different from the zero and unit ideals can be represented uniquely as a product of powers of finitely many prime ideals different from the zero and unit ideals. These prime ideals have no proper divisor different from the unit ideal.*

ğ 9.
The Axioms as Consequences of the Assumed Decomposition.

Conversely, in order to infer the axioms from the existence of the usual ideal decomposition — which by Theorem VI follows from axioms I through V — the decomposition must be assumed in the following form.

Assumption. *In the commutative ring $\mathfrak{R}$, every ideal not generated by the zero or the unit element is representable uniquely as a product of powers of prime ideals. These prime ideals are simple ideals not generated by the unit element — i.e. they have no proper divisor different from $\mathfrak{o}$; conversely all simple ideals are prime ideals. The uniqueness is to hold in the sharp form that*

$$\mathfrak{a}^\varrho \neq \mathfrak{a}^{\varrho+1}$$

for every ideal not generated by the zero or by the unit element.

The existence of an identity element is not assumed here. If no identity element exists, the condition "not generated by the unit element" is no restriction.

1. Proof of axiom III (existence of the identity element). Suppose axiom III is not satisfied. It is to be shown that $\mathfrak{o}^2$ becomes a simple ideal without being prime, contrary to the assumption. By the sharp uniqueness assumption, $\mathfrak{o} \neq \mathfrak{o}^2$; hence $\mathfrak{o} \not\equiv 0(\mathfrak{o}^2)$, but $\mathfrak{o}^2 \equiv 0(\mathfrak{o}^2)$, and so $\mathfrak{o}^2$ is not prime. It is, however, simple: it cannot be divisible by any prime ideal different from $\mathfrak{o}$, and by the assumed product representation it has no divisors except $\mathfrak{o}$ and $\mathfrak{o}^2$.

[31] The proof of auxiliary result 3 under the assumption of auxiliary result 2 is found in Masazo Sono, *On Congruences II*, ğğ9 and 10. Compare note 19.

2. Proof of axiom IV (ring without zero divisors). If a is a zero divisor, say $ab = 0$ with $a \neq 0$ and $b \neq 0$, then multiplication of the product representations of the principal ideals generated by a and b gives

$$(0) = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_k^{\varrho_k},$$

where the $\mathfrak{p}_i$ are different from the zero and unit ideals, the latter because the identity element has already been proved to exist. Take the representation to be shortest, in the sense that deleting any factor yields a proper divisor of the zero ideal; this need not be automatic, since no uniqueness assumption has been made about the zero ideal. If only one prime ideal occurs, then

$$(0) = \mathfrak{p}^{\varrho} = \mathfrak{p}^{\varrho+1},$$

contrary to the sharp uniqueness demand. If more than one prime ideal occurs, then

$$\mathfrak{p}_1^{\varrho_1+1} = (\mathfrak{p}_1^{\varrho_1+1}, \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_k^{\varrho_k}) = \mathfrak{p}_1^{\varrho_1}(\mathfrak{p}_1, \mathfrak{p}_2^{\varrho_2} \cdots \mathfrak{p}_k^{\varrho_k}) = \mathfrak{p}_1^{\varrho_1};$$

because, by the existence of the identity element, $\mathfrak{p}_1$ is coprime to all the other prime ideals. This again contradicts the sharp uniqueness condition.

3. Proof of axioms I and II (the chain conditions). The assumptions give, for every ideal different from the zero ideal: *divisibility implies a product representation.* Thus from $\mathfrak{m} \equiv 0(\mathfrak{a})$ and $\mathfrak{a} \neq \mathfrak{o}$ follows $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ with $\mathfrak{b} \not\equiv 0(\mathfrak{m})$. Let

$$\mathfrak{m} \equiv 0(\mathfrak{a}); \qquad \mathfrak{m} = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r}, \qquad \mathfrak{a} = \overline{\mathfrak{p}}_1^{\sigma_1} \cdots \overline{\mathfrak{p}}_{\bar{r}}^{\sigma_{\bar{r}}};$$

then every $\overline{\mathfrak{p}}$ is identical with some $\mathfrak{p}$, and $\sigma_i \leq \varrho_i$. The assertion therefore follows with $\mathfrak{b} = \mathfrak{p}_1^{\varrho_1-\sigma_1} \cdots \mathfrak{p}_r^{\varrho_r-\sigma_r}$, where of course some of the σ_i may be zero. Thus $\mathfrak{m}$ has only the finitely many divisors corresponding to the combinations $0 \leq \sigma_i \leq \varrho_i$; consequently the double-chain condition holds in the residue-class ring modulo $\mathfrak{m}$. Axioms I and II are thereby proved: the divisor-chain condition also holds in $\mathfrak{R}$ itself, since every proper divisor of the zero ideal is different from the zero ideal.

The proof of axiom V, integral closedness in the quotient field, uses the standard consequences of ideal decomposition, which must therefore first be derived.

4. *The residue-class ring modulo every ideal different from the zero ideal is a principal-ideal ring.* The ideal may be assumed different from the unit ideal, since for the residue-class ring consisting only of the zero element the assertion is immediate.

If the ideal is first primary, $\mathfrak{q} = \mathfrak{p}^{\varrho}$, and if $c \equiv 0(\mathfrak{p})$ but $c \not\equiv 0(\mathfrak{p}^2)$, then by 3 one has $\mathfrak{o}c = \mathfrak{p}\mathfrak{a}$ with $(\mathfrak{a}, \mathfrak{p}) = \mathfrak{o}$. Consequently

$$\mathfrak{p}^{\sigma} = (\mathfrak{o}c^{\sigma}, \mathfrak{p}^{\varrho}) \qquad \text{for every } \sigma \leq \varrho;$$

so every ideal in the residue-class ring modulo a primary ideal is principal. In general, if

$$\mathfrak{m} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdots \mathfrak{q}_r, \qquad \text{with } \mathfrak{q}_i = \mathfrak{p}_i^{\varrho_i},$$

and the corresponding representation of the residue-class ring as a direct sum is

$$\mathfrak{R} \mid \mathfrak{m} = \overline{\mathfrak{a}}_1 + \cdots + \overline{\mathfrak{a}}_r,$$

then $\overline{\mathfrak{a}}_i$ is isomorphic to $\mathfrak{R} \mid \mathfrak{q}_i$ (ğ 4, 5), and consequently every ideal of $\overline{\mathfrak{a}}_i$ is principal. If $\overline{\mathfrak{c}}$ is any ideal of the residue-class ring, then $\overline{\mathfrak{a}}_i\overline{\mathfrak{c}}$ is a principal ideal $\overline{\mathfrak{a}}_i\overline{c}_i$; hence

$$\overline{\mathfrak{c}} = \overline{\mathfrak{o}}\,\overline{\mathfrak{c}} = \overline{\mathfrak{a}}_1\overline{\mathfrak{c}} + \cdots + \overline{\mathfrak{a}}_r\overline{\mathfrak{c}} = \overline{\mathfrak{a}}_1\overline{c}_1 + \cdots + \overline{\mathfrak{a}}_r\overline{c}_r = \overline{\mathfrak{a}}_1\overline{c} + \cdots + \overline{\mathfrak{a}}_r\overline{c} = \overline{\mathfrak{o}}\,\overline{c},$$

where $\overline{c} = \overline{c}_1 + \cdots + \overline{c}_r$. Indeed, since $\overline{\mathfrak{a}}_i\overline{\mathfrak{a}}_k = (0)$ and $\overline{c}_i \equiv 0(\overline{\mathfrak{a}}_i)$, the principal ideals $\overline{\mathfrak{a}}_i\overline{c}_i$ and $\overline{\mathfrak{a}}_i\overline{c}$ of $\overline{\mathfrak{a}}_i$ agree.

The theorem on principal-ideal residue rings also has the following familiar form:

If $\mathfrak{c}$ is any ideal, it can be transformed into a principal ideal by multiplication with an ideal coprime to a prescribed ideal $\mathfrak{b}$.

For, putting $\mathfrak{m} = \mathfrak{b}\mathfrak{c}$, the ideal $\mathfrak{c}$ becomes principal modulo $\mathfrak{m}$; that is,

$$\mathfrak{c} = (\mathfrak{o}c, \mathfrak{m}) = (\mathfrak{c}\mathfrak{a}, \mathfrak{c}\mathfrak{b}) = \mathfrak{c}(\mathfrak{a}, \mathfrak{b});$$

so that $\mathfrak{o}c = \mathfrak{c}\mathfrak{a}$ and $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$.

5. Theory of fractional ideals. A fractional ideal means a finite $\mathfrak{R}$-module in the quotient field $\mathfrak{K}$.

Theorem. *The nonzero finite $\mathfrak{R}$-modules in $\mathfrak{K}$ form an Abelian group under multiplication.*

The product of two finite $\mathfrak{R}$-modules is again a finite $\mathfrak{R}$-module; multiplication is associative and commutative; since $\mathfrak{A} = \mathfrak{o}\mathfrak{A}$, the unit ideal is the identity element of the system. It remains only to show that the equation

$$\mathfrak{A}\mathfrak{X} = \mathfrak{o}$$

always has a solution in the system of finite $\mathfrak{R}$-modules.

Preliminary remark. If the equation $\mathfrak{A}\mathfrak{X} = \mathfrak{B}$ has one and only one solution, then $\mathfrak{X}$ is the module quotient $\mathfrak{B} : \mathfrak{A}$ (ğ 5, 4). For

$$\mathfrak{X} \equiv 0(\mathfrak{B} : \mathfrak{A}), \qquad \mathfrak{B} = \mathfrak{A}\mathfrak{X} \equiv 0(\mathfrak{A}(\mathfrak{B} : \mathfrak{A})) \equiv 0(\mathfrak{B}) \quad \text{or} \quad \mathfrak{A} \cdot (\mathfrak{B} : \mathfrak{A}) = \mathfrak{B}.$$

If first $\mathfrak{A}$ is a *principal module*, $\mathfrak{A} = (\alpha)$, then $\mathfrak{X} = (e/\alpha)$ is a solution of $\mathfrak{A}\mathfrak{X} = \mathfrak{o}$, and $\mathfrak{X}$ is again a finite $\mathfrak{R}$-module. It follows that *every finite $\mathfrak{R}$-module is the module quotient of two ideals of $\mathfrak{R}$*, which justifies the term fractional ideal. Indeed, let $\tau_1, \ldots, \tau_r$ be a module basis of $\mathfrak{T}$, let $\tau_i = t_i/a$, and let $\mathfrak{t}$ be the ideal generated by the t_i in $\mathfrak{R}$. Then $\mathfrak{o}a \cdot \mathfrak{T} = \mathfrak{t}$, whence by the preliminary remark $\mathfrak{T} = (\mathfrak{t} : \mathfrak{o}a)$, the quotient being taken in $\mathfrak{R}$.

The solution of $\mathfrak{A}\mathfrak{X} = \mathfrak{o}$ can now be given generally. Put $\mathfrak{A} = \mathfrak{a} : \mathfrak{o}c$, and choose $\mathfrak{b}$ so that $\mathfrak{a}\mathfrak{b}$ is the principal ideal $\mathfrak{o}a$. Then

$$\mathfrak{A}c = \mathfrak{a}, \qquad \text{and hence} \qquad \mathfrak{A}\mathfrak{b}c = \mathfrak{o}a \quad \text{or} \quad \mathfrak{A} \cdot (\mathfrak{b}c : \mathfrak{o}a) = \mathfrak{o}.$$

Here $\mathfrak{X}$, as the quotient of an ideal by a principal ideal, is again a finite $\mathfrak{R}$-module. From the group property thus *proved* it also follows that the *module quotient of any two ideals* $\mathfrak{a} : \mathfrak{b}$, as the solution of the equation $\mathfrak{b}\mathfrak{X} = \mathfrak{a}$, is a *finite $\mathfrak{R}$-module.*

6. From the group property follow further consequences.

6 α. *Cancellation is possible*; that is, from $\mathfrak{T} = \mathfrak{A}\mathfrak{M} : \mathfrak{B}\mathfrak{M}$ follows $\mathfrak{T} = \mathfrak{A} : \mathfrak{B}$, and conversely. For from $\mathfrak{T}\mathfrak{B}\mathfrak{M} = \mathfrak{A}\mathfrak{M}$ comes $\mathfrak{T}\mathfrak{B} = \mathfrak{A}$, and conversely.

6 β. *Every fractional ideal (finite $\mathfrak{R}$-module) admits a representation $\mathfrak{C} = \mathfrak{a} : \mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are coprime; this condition determines $\mathfrak{a}$ and $\mathfrak{b}$ uniquely.* Existence follows from 5 and 6 α. From $\mathfrak{C} = \mathfrak{a} : \mathfrak{b} = \overline{\mathfrak{a}} : \overline{\mathfrak{b}}$ follows $\mathfrak{a}\overline{\mathfrak{b}} = \mathfrak{b}\overline{\mathfrak{a}}$, and hence uniqueness when both $\mathfrak{a}, \mathfrak{b}$ and $\overline{\mathfrak{a}}, \overline{\mathfrak{b}}$ are assumed pairwise coprime.

6 γ. *Every principal module $\mathfrak{o}\eta$ generated by a nonintegral element (i.e. by an element belonging to $\mathfrak{K}$ and not to $\mathfrak{R}$) admits a representation as a quotient of principal ideals such that no power of the numerator is divisible by the denominator.* Let the reduced representation be $\mathfrak{o}\eta = \mathfrak{b} : \mathfrak{c}$, so $(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o}$; choose $\mathfrak{a}$ according to 4 so that $\mathfrak{o}b = \mathfrak{b}\mathfrak{a}$ and $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{o}$. Then

$$\mathfrak{o}\eta = \mathfrak{a}\mathfrak{b} : \mathfrak{a}\mathfrak{c} = \mathfrak{o}b : \mathfrak{a}\mathfrak{c},$$

and since $\mathfrak{a}\mathfrak{c} = \mathfrak{o}b : \mathfrak{o}\eta$, the ideal $\mathfrak{a}\mathfrak{c}$ is principal as well; thus

$$\mathfrak{o}\eta = \mathfrak{o}b : \mathfrak{o}c.$$

No power of $\mathfrak{a}\mathfrak{b}$ is divisible by $\mathfrak{c}$, because $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{o}$ and $(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o}$.

7. *Proof of axiom V, integral closedness in the quotient field.* By 6 γ, *every nonintegral element of $\mathfrak{K}$ has a quotient representation*

$$\eta = a/c$$

such that, in $\mathfrak{R}$, no power of the numerator is divisible by the denominator. For from $\mathfrak{o}\eta = \mathfrak{o}b : \mathfrak{o}c$ it follows that η differs from the quotient b/c only by a unit of $\mathfrak{R}$. Such an element η cannot satisfy an equation characterizing it as integral over $\mathfrak{R}$; for from

$$\eta^n + r_1\eta^{n-1} + \cdots + r_n = 0$$

one would obtain $a^n \equiv 0(\mathfrak{o}c)$ in $\mathfrak{R}$.

8. *Consequence: If axioms I through IV hold in a commutative ring $\mathfrak{R}$, and every primary ideal is irreducible, then axiom V, integral closedness in the quotient field, also holds.* Because of axioms I through III, every prime-ideal power $\mathfrak{p}^\varrho$ is primary; in particular $\mathfrak{p}^2$ is primary and therefore irreducible by assumption. From this one must prove

$$\mathfrak{p} = (\mathfrak{o}c, \mathfrak{p}^2).$$

Then, by the auxiliary result ğ 8, 3, every primary ideal is a prime-ideal power; together with the other assumptions, 7 gives integral closedness.

By the divisor-chain condition,

$$\mathfrak{p} = (\mathfrak{o}c_1, \ldots, \mathfrak{o}c_k, \mathfrak{p}^2),$$

where only residue classes modulo $\mathfrak{p}$ are relevant as multipliers of the c_i, and the c_i may be assumed linearly independent over the residue-class field modulo $\mathfrak{p}$. If $k > 1$, this linear independence gives a representation

$$\mathfrak{p}^2 = [\mathfrak{q}_1, \mathfrak{q}_2], \qquad \mathfrak{q}_1 = (\mathfrak{o}c_1, \mathfrak{p}^2), \qquad \mathfrak{q}_2 = (\mathfrak{o}c_2, \ldots, \mathfrak{o}c_k, \mathfrak{p}^2),$$

with both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ proper divisors of $\mathfrak{p}^2$; hence $\mathfrak{p}^2$ would be reducible, contrary to the assumption. Thus $\mathfrak{p} = (\mathfrak{o}c, \mathfrak{p}^2)$, and the asserted consequence is proved.

Conversely, as a consequence of axioms I through V, every primary ideal is immediately irreducible: a prime-ideal power $\mathfrak{p}^\varrho$ cannot be the least common multiple of proper divisors of the form $\mathfrak{p}^\sigma$ and $\mathfrak{p}^\tau$.

9. *If zero divisors are allowed in the ring, then axioms I through III and integral closedness in the quotient ring do not imply that every primary ideal is irreducible*[32]. Let $\mathfrak{T}$ be a ring in which all axioms I through IV except integral closedness hold; such rings exist, for instance the finite orders distinct from the full system of integral quantities in a finite extension field of the quotient field of $\mathfrak{R}$, when axioms I through V hold in $\mathfrak{R}$ (ğ 3, 2). By the consequence under 8 there is in $\mathfrak{T}$ a reducible primary ideal $\mathfrak{q}$. Let $\mathfrak{p}^\varrho$ be a proper multiple of $\mathfrak{q}$, and let $\overline{\mathfrak{R}}$ be the residue-class ring $\mathfrak{T} \mid \mathfrak{p}^\varrho$, in which the ideal $\overline{\mathfrak{q}}$ corresponding to $\mathfrak{q}$ is a nonzero reducible primary ideal. In $\overline{\mathfrak{R}}$ axioms I through III hold, and integral closedness in the quotient ring also holds. For every element of $\mathfrak{T}$ not divisible by $\mathfrak{p}$ is coprime to $\mathfrak{p}^\varrho$; hence all regular elements of $\overline{\mathfrak{R}}$ are units, and $\overline{\mathfrak{R}}$ coincides with its quotient ring.

ğ 10.
The double-chain condition and composition series.

We now show that, for arbitrary module domains (ğ 2) assumed to be well-ordered, the *assumption that the double-chain condition holds* — every divisor chain and every multiple chain of modules terminates after finitely many steps — is identical with the *assumption that a composition series exists*[33]. Specializing the module domain to a commutative ring gives the corresponding facts for the system of all ideals of the ring; under 2, module isomorphism is then throughout to be replaced by ring isomorphism.

A module domain $\mathfrak{G}$ is called *simple* if in $\mathfrak{G}$ there are no $\mathfrak{R}$-modules besides $\mathfrak{G}$ itself and the zero module $\mathfrak{E}$. A module $\mathfrak{A}$ is called *simple in* $\mathfrak{G}$ if $\mathfrak{G} \mid \mathfrak{A}$ is simple (greatest normal divisor).

A multiple chain

$$\mathfrak{G}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$$

is called a composition series of $\mathfrak{G}$ *of length* r if all modules in the chain are distinct and if each module is *simple in the preceding one*; that is, if the residue-class modules (the quotient groups) $\mathfrak{A}_{i-1} \mid \mathfrak{A}_i$ are simple module domains, as are $\mathfrak{G} \mid \mathfrak{A}_1$ and $\mathfrak{A}_r$. By forming the residue-class module $\mathfrak{G} \mid \mathfrak{A}$, the case in which a composition series exists from $\mathfrak{G}$ down to $\mathfrak{A} \neq \mathfrak{E}$ is reduced to the absolute case.

1. *If the double-chain condition is assumed in* $\mathfrak{G}$*, then a composition series exists in* $\mathfrak{G}$ — provided $\mathfrak{G} \neq \mathfrak{E}$. From the assumed well-ordering of $\mathfrak{G}$ and the divisor-chain condition, one obtains as in ğ 6, by quasi-lexicographic ordering, a well-ordering of the system of all modules. This well-ordering, together with the divisor-chain condition, gives the existence of at least one module simple in $\mathfrak{G}$. Namely, let $\mathfrak{G}_1$ be the first proper divisor of $\mathfrak{G}$ in the well-ordering; generally let $\mathfrak{G}_i$ be the first proper divisor of $\mathfrak{G}_{i-1}$. The well-determined chain

$$\mathfrak{G}, \mathfrak{G}_1, \ldots, \mathfrak{G}_i, \ldots$$

terminates after finitely many steps and therefore necessarily leads to a module $\mathfrak{A}_1$ simple in $\mathfrak{G}$. If $\mathfrak{A}_1 \neq \mathfrak{E}$, the same procedure gives a module $\mathfrak{A}_2$ simple in $\mathfrak{A}_1$; in general, if $\mathfrak{A}_{i-1} \neq \mathfrak{E}$, there is a module $\mathfrak{A}_i$ simple in $\mathfrak{A}_{i-1}$. This gives a well-determined multiple chain

$$\mathfrak{G}, \mathfrak{A}_1, \ldots, \mathfrak{A}_i, \ldots,$$

[32] Compare note 19.

[33] The modules of the domain are abelian groups with respect to addition, in fact *generalized* abelian groups, since the multiplier domain consists of the elements of $\mathfrak{R}$. Since they are abelian groups, the concept of composition series coincides here with that of principal series. The theorems of this paragraph remain valid if, under "modules," one understands the totality of normal divisors of an arbitrary noncommutative, even generalized, group. The notation, slightly different from the earlier one, is meant to recall group theory.

which terminates by the multiple-chain condition and is therefore a composition series of $\mathfrak{G}$.

2. *If a composition series exists in $\mathfrak{G}$, then the double-chain condition holds in $\mathfrak{G}$.* The proof is by complete induction and does not require a well-ordering of $\mathfrak{G}$. In the course of the induction one obtains at the same time a proof of the Jordan–Hölder theorem under the sole assumption that a composition series exists[34].

If $\mathfrak{G}$ is simple, so that $r = 0$ and the only composition series is $\mathfrak{G}, \mathfrak{E}$, then the following assertions hold:

α) Through every module simple in $\mathfrak{G}$ one can draw a composition series.
β) Jordan–Hölder theorem: every composition series has the same length, and the system of quotient groups (residue-class modules) agrees up to order; corresponding quotient groups are isomorphic.
γ) Through every module different from $\mathfrak{G}$ one can draw a composition series.
δ) The multiple-chain condition holds.
ε) The divisor-chain condition holds.

The assertions α) through ε) may therefore be assumed to hold for every module domain possessing a composition series of length $\bar{r} < r+1$. We prove them under the *assumption that in $\mathfrak{G}$ there is a composition series*

$$\mathfrak{G}, \mathfrak{A}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$$

of length $r+1$.

2α. If there is no module simple in $\mathfrak{G}$ other than $\mathfrak{A}$, there is nothing to prove. Let $\mathfrak{B}$ be simple in $\mathfrak{G}$ and $\mathfrak{B} \neq \mathfrak{A}$. Since $\mathfrak{A}$ and $\mathfrak{B}$ are both simple in $\mathfrak{G}$ and are distinct, necessarily $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{G}$. Put $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$. By the second isomorphism theorem (ğ 4, 2),

$$\mathfrak{G} \mid \mathfrak{B} \simeq \mathfrak{A} \mid \mathfrak{M} \qquad \text{and} \qquad \mathfrak{G} \mid \mathfrak{A} \simeq \mathfrak{B} \mid \mathfrak{M}.$$

Thus $\mathfrak{M}$ is simple in $\mathfrak{A}$ and in $\mathfrak{B}$. Since $\mathfrak{A}$ has a composition series of length $r < r+1$, the induction hypotheses α and β give in $\mathfrak{A}$ a composition series of length r through $\mathfrak{M}$, say

$$\mathfrak{A}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E};$$

consequently

$$\mathfrak{G}, \mathfrak{B}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E}$$

is a composition series of $\mathfrak{G}$ passing through $\mathfrak{B}$.

2β. To prove the Jordan–Hölder theorem, let

$$(1) \quad \mathfrak{G}, \mathfrak{A}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E} \qquad \text{and} \qquad (2) \quad \mathfrak{G}, \mathfrak{B}, \mathfrak{B}_1, \ldots, \mathfrak{B}_s, \mathfrak{E}, \quad s \geq r,$$

be two composition series of $\mathfrak{G}$. If $\mathfrak{A} = \mathfrak{B}$, the result follows from the induction assumption for length $r < r+1$. Otherwise compare them with the series constructed under 2α,

$$(3) \quad \mathfrak{G}, \mathfrak{A}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E} \qquad \text{and} \qquad (4) \quad \mathfrak{G}, \mathfrak{B}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E}.$$

By the induction hypothesis, the system of quotient groups of (1) and (3) agrees; likewise that of (2) and (4), since the tail of (4) beginning with $\mathfrak{B}$ is a composition series of length r. Thus $s = r$. The isomorphisms under 2α give agreement between (3) and (4), and hence between (1) and (2). This proves the Jordan–Hölder theorem.

2γ. Preliminary remark. *Let $\mathfrak{A}, \mathfrak{B}, \mathfrak{H}$ be modules of $\mathfrak{G}$, and suppose $\mathfrak{B}$ is simple in $\mathfrak{A}$. Then the modules $(\mathfrak{B}, \mathfrak{H})$ and $(\mathfrak{A}, \mathfrak{H})$ either coincide, or $(\mathfrak{B}, \mathfrak{H})$ is simple in $(\mathfrak{A}, \mathfrak{H})$.* By the second isomorphism theorem (ğ 4, 2),

$$(\mathfrak{A}, \mathfrak{B}, \mathfrak{H}) \mid (\mathfrak{B}, \mathfrak{H}) \simeq \mathfrak{A} \mid [\mathfrak{A}, (\mathfrak{B}, \mathfrak{H})],$$

or, since $\mathfrak{B} \equiv 0(\mathfrak{A})$,

$$(\mathfrak{A}, \mathfrak{H}) \mid (\mathfrak{B}, \mathfrak{H}) \simeq \mathfrak{A} \mid \mathfrak{C}, \qquad \mathfrak{C} = [\mathfrak{A}, (\mathfrak{B}, \mathfrak{H})].$$

[34] Compare Masazo Sono (note 19), *On Congruences I*, ğğ 11–13, for the case of rings. There the analogue of a composition series in noncommutative groups is also treated: series $\mathfrak{R}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$, where each $\mathfrak{A}_i$ is an ideal and is simple in $\mathfrak{A}_{i-1}$, without necessarily being an ideal in $\mathfrak{R}$. The foregoing arguments remain valid for noncommutative groups if, by a multiple chain, one means a chain $\mathfrak{G}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \ldots$ in which each $\mathfrak{A}_i$ is normal in $\mathfrak{A}_{i-1}$, and divisor chains are defined correspondingly. Compare also Dedekind, "Über die von drei Moduln erzeugte Dualgruppe," Math. Ann. 53 (1900), pp. 371–403. There, for much more general domains (module groups), the Jordan–Hölder theorem is likewise proved (ğ 6, XVI) under the existence assumption alone. In place of the second isomorphism theorem there occurs a somewhat weaker correspondence relation, and consequently the statement of the theorem is also somewhat weaker; the principle of the proof is identical with the one given here.

Here $\mathfrak{C} \equiv 0(\mathfrak{A})$; on the other hand $\mathfrak{B} \equiv 0(\mathfrak{C})$, because $\mathfrak{B} \equiv 0(\mathfrak{A})$ and $\mathfrak{B} \equiv 0((\mathfrak{B}, \mathfrak{H}))$. Hence $\mathfrak{C}$ lies between $\mathfrak{A}$ and $\mathfrak{B}$ and is therefore, by assumption, identical with $\mathfrak{A}$ or $\mathfrak{B}$. This proves the preliminary remark.

Now let

$$\mathfrak{G}, \mathfrak{A}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$$

be a composition series of $\mathfrak{G}$, and let $\mathfrak{H}$ be an arbitrary module of $\mathfrak{G}$ different from $\mathfrak{G}$. To show that a composition series passes through $\mathfrak{H}$, form

$$\mathfrak{G}, (\mathfrak{A}, \mathfrak{H}), (\mathfrak{A}_1, \mathfrak{H}), \ldots, (\mathfrak{A}_r, \mathfrak{H}), \mathfrak{H}.$$

By the preliminary remark, the distinct modules among these, say $\mathfrak{G}, \mathfrak{C}, \mathfrak{C}_1, \ldots, \mathfrak{C}_s, \mathfrak{H}$, form a composition series from $\mathfrak{G}$ to $\mathfrak{H}$; thus $\mathfrak{C}$ — which in the special case 2α coincides with $\mathfrak{H}$ — is simple in $\mathfrak{G}$. By 2α, $\mathfrak{C}$ possesses a composition series of length $r < r + 1$, and consequently, by the induction hypothesis, one can draw in $\mathfrak{C}$ a composition series through $\mathfrak{H}$; adjoining $\mathfrak{G}$ gives in $\mathfrak{G}$ a composition series through $\mathfrak{H}$. Repeating the argument shows that such a series may in particular be chosen as an extension of the series just constructed from $\mathfrak{C}$ to $\mathfrak{H}$.

2δ. Proof of the multiple-chain condition. Suppose again that a composition series of length $r + 1$ exists in $\mathfrak{G}$, and let

$$\mathfrak{G}, \mathfrak{B}, \mathfrak{B}_1, \ldots, \mathfrak{B}_\nu, \ldots$$

be a multiple chain, each module being a proper multiple of the preceding one. That the chain begins with $\mathfrak{G}$ is no restriction of generality, since $\mathfrak{G}$ may always be adjoined as first term. By 2γ there is a composition series through $\mathfrak{B}$, and hence $\mathfrak{B}$ has a composition series of shorter length. By the induction hypothesis, the chain

$$\mathfrak{B}, \mathfrak{B}_1, \ldots, \mathfrak{B}_\nu, \ldots$$

terminates after finitely many steps. Hence the same is true after adjoining $\mathfrak{G}$.

2ε. Proof of the divisor-chain condition. Again assume a composition series of length $r + 1$ in $\mathfrak{G}$, and let

$$\mathfrak{E}, \mathfrak{C}, \mathfrak{C}_1, \ldots, \mathfrak{C}_\nu, \ldots$$

be a divisor chain, each module being a proper divisor of the preceding one. Again there is no restriction in assuming that the chain begins with $\mathfrak{E}$. By 2γ there is a composition series through $\mathfrak{C}$, and hence in $\mathfrak{G} \mid \mathfrak{C}$ there is a composition series of shorter length. By the induction hypothesis, the divisor chain

$$\mathfrak{C} \mid \mathfrak{C}, \mathfrak{C}_1 \mid \mathfrak{C}, \ldots, \mathfrak{C}_\nu \mid \mathfrak{C}, \ldots$$

terminates after finitely many steps. By the one-to-one correspondence furnished by the first isomorphism theorem (ğ 4, 2), the same holds for the original chain beginning with $\mathfrak{C}$, and hence also for the chain with $\mathfrak{E}$ adjoined.

The equivalence of the two assumptions — existence of a composition series and the double-chain condition — is thereby proved.

(Received August 13, 1925.)

31. The Discriminant Theorem for Orders of an Algebraic Number Field or Function Field.

Journal f. d. reine u. angew. Math. 157 (1927), pp. 82–104
By *Emmy Noether* in Göttingen.

Dedekind's discriminant theorem says, as is well known: a prime number enters the field discriminant if and only if it is divisible at least by the square of a prime ideal.

I show in what follows that this theorem remains valid for all finite orders of a finite algebraic number field, that is, for all such rings of algebraic integers which contain the ring of all rational integers, in the following form: a prime number p enters the discriminant of an order if and only if, in the decomposition valid in the order of the principal ideal (p) into greatest primary components, at least one proper primary ideal occurs, that is, one which is not a prime ideal.[1]

Since for the principal order, the system of all integers of the field, there are no further primary ideals except powers of prime ideals, Dedekind's theorem follows by specialization.

The proof of the theorem is reduced, by passing to the residue-class ring of the order modulo (p), to the decomposition theory of those rings which are of finite rank with respect to a field contained in the ring, that is, which form a commutative system of hypercomplex quantities with principal identity and coefficients from that same field. Here, in particular, the coefficient field is the residue-class field of the rational integers modulo p, and the decomposition of (p) corresponds in the residue-class ring to the decomposition of the zero ideal.

Thus if such a ring of finite rank is called completely reducible when its zero ideal can be represented as the least common multiple of finitely many prime ideals, the question is to find criteria for complete reducibility. As such a criterion one first obtains that, for a perfect field as coefficient domain, the ring is completely reducible if and only if the extension ring with algebraically closed coefficient domain is completely reducible. For this extension ring, however, the nonvanishing of the discriminant is very easily recognized as a necessary and sufficient criterion for complete reducibility;[2] and since the discriminant of the order modulo each prime number passes into the discriminant of the residue-class ring, the discriminant theorem is thereby proved.[3]

If one considers function fields instead of number fields, the order must now contain the ground domain of all rational integral functions, respectively, for algebraic functions of several indeterminates or for integral algebraic functions, the ground domain of all integral functionals with rational integral coefficients. In that case, the case of an imperfect coefficient domain can also occur in the residue-class ring, for example when, in the case of an integral functional domain, one takes the residue-class ring modulo a prime number. For an imperfect field as coefficient domain one must distinguish between prime ideals of the first and of the second kind according as the residue field modulo the prime ideal is an extension field of the first or of the second kind,[4] and correspondingly between complete reducibility of the first and of the second kind. The criteria stated above refer throughout to complete reducibility of the first kind, which alone occurs in the perfect case. Hence, in the most general case, the discriminant theorem says that a prime element of the ground domain enters the discriminant of an order if and only if, in the ideal decomposition of (p), at least one properly primary component or one prime ideal of the second kind occurs.

For the principal order this fact was first noticed in examples by Kronecker, after the Festschrift had still given, erroneously, the formulation valid for the principal order of a number field, though without a complete proof. For the principal order Ostrowski[5] gave a proof of the above discriminant theorem and further ramification theorems attached to it; at the same time a detailed survey of the literature is found there. Finally, the discriminant theorem for all orders of relative fields follows as a direct consequence, by passing to the quotient ring with respect to each prime ideal of the ground domain. The idea of this passage, which is known in the special case, was emphasized in principle by W. Krull;[6] a systematic theory of the

[1] Cf. E. Noether, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96 (1926), pp. 26–61. For all definitions reference is made to this paper, cited below as "Ideal Theory". In what follows, "order" always means "finite order", and "ring" a commutative ring.

[2] In a special case Hilbert argues similarly: Zur Theorie der aus n Haupteinheiten gebildeten komplexen GröSSen, Gött. Nachr. 1896.

[3] Related investigations, also in the noncommutative case, but restricted to the principal order (maximal domain) and assuming rational integral number coefficients, are found in the recently published paper of A. Speiser, *Allgemeine Zahlentheorie*, Naturf. Gesellschaft Zürich 71 (1926), pp. 8–48. Cf. also the American literature cited there.

[4] In Steinitz's familiar formulation, J. f. M. 137. Cf. the note to §2, no. 4, of this paper.

[5] A. Ostrowski, Zur arithmetischen Theorie der algebraischen GröSSen, Nachr. Gött. Ges. d. Wissensch. 1919.

[6] Cf. his Danzig lecture, Jhrbr. d. D. Math. Ver. 34, p. 121.

quotient ring in the framework of more general investigations is given by H. Grell.[7]

The uniform treatment of all orders given here, and of perfect and imperfect coefficient domains, rests, besides the use of ideal theory, on taking from the outset the theory of rings of finite rank, and hence the general concept of a finite extension, as the basis, and not the concept of an extension generated by a primitive element. The module basis of an order, together with the relations among its elements, therefore takes the place of the powers of a primitive element of the field and of the defining equation,[8] respectively of the powers of the fundamental form and of the fundamental equation.

Such a module basis passes, modulo every prime element of the ground domain, into a basis of the residue-class ring, whereas this need not hold even for the principal order when the basis consists of powers of a primitive element; nor for the basis consisting of powers of the fundamental form as soon as integral algebraic functions of several indeterminates are involved.[9] Expressed differently: the residue-class ring of the polynomial domain in one indeterminate with coefficients in the ground domain, modulo an arbitrary defining equation, or even modulo the fundamental equation, need not be isomorphic modulo p to the residue-class ring of the principal order modulo (p). The main difficulties in the customary presentations lie in this disappearance of the isomorphism. Since this auxiliary polynomial domain does not occur here, these difficulties are thereby avoided automatically. At the same time the additive decomposition theory of the residue-class ring can be understood as the equivalent of the multiplicative decomposition of the equation; here too, decomposition into relatively prime factors corresponds to an additive decomposition in the polynomial residue-class ring.

It should be noted that the discriminant theorem can represent only the first theorem of a general ramification theory of orders, just as in the principal order the discriminant theorem is accompanied by the more refined theory of the ramification ideal, which there permits a more precise determination of exponents. This determination of exponents, which rests on the power representation of the primary factors of the equations, can be interpreted as the determination of the length of a composition series from p to $q = p^e$, and will presumably occur in this form in the general ramification theory.

§1. Extension rings of fields

1. We first place in front a few remarks on arbitrary rings. If $\mathfrak{T}$ is a ring and S a system of elements of $\mathfrak{T}$, then by the "ring derived from S in $\mathfrak{T}$" is meant the intersection of all rings in $\mathfrak{T}$ which contain S. Correspondingly one defines the "ideal derived from S in $\mathfrak{T}$", or the "P-module derived from S in $\mathfrak{T}$", when P is a subring of $\mathfrak{T}$.[10]

If $\mathfrak{R}$ is a subring of $\mathfrak{T}$ and S a system of elements of $\mathfrak{T}$, the ring derived from $\mathfrak{R}$ and S in $\mathfrak{T}$ is denoted as the ring $\mathfrak{R}[S]$ arising by ring-adjunction of S to $\mathfrak{R}$. This ring consists of all polynomials in the elements of S with coefficients from $\mathfrak{R}$, where the equality and operation relations are fixed by the equality and operation relations in $\mathfrak{T}$. Because of these already fixed equality and operation relations it may suffice, in a special case, to form only a subsystem of all polynomials, for instance only all linear forms in S with coefficients from $\mathfrak{R}$. Such a special case occurs, for example (cf. no. 2), when $\mathfrak{R}$ is a ring with identity element and S is a field with the same identity element: all linear combinations $\sum c_i\gamma_i$, where c_i belongs to S and γ_i to $\mathfrak{R}$, form the ring $\mathfrak{R}[S]$.

But when only the ring $\mathfrak{R}$ is given, and in addition a system S of elements not contained in $\mathfrak{R}$ with equality relations, or also mutual operation relations, one can also construct the extension ring $\mathfrak{R}[S]$ arising by adjunction of S to $\mathfrak{R}$. One shows that there is always a ring containing $\mathfrak{R}$ and S, namely the ring formally consisting of all polynomials in S with coefficients from $\mathfrak{R}$, with the usual operation rules fixed. For the definition of equality, aside from the operation rules, full freedom is still possible, except for the restriction that the equality definitions valid in $\mathfrak{R}$ and S must be included. Thus it is necessary only that those polynomials be set equal which, by virtue of equality in $\mathfrak{R}$ and S and by virtue of the operations, can be formed from equal elements of $\mathfrak{R}$ and S in the same way. The ring $\mathfrak{T}$ so constructed, containing $\mathfrak{R}$ and S, is then identical with the ring derived in $\mathfrak{T}$ from $\mathfrak{R}$ and S.[11]

2. Extension rings of fields. From now on assume rings $\mathfrak{R}$ with identity element, containing a field P as a subring, and therefore over-rings of fields. The identity element e of $\mathfrak{R}$ is then also the identity element

[7] *Beziehungen zwischen den Idealen verschiedener Ringe* (to appear in Math. Annalen).

[8] This point of view is closely connected with Dedekind's view of higher complex numbers: Zur Theorie der aus n Haupteinheiten gebildeten komplexen GröSSen, Gött. Nachr. 1885.

[9] Cf. Ostrowski, loc. cit., "irregularity of the first kind".

[10] Cf. Ideal Theory, §1.

[11] Cf. Steinitz's construction of the quotient field.

of P, and the ring is a P-module.

If $\overline{P}$ is an overfield of P, the extension ring $\overline{\mathfrak{R}} = \mathfrak{R}[\overline{P}]$ arising by ring-adjunction of $\overline{P}$ to $\mathfrak{R}$ is to be explained as follows.

It is assumed that the set-theoretic intersection $[\mathfrak{R}, \overline{P}]$ of $\mathfrak{R}$ and $\overline{P}$ is P, and further that between the elements of $\mathfrak{R}$ and $\overline{P}$ not belonging to P no operation relations exist. This assumption can always be achieved by replacing $\overline{P}$ by an equivalent extension field of P, or also by replacing $\mathfrak{R}$ by an equivalent extension ring.[12]

As elements of $\overline{\mathfrak{R}}$ one declares all formally formed linear combinations

$$\bar{c}_{i_1}\gamma_{i_1} + \cdots + \bar{c}_{i_\sigma}\gamma_{i_\sigma},$$

where the $\bar{c}_i$ run through all elements of $\overline{P}$ and the γ_i through all elements of $\mathfrak{R}$.[13] The definition is to be unique; that is, if the γ are replaced by elements equal to them in $\mathfrak{R}$, and the $\bar{c}$ by elements equal to them in $\overline{P}$, then the element in $\overline{\mathfrak{R}}$ is also to be declared equal.

As sum one defines, uniquely in the sense that replacing a summand by an equal one in the equality definition to be fixed gives the same result,

$$\sum \bar{c}_i\gamma_i + \sum \bar{d}_i\gamma_i = \sum(\bar{c}_i + \bar{d}_i)\gamma_i.$$

Here zeros may occur among the $\bar{c}$ and $\bar{d}$, whereby formally the same γ_i occur.

As product one defines, in the same sense uniquely,

$$\sum \bar{c}_i\gamma_i \cdot \sum \bar{d}_k\gamma_k = \sum \bar{c}_i\bar{d}_k\gamma_i\gamma_k.$$

For the equality definition it is declared that, if $\gamma_{i_1}, \ldots, \gamma_{i_\sigma}$ are linearly independent with respect to P, then two elements

$$\bar{c}_{i_1}\gamma_{i_1} + \cdots + \bar{c}_{i_\sigma}\gamma_{i_\sigma} \quad \text{and} \quad \bar{d}_{i_1}\gamma_{i_1} + \cdots + \bar{d}_{i_\sigma}\gamma_{i_\sigma}$$

are equal if and only if $\bar{c}_{i_\lambda}$ is equal to $\bar{d}_{i_\lambda}$ in $\overline{P}$ for every λ. Expressed differently: elements of $\mathfrak{R}$ linearly independent with respect to P are declared to be linearly independent with respect to $\overline{P}$.

By the definitions of sum and product the equality definition for all elements of $\overline{\mathfrak{R}}$ is thereby given. Indeed their expressibility by linearly independent elements from $\mathfrak{R}$ follows. For from a relation

$$\mu = c_1\gamma_1 + \cdots + c_s\gamma_s \quad \text{in } \mathfrak{R}$$

one obtains, by multiplication with $\bar{b} = \bar{b}e$ according to the product definition,

$$\bar{b}\mu = \bar{b}e \cdot (c_1\gamma_1 + \cdots + c_s\gamma_s) = \bar{b}c_1\gamma_1 + \cdots + \bar{b}c_s\gamma_s,$$

and hence, by the sum definition, the expressibility of all elements by linearly independent elements from $\mathfrak{R}$.

Consequently, if all elements have been expressed by linearly independent elements from $\mathfrak{R}$, the equality definition is equality of coefficients in $\overline{P}$. It therefore agrees, for elements belonging simultaneously to $\mathfrak{R}$ and $\overline{\mathfrak{R}}$ or to $\overline{P}$ and $\overline{\mathfrak{R}}$, with the equality valid there; whereas for the remaining elements of $\overline{\mathfrak{R}}$ the equality valid in $\mathfrak{R}$ and $\overline{P}$ says nothing beyond the uniqueness required in the definition, because of the intersection assumption and the further condition.[14] Similarly, the requirement that sum and product be unique entails no further relations, since equal elements may be assumed coefficientwise equal, and hence formally give the same sum and product expressions.

One now verifies at once that all axioms of the ring operation are fulfilled; thus the extension ring $\mathfrak{R}[\overline{P}]$ generated by ring-adjunction always exists.

3. Ideals in $\mathfrak{R}$ and $\overline{\mathfrak{R}}$. If $\mathfrak{a}$ is an ideal in $\mathfrak{R}$, then the module product $\overline{\mathfrak{R}}\mathfrak{a}$ is an ideal $\bar{\mathfrak{a}}$ in $\overline{\mathfrak{R}}$, the extension ideal of $\mathfrak{a}$. At the same time $\bar{\mathfrak{a}}$ is the ideal derived from $\mathfrak{a}$ in $\overline{\mathfrak{R}}$; it consists of all linear combinations $\sum \bar{c}_i a_i$, the sum in each case being over finitely many elements, where the a_i run through all elements of $\mathfrak{a}$ and the $\bar{c}_i$ through all elements of $\overline{P}$.

If $\bar{\mathfrak{b}}$ is an ideal in $\overline{\mathfrak{R}}$, then the intersection $[\bar{\mathfrak{b}}, \mathfrak{R}]$ is an ideal $\mathfrak{b}$ in $\mathfrak{R}$, the contraction ideal of $\bar{\mathfrak{b}}$.[15] Every

[12] Two extension fields of P are called "equivalent", following Steinitz, if they can be placed in isomorphism with one another in such a way that P corresponds elementwise to itself. Equivalent extension rings of P are to be defined correspondingly. By introducing new symbols one can always produce equivalent extensions; this freedom in the use of equivalent extensions is essential for what follows.

[13] In general, elements from $\mathfrak{R}$ or $\overline{\mathfrak{R}}$ are denoted by Greek letters, and elements from P or $\overline{P}$ by Latin letters.

[14] Without this assumption there would be at least one element $\bar{c}$ belonging to $\overline{P}$ but not to P, for which $\bar{c} = \bar{c}e = \gamma$ would hold. Then, by the equality definition in $\overline{\mathfrak{R}}$, e and γ would indeed be linearly independent with respect to P, but dependent with respect to $\overline{P}$. Because of the relations between elements of $\overline{P}$ and $\mathfrak{R}$, the above equality definition would then not be possible; think, for instance, of the lowering of degree of a finite extension field when the ground field is replaced by an intermediate field. The above extension is, by contrast, characterized by the possibility of the appearance of new zero divisors. Thus, for example, the residue-class ring of the polynomial domain with rational coefficients P modulo $x^2 + 1$ is a ring without zero divisors, isomorphic to the field $P(\sqrt{-1})$, whereas on passing to the polynomial domain with coefficients from $P(\sqrt{-1})$ zero divisors occur, corresponding to $(x + i)(x - i) = x^2 + 1$, although no factor is divisible by $x^2 + 1$. The corresponding statement holds, for example, for every finite number field; this is the conception first expressed by Dedekind for the higher complex numbers. Cf. on this point §6, no. 4, at the end.

[15] In H. Grell's notation, in the work cited in note 6 on p. 83 of the original.

ideal $\mathfrak{a}$ of $\mathfrak{R}$ is a contraction ideal, namely of its extension ideal $\overline{\mathfrak{a}}$. Indeed, every element a of $[\mathfrak{R}, \overline{\mathfrak{a}}]$ is of the form $\sum \bar{c}_i a_i$, where the a_i may be assumed linearly independent with respect to P or $\overline{P}$. Thus the elements a, a_i become linearly dependent in $\overline{\mathfrak{R}}$, and hence, by the equality definition, also in $\mathfrak{R}$; therefore a belongs to $\mathfrak{a}$. Since the converse also holds, $\mathfrak{a} = [\mathfrak{R}, \overline{\mathfrak{a}}]$.

If $\overline{\mathfrak{p}}$ is a prime ideal in $\overline{\mathfrak{R}}$, then $\mathfrak{p} = [\mathfrak{R}, \overline{\mathfrak{p}}]$ is a prime ideal in $\mathfrak{R}$. For, by the second isomorphism theorem,[16] the residue-class ring $\mathfrak{R}/\mathfrak{p}$ is isomorphic to a subring of $\overline{\mathfrak{R}}/\overline{\mathfrak{p}}$, and hence is a ring without zero divisors. Namely, there is the ring isomorphism

$$(\mathfrak{R}, \overline{\mathfrak{p}})/\overline{\mathfrak{p}} \simeq \mathfrak{R}/[\mathfrak{R}, \overline{\mathfrak{p}}],$$

where $(\mathfrak{R}, \overline{\mathfrak{p}})$ denotes the sum, the greatest common divisor, of the modules $\mathfrak{R}$ and $\overline{\mathfrak{p}}$.

§2. Rings of finite rank. Representation as a direct sum

1. Rings of finite rank. If $\mathfrak{R}$ is a finite P-module, then $\mathfrak{R}$ is of finite rank, say k, with respect to P: that is, there are k, and no more, elements in $\mathfrak{R}$ linearly independent with respect to P, and every system of k elements of $\mathfrak{R}$ linearly independent with respect to P consequently forms a module basis of $\mathfrak{R}$. If a P-module $\mathfrak{B}$ of finite rank is divisible by another $\mathfrak{A}$ of the same finite rank, $\mathfrak{B} = O(\mathfrak{A})$, then they are therefore identical.

From now on assume that $\mathfrak{R}$ has finite rank n with respect to P. Then every P-module in $\mathfrak{R}$ has finite rank. Thus in every proper chain of divisors or multiples of P-modules in $\mathfrak{R}$, the rank of each module must be larger, respectively smaller, than the rank of the immediately preceding one; the chains break off after finitely many steps. In particular, the "double-chain theorem" holds for the system of all ideals in $\mathfrak{R}$.

It follows from this[17] that a prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ has no proper divisor different from the identity ideal; hence the residue-class ring $\mathfrak{R}/\mathfrak{p}$ modulo a prime ideal different from the identity ideal is a field. If $\mathfrak{q}$ is a primary ideal belonging to $\mathfrak{p}$, that is, $\mathfrak{q} = O(\mathfrak{p})$ and $\mathfrak{p}^\rho = O(\mathfrak{q})$, then the residue-class ring $\mathfrak{R}/\mathfrak{q}$ is a primary ring, that is, a ring in which a power, here in any case already the ρ-th, of every zero divisor vanishes; and $\mathfrak{R}/\mathfrak{q}$ contains only zero divisors and units. The latter follows immediately from the fact that every ideal not divisible by $\mathfrak{p}$ is relatively prime to $\mathfrak{p}$, and hence also to $\mathfrak{q}$.

From the double-chain theorem and from the existence of the identity element it follows further[18] that every ideal $\mathfrak{a}$ of $\mathfrak{R}$ can be represented uniquely as a product of finitely many pairwise relatively prime primary ideals. Because of relative primeness this product is equal to the least common multiple and corresponds to a representation of the residue-class ring $\mathfrak{R}/\mathfrak{a}$ as a direct sum of primary rings.[19] That is, $\mathfrak{R}/\mathfrak{a}$ is the greatest common divisor of these rings, and the sum representation of every element of $\mathfrak{R}/\mathfrak{a}$ is unique.

2. Representation of rings of finite rank as direct sums of primary rings. Suppose that the representation of the zero ideal of $\mathfrak{R}$ is given by

$$(0) = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_r = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r],$$

and let the corresponding representation as a direct sum be

$$\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_2 + \cdots + \mathfrak{R}_r, \qquad \mathfrak{R}_i\mathfrak{R}_k = (0)\ (i \neq k), \qquad \mathfrak{R}_i^2 = \mathfrak{R}_i, \qquad \mathfrak{R}\mathfrak{R}_i = \mathfrak{R}_i.$$

Then $\mathfrak{R}_i$ is an ideal of $\mathfrak{R}$, namely

$$\mathfrak{R}_i = \mathfrak{q}_1 \cdots \mathfrak{q}_{i-1}\mathfrak{q}_{i+1} \cdots \mathfrak{q}_r = [\mathfrak{q}_1, \ldots, \mathfrak{q}_{i-1}, \mathfrak{q}_{i+1}, \ldots, \mathfrak{q}_r],$$

$$\mathfrak{q}_i = \mathfrak{R}_1 + \cdots + \mathfrak{R}_{i-1} + \mathfrak{R}_{i+1} + \cdots + \mathfrak{R}_r,$$

and $\mathfrak{R}_i$ is isomorphic to the residue-class ring $\mathfrak{R}/\mathfrak{q}_i$: to each element γ_i of $\mathfrak{R}_i$ corresponds the class represented by γ_i in $\mathfrak{R}/\mathfrak{q}_i$.[20] If $\mathfrak{a}$ is any ideal of $\mathfrak{R}$, then the distributive law gives

$$\mathfrak{a} = \mathfrak{R}\mathfrak{a} = \mathfrak{R}_1\mathfrak{a} + \cdots + \mathfrak{R}_r\mathfrak{a} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_r;$$

[16] Ideal Theory, §4, no. 3. The theorem is there stated only for ideals of the same ring; the same consideration shows its validity in the above form for arbitrary ideals $\overline{\mathfrak{a}}$ of $\overline{\mathfrak{R}}$. The ring homomorphism $\overline{\mathfrak{R}} \to \overline{\mathfrak{R}}/\overline{\mathfrak{a}}$ induces, for the subring $\mathfrak{R}$ of $\overline{\mathfrak{R}}$, the ring homomorphism $\mathfrak{R} \sim (\mathfrak{R}, \overline{\mathfrak{a}})/\overline{\mathfrak{a}}$. Under this homomorphism all and only the elements of $[\mathfrak{R}, \overline{\mathfrak{a}}]$ correspond to the zero element, and hence the ring isomorphism $(\mathfrak{R}, \overline{\mathfrak{a}})/\overline{\mathfrak{a}} \simeq \mathfrak{R}/[\mathfrak{R}, \overline{\mathfrak{a}}]$ follows. The classes can be represented on the right and on the left by the same elements of $\mathfrak{R}$, for at each step of the proof the elements are assigned to the classes represented by them.

[17] Ideal Theory, §7, no. 2.

[18] Ideal Theory, §7, no. 3, Theorem V.

[19] Ideal Theory, §4, no. 5. What is added in the present compilation is found scattered in many places in the literature.

[20] Ideal Theory, §4, no. 5.

here, since $\mathfrak{a}_i = \mathfrak{R}_i\mathfrak{a} = \mathfrak{R}\mathfrak{a}_i$, the components $\mathfrak{a}_i$ are ideals both in $\mathfrak{R}_i$ and in $\mathfrak{R}$. As ideals, the $\mathfrak{a}_i$, like the $\mathfrak{R}_i$ themselves, are finite P-modules; because the sum is direct, their ranks add to the rank of $\mathfrak{a}$, respectively of $\mathfrak{R}$.

If the sum representation of the identity element is given by

$$e = \varepsilon_1 + \cdots + \varepsilon_r, \qquad \varepsilon_i\varepsilon_k = 0 \ (i \neq k), \qquad \varepsilon_i^2 = \varepsilon_i, \qquad \varepsilon_i \equiv e \pmod{\mathfrak{q}_i},$$

then the representation of every element γ of $\mathfrak{R}$ is obtained uniquely as

$$\gamma = \gamma e = \gamma\varepsilon_1 + \cdots + \gamma\varepsilon_r = \gamma_1 + \cdots + \gamma_r,$$

where the component $\gamma_i = \gamma\varepsilon_i$ is an element of $\mathfrak{R}_i$; at the same time $\mathfrak{R}_i = \mathfrak{R}\varepsilon_i$. From the "orthogonality relations" one obtains

$$\gamma\delta = (\gamma_1\varepsilon_1 + \cdots + \gamma_r\varepsilon_r)(\delta_1\varepsilon_1 + \cdots + \delta_r\varepsilon_r) = \gamma_1\delta_1\varepsilon_1 + \cdots + \gamma_r\delta_r\varepsilon_r.$$

Thus $\gamma_i\delta_i$ is the i-th component of the product, and similarly $\gamma_i + \delta_i$ is the i-th component of the sum, facts which also follow from the homomorphism from $\mathfrak{R}$ to $\mathfrak{R}_i$.

The ring $\mathfrak{R}_i$ contains a subfield $P_i = P\varepsilon_i$ isomorphic to P and is of finite rank with respect to P_i; this rank is equal to the rank possessed by $\mathfrak{R}_i$ as a P-module. For for every element c of P, one has $c\varepsilon_i \equiv ce \equiv c \pmod{\mathfrak{q}_i}$, and hence $c\varepsilon_i \neq 0$ as soon as $c \neq 0$; the homomorphism between P and P_i becomes an isomorphism. Further, every linear dependence with respect to P of elements of $\mathfrak{R}_i$ passes, by multiplication with ε_i, into such a dependence with respect to P_i; conversely, because $P_i = P\varepsilon_i$, every relation with respect to P_i is at the same time a relation with respect to P. Thus the ranks with respect to P and P_i agree.

3. Direct sum representation of extension rings. If

$$\mathfrak{R} = \mathfrak{R}_1 + \cdots + \mathfrak{R}_r,$$

then for $\overline{\mathfrak{R}}$ a representation

$$\overline{\mathfrak{R}} = \overline{\mathfrak{R}}_1 + \cdots + \overline{\mathfrak{R}}_r$$

holds, where $\overline{\mathfrak{R}}_i$ denotes the extension ideal of $\mathfrak{R}_i$ in $\overline{\mathfrak{R}}$, at the same time the ring derived from $\mathfrak{R}_i$ in $\overline{\mathfrak{R}}$. Indeed, from $(0) = \mathfrak{q}_1 \cdots \mathfrak{q}_r$, multiplication by $\overline{\mathfrak{R}}$ gives the product representation $(0) = \overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_r$, where the $\overline{\mathfrak{q}}_i$ are again pairwise relatively prime. Hence one obtains a direct-sum representation for $\overline{\mathfrak{R}}$, and since the i-th component of this representation is given by

$$\overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_{i-1}\,\overline{\mathfrak{q}}_{i+1} \cdots \overline{\mathfrak{q}}_r,$$

it is equal to the extension ideal of $\mathfrak{R}_i$. But by §1, no. 3, this extension ideal is identical with the extension ring $\mathfrak{R}_i[\overline{P}_i]$ formed from $\mathfrak{R}_i$ with respect to $\overline{P}_i = \overline{P}\varepsilon_i$; therefore in extensions it suffices to extend the individual components. In general $\overline{\mathfrak{R}}_i$ will then no longer be a primary ring.

4. Prime ideals of the first and second kind. By no. 1, the residue-class ring $\mathfrak{R}/\mathfrak{p}$ modulo every prime ideal different from the identity ideal is a field. This field possesses a subfield $(P) = (P, \mathfrak{p})/\mathfrak{p} = P/[P, \mathfrak{p}] \simeq P$ isomorphic to P, since $\mathfrak{p}$ can contain no nonzero element from P; hence (P) consists of all and only the classes which can be represented by elements of P.[21] Thus $\mathfrak{R}/\mathfrak{p}$ is of finite rank with respect to (P), hence is a finite algebraic extension field. According as this extension is of the first or second kind,[22] $\mathfrak{p}$ is to be called a prime ideal of the first or of the second kind.

§3. Completely Reducible Rings.

1. The ring $\mathfrak{R}$ is called *completely reducible* if, in the product representation of its zero ideal (§2, 2), all primary components become prime ideals; or — what is identical with this by §2, 1 and 2 — if $\mathfrak{R}$ can be represented as a direct sum of finitely many fields. The completely reducible ring is called completely reducible of the first kind if all prime ideals are of the first kind (§2, 4); in the opposite case it is called completely reducible of the second kind.

[21] Cf. the note to §1, no. 3, on the second isomorphism theorem.

[22] In the familiar terminology of Steinitz: an algebraic extension is called of the first kind if every element is a zero of a prime function which, in a suitable extension field, decomposes into distinct linear factors; otherwise it is of the second kind.

If P is a perfect field, then only complete reducibility of the first kind occurs; in particular, this is always the case for an algebraically closed field. In what follows $\overline{P}$ denotes specifically the algebraically closed field derived from P, and $\overline{\mathfrak{R}}$ is equal to $\mathfrak{R}[\overline{P}]$.

2. **Theorem.** *The ring $\mathfrak{R}$ is completely reducible of the first kind if and only if the extension ring $\overline{\mathfrak{R}} = \mathfrak{R}[\overline{P}]$, with $\overline{P}$ algebraically closed, is completely reducible (of the first kind).*

The proof proceeds in three steps.

2 a. From complete reducibility of $\overline{\mathfrak{R}}$ — more generally, of any extension ring — there follows complete reducibility (of the first or second kind) of $\mathfrak{R}$. For by hypothesis the zero ideal of $\overline{\mathfrak{R}}$ has a representation as the least common multiple of prime ideals:

$$(\overline{0}) = [\overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_s].$$

By taking intersections one obtains in $\mathfrak{R}$ the representation of the zero ideal

$$(0) = [[\mathfrak{R}, \overline{\mathfrak{p}}_1], \ldots, [\mathfrak{R}, \overline{\mathfrak{p}}_s]],$$

and the ideals $[\mathfrak{R}, \overline{\mathfrak{p}}_i]$ are prime ideals by §1, 3.

2 b. From complete reducibility of the first kind of $\mathfrak{R}$ there follows complete reducibility of the first kind of $\overline{\mathfrak{R}}$, and more generally complete reducibility of the first kind of every intermediate ring between $\mathfrak{R}$ and $\overline{\mathfrak{R}}$.

Since, by §2, 3, a representation of $\mathfrak{R}$ as a direct sum gives a corresponding representation of $\overline{\mathfrak{R}}$ such that each component $\overline{\mathfrak{R}}_i$ becomes the extension ring $\mathfrak{R}_i[\overline{P}_i]$ — where $\overline{P}_i$ is an extension field isomorphic to $\overline{P}$ of the subfield P_i of the component $\mathfrak{R}_i$ isomorphic to P — it suffices to consider the individual component $\mathfrak{R}_i$. Thus, without loss of generality, $\mathfrak{R}$ may be assumed to be a field, indeed a finite extension field of the first kind over its subfield P. Then $\mathfrak{R}$ is generated by adjoining a primitive element of the first kind to P; equivalently, $\mathfrak{R}$ is isomorphic to the residue-class ring $P[x] \,|\, f(x)$, where $f(x)$ is a prime function of the first kind in the polynomial domain $P[x]$ in one indeterminate x. If Ω is an extension field of P, then $\Omega[x] \,|\, f(x)$ is isomorphic to $\mathfrak{R}[\Omega]$; for, in passing from $P[x]$ to $\Omega[x]$, the rank of the residue-class ring is preserved — equal to the degree of $f(x)$ — so that precisely the construction of the extension ring given in §1, 2 is involved. In $\Omega[x]$ the polynomial $f(x)$ decomposes into pairwise coprime prime functions of the first kind, each of which generates a prime ideal in $\Omega[x]$; hence $\Omega[x] \,|\, f(x)$, and therefore by the isomorphism also $\mathfrak{R}[\Omega]$, is completely reducible of the first kind. Since this holds for every extension field Ω, in particular also for the algebraically closed field $\overline{P}$, 2 b is proved.

2 c. If $\mathfrak{R}$ is completely reducible of the second kind, then $\overline{\mathfrak{R}}$ is not completely reducible.

As in 2 b, it suffices to suppose that $\mathfrak{R}$ is a field, and indeed a finite extension field of the second kind over P. It must be shown that in the representation of $\overline{\mathfrak{R}}$ as a direct sum of primary rings at least one proper primary component occurs. For this it is enough to exhibit a nonzero element of $\overline{\mathfrak{R}}$ some power of which vanishes. For if $\bar{\beta} \neq 0$, at least one component $\bar{\beta}_\lambda$ must be nonzero; and if $\bar{\beta}^\sigma = 0$, then $\bar{\beta}_\lambda^\sigma = 0$ (§2, 2, the homomorphism from $\overline{\mathfrak{R}}$ to $\overline{\mathfrak{R}}_\lambda$), and hence $\overline{\mathfrak{R}}_\lambda$ is not a field.

Let γ be an element of the second kind in $\mathfrak{R}$, of exponent $f \geq 1$, and let

$$F(\gamma) = \gamma^{kp^f} + c_1\gamma^{(k-1)p^f} + \cdots + c_k = 0$$

be the equation of lowest degree satisfied by γ over P, where p denotes the characteristic of P. The elements

$$e, \gamma, \gamma^2, \ldots, \gamma^{kp^f-1}$$

of $\mathfrak{R}$ are therefore linearly independent over P and consequently remain, by the definition of equality, linearly independent over $\overline{P}$ in $\overline{\mathfrak{R}}$. If one now sets

$$G(\gamma) = \gamma^{kp^{f-1}} + \sqrt[p]{c_1}\,\gamma^{(k-1)p^{f-1}} + \cdots + \sqrt[p]{c_k},$$

then $G(\gamma)$ is a nonzero element of $\overline{\mathfrak{R}}$; for, since $p > 1$ and $f \geq 1$, the exponent kp^{f-1} is always smaller than kp^f, and no dependence among the powers of γ occurring in $G(\gamma)$ can exist. But $(G(\gamma))^p = F(\gamma)$ and hence vanishes. Thus 2 c is proved.

From 2 a and 2 c it follows that complete reducibility (of the first kind) of $\overline{\mathfrak{R}}$ implies complete reducibility of the first kind of $\mathfrak{R}$; 2 b gives the converse. This proves the theorem in 2.

3. **Corollary.** *If $\mathfrak{R}$ is completely reducible of the first kind, then $\overline{\mathfrak{R}}$ is a direct sum of rings of rank one, hence of fields isomorphic to $\overline{P}$. Such a decomposition into rings of rank one already exists in a ring $\mathfrak{R}[\Omega]$, where Ω is a finite extension field of P.*

For by 2 b the ring $\overline{\mathfrak{R}}$ becomes a direct sum of fields which, as finite extensions of subfields isomorphic to $\overline{P}$ (§2, 2), coincide with those subfields because $\overline{P}$ is algebraically closed. Thus one obtains

$$\overline{\mathfrak{R}} = \overline{P}\bar{e}_1 + \cdots + \overline{P}\bar{e}_n, \qquad e = \bar{e}_1 + \cdots + \bar{e}_n;$$

the components $\bar{e}_\lambda$ of e at the same time form a linearly independent module basis of $\overline{\mathfrak{R}}$.

If the $\bar{e}_\lambda$ are represented, according to §1, 2, as linear combinations of elements γ of $\mathfrak{R}$ with coefficients in $\overline{P}$, then the system of all these coefficients determines a finite extension field Ω of P. Hence the $\bar{e}_\lambda$ already belong to $\mathfrak{R}[\Omega]$, and from the module-basis property one obtains

$$\mathfrak{R}[\Omega] = \Omega\bar{e}_1 + \cdots + \Omega\bar{e}_n.$$

Thus already in $\mathfrak{R}[\Omega]$ there is a decomposition into rings of rank one, and in every intermediate ring between $\mathfrak{R}[\Omega]$ and $\overline{\mathfrak{R}}$ the indecomposable components arise as extension rings of the $\Omega\bar{e}_i$. [23]

§4. Matrix Representation, Traces and Discriminants for Rings of Finite Rank.

In this and the next section the assumptions on the underlying ring are slightly more general than before, so as also to include orders in number fields and function fields. What is involved is a general and uniform formulation of essentially known facts.

Assumption: $\mathfrak{R}$ is an extension ring of a ring Σ without zero divisors; the identity element of $\mathfrak{R}$ already lies in Σ. For every Σ-module in $\mathfrak{R}$ — in particular for $\mathfrak{R}$ itself — there exists at least one finite module basis consisting of elements linearly independent over Σ. Besides $a_1, \ldots, a_s$, the elements $\beta_1, \ldots, \beta_s$ form a linearly independent module basis of the same Σ-module if and only if the transformation determinant is a unit of Σ.

The assumption is plainly fulfilled for the rings of finite rank considered up to now, where Σ is the field P. It is also fulfilled for orders in number fields and function fields, where Σ is respectively the ring of rational integers or the functional domain.[24]

1. Matrix rings homomorphic to $\mathfrak{R}$. Let $a_1, \ldots, a_s$ be a linearly independent Σ-module basis of the ideal $\mathfrak{a}$, and let γ be any element of $\mathfrak{R}$. Then γa_i also belongs to $\mathfrak{a}$, and there are equations with coefficients in Σ[25]:

$$\gamma a_i = c_{1i}a_1 + \cdots + c_{si}a_s, \qquad (i = 1, \ldots, s);$$

or in matrix form, if $(\tau_1, \ldots, \tau_s)$ denotes the one-row matrix formed from these elements,

$$(\gamma a_1, \ldots, \gamma a_s) = (a_1, \ldots, a_s)\begin{pmatrix} c_{11} & \cdots & c_{1s} \\ \vdots & & \vdots \\ c_{s1} & \cdots & c_{ss} \end{pmatrix} = (a_1, \ldots, a_s)C.$$

As γ runs through all elements of $\mathfrak{R}$, the totality of matrices C assigned by means of the basis a_i forms a ring $R_\mathfrak{a}$ homomorphic to $\mathfrak{R}$; $R_\mathfrak{a}$ is isomorphic to the residue-class ring $\mathfrak{R} \,|\, ((0) : \mathfrak{a})$, where $(0) : \mathfrak{a}$ denotes the ideal quotient of the zero ideal by $\mathfrak{a}$. For to the difference $\beta - \gamma$ there is plainly assigned $B - C$, and the same holds for the product, since

$$(\beta\gamma a_1, \ldots, \beta\gamma a_s) = (\beta a_1, \ldots, \beta a_s)C = (a_1, \ldots, a_s)BC.$$

[26] To the elements c of Σ there correspond in particular the diagonal matrices cE, where E denotes the matrix corresponding to the identity element e, namely $\begin{pmatrix} e & & \\ & \ddots & \\ & & e \end{pmatrix}$. Since moreover exactly those elements γ for which $\gamma\mathfrak{a}$ is the zero ideal are assigned the zero matrix, the stated isomorphism follows.

[23] The smallest such extension field Ω may be characterized as the compositum of the Galois fields determined by the components $\mathfrak{R}_i = \mathfrak{R}e_i$ of $\mathfrak{R}$. Namely, choose $f_i(x)$ as in 2 b so that $P[x] \,|\, f_i(x)$ is isomorphic to the component $\mathfrak{R}_i$, and let $\Omega^{(i)}$ be the Galois extension field lying in $\overline{P}$ which just suffices to split $f_i(x)$ into linear factors. Then Ω is the compositum of all $\Omega^{(i)}$. The splitting of $f_i(x)$ into linear factors corresponds to a representation of $\Omega^{(i)}[x] \,|\, f_i(x)$ as a direct sum of fields of rank one; $\Omega^{(i)}$ is the smallest extension field in which this happens. By isomorphism the same holds for $\mathfrak{R}_i[\Omega^{(i)}e_i]$ and hence for $\mathfrak{R}[\Omega]$.

[24] Cf. *Ideal Theory*, §3.

[25] Elements of Σ are denoted by Latin letters.

[26] The notation is arranged so that it remains valid for noncommutative rings $\mathfrak{R}$, provided that Σ is assumed to commute with all elements.

A basis $\bar{a}$ of $\mathfrak{a}$ generates a matrix ring isomorphic to $R_\mathfrak{a}$, indeed equivalent to it: $R_{\bar{\mathfrak{a}}} = P^{-1}R_\mathfrak{a}P$. Let $\bar{a}_1, \ldots, \bar{a}_s$ be another linearly independent Σ-module basis, so that

$$(\bar{a}_1, \ldots, \bar{a}_s) = (a_1, \ldots, a_s)P,$$

where the determinant of P is a unit of Σ. It follows that

$$(\gamma\bar{a}_1, \ldots, \gamma\bar{a}_s) = (a_1, \ldots, a_s)CP = (\bar{a}_1, \ldots, \bar{a}_s)P^{-1}CP,$$

or $R_{\bar{\mathfrak{a}}} = P^{-1}R_\mathfrak{a}P$.

2. Ideal classes and representation classes. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{R}$ belong to the same ideal class if, viewed as $\mathfrak{R}$-modules, they are isomorphic; that is, if their elements can be put into one-to-one correspondence in such a way that difference and multiplication by the same element of $\mathfrak{R}$ correspond, so that $a \simeq \beta$ always implies $\gamma a \simeq \gamma\beta$ for arbitrary $\gamma \in \mathfrak{R}$.

Two rings $R_\mathfrak{a}$ and $R_{\bar{\mathfrak{a}}}$ produced by matrix representation as in 1 belong to the same representation class if they are equivalent, that is, if there is a unimodular matrix P such that $R_{\bar{\mathfrak{a}}} = P^{-1}R_\mathfrak{a}P$.[27]

Ideal classes and representation classes correspond one-to-one. It was shown in 1 that different module bases of the same ideal generate rings $R_\mathfrak{a}$, $R_{\bar{\mathfrak{a}}}$ belonging to the same representation class; moreover, different ideals $\mathfrak{a}$, $\mathfrak{b}$ in the same ideal class likewise generate rings in the same representation class. For let $\beta_1, \ldots, \beta_s$ be the basis of $\mathfrak{b}$ corresponding under the isomorphism to the basis $a_1, \ldots, a_s$ of $\mathfrak{a}$. Then γa_i and $\gamma\beta_i$ correspond, as do $c_{1i}a_1 + \cdots + c_{si}a_s$ and $c_{1i}\beta_1 + \cdots + c_{si}\beta_s$; hence the rings $R_\mathfrak{a}$ and R_β are identical.

Conversely, suppose $R_\mathfrak{a}$ and $R_{\bar{\beta}}$ belong to the same representation class, so that $R_{\bar{\beta}} = P^{-1}R_\mathfrak{a}P$, where the a_i form a basis of $\mathfrak{a}$ and the $\bar{\beta}_i$ a basis of $\mathfrak{b}$. Then

$$(\beta_1, \ldots, \beta_s) = (\bar{\beta}_1, \ldots, \bar{\beta}_s)P^{-1}$$

is also a basis of $\mathfrak{b}$, and $R_\beta = PR_{\bar{\beta}}P^{-1} = R_\mathfrak{a}$. Associate to each element $a = c_1a_1 + \cdots + c_sa_s$ of $\mathfrak{a}$ the element $\beta = c_1\beta_1 + \cdots + c_s\beta_s$ of $\mathfrak{b}$. This correspondence is one-to-one, and sums and differences correspond. From $R_\mathfrak{a} = R_\beta$ it follows further that γa_i and $\gamma\beta_i$ correspond, since they can be expressed by the same linear forms in the a_i and β_i, respectively. Thus γa and $\gamma\beta$ correspond in general, and the ideals $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same ideal class. The class of the unit ideal is called the *principal class*; every basis of $\mathfrak{R}$ therefore gives the principal class as its representation class.

3. Trace of an element with respect to a class. Let C be the matrix assigned to the element γ of $\mathfrak{R}$ in $R_\mathfrak{a}$. Passing from $R_\mathfrak{a}$ to $R_{\bar{\mathfrak{a}}}$ shows that the determinant $|C|$, and more generally $|tE - C|$, where t is an indeterminate, is an invariant of the representation class. By 2 it is therefore also an invariant of the ideal class, briefly a *class invariant*. Thus the individual coefficients of t in $|tE - C|$ are class invariants. In particular, the coefficient of $(-t^{s-1})$ is called the *trace of γ with respect to the class*; in symbols,

$$S_{(\mathfrak{a})}(\gamma) = c_{11} + c_{22} + \cdots + c_{ss}.$$

The constant coefficient $\pm|C|$ is called the *norm of γ with respect to the class.*

For a fixed class $(\mathfrak{a})$ the traces $S_{(\mathfrak{a})}(\gamma)$ form a Σ-module to which $\mathfrak{R}$, viewed as a Σ-module, is homomorphic. For the ring homomorphism from $\mathfrak{R}$ to $R_\mathfrak{a}$ proved in 1 gives $(\beta - \gamma) \sim (B - C)$ and $c\beta \sim cEB = cB$. Hence

$$S_{(\mathfrak{a})}(\beta - \gamma) = S_{(\mathfrak{a})}(\beta) - S_{(\mathfrak{a})}(\gamma), \qquad S_{(\mathfrak{a})}(c\beta) = cS_{(\mathfrak{a})}(\beta),$$

which proves the module property and the homomorphism.

Remark: If $\mathfrak{R}$ is a ring without zero divisors, then the trace of an element is defined independently of the class; one may therefore speak simply of the trace. The same holds for the norm. For in a ring without zero divisors every ideal different from the zero ideal has the rank of the ring; hence every basis of an ideal is at the same time a basis of the unit ideal in the quotient field. All traces and norms are therefore generated in the quotient field by the unit ideal and are consequently independent of the class in $\mathfrak{R}$.

4. Discriminant of an ideal with respect to a class. It is not the discriminant itself, but only the principal ideal derived from it in Σ, that becomes an invariant of the ideal and the class.

Let $\varrho_1, \ldots, \varrho_s$ and $\bar{\varrho}_1, \ldots, \bar{\varrho}_s$ be two linearly independent Σ-module bases of an ideal $\mathfrak{r}$ of $\mathfrak{R}$. *The determinants $|S_{(\mathfrak{a})}(\varrho_i\varrho_k)|$ and $|S_{(\mathfrak{a})}(\bar{\varrho}_i\bar{\varrho}_k)|$ differ only by the square of a unit of Σ as a factor.* This holds for the two

[27] The question, settled in special cases, whether every homomorphic matrix ring can be generated by an ideal of $\mathfrak{R}$ as in 1 — possibly allowing linearly dependent bases — is not considered here. By definition, the representation classes consist only of matrix rings generated by ideals of $\mathfrak{R}$ as in 1.

determinants $|(\varrho_i\varrho_k)|$ and $|(\bar\varrho_i\bar\varrho_k)|$, which differ by the square of the transformation determinant between ϱ and $\bar\varrho$. By the module homomorphism proved in 3, the same linear relations hold between $S_{(\mathfrak{a})}(\varrho_i\varrho_k)$ and $S_{(\mathfrak{a})}(\bar\varrho_i\bar\varrho_k)$ as between $\varrho_i\varrho_k$ and $\bar\varrho_i\bar\varrho_k$; under the cogredient transformation the determinant therefore acquires the same factor.

Every determinant $|S_{(\mathfrak{a})}(\varrho_i\varrho_k)|$ is called a *discriminant of* $\mathfrak{r}$ *with respect to the class* $(\mathfrak{a})$, determined up to the square of a unit; the principal ideal derived from it in Σ is called the *discriminant ideal*.

Remark: If $\mathfrak{R}$ *is a ring without zero divisors, then the discriminant of an ideal is independent of the class used.*

For this independence holds by 3 for each individual entry of the determinant.

§5. Direct Sums of Classes.

1. Direct sum of the ideal class or representation class. If the ideal $\mathfrak{a}$ is a direct sum, $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$, then from the isomorphism it follows that every ideal $\bar{\mathfrak{a}}$ in the class is also a direct sum, $\bar{\mathfrak{a}} = \bar{\mathfrak{b}} + \bar{\mathfrak{c}}$. Here $\bar{\mathfrak{b}}$ is respectively isomorphic to $\mathfrak{b}$ and $\bar{\mathfrak{c}}$ to $\mathfrak{c}$, the ideals being regarded as $\mathfrak{R}$-modules; one may therefore speak of the *direct sum of the ideal class* and of the *component classes*.

If a ring $R_{\mathfrak{a}}$ in a representation class is a direct sum of subrings which are at the same time ideals in $R_{\mathfrak{a}}$, then by isomorphism the same is true for every ring $R_{\bar{\mathfrak{a}}}$ in the representation class, and the components are equivalent rings. Thus one may speak of the *direct sum of the representation class* and of the *component classes*.

The direct sum of the representation class corresponds to the direct sum of the ideal class; in this sense one speaks of the direct sum of the class.[28] Let $\beta_1, \ldots, \beta_l$ be a basis of $\mathfrak{b}$ and $\gamma_1, \ldots, \gamma_m$ a basis of $\mathfrak{c}$. Since the sum is direct, the β's and γ's together form a linearly independent basis a of $\mathfrak{a}$. If $R_{\mathfrak{a}}$ is the matrix ring generated by this basis, then the matrix in $R_{\mathfrak{a}}$ assigned to an arbitrary element δ of $\mathfrak{R}$ has the form $\left(\begin{smallmatrix} D^{(\beta)} & 0 \\ 0 & D^{(\gamma)} \end{smallmatrix}\right)$. Define $R^{(\beta)}$ to be the system of all matrices $\left(\begin{smallmatrix} D^{(\beta)} & 0 \\ 0 & 0 \end{smallmatrix}\right)$, and define $R^{(\gamma)}$ correspondingly. It remains to show that $R^{(\beta)}$ and $R^{(\gamma)}$ are subrings of $R_{\mathfrak{a}}$ and that $R_{\mathfrak{a}}$ is their direct sum; at the same time $R^{(\beta)}$ and $R^{(\gamma)}$ are respectively isomorphic to the rings R_β and R_γ generated from $\mathfrak{b}$ and $\mathfrak{c}$.

Indeed, by homomorphism $R^{(\beta)}$ corresponds to all elements δ of $\mathfrak{R}$ for which $\delta\mathfrak{c}$ vanishes, that is, to the elements of the quotient ideal $(0) : \mathfrak{c}$. Hence $R^{(\beta)}$ is an ideal in $R_{\mathfrak{a}}$, and the same holds for $R^{(\gamma)}$. The ring $R_{\mathfrak{a}}$ is the sum of these ideals, and the sum is direct because the product $R^{(\beta)}R^{(\gamma)}$ vanishes. Finally, assigning the matrix $D^{(\beta)}$ to the matrix in $R^{(\beta)}$ containing $D^{(\beta)}$ and zeros gives an isomorphism between $R^{(\beta)}$ and R_β; in this sense the component classes $(\mathfrak{b})$ and $(\mathfrak{c})$ of the ideal class of $\mathfrak{a}$ correspond to the component classes of $R_{\mathfrak{a}}$.

2. Behavior of trace and discriminant under direct sums of classes. If $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$ and the matrix $\left(\begin{smallmatrix} D^{(\beta)} & 0 \\ 0 & D^{(\gamma)} \end{smallmatrix}\right)$ is used to determine the trace $S_{(\mathfrak{a})}(\delta)$, then, taking 1 into account, one reads off:

The trace of an element, taken with respect to a class, is the sum of the traces taken with respect to the component classes.

Because the product $\mathfrak{bc}$ vanishes, one reads off further:

If β *is an element of* $\mathfrak{b}$*, then* $S_{(\mathfrak{a})}(\beta) = S_{(\mathfrak{b})}(\beta)$*; the trace of* β *taken with respect to the class* $(\mathfrak{a})$ *equals its trace taken with respect to the class* $(\mathfrak{b})$.

Taking §4, 4 into account, it follows further:

The discriminant ideal of the component ideal $\mathfrak{b}$*, taken with respect to the class* $(\mathfrak{a})$*, equals the discriminant ideal of* $\mathfrak{b}$ *taken with respect to the component class* $(\mathfrak{b})$.

Finally:

The discriminant ideal of $\mathfrak{a}$*, taken with respect to the class* $(\mathfrak{a})$*, equals the product of the discriminant ideals of the components, taken with respect to the component classes.* For if the basis of the β's and γ's corresponding to the direct sum is used both in forming the discriminant and in forming the trace, a basis of the discriminant ideal of $\mathfrak{a}$ with respect to $(\mathfrak{a})$ is given by

$$\begin{vmatrix} S_{(\mathfrak{a})}(\beta_i\beta_k) & 0 \\ 0 & S_{(\mathfrak{a})}(\gamma_\mu\gamma_\nu) \end{vmatrix} = \begin{vmatrix} S_{(\mathfrak{b})}(\beta_i\beta_k) & 0 \\ 0 & S_{(\mathfrak{c})}(\gamma_\mu\gamma_\nu) \end{vmatrix} \quad \begin{pmatrix} i,k = 1,\ldots,l, \\ \mu,\nu = 1,\ldots,m \end{pmatrix}.$$

3. Passage to extension rings. Let $\overline{\Sigma}$ be an extension ring without zero divisors of Σ such that the intersection of $\mathfrak{R}$ and $\overline{\Sigma}$ is Σ; let the extension ring $\overline{\mathfrak{R}} = \mathfrak{R}[\overline{\Sigma}]$ obtained by adjoining $\overline{\Sigma}$ be defined, as in §1, 2, as a ring of the same rank.

[28] The question to what extent all direct sums of representation classes can be produced by direct sums of ideal classes is again not taken up here.

If $\mathfrak{a}$ and $\mathfrak{r}$ are ideals in $\mathfrak{R}$ and $\bar{\mathfrak{a}}$ and $\bar{\mathfrak{r}}$ their extension ideals in $\overline{\mathfrak{R}}$, then the discriminant ideal of $\bar{\mathfrak{r}}$, taken with respect to $(\bar{\mathfrak{a}})$, is likewise the extension ideal in $\overline{\Sigma}$ of the discriminant ideal of $\mathfrak{r}$ taken with respect to $(\mathfrak{a})$. For every basis of $\mathfrak{a}$ or $\mathfrak{r}$ is also an $\overline{\Sigma}$-module basis of $\bar{\mathfrak{a}}$ or $\bar{\mathfrak{r}}$, so bases of $\mathfrak{a}$ and $\mathfrak{r}$ may be used in constructing the discriminant of $\bar{\mathfrak{r}}$ with respect to $(\bar{\mathfrak{a}})$. In particular, the discriminant ideal of $\overline{\mathfrak{R}}$ with respect to the principal class $(\overline{\mathfrak{R}})$ is the extension ideal of that of $\mathfrak{R}$ with respect to the principal class $(\mathfrak{R})$. The ideal so defined in Σ, respectively $\overline{\Sigma}$, is briefly called the *discriminant ideal of the ring.*

§6. Discriminant Criterion for Complete Reducibility of the First Kind.

From now on $\mathfrak{R}$ is again assumed to be an extension ring of a field P, and $\overline{P}$ is an extension field of P. The nonvanishing of the discriminant will turn out to be the necessary and sufficient condition for complete reducibility of the first kind. By §5, no. 3, the discriminant ideal of $\mathfrak{R}$ can be determined by means of the extension ring $\overline{\mathfrak{R}} = \mathfrak{R}[\overline{P}]$; and by §5, no. 2, it suffices to restrict attention to the primary rings of which $\overline{\mathfrak{R}}$ is additively composed. We shall therefore first consider discriminant ideals of primary rings.

1. Special P-module bases. If $\mathfrak{a}$ and $\mathfrak{t}$ are ideals of $\mathfrak{R}$ and $\mathfrak{a}$ is divisible by $\mathfrak{t}$, then every basis $a_1, \ldots, a_s$ of $\mathfrak{a}$ can be completed, by adjoining elements $\tau_{s+1}, \ldots, \tau_t$, to a linearly independent module basis of $\mathfrak{t}$[29]. This is an immediate consequence of the assumed finite rank over the field P.

Now suppose that $\mathfrak{R}$ is a *primary ring*; let $\mathfrak{p}$ be the prime ideal belonging to the zero ideal and ϱ its exponent, so that $\mathfrak{p}^\varrho = (0)$ and $\mathfrak{p}^{\varrho-1} \neq (0)$. A special P-module basis of $\mathfrak{R}$ is obtained by successively completing a basis of $\mathfrak{p}^{\varrho-1}$ to one of $\mathfrak{p}^{\varrho-2}$ and, in general, a basis of $\mathfrak{p}^\lambda$ to one of $\mathfrak{p}^{\lambda-1}$, with $\mathfrak{R}$ counted as $\mathfrak{p}^0$. With such a basis one can show:

If $\mathfrak{R}$ is a primary ring, then the trace, taken with respect to the principal class (§4, no. 2), of every element divisible by the corresponding prime ideal $\mathfrak{p}$ vanishes. Indeed, let

$$\pi_{0,1}, \ldots, \pi_{0,i_0}; \quad \pi_{1,1}, \ldots, \pi_{1,i_1}; \quad \ldots; \quad \pi_{\varrho-1,1}, \ldots, \pi_{\varrho-1,i_{\varrho-1}}$$

be such a special P-module basis, with

$$\pi_{\lambda,j} \equiv 0 \pmod{\mathfrak{p}^\lambda}, \qquad \pi_{\lambda,j} \not\equiv 0 \pmod{\mathfrak{p}^{\lambda+1}}.$$

From $\pi \equiv 0 \pmod{\mathfrak{p}}$ it follows that $\pi\pi_{\lambda,j} \equiv 0 \pmod{\mathfrak{p}^{\lambda+1}}$; hence the matrix assigned to π by means of this basis has only zeros on the diagonal, and the trace of π vanishes.

2. Discriminant ideals of primary rings with algebraically closed subring P. If the zero ideal of $\mathfrak{R}$ is a prime ideal and P is algebraically closed, then $\mathfrak{R}$ is of rank one and hence identical with P (§3, no. 3); the identity element e may be taken as module basis. Thus

$$S_{(\mathfrak{R})}(e^2) = S_{(\mathfrak{R})}(e) = e,$$

and the discriminant ideal is the unit ideal.

The discriminant ideal of a proper primary ring with algebraically closed subring P is the zero ideal. If one uses for $\mathfrak{R}$ the special module basis given in no. 1—or merely completes any basis of $\mathfrak{p}$ to a basis of $\mathfrak{R}$—then i_0 is one, since the residue-class ring $\mathfrak{R}/\mathfrak{p}$ is of rank one; the identity element e may be taken as $\pi_{0,1}$. All basis products different from e^2 are then divisible by $\mathfrak{p}$, and their trace with respect to the principal class vanishes. Consequently the discriminant vanishes as a determinant of at least two rows—$\mathfrak{R}$ was assumed properly primary and therefore must possess at least one basis element different from e—in which every entry other than $S_{(\mathfrak{R})}(e^2)$ vanishes.

3. Theorem. *The ring $\mathfrak{R}$ of finite rank over a subfield P is completely reducible of the first kind if and only if its discriminant ideal is the unit ideal in P; in other words, if and only if the discriminant, determined up to the square of a unit, is nonzero.*

Complete reducibility of the first kind is, by §3, no. 2, identical with the assertion that the extension ring $\overline{\mathfrak{R}} = \mathfrak{R}[\overline{P}]$ is completely reducible, that is, that its indecomposable components are fields isomorphic to $\overline{P}$. By §5, no. 3, the discriminant ideals of $\mathfrak{R}$ and $\overline{\mathfrak{R}}$ are simultaneously the zero ideal or the unit ideal; and by §5, no. 2, the discriminant ideal of $\overline{\mathfrak{R}}$ is the product of the discriminant ideals of its components, taken with respect to those components. The individual discriminant ideals arise from those considered in no. 2—where

[29] The matrix representation of an arbitrary element γ furnished by this basis then has the form $\left(\begin{smallmatrix} C_a & 0 \\ C_1 & C_2 \end{smallmatrix}\right)$; conversely, such a matrix representation furnished by $\mathfrak{t}$ implies the existence of a multiple $\mathfrak{a}$ of $\mathfrak{t}$. Since under complete reducibility the indecomposable components possess no ideal different from the zero or unit ideal, such a representation cannot occur in the representation class of these component ideals. If one also uses the connection, given in §5, no. 1, between direct sums of classes, one arrives at the definition of complete reducibility customary in the literature.

the components occur as rings considered in themselves and not as ideals of $\overline{\overline{\mathfrak{R}}}$—by replacing, in each case, the field $\bar{P}_i = \overline{P}\bar{\varepsilon}_i$ isomorphic to $\overline{P}$ by $\overline{P}$ itself. Hence, if $\overline{\overline{\mathfrak{R}}}$ is completely reducible, its discriminant ideal, being a product of unit ideals, is itself the unit ideal; whereas if $\overline{\overline{\mathfrak{R}}}$ is not completely reducible, at least one component has discriminant ideal equal to the zero ideal, and consequently the discriminant ideal of $\overline{\overline{\mathfrak{R}}}$ is zero. This proves the theorem.

4. Representation of trace, norm, and discriminant by conjugate elements in the case of complete reducibility of the first kind. Let, by §3, no. 3, in the case of complete reducibility of the first kind,

$$\mathfrak{R}[\Omega] = \Omega\bar{\varepsilon}_1 + \cdots + \Omega\bar{\varepsilon}_n$$

be a representation as a direct sum of rings of rank one—hence of fields isomorphic to Ω—and let Ω be the smallest extension field in which such a representation is possible. The n components of $\mathfrak{R}$ are then given by $K_i\bar{\varepsilon}_i$, where each K_i is a subfield of Ω and $\mathfrak{R}$ is homomorphic to K_i. We shall express trace, norm, and discriminant (with respect to the principal class) by elements of the K_i.

Taking $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_n$ as module basis, every element

$$\gamma = c_1\bar{\varepsilon}_1 + \cdots + c_n\bar{\varepsilon}_n$$

is assigned the diagonal matrix with diagonal entries $c_1, \ldots, c_n$, where c_i belongs to K_i whenever γ belongs to $\mathfrak{R}$. Consequently

$$S(\gamma) = c_1 + \cdots + c_n, \qquad N(\gamma) = c_1 \cdots c_n,$$

where $S(\gamma)$ denotes the trace and $N(\gamma)$ the norm with respect to the principal class.

If further $a_1, \ldots, a_n$ is a module basis of $\mathfrak{R}$ consisting of elements of $\mathfrak{R}$, its discriminant $|S(a_ia_k)|$ can be expressed by elements of all the K_i. Write

$$a_i = a_i^{(1)}\bar{\varepsilon}_1 + \cdots + a_i^{(n)}\bar{\varepsilon}_n.$$

Then

$$a_ia_k = a_i^{(1)}a_k^{(1)}\bar{\varepsilon}_1 + \cdots + a_i^{(n)}a_k^{(n)}\bar{\varepsilon}_n, \qquad S(a_ia_k) = a_i^{(1)}a_k^{(1)} + \cdots + a_i^{(n)}a_k^{(n)},$$

and therefore

$$|S(a_ia_k)| = \left|\sum_\lambda a_i^{(\lambda)}a_k^{(\lambda)}\right| = \begin{vmatrix} a_1^{(1)} & \cdots & a_n^{(1)} \\ \vdots & & \vdots \\ a_1^{(n)} & \cdots & a_n^{(n)} \end{vmatrix}^2.$$

If in particular $\mathfrak{R}$ itself is a field, hence an extension field of the first kind of the subfield P, then the homomorphism from $\mathfrak{R}$ to K_i becomes an isomorphism under which the elements of P correspond to themselves—for the component of P is $P\bar{\varepsilon}_i$. Since they all lie in the common containing field Ω, the K_i are therefore conjugate fields with respect to P; and the n isomorphisms are all distinct, as the determinant representation above of the nonzero discriminant $|S(a_ia_k)|$ shows.

Thus, if $\mathfrak{R}$ is a field, the representation as a direct sum in $K_1, \ldots, K_n$ yields the n conjugate extension fields of degree n over P, lying in the Galois extension field and isomorphic to $\mathfrak{R}$. The representation of trace, norm, and discriminant becomes the familiar representation by conjugate elements. It should again be emphasized that $\mathfrak{R}$ is assumed only as a field equivalent to the K_i, and not as a field already lying in the Galois extension field Ω[30].

§7. The Discriminant Theorem for the Orders of an Algebraic Number or Function Field.

1. The number fields and function fields under consideration—where, for algebraic functions of more than one indeterminate and for integral algebraic functions, an extension of the functional domain is involved—all fit the following field type, with a fixed notion of integral elements[31]:

Let $\mathfrak{H}$ be a *principal ideal domain without zero divisors and with identity* (the ring of rational integers, the polynomial domain in one indeterminate with coefficients in a field, or the functional domain), and let $\mathfrak{R}'$ be its *quotient field*; let $\mathfrak{L}$ be a *finite extension of the first kind* of $\mathfrak{R}'$, and let $\mathfrak{S}$ be the *ring of all quantities*

[30] Cf. the final note to §1, no. 2.

[31] *Ideal Theory*, §3, nos. 3 and 4.

in $\mathfrak{L}$ integral with respect to $\mathfrak{H}$[32]*. Every subring of $\mathfrak{S}$ that contains $\mathfrak{H}$ is called an order; $\mathfrak{S}$ itself is called the principal order.*

Every $\mathfrak{H}$-module in $\mathfrak{S}$, in particular every ideal of an order and the order itself, possesses a *linearly independent module basis* over $\mathfrak{H}$[33]. If $\mathfrak{L}$ has degree n over $\mathfrak{R}'$, it is enough to restrict attention to orders of rank n over $\mathfrak{H}$, since every order of lower rank generates by passage to quotients an intermediate field of $\mathfrak{R}'$ and $\mathfrak{L}$ of that same degree, for which all the assumptions remain valid.

Every order $\mathfrak{T}$ is therefore a ring satisfying the more general assumptions of §4 and §5, and indeed a ring without zero divisors; hence the discriminant $D_{\mathfrak{T}}$ of the order is uniquely determined up to the square of a unit of $\mathfrak{H}$ as a factor. This discriminant is at the same time, up to a unit of $\mathfrak{R}'$ as a factor, identical with the discriminant of the field $\mathfrak{L}$, viewed as an $\mathfrak{R}'$-module, and is therefore *nonzero*, since $\mathfrak{L}$ was assumed to be an extension of the first kind (§6, no. 3). The discriminant also admits the representation, given in §6, no. 4, by the square of the determinant of conjugate basis elements.

The ideal theory in $\mathfrak{T}$ is given by the theorem[34]: *In $\mathfrak{T}$, every nonzero ideal can be represented uniquely as a product of finitely many pairwise coprime primary ideals whose corresponding prime ideals have no proper divisor different from the unit ideal.*

2. Passage from the order to rings of finite rank over a field. Let p be a prime element of $\mathfrak{H}$, so that the principal ideal $\mathfrak{H}p$ derived from p in $\mathfrak{H}$ is a prime ideal different from the zero and unit ideals; let $\mathfrak{T}p$ denote correspondingly the principal ideal derived from p in $\mathfrak{T}$[35]. *The residue-class ring $\mathfrak{R} = \mathfrak{T}/\mathfrak{T}p$ becomes a ring of rank n over a subfield P isomorphic to the field $\mathfrak{H}/\mathfrak{H}p$; $\mathfrak{T}$ is homomorphic to $\mathfrak{T}/\mathfrak{T}p$.*

The homomorphism $\mathfrak{T} \sim \mathfrak{T}/\mathfrak{T}p$ holds generally for every residue-class ring. That $\mathfrak{R}$ contains a subfield P isomorphic to $\mathfrak{H}/\mathfrak{H}p$ follows from the second isomorphism theorem[36]; for the subring $(\mathfrak{H}, \mathfrak{T}p)/\mathfrak{T}p$ is isomorphic to $\mathfrak{H}/[\mathfrak{H}, \mathfrak{T}p] = \mathfrak{H}/\mathfrak{H}p$.

Finally, $\mathfrak{R}$ also has rank n over P. Let $a_1, \ldots, a_n$ be a linearly independent module basis of $\mathfrak{T}$ over $\mathfrak{H}$, and let $(a_1), \ldots, (a_n)$ be the residue classes determined by the a_i modulo $\mathfrak{T}p$. Every linear dependence of the (a_i) over P would arise under the homomorphism from a congruence

$$c_1 a_1 + \cdots + c_n a_n \equiv 0 \pmod{\mathfrak{T}p},$$

hence from a relation

$$c_1 a_1 + \cdots + c_n a_n = p\gamma,$$

where γ belongs to $\mathfrak{T}$. From the representability of γ by the basis a_i and the uniqueness of this representation, it follows that every c_i is divisible by p; consequently the element (c_i) of P vanishes. This proves the linear independence of the (a_i) over P.

Under the homomorphism, the discriminant $D_{\mathfrak{T}}$ of $\mathfrak{T}$ passes into the discriminant of $\mathfrak{R}$, and the ideal decomposition of $\mathfrak{T}p$ in $\mathfrak{T}$ passes into the decomposition of the zero ideal of $\mathfrak{R}$. Because of the linear independence of the (a_i) just proved, the discriminant of $\mathfrak{R}$ can be formed from this basis as $|S((a_i)(a_k))|$ and therefore arises under the homomorphism from the discriminant $|S(a_i a_k)|$ of $\mathfrak{T}$ formed by means of the basis a_i. Here the matrix representation, and not the representation by conjugate elements—which is valid for $\mathfrak{T}$ but not necessarily for $\mathfrak{R}$—is used in defining the trace; the trace, and hence the discriminant, therefore arises by ring operations from ring elements.

If

$$\mathfrak{T}p = \mathfrak{q}_1 \cdots \mathfrak{q}_r = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

is the representation of $\mathfrak{T}p$ in $\mathfrak{T}$, it passes under the homomorphism into

$$(0) = [(\mathfrak{q}_1), \ldots, (\mathfrak{q}_r)]$$

in $\mathfrak{R}$. By the first isomorphism theorem[37], $\mathfrak{R}/(\mathfrak{q}_i)$ is isomorphic to $\mathfrak{T}/\mathfrak{q}_i$; hence $\mathfrak{q}_i$ and $(\mathfrak{q}_i)$ are simultaneously proper primary ideals or prime ideals, and the $(\mathfrak{q}_i)$ are pairwise coprime by homomorphism.

3. Discriminant theorem. *A prime element p of $\mathfrak{H}$ divides the discriminant $D_{\mathfrak{T}}$ of an order $\mathfrak{T}$ if and only if, in the decomposition of the principal ideal $\mathfrak{T}p$ into pairwise coprime primary components in $\mathfrak{T}$, at*

[32] For the definition of quantities integral with respect to a ring, cf. *Ideal Theory*, §1, no. 3.

[33] *Ideal Theory*, §3, no. 1.

[34] *Ideal Theory*, §7, no. 3.

[35] This notation for principal ideals will be used from now on in order to indicate at the same time the ring in which they are being considered.

[36] Cf. the final note to §1.

[37] Cf. *Ideal Theory*, §4, no. 3, and §6 (after Theorem II).

least one proper primary component or at least one prime ideal of the second kind occurs[38].

If the residue field $\mathfrak{H}/\mathfrak{H}p$ is perfect, then every prime element p that divides $D_{\mathfrak{T}}$—and only such a p—has at least one proper primary component. If $\mathfrak{H}/\mathfrak{H}p$ is perfect and $\mathfrak{T}$ is chosen to be the principal order $\mathfrak{S}$, then p divides the discriminant if and only if it is divisible by at least the square of a prime ideal of $\mathfrak{S}$.

For, by the correspondence between the ideal decomposition of the principal ideal $\mathfrak{T}p$ in $\mathfrak{T}$ and that of the zero ideal in $\mathfrak{R} = \mathfrak{T}/\mathfrak{T}p$ (cf. no. 2), the occurrence of a proper primary component or of a prime ideal of the second kind in $\mathfrak{T}p$ means that $\mathfrak{R}$ is *not* completely reducible of the first kind. By §6, no. 3, this is the case if and only if the discriminant of $\mathfrak{R}$ vanishes, which by the homomorphism in no. 2 says precisely that $D_{\mathfrak{T}}$ is divisible by p.

§8. The Discriminant Theorem for the Orders of Relative Fields.

If instead of the principal ideal domain $\mathfrak{H}$ one already takes as the starting ring the principal order of a number field or function field—more generally, a *multiplication ring*[39], that is, a ring in which the ideal theory of the principal order holds—then in place of the discriminant $D_{\mathfrak{T}}$ there appears the discriminant ideal of $\mathfrak{T}$ with respect to $\mathfrak{H}$[40]; the discriminant theorem transfers completely by means of the following considerations.

1. Let $\mathfrak{H}$ be a *multiplication ring*, that is, a ring without zero divisors and with identity, in which every ideal different from the zero and unit ideals can be represented uniquely as a power product of prime ideals, and where these prime ideals have no proper divisor different from the unit ideal[41]. Let $\mathfrak{R}', \mathfrak{L}, \mathfrak{S}, \mathfrak{T}$ be defined as in §7, no. 1; then the ideal theory stated in §7, no. 1 holds in $\mathfrak{T}$[42].

In particular, if a multiplication ring $\mathfrak{H}$ has only one prime ideal different from the zero and unit ideals, then $\mathfrak{H}$ is a principal ideal domain. For let $\mathfrak{p}$ be this prime ideal and choose $p \equiv 0 \pmod{\mathfrak{p}}$, $p \not\equiv 0 \pmod{\mathfrak{p}^2}$. Since by hypothesis every ideal different from the zero and unit ideals is a power of $\mathfrak{p}$, this holds in particular for the principal ideal $\mathfrak{H}p$. Because $p \not\equiv 0 \pmod{\mathfrak{p}^2}$, it follows necessarily that $\mathfrak{H}p = \mathfrak{p}$; hence every power of $\mathfrak{p}$ is a principal ideal. The zero and unit ideals are principal as well.

2. Trace and discriminant ideal. The trace of every element γ of $\mathfrak{T}$ is *defined as the trace of γ in $\mathfrak{L}$, where $\mathfrak{L}$ is regarded as an $\mathfrak{R}'$-module*; every system of n elements of $\mathfrak{L}$ linearly independent over $\mathfrak{R}'$ may therefore be chosen as a basis for producing a matrix representation that defines the trace. If $a_1, \ldots, a_n$ is such a system, then, since $\mathfrak{L}$ is assumed to be an extension of the first kind, $|S(a_i a_k)|$ is a nonzero element of $\mathfrak{R}'$, indeed the square of the determinant of the conjugate basis elements (§6, no. 4). From the integral closedness of $\mathfrak{H}$ in $\mathfrak{R}'$[43] it follows that $|S(a_i a_k)|$ belongs to $\mathfrak{H}$ as soon as all a_i belong to $\mathfrak{S}$.

Discriminant ideal: Let $\tau_1, \ldots, \tau_n$ run through all systems of n elements of $\mathfrak{T}$, and form for each system the determinant $|S(\tau_i \tau_k)|$, which is an element of $\mathfrak{H}$ and is nonzero whenever the τ_i are linearly independent. *The ideal in $\mathfrak{H}$ derived from the totality of these determinants is called the discriminant ideal of the order $\mathfrak{T}$ with respect to $\mathfrak{H}$;* it is therefore different from the zero ideal.

If further $\beta_1, \ldots, \beta_m$, with $m \geq n$, is an $\mathfrak{H}$-module basis of $\mathfrak{T}$ (which always exists)[44], then the finitely many determinants corresponding to systems of n of the β's form an ideal basis of the discriminant ideal. This follows from the module homomorphism from $\mathfrak{T}$ to the system of traces from $\mathfrak{T}$ (§4, no. 3). Indeed, the determinants $|(\tau_i \tau_k)|$ formed from the products $\tau_i \tau_k$ are expressible linearly, with coefficients in $\mathfrak{H}$, in terms of the finitely many determinants $|(\beta_i \beta_k)|$ corresponding to systems of n of the β's; therefore the same holds for the $|S(\tau_i \tau_k)|$ in terms of the $|S(\beta_i \beta_k)|$. If in particular the order possesses a linearly independent module basis $a_1, \ldots, a_n$, then $|S(a_i a_k)|$ may be taken as a basis of the discriminant ideal; the definition agrees with that of §7, no. 1.

---

[38] An example of the occurrence of prime ideals of the second kind is the following. Let $\mathfrak{H}$ be the functional domain derived from all polynomials in x with rational-integer coefficients, let $\mathfrak{R}'$ be its quotient field, and let $\mathfrak{L}$ be the extension field obtained by adjoining $\sqrt{x}$. Consider the order $\mathfrak{T}$ with module basis $1, \sqrt{x}$ over $\mathfrak{H}$ (as the substitution $x = y^2$ shows, this is the principal order). The discriminant is $\left|\begin{smallmatrix} 1 & \sqrt{x} \\ 1 & -\sqrt{x} \end{smallmatrix}\right|^2 = 2^2 x$; the principal ideal $\mathfrak{T}2$ remains a prime ideal in $\mathfrak{T}$, but one of the second kind. Indeed, because of the module basis $1, \sqrt{x}$, the order $\mathfrak{T}$ is isomorphic to the residue-class ring $\mathfrak{H}[t]/(t^2 - x)$, where t is a new indeterminate; consequently $\mathfrak{T}/\mathfrak{T}2 = \mathfrak{R}$ is isomorphic to $P[t]/(t^2 - x)$, where P is the field of all rational functions in x and the indeterminates occurring in the functional domain, with coefficients modulo 2. Since $t^2 - x$ is a prime function in $P[t]$, and indeed a prime function of the second kind, $\mathfrak{R}$ is a field and an extension field of the second kind of P; hence $\mathfrak{T}2$ is a prime ideal of the second kind. By contrast, $\mathfrak{T}x = (\mathfrak{T}\sqrt{x})^2$ is properly primary. It is not generally true that $\mathfrak{R}$ is generated over P by adjoining one element: one need only replace the single indeterminate x by x and y to see, in the order derived from $1, \sqrt{x}, \sqrt{y}, \sqrt{xy}$—which again is the principal order—that the principal ideal $\mathfrak{T}2$ is a prime ideal of the second kind for which $\mathfrak{R}$ is generated over P only after adjoining two elements. For these examples cf. Ostrowski, loc. cit.

[39] I take the short designation "multiplication ring" from W. Krull's note, *Über Multiplikationsringe*, Heidelberger Berichte, 1925, 5th paper, no. 3. Krull, however, calls the rings without zero divisors occurring here "regular multiplication rings".

[40] In the literature, in the case of "relative number fields", only the discriminant ideal of the principal order occurs, the "relative discriminant". Cf. Hilbert, *Zahlbericht*, §14, and Hecke, *Theorie der algebraischen Zahlen*, §38.

[41] For the axiomatic theory of multiplication rings, cf. *Ideal Theory*, for example the introduction.

[42] *Ideal Theory*, §3, no. 2, and §7, no. 3.

[43] *Ideal Theory*, §9, no. 7.

[44] *Ideal Theory*, §9, and §3, no. 1.

3. Passage to the quotient ring[45]**.** If $\mathfrak{a}$ is any ideal of $\mathfrak{T}$, the quotient ring $\mathfrak{T}_\mathfrak{a}$ is defined as the totality of elements of the quotient field $\mathfrak{L}$ of $\mathfrak{T}$ whose denominator is an element of $\mathfrak{T}$ prime to $\mathfrak{a}$[46]. Apart from the zero and unit ideals, the ring $\mathfrak{T}_\mathfrak{a}$ has no prime ideals other than the extension ideals of the prime ideals belonging to $\mathfrak{a}$. There is a one-to-one correspondence, with isomorphism of residue-class rings, between all ideals of $\mathfrak{T}_\mathfrak{a}$ different from the zero and unit ideals and those ideals of $\mathfrak{T}$ whose corresponding prime ideals are among those belonging to $\mathfrak{a}$; moreover the zero and unit ideals correspond one-to-one.

The same considerations apply to the multiplication ring $\mathfrak{H}$. If in particular $\mathfrak{p}$ is a prime ideal, then $\mathfrak{H}_\mathfrak{p}$ has only one prime ideal different from the zero and unit ideals; by the isomorphism of residue-class rings, $\mathfrak{H}_\mathfrak{p}$ is, with $\mathfrak{H}$, a multiplication ring, and by no. 1 it is therefore a principal ideal domain. A basis of the prime ideal derived from $\mathfrak{p}$ becomes a prime element p of $\mathfrak{H}_\mathfrak{p}$. The extension ideal of any ideal $\mathfrak{c}$ of $\mathfrak{H}$ is generated by the primary component of $\mathfrak{c}$ belonging to $\mathfrak{p}$, and is therefore equal to $(p)^e$ or to the unit ideal according as $\mathfrak{p}$ occurs in $\mathfrak{c}$—to the e-th power—or does not occur in $\mathfrak{c}$. It follows further that, if the extensions of two ideals $\mathfrak{b}$ and $\mathfrak{c}$ of $\mathfrak{H}$ agree in *all* quotient rings $\mathfrak{H}_\mathfrak{p}$, then $\mathfrak{b}$ and $\mathfrak{c}$ are identical; for they are divisible by the same prime ideals $\mathfrak{p}$ and to the same powers.

4. The discriminant ideal under passage to the quotient ring. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{H}$ and let $\mathfrak{P} = \mathfrak{T}\mathfrak{p}$ denote its extension ideal in $\mathfrak{T}$. *The quotient ring $\mathfrak{T}_\mathfrak{P}$ possesses a module basis consisting of linearly independent elements over the principal ideal domain $\mathfrak{H}_\mathfrak{p}$; at the same time $\mathfrak{T}_\mathfrak{P}$ is a finite $\mathfrak{H}_\mathfrak{p}$-order in the extension field $\mathfrak{L}$ of the quotient field $\mathfrak{R}'$ of $\mathfrak{H}_\mathfrak{p}$*[47]*. Thus in $\mathfrak{T}_\mathfrak{P}$, with respect to $\mathfrak{H}_\mathfrak{p}$, the discriminant theorem (§7, no. 3) holds.*

The discriminant $D_{\mathfrak{T}_\mathfrak{P}}$ is then a basis of the extension ideal, taken in $\mathfrak{H}_\mathfrak{p}$, of the discriminant ideal of $\mathfrak{T}$ with respect to $\mathfrak{H}$. Choose, as is always possible, elements $a_1, \ldots, a_n$ of $\mathfrak{T}$ as an $\mathfrak{H}_\mathfrak{p}$-module basis of $\mathfrak{T}_\mathfrak{P}$. Then $|S(a_i a_k)|$ belongs to the discriminant ideal, and by no. 1 every determinant $|S(\tau_i \tau_k)|$ in $\mathfrak{H}_\mathfrak{p}$ is divisible by $|S(a_i a_k)|$[48].

5. General discriminant theorem. *A prime ideal $\mathfrak{p}$ of a multiplication ring $\mathfrak{H}$ occurs in the discriminant ideal of an order with respect to $\mathfrak{H}$ if and only if, in the ideal decomposition of $\mathfrak{T}\mathfrak{p}$ into pairwise coprime primary components in $\mathfrak{T}$, at least one proper primary component or at least one prime ideal of the second kind occurs.*

From nos. 3 and 4 it follows that a prime ideal $\mathfrak{p}$ of $\mathfrak{H}$ occurs in the discriminant ideal of $\mathfrak{T}$ if and only if the prime element p of $\mathfrak{H}_\mathfrak{p}$ divides the discriminant $D_{\mathfrak{T}_\mathfrak{P}}$. But this is identical with saying that the residue-class ring $\mathfrak{T}_\mathfrak{P}/\mathfrak{T}_\mathfrak{P} p$ is not completely reducible of the first kind; and since by no. 3 this residue-class ring is isomorphic to $\mathfrak{T}/\mathfrak{T}\mathfrak{p}$, the general discriminant theorem is proved.

As a specialization to relative discriminants of number fields one obtains:

A prime ideal $\mathfrak{p}$ of the principal order of a number field occurs in the relative discriminant of an extension field if and only if $\mathfrak{p}$ is divisible in the principal order of the extension field by the square of a prime ideal.

Göttingen, March 30, 1926.

---

[45] For proofs of all the theorems cited in this number, cf. H. Grell's paper cited on p. 83 in note 6.

[46] Since the prime ideals of $\mathfrak{T}$ have no proper divisor different from the unit ideal, "prime to" here is identical with "coprime" in the ideal-theoretic sense.

[47] For the proof, cf. H. Grell.

[48] This also gives—when $\mathfrak{H}$ is the principal order of an algebraic number field—agreement with the relative discriminant defined by Hilbert (which is known to agree with Hecke's definition). Let $\omega_1, \ldots, \omega_m$ be an $\mathfrak{H}$-module basis of the principal order of the relative field—Hilbert chooses in particular a module basis over the ring of rational integers—and, following Hilbert, form all determinants from systems of n basis elements and their conjugates. The "relative discriminant" is the ideal in $\mathfrak{H}$ derived from the products of every two (equal or different) such determinants. Hence in $\mathfrak{H}_\mathfrak{p}$ the relative discriminant passes into the square of the determinant of the basis $a_1, \ldots, a_n$ and its conjugate elements, that is, into $|S(a_i a_k)|$. The extensions of the relative discriminant and of the discriminant ideal (of the relative principal order) therefore agree in every quotient ring $\mathfrak{H}_\mathfrak{p}$; by the conclusion of no. 3, the two ideals are identical.

32. Joint with R. Brauer: On Minimal Splitting Fields of Irreducible Representations

Sitz. Ber. d. PreuSS. Akad. d. Wiss. 1927, pp. 221–228.

On Minimal Splitting Fields of Irreducible Representations.

By Privatdozent Dr. Richard Brauer
in Königsberg
and Prof. Dr. Emmy Noether
in Göttingen.

(Presented by Mr. Schur.)

The question of the number fields of smallest degree over a ground field P in which a representation of a finite group that is irreducible over P decomposes into absolutely irreducible constituents was first treated by I. Schur.[1] Suppose, for example, that P contains the character of such a constituent. Schur then showed that the degree of these fields relative to P – the index – agrees with the number of those absolutely irreducible constituents which all belong to the same class; that consequently the same field is already determined by the requirement of splitting off one absolutely irreducible constituent; and further that the degree of every field, relative to P, in which such a splitting occurs is a multiple of the index. All these fields are to be called splitting fields, also in the case where P does not contain the character. By an example Schur showed that the splitting fields of smallest degree need not be isomorphic. If P contains no corresponding simple character, then the splitting fields must comprise the field of such a character and its conjugates with respect to P; the absolutely irreducible representations belonging to different conjugate characters are indeed conjugate, but plainly belong to different classes. To split off a system of absolutely irreducible representations of one class, here too it suffices to take the field of the corresponding character and one of the corresponding splitting fields.

In what follows the question of splitting fields is pursued further. The splitting fields of smallest degree can be characterized by assigned non-commutative division rings; the general splitting fields by two-sided simple rings invariantly connected with these non-commutative division rings. Further, by means of the example of the quaternion division ring, it is shown that the degrees of minimal splitting fields are not bounded; here a splitting field is called minimal if none of its proper subfields is a splitting field. This unboundedness follows essentially from a number-theoretic existence theorem whose proof is supplied by H. Hasse in the immediately following note. The example, however, is also treated elementarily by computation – more in the way of verification; and thus, without using the general theory and the number-theoretic existence theorem, the unboundedness of the degrees is shown by proving elementarily a less far-reaching, but sufficient, existence theorem.[2] It should also be noted that in this example we are again dealing with splitting fields of a finite group, namely the quaternion group, which also underlies Schur's example. The representations given there are simultaneously (isomorphic) representations of the quaternion division ring.

1. Characterization of the Splitting Fields

First let us briefly assemble the basic concepts. Let $\mathfrak{S}$ denote a hypercomplex system with respect to a field P_0. By a representation Γ of $\mathfrak{S}$ – in P – one means a system of matrices with elements from P, in such a way that Γ becomes a homomorphic image of $\mathfrak{S}$, and that diagonal matrices $p_0 E$ are assigned to the elements p_0 from P_0; hence P must contain P_0. A representation Γ together with all its transforms $P^{-1}\Gamma P$ forms a

[1] Arithmetische Untersuchungen über endliche Gruppen, Sitzungsber. d. Berl. Ak. d. Wiss. 1906, p. 164. Beiträge zur Theorie der Gruppen linearer Substitutionen, Transact. of the Am. Math. Soc. Ser. 2, Vol. XV, 1909, p. 159. In the second paper the results are transferred to completely reducible hypercomplex systems. A representation is collected into one class together with all its transforms (similar representations).

[2] This example is due to E. Noether; it rests on a modification of one due to R. Brauer, in which the existence of a minimal splitting field whose degree exceeds the index was shown in general. The elementary treatment of the example is due to R. Brauer. The characterization of the splitting fields goes back to investigations of the authors, which otherwise pursue separate goals. For E. Noether the matter is a construction of representation theory on the basis of module and ideal theory, under general finiteness hypotheses; for R. Brauer it is the construction of non-commutative division rings of finite degree over a given commutative perfect ground field, with the help of factor systems. The authors arrived independently at the characterization of splitting fields of smallest degree, R. Brauer for perfect ground fields, E. Noether without this restriction. R. Brauer found the characterization of the general splitting fields in connection with a question of E. Noether concerning the possibility of non-commutative embedding; E. Noether was able here also to remove the restriction to a perfect ground domain.

representation class. The representations of finite groups G are included in the representations so defined; the assigned hypercomplex system $\mathfrak{S}$, the "group ring", consists of all "group numbers", i.e. of all linear combinations of the group elements, with coefficients from P_0, the original group elements being regarded as linearly independent and multiplication being defined by group multiplication and the laws of arithmetic. The notions "reducible", "irreducible", "completely reducible", and "absolutely irreducible" representations are defined as usual; the terminology is to be extended to representation classes. A system $\mathfrak{S}$ is called "completely reducible in P" if all its representation classes in P are completely reducible.

Now assume $\mathfrak{S}$ to be completely reducible in P_0; assume P_0 to be a perfect field, so that the same is true for every algebraic extension P of P_0. The representation classes remain completely reducible under every extension P of P_0.[3] The center of $\mathfrak{S}$ becomes a direct sum of finitely many fields; every extension P of P_0 isomorphic to such a field K is the field of a (simple) character. If P_0 is extended to a P isomorphic to K, then there splits off from $\mathfrak{S}$ a two-sided simple ring to which the absolutely irreducible representation class of the character is assigned. By Wedderburn's theorem this ring is the direct product of a matrix ring over P with a non-commutative division ring $\mathfrak{A}$, uniquely determined up to isomorphism, whose center is P and which has degree m^2 relative to P, where m denotes the Schur index belonging to the character. Every splitting field of $\mathfrak{S}$ – with respect to the representation belonging to the character – is at the same time one of $\mathfrak{A}$ with respect to the representations in P, and conversely. The conjugate representations of $\mathfrak{S}$ are obtained by starting from the corresponding two-sided simple ring over P_0; its assigned division ring $\mathfrak{A}_0$ becomes isomorphic to $\mathfrak{A}$ and has K as center. Thus the problem of splitting fields is completely reduced to that of the assigned non-commutative division ring $\mathfrak{A}$ and its splittings.[4] In particular one has the theorem:

All maximal commutative subfields of $\mathfrak{A}$ have the same degree m relative to P, where m denotes the Schur index. All these maximal commutative subfields are splitting fields of smallest degree, and every splitting field of smallest degree is contained among them. The degree of every splitting field is a multiple of m. The ring $\mathfrak{A}$ has only one absolutely irreducible representation class and likewise only one irreducible representation class with respect to P.

For the characterization of the general splitting fields, let $\mathfrak{A}_r$ denote the direct product of $\mathfrak{A}$ with the matrix ring of degree r^2 over P (the system of all r-rowed matrices with elements from P). Then $\mathfrak{A}_r$ is two-sided simple, with $\mathfrak{A}$ as assigned non-commutative division ring; and every two-sided simple ring, hypercomplex over P, to which $\mathfrak{A}$ is assigned, is obtained in this way. $\mathfrak{A}_r$ is also characterized as the system of all r-rowed matrices with elements from $\mathfrak{A}$.

Every splitting field of $\mathfrak{A}$ of degree mr – if such a field exists – is isomorphic to a maximal commutative subfield of $\mathfrak{A}_r$. Conversely, all maximal commutative subfields of $\mathfrak{A}_r$ are splitting fields, each of degree ms, where s is a divisor of r. In the regular case all maximal commutative subfields of $\mathfrak{A}_r$ have degree mr. Here by the regular case is meant: the ground field P has the property that for every commutative field Σ over P which is finite over P, there are still commutative extensions over Σ of arbitrary degree.[5]

Whether among these splitting fields, for $r > 1$, minimal ones also occur is not yet decided by the embedding in $\mathfrak{A}_r$. That this actually can be the case for infinitely many r is shown by the following example.

2. The Unboundedness of the Degrees of Minimal Splitting Fields

For this unboundedness the quaternion division ring is now to be given as an example, regarded as a hypercomplex system over the field P of rational numbers, with the basis elements i, j, k besides the unit 1 and with the familiar relations:

$$i^2 = j^2 = k^2 = -1; \qquad ij = k; \quad jk = i; \quad ki = j; \quad ji = -k; \quad kj = -i; \quad ik = -j.$$

It will be shown that all and only those algebraic number fields are splitting fields for which, after adjunction, there exists an "idempotent" element r, so that $r^2 = r$, with r different from both the zero element and the unit element. These number fields can also be characterized as those in which (-1) is representable as a sum

[3] If P_0 is not perfect, complete reducibility is preserved if and only if the components K of the center become "extensions of the first kind" of P_0. Under this hypothesis all further consequences in the text remain valid.

[4] This corresponds to Schur's reduction to the system of matrices over P which commute with the irreducible representation of $\mathfrak{S}$ in P. The transposes of these matrices give a representation of $\mathfrak{A}$ in P.

[5] Thus, for example, no regular case occurs when P is the field of all real numbers.

of three squares, and consequently as a sum of two squares.[6] Indeed, set

$$r = \alpha + \frac{1}{2}\beta i + \frac{1}{2}\gamma j + \frac{1}{2}\delta k;$$

then

$$r^2 = \left(\alpha^2 - \frac{1}{4}\beta^2 - \frac{1}{4}\gamma^2 - \frac{1}{4}\delta^2\right) + \alpha\beta i + \alpha\gamma j + \alpha\delta k,$$

so that $r^2 = r$ is equivalent to

$$4\alpha^2 - 4\alpha - \beta^2 - \gamma^2 - \delta^2 = 0; \quad 2\alpha\beta - \beta = 0; \quad 2\alpha\gamma - \gamma = 0; \quad 2\alpha\delta - \delta = 0,$$

and hence, since β, γ, δ are not to vanish simultaneously, equivalent to

$$(-1) = \beta^2 + \gamma^2 + \delta^2.$$

That every such idempotent element produces a splitting, and that the existence of such an idempotent element is necessary for the splitting, follows from these facts: every irreducible representation of a completely reducible system is generated by a one-sided simple ideal, more precisely by the corresponding ideal class, and every such ideal class generates the representation. These one-sided simple ideals all occur in a one-sided direct-sum decomposition, and this decomposition determines the "primitive" idempotent elements that become the components of the unit. Conversely, every idempotent element gives a direct-sum decomposition $\mathfrak{S} = r\mathfrak{S} + (e-r)\mathfrak{S}$, where e denotes the unit; the "primitive" ones split off simple ideals.[7] A non-commutative division ring, regarded as a hypercomplex system with respect to its center, becomes – when extended to a hypercomplex system with respect to a splitting field – a direct sum of m absolutely simple one-sided ideals, where m is the Schur index.

In the case of the quaternion division ring, m is two; hence every idempotent element $\neq 0$ and $\neq 1$ already produces the decomposition into absolutely simple ideals to which the splitting into absolutely irreducible representation classes corresponds. This characterizes the indicated fields as splitting fields.

It follows further: all cyclic fields Ω_n of degree 2^n over the field of rational numbers in which (-1) can be represented as a sum of two squares are minimal splitting fields of the quaternion division ring. For a splitting field cannot be real, because of the representation of (-1) as a sum of squares; on the other hand, the subfield of Ω_n of degree 2^{n-1} – and therefore every proper subfield of Ω_n – is necessarily real, being the intersection of Ω_n with the field of all real algebraic numbers. Namely, Ω_n is a Galois field of degree two over this intersection, which therefore must coincide with the subfield of degree 2^{n-1}.

According to Hasse's existence theorem[8] there are such fields Ω_n for every n; the degrees of minimal splitting fields are not bounded. In fact, every power of the index occurs here as the degree of a minimal splitting field.[9]

---

[6] That representability of (-1) as a sum of three squares always implies such representability as a sum of two follows from the identity

$$(c^2 + d^2)(a^2 + b^2 + c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 + (c^2 + d^2)^2,$$

which follows, for example, from the product theorem for norms of quaternions. Instead of requiring the existence of an idempotent element, it would also have sufficed for the splitting to require an element of vanishing norm.

[7] The connection between primitive idempotent elements and irreducible representations is already found in the dissertation of M. Herzberger: Über Systeme hyperkomplexer GröSSen, Chapter 4, Berlin 1923. That simple ideals generate irreducible representations is shown in the commutative case, for example, by E. Noether, Der Diskriminantensatz für Ordnungen, Crelle 157 (1926); in the non-commutative case by W. Krull, Theorie und Anwendung der verallgemeinerten Abelschen Gruppen, Heidelberger Berichte 1926. Cf. also the closing remarks in Speiser's group theory. If $a_1, \ldots, a_m$ denotes a basis of the ideal with respect to the splitting field, and c an arbitrary ring element, so that $a_i c = \gamma_{i1} a_1 + \cdots + \gamma_{im} a_m$, then (γ_{ik}) is the matrix assigned to c; the fact that all irreducible representations are generated by ideals lies deeper.

[8] The existence of Ω_n can already be read from the parameter representation of cyclic fields of degree 4, as given for example in Weber (Kleines Lehrbuch der Algebra, ğ 93).

[9] Subsequently R. Brauer was able to show further that there are even minimal splitting fields of the quaternion division ring of every even degree, hence of all degrees possible at all for splitting fields. Such a field $P(\Xi)$ may be defined for every $n \geq 2$ by the equation

$$f(\Xi) = \Xi^{2n} + a^2 p^2 \Xi^2 + b^2 p^2 \beta = 0; \quad \text{therefore} \quad -1 = \left(\frac{ap}{\Xi^{n-1}}\right)^2 + \left(\frac{bp\varrho}{\Xi^n}\right)^2,$$

where, by suitable choice of a, b, p, ϱ, one can achieve that 1. $f(x)$ is irreducible for every n; 2. $P(\Xi)$ has only the one subfield $P(\Xi^2)$ different from P; 3. $P(\Xi^2)$ also has real fields among its conjugates, and thus cannot be a splitting field. One possible choice of a, b, p, ϱ is, for example,

$$f(x) = x^{2n} + (2^5 \cdot 9)4x^2 + 9 \cdot 64.$$

The proof rests on a modification of a method of Furtwängler for constructing primitive equations (Math. Ann. 85, p. 34, ğ 3), but is rather laborious in the detailed execution.

3. Elementary Treatment of the Splitting Fields of the Quaternion Division Ring

Let Ω denote the representation of the quaternion group formed from the following eight matrices:[10]

$$\pm E = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \pm I = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \pm J = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \pm K = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The group ring generated by Ω is precisely a representation of the quaternion division ring regarded as a hypercomplex system; we shall show elementarily that Ω is representable in a field K if and only if -1 is representable in K as a sum of two squares.

a) Let $\Omega^* = T^{-1}\Omega T$ be a representation rational over a field K, and put $I^* = T^{-1}IT$, $J^* = T^{-1}JT$. Since J and J^* are two similar matrices rational over K, there is also a transformation R rational over K which carries J^* into J,

$$R^{-1}J^*R = J.$$

If Ω^* is replaced from the start by the likewise K-rational representation $R^{-1}\Omega^*R$, one sees that, without restriction, one may assume $J^* = J$. Let

$$I^* = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad (a, b, c, d \text{ numbers from } K).$$

From $IJ = -JI$ it follows that $I^*J^* = -J^*I^*$, and because $J^* = J$ this gives

$$a = -d, \qquad b = c.$$

From $I^2 = -E$ it follows that $I^{*2} = -E$, hence

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}^2 = \begin{pmatrix} a^2 + b^2 & 0 \\ 0 & a^2 + b^2 \end{pmatrix},$$

so $a^2 + b^2 = -1$; consequently -1 is indeed representable in K as a sum of two squares.

b) Conversely, suppose that -1 is representable in a field K as a sum of two squares. If, say, $-1 = a^2 + b^2$, set

$$I^* = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \qquad J^* = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad K^* = I^*J^*.$$

A straightforward calculation shows that $\pm E$, $\pm I^*$, $\pm J^*$, $\pm K^*$ form a group rational over K and similar to Ω.[11]

It remains to show that for infinitely many n there are cyclic fields of degree 2^n which are minimal splitting fields of the quaternion group.

Let p be a rational prime such that, for some suitable $r > 0$,

$$(*) \qquad 2^r + 1 \equiv 0 \pmod{p}$$

and let 2^n be the highest power of 2 dividing $p - 1$.

First we show that primes p occur for infinitely many values of n. Let k be any positive rational integer, and let p be a prime divisor of $2^{2^k} + 1$. Then the congruence required for p is fulfilled with $r = 2^k$. Further, $2 \pmod{p}$ has exponent 2^{k+1}, and therefore, for the highest power 2^n dividing $p-1$, the number n is greater than k. Thus in any case there are arbitrarily large n to which primes p correspond.

Let ε be a primitive p-th root of unity. We now show that in $P(\varepsilon)$ the number -1 can be represented as a sum of two squares,

$$-1 = a^2 + b^2 = (a + ib)(a - ib) \qquad (a, b \text{ numbers from } P(\varepsilon)).$$

This is equivalent to saying that in the field of $(4p)$-th roots of unity, $P(\varepsilon, i) = P(\varepsilon \cdot i)$, there are numbers whose relative norm with respect to $P(\varepsilon)$ is exactly -1.

[10] Cf. Sylvester, Math. Papers Vol. III p. 647, Vol. IV p. 122.

[11] The characterization of the splitting fields can also be obtained easily with the help of factor systems.

The number $1 + i\varepsilon^\nu$ $(\nu = 1, 2, \ldots, p-1)$ has relative norm $(1 + i\varepsilon^\nu)(1 - i\varepsilon^\nu) = 1 + \varepsilon^{2\nu}$; consequently all numbers $1 + \varepsilon^\nu$ $(\nu = 1, 2, \ldots, p-1)$ are relative norms of numbers from $P(\varepsilon i)$ relative to the ground field $P(\varepsilon)$. Therefore the same holds for

$$\Pi = \prod_{\nu=0}^{r-1}(1 + \varepsilon^{2^\nu}) = (1 + \varepsilon)(1 + \varepsilon^2)(1 + \varepsilon^4)\cdots(1 + \varepsilon^{2^{r-1}}) = \sum_{\lambda=0}^{2^r-1} \varepsilon^\lambda.$$

If one adjoins to Π the term $\varepsilon^{2^r} = \varepsilon^{-1} = \varepsilon^{p-1}$ (by $(*)$), then $\Pi + \varepsilon^{p-1}$ becomes a sum of pieces $1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^{p-1} = 0$, and consequently

$$\Pi = -\varepsilon^{-1}.$$

Now ε too is the relative norm of a number from $P(\varepsilon i)$, namely of $\varepsilon^{(p+1)/2}$. Hence the analogous statement holds for

$$\Pi\varepsilon = -1.$$

Therefore -1 is representable in $P(\varepsilon)$ as a sum of two squares;[12] $P(\varepsilon)$ is a splitting field for the quaternion group.

Let K be the cyclic field of degree 2^n contained in $P(\varepsilon)$. We assert that K too is a splitting field.[13] Let m be the index of the quaternion division ring with respect to K as ground field. Then $m = 1$ or $m = 2$. But since there is a splitting field $P(\varepsilon)$ of odd relative degree $(p-1)/2^n$ with respect to K, the second case is impossible; hence $m = 1$. This means precisely that K is a splitting field.

Thus there are, for infinitely many n, cyclic fields of degree 2^n which are minimal splitting fields.

---

[12] For primes of the form $8n \pm 3$ this argument is already found in E. Landau, Über die Darstellung definiter Funktionen durch Quadrate, Math. Ann. vol. 62, pp. 272–285.

[13] The choice of the cyclic splitting field of degree 2^n as a subfield of a cyclotomic field is modeled on Hasse's example.

33. Hypercomplex quantities and representation theory in arithmetic conception

Atti Congresso Bologna 2 (1928), pp. 71–73.

Emmy Noether (Göttingen – Germany)

Hypercomplex Quantities and Representation Theory in Arithmetic Conception[1]

I would like to show you how representation theory—in particular, therefore, the representation of groups—can be regarded as a theory of module and ideal classes, and how these latter can in turn be subordinated to a generalized concept of group, that of groups with operators.[2]

By a *representation of a group*—in a prescribed field P—one understands, as is well known, the following. To the elements $a, b, \ldots$ of the group $\mathfrak{G}$ there are assigned matrices $A, B, \ldots$ with coefficients in P, in such a way that the product AB corresponds to the product ab; the system of matrices becomes a homomorphic image of the group. Together with this representation, one also has a representation of the "group ring," which consists of all "group numbers," that is, all linear combinations $a\alpha + b\beta + \cdots + c\gamma$, where $a, b, \ldots, c$ and $\alpha, \beta, \ldots, \gamma$ range respectively over arbitrary finite collections of group elements and elements of P (the $a, b, \ldots, c$ being regarded as linearly independent, and multiplication being defined by group multiplication and the laws of arithmetic). The representation of the group ring is at the same time homomorphic with respect to addition; the representation of groups is thus subsumed under the general problem of the *representation of rings*, in which homomorphism with respect to addition and multiplication is required.

Two problems are essential here. The first is the *reduction of a given* representation and the question of the uniqueness of the irreducible constituents that occur in it; the second is the question of the totality of the possible representations—say, only the irreducible ones—of a given ring in a given, not necessarily commutative, division ring.

The first problem is by far the simpler one; this is already shown by the fact that no special hypotheses of any kind are needed either on the ring to be represented or on the—in general non-commutative—representation division ring. The fact that the representation is by matrices of fixed degree supplies all the necessary finiteness hypotheses. The problem can be treated completely by means of the theory of groups with operators, and I shall therefore briefly discuss it.

A group $\mathfrak{B}$ is called a *group with a domain of operators* if, at the same time, there is given a system of symbols $\Theta, H, \ldots$—the operators—such that the combination $\Theta(a), H(a), \ldots$ is uniquely defined for every a in $\mathfrak{B}$ and yields an element of $\mathfrak{B}$, and such that the distributive law is satisfied: $\Theta(ab) = \Theta(a)\Theta(b)$. Two groups with the same domain of operators are called operator-isomorphic if they are isomorphic in the usual sense and if, moreover, from the correspondence of a and $\bar{a}$ there follows also that of $\Theta(a)$ and $\Theta(\bar{a})$, of $H(a)$ and $H(\bar{a})$, and so on. If as subgroups one then admits only those which themselves admit the domain of operators (so that a group is called simple if it has no admissible proper normal divisor except the identity), then the Jordan–Hölder theorem on composition series remains valid in the form: if a group with a domain of operators has a composition series at all, then the system of factor groups is uniquely determined up to ordering in the sense of operator-isomorphism. Under the same hypothesis, there also holds the theorem on the decomposition, unique in the sense of operator-isomorphism, into directly indecomposable factors.

The connection with the representation problem is given by the fact that, among the groups with operators, one finds in particular ideals and modules, these being regarded as abelian groups with respect to addition, while the operators are given by multiplication with the ring elements. Every representation, however, is generated by a representation module, i.e. by a module with respect to the ring and the representation division ring. More precisely, every module class, i.e. every class of representation modules operator-isomorphic to one another, generates the same representation. Thus the question of uniqueness of the reduction of a representation is answered by the composition-series theorem and by the theorem on the direct product.

---

[1] A detailed account will appear in the *Mathematische Zeitschrift*; a continuation there will also discuss non-commutative Galois theory. For "splitting fields," see also R. Brauer and E. Noether, *Ber. Berl. Ak.* 1927, and, for general structure theorems, G. Köthe's lecture in these *Atti*.

[2] Groups with operators go back to W. Krull (*Math. Z.* 23) and O. Schmidt (*Math. Z.* 29). The treatment given here of the problem of reducing a given representation also derives—when restricted to commutative representation fields—from W. Krull (*Theorie und Anwendung der verallgemeinerten Abelschen Gruppen*, Heidelberger Ber. 1926).

Applied to the representation module, the composition series gives, for each matrix, a reduction of the form

$$\begin{pmatrix} B_1 & 0 & 0 \\ & B_2 & 0 \\ A_{ik} & \cdots & B_r \end{pmatrix},$$

where the diagonal matrices corresponding to the factor groups generate an "irreducible" representation, i.e. one that itself no longer admits such a reduction.

Since the classes of these factor groups are uniquely determined, the same holds for the diagonal representations (uniquely in the sense of equivalence of representations). Analogously, the theorem on the direct product gives the uniqueness of the "decomposition" into "indecomposable" constituents:

$$\begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \cdots & \\ & & & C_s \end{pmatrix},$$

where each C_i can then still be reduced uniquely according to the composition-series theorem.

I would like to sketch the *second problem* for the case of representations of hypercomplex systems, more generally of rings, which satisfy the "double-chain theorem." The result is that every irreducible (simple) module class is an ideal class; hence the composition series from one-sided ideals already supply all irreducible representations through their factor groups. More precisely, the composition series in the residue-class ring modulo the radical suffice, the latter becoming a "completely reducible" ring. The problem is thereby reduced to the structural investigation of completely reducible rings; and thus it proves appropriate to take as starting point the representations in the automorphism division rings. This is to be understood as follows. All simple (right) ideals of a two-sided simple component of such a ring belong to the same class, and therefore have the same automorphism ring, which, because of the simplicity of the ideals, becomes a division ring; at the same time it is the automorphism ring of the simple left ideals. The simple ring itself becomes isomorphic to the system of all matrices over the automorphism division ring; and from this representation spring all representations with respect to a subfield, in particular with respect to the coefficient domain of the hypercomplex system, by replacing the elements of the automorphism division ring themselves by assigned matrices. Thus the Wedderburn structure theorem known in the case of hypercomplex systems is reinterpreted here through the concept of the automorphism division ring, a concept originating in general group theory, and is at the same time recognized as the source of the representation theory of hypercomplex systems. The new questions of the Galois theory of non-commutative division rings arise; they are closely connected with the question of "splitting fields." At the same time, an outlook is obtained toward structure theorems for general rings that are not completely reducible, by means of the automorphism rings of the indecomposable ideals. Group theory, in its extension to the most general groups with operators, here again proves itself to be the ordering principle.

34. Hypercomplex Quantities and Representation Theory

Math. Zs. 30 (1929), pp. 641–692.

Hypercomplex Quantities and Representation Theory[1].

By

Emmy Noether in Göttingen.

Introduction.

The most important general theorems on hypercomplex systems go back to Molien (Math. Annalen vol. 41 and the Dorpat reports of 1897). Essentially independently of this, Frobenius soon afterward developed the theory of hypercomplex systems and of their representations – in particular the representation theory of finite groups – as a unified theory. The basis is the concept, due to Dedekind, of the group determinant, more generally the determinant of an arbitrary hypercomplex system. Frobenius shows that to the various irreducible factors of this determinant (where the coefficient domain is always the field of all complex numbers) there correspond the various irreducible representation classes, and that in this way all irreducible representation classes are exhausted. Such a representation class is completely characterized by its "character system"; in the case of finite groups this character system arises by decomposing the determinant of the commutative hypercomplex system derived from the classes of conjugate elements of the group. This determinant decomposes into linear factors, with the characters as coefficients – a direct generalization of the result first obtained by Dedekind, namely that the group determinant of a finite Abelian group decomposes into linear factors whose coefficients are the different characters of the Abelian group (correspondence with Frobenius).

These conceptually simple and transparent results, however, are obtained by Frobenius through laborious calculation. The later development aimed at a simplified derivation of these results, and at the same time at their extension when an arbitrary field is taken as coefficient domain. This later development proceeded in completely separate ways for hypercomplex systems and for representation theory. Hypercomplex systems received an arithmetical treatment through Wedderburn: every hypercomplex system is uniquely a direct sum of two-sided directly indecomposable rings; for systems without radical these indecomposable rings become isomorphic to the system of all n-rowed matrices with elements from an assigned, not necessarily commutative, division ring – determined essentially uniquely.[2] Representation theory received an elementary foundation through Burnside and I. Schur, who proceeded directly from a given representation, independently of the hypercomplex system, and operated with matrix theorems. In particular Schur treated the question of the number fields of smallest degree in which a representation irreducible over a given field decomposes absolutely. These absolutely irreducible constituents belong to finitely many conjugate representation classes. The degree of the number fields sought is equal to the product of the number of these classes by the index (the number of constituents in each of the conjugate classes). The chief auxiliary tool of Schur's theory is the system of all matrices commuting with an irreducible representation.[3]

In the following purely arithmetical foundation, hypercomplex quantities and representation theory again appear as one unified whole – as a special case of a general theory of non-commutative rings satisfying only certain finiteness conditions. More precisely, this is a theory of module and ideal classes with respect to these rings, with the main result that the irreducible module classes are already exhausted by the corresponding ideal classes; in particular, for rings without radical all module classes decompose into irreducible ones (become completely reducible). This is the arithmetical equivalent of Frobenius's result that the irreducible factors of the regular group (respectively system) determinant already exhaust the totality of irreducible representation classes, and that complete reducibility of representations holds for systems without radical. Namely, the consideration of the system determinant and its decomposition can be interpreted as a transition to the norm, whereas here the direct-sum decomposition of the ideals and their composition series are treated directly. Representation theory, by means of the concept of the representation module, becomes a theory of

[1] What follows is a free elaboration, prepared by B. L. van der Waerden, of my lectures of the winter semester 1927/28. We prepared the text for print jointly. I am also indebted to B. L. van der Waerden for a number of critical remarks.

[2] Cf. the references in Dickson, *Algebras and their Arithmetics* (German edition: *Algebren und ihre Zahlentheorie*, Zürich 1927).

[3] Cf. the references in Chapter 10 of Speiser's group theory.

module classes.

The introduction of module and ideal classes has a purely group-theoretic basis. Modules and ideals are regarded as Abelian groups with respect to addition, restricted by the condition that they admit certain multiplications by ring elements: they form "groups with operators" (ğ1). For such groups, in place of the ordinary isomorphism there appears the "operator isomorphism" (ğ2); groups that are operator-isomorphic to one another (within a fixed domain) are collected into a class – a class concept that, for example in the case of the ideals of a number field, coincides with the usual one. The theory of groups with operators goes back to W. Krull and O. Schmidt (cf. note 6); it is developed systematically in Chapter I. The theorems that remain valid here as well – on composition series, direct product (respectively sum), and completely reducible groups; uniqueness theorems in the sense of the class division just mentioned – form the basis of everything that follows.

They first yield the general uniqueness theorems for the irreducible diagonal constituents of arbitrary representations (Chapter III, ğ16), on the basis of the one-to-one correspondence of representation classes with the classes of representation modules, hence with classes of groups with operators. The further question of the totality of representations requires a more precise study of the structure of the rings to be represented, thus, in the special case, of hypercomplex systems. In Chapter II the results of Wedderburn are obtained anew and carried further, on the basis of the group-theoretic conception according to which one-sided ideals stand in the foreground. It turns out that the "multiple-chain theorem" for right ideals, or the identical "minimal condition" (in every set of right ideals there is at least one minimal member within the set), suffices as a finiteness condition.[4] One obtains the identity of the rings without radical satisfying the minimal condition with the (right) completely reducible rings with identity element. In such rings all simple right ideals of a two-sided indecomposable ring belong to the same class and therefore possess – as groups with operators – the same automorphism ring, which, because of the simplicity of the ideals, becomes a division ring. This automorphism division ring of the class is what mediates the matrix representation found by Wedderburn.

This matrix representation in the automorphism division ring also solves the representation problem in the completely reducible case, as soon as representation with respect to the automorphism division ring or to its subfields is required – in particular with respect to the coefficient domain of a hypercomplex system. There are – this is a direct consequence of the theorem reducing module classes to ideal classes – no further irreducible representations beyond the Wedderburn representation and those that arise from it when the elements of the automorphism division ring are replaced in the natural way by matrices over a subfield.

Thus in the completely reducible case there are as many different irreducible representation classes as ideal classes; their number agrees with the number of different two-sided indecomposable, hence simple, rings. This number is finally again identical with the number of indecomposable components of the center, which become commutative fields. In the case of hypercomplex systems with algebraically closed coefficient domain, these latter fields are completely determined by the different ring homomorphisms (irreducible representations) of the center; up to a numerical factor these are precisely the characters.

The results obtained also give, at the same time, a survey of the irreducible representations of systems with radical, insofar as these can be reduced to the representations of the residue class ring modulo the radical, which becomes a system without radical.

As will be shown later, for hypercomplex systems without radical the theory of "splitting fields" also follows from the automorphism division ring: that is, the theory of commutative extensions of the coefficient domain in which the representations decompose into absolutely irreducible representations – equivalently, in which a direct-sum decomposition into absolutely simple right ideals occurs. The splitting fields are identical with those of the automorphism division ring, and all splitting fields of smallest degree are isomorphic to the maximal commutative subfields of the automorphism division ring. The connection with Schur's investigations mentioned above is established by the fact that the transposes of the matrices commuting with the representation supply precisely a representation of the automorphism division ring.[5] These theorems are to be developed systematically in the framework of a Galois theory of non-commutative division rings.

The underlying concepts – operator homomorphism and automorphism ring – also yield the structure of general rings with radical that satisfy only the minimal condition; this will be carried out from another side.

[4]Wedderburn's methods of proof can be transferred if the "double chain theorem" is assumed. Cf. E. Artin, Zur Theorie der hyperkomplexen Zahlen, Hamb. Abh. 1927. Cf. also A. Suschkewitsch, Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit, Math. Annalen 99 (1928), pp. 30–50, where parallel structure theorems are developed for (finite) domains with only one associative, non-invertible operation. The splitting of the "kernel" in Suschkewitsch into right and left groups corresponds to the representation of a two-sided simple ring with identity element as a sum of right and left ideals.

[5]Cf. R. Brauer–E. Noether, Über minimale Zerfällungskörper irreduzibler Darstellungen, Sitz.-Ber. PreuSS. Akad. Wiss. 1927, p. 221.

Chapter I. Group-Theoretic Foundations

ğ 1. Groups with operators[6].

Let $\mathfrak{G}$ be a group (finite or infinite), with elements $a, b, \ldots$. By an operator domain Ω for the group $\mathfrak{G}$ is meant a set of new symbols $H, \Theta, \ldots$, such that to every a in $\mathfrak{G}$ and every Θ in Ω there is assigned a uniquely defined Θa in $\mathfrak{G}$, and such that the distributive law holds:

$$\Theta(ab) = \Theta a \cdot \Theta b.$$

Accordingly, every operator defines a homomorphism of the group into itself, where the group is mapped either onto itself or onto a subgroup. The identity element goes into the identity element, and inverses go into inverses.

An operator domain is called *absolute* if different operators also define different homomorphisms. From an arbitrary operator domain one obtains an absolute one by equating all those elements which generate the same homomorphism. An absolute operator domain is a one-to-one image of a subset of the set of all homomorphisms of the group into itself.

An *admissible subgroup* $\mathfrak{H}$ of $\mathfrak{G}$ – with respect to a fixed operator domain Ω – is a subgroup which admits the operator domain, that is, for which Θa lies in $\mathfrak{H}$ for every a in $\mathfrak{H}$ and Θ in Ω.

Examples. 1. Let the operators be the inner automorphisms: $\Theta a = c^{-1}ac$. The admissible subgroups are the normal divisors.

2. Let the operators be all automorphisms. The admissible subgroups are the "characteristic subgroups", which go into themselves under all automorphisms.

3. Let $\mathfrak{G}$ be a ring, i.e. an Abelian group with respect to addition, in which a multiplication is also defined, with the properties

$$\begin{aligned} r(a+b) &= ra + rb, \\ (a+b)r &= ar + br, \\ ab \cdot c &= a \cdot bc. \end{aligned}$$

Every element r simultaneously defines two operators: the operators rx and xr. The admitted subgroups are the "ideals" $\mathfrak{a}$, namely: left-sided ideals, which admit the operations rx: $r\mathfrak{a} \subseteq \mathfrak{a}$; right-sided ideals, which admit the operations xr: $\mathfrak{a}r \subseteq \mathfrak{a}$; and two-sided ideals, which admit both operations. All ideals become trivial ($= \{0\}$ or $= \mathfrak{G}$) when the ring $\mathfrak{G}$ is a division ring, i.e. when $\mathfrak{G} - \{0\}$ is a group with respect to multiplication.[7]

4. *Modules with respect to a ring* $\mathfrak{o}$. Let $\mathfrak{o}$ be a ring, and $\mathfrak{M}$ an Abelian group written additively. Suppose a multiplication $r \cdot a$ of elements of $\mathfrak{o}$ with elements of $\mathfrak{M}$ is given; the product is to lie again in $\mathfrak{M}$. One requires:

$$\left.\begin{aligned} r(a+b) &= ra + rb, \\ rs \cdot a &= r \cdot sa, \\ (r+s)a &= ra + sa, \end{aligned}\right\} \qquad r, s \in \mathfrak{o}, \quad a, b \in \mathfrak{M}.$$

Then $\mathfrak{M}$ is called an $\mathfrak{o}$-module; more precisely, since the multipliers from $\mathfrak{o}$ are written on the left, a left $\mathfrak{o}$-module. The ring $\mathfrak{o}$ is at the same time an operator domain. If it is absolute, i.e. if different ring elements also yield different operations, one speaks of an *absolute multiplier domain* for the module $\mathfrak{M}$.

As above, one can pass from an arbitrary multiplier domain to the absolute one by equating the elements which generate the same operation. The absolute multiplier domain is again a ring. The admissible subgroups of a module $\mathfrak{M}$ are called *submodules*. If, in particular, $\mathfrak{o} = \mathfrak{M}$, then one obtains the left ideals again.[8]

5. *Bimodules.* If $\mathfrak{M}$ is simultaneously a left $\mathfrak{o}$-module and a right $\mathfrak{o}'$-module, and if moreover for a in $\mathfrak{o}$, α in $\mathfrak{M}$, and a' in $\mathfrak{o}'$ one always has

$$a \cdot \alpha a' = a\alpha \cdot a',$$

then $\mathfrak{M}$ is called a bimodule.

---

[6] The concepts explained here come from W. Krull, *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Zeitschr. 23 (1925), pp. 161–196, and O. Schmidt, *Über unendliche Gruppen mit endlicher Kette*, Math. Zeitschr. 29 (1928), pp. 34–41.

[7] Thus neither for rings nor for division rings is the commutative law of multiplication assumed.

[8] In the same way one requires for right modules:

$$\begin{aligned} (a+b)r &= ar + br, \\ a \cdot rs &= ar \cdot s, \\ a(r+s) &= ar + as. \end{aligned}$$

6. *The automorphism ring of an Abelian group.*[9] For the endomorphisms of an Abelian group (written additively) one can define an addition and a multiplication by the formulas

$$(H+\Theta)a = Ha + \Theta a, \qquad (H\Theta)a = H(\Theta a).$$

The operations so defined plainly again represent homomorphisms, and therefore again belong to the system. The system forms a ring, and the Abelian group can, according to 4, be regarded as a module with respect to this ring.

In what follows, by "subgroups" we shall always mean admissible subgroups. The intersection $\mathfrak{A} \cap \mathfrak{B}$ of two admissible subgroups is again an admissible subgroup. So is the product $\mathfrak{AB}$, provided at least one of the two subgroups $\mathfrak{A}, \mathfrak{B}$ is a normal divisor.

ğ 2. The isomorphism theorems

A mapping of a group $\mathfrak{G}$ onto a group $\overline{\mathfrak{G}}$ – where $\mathfrak{G}$ and $\overline{\mathfrak{G}}$ are to possess the same operator domain – is called an operator homomorphism if, first, it is a homomorphism in the ordinary sense ($ab \mapsto \bar{a}\bar{b}$), and if, second, whenever a maps to $\bar{a}$, the element Θa maps to $\Theta\bar{a}$.[10] Notation: $\mathfrak{G} \sim \overline{\mathfrak{G}}$. If the correspondence is one-to-one, it is called an operator isomorphism. Notation: $\mathfrak{G} \simeq \overline{\mathfrak{G}}$. As for ordinary groups, one proves the homomorphism theorem:

If $\overline{\mathfrak{G}}$ is an operator-homomorphic image of $\mathfrak{G}$, then $\overline{\mathfrak{G}}$ is operator-isomorphic to a factor group $\mathfrak{G}/\mathfrak{N}$, where $\mathfrak{N}$ is an admissible normal divisor, consisting of all elements of $\mathfrak{G}$ that correspond to the identity in $\overline{\mathfrak{G}}$. Conversely, every admissible normal divisor $\mathfrak{N}$ defines a factor group $\mathfrak{G}/\mathfrak{N}$ which admits the operator domain of $\mathfrak{G}$ and is an operator-homomorphic image of $\mathfrak{G}$.

A group is called *simple* if it has no normal divisors other than itself and the identity group. Every homomorphism of a simple group is either an isomorphism, or else assigns the identity element to every element.

First isomorphism theorem. Let $\overline{\mathfrak{G}}$ be a homomorphic image of $\mathfrak{G}$, let $\overline{\mathfrak{A}}$ be a normal divisor of $\overline{\mathfrak{G}}$, and let $\mathfrak{A}$ be the totality of those elements of $\mathfrak{G}$ to which elements of $\overline{\mathfrak{A}}$ are assigned. Then $\mathfrak{A}$ is again a normal divisor, and

$$\overline{\mathfrak{G}}/\overline{\mathfrak{A}} \sim \mathfrak{G}/\mathfrak{A}. \tag{1}$$

Proof. $\mathfrak{G} \sim \overline{\mathfrak{G}}$, $\overline{\mathfrak{G}} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{A}}$, hence $\mathfrak{G} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{A}}$. Therefore $\overline{\mathfrak{G}}/\overline{\mathfrak{A}}$ is isomorphic to a factor group in $\mathfrak{G}$; the corresponding normal divisor is the totality of elements that correspond to the identity in $\overline{\mathfrak{G}}/\overline{\mathfrak{A}}$; this is precisely $\mathfrak{A}$.

Addendum. If, according to the homomorphism theorem, one sets $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$, then $\mathfrak{A}$ certainly contains $\mathfrak{N}$. From $\mathfrak{A}$ one can recover $\overline{\mathfrak{A}}$: $\overline{\mathfrak{A}} = \mathfrak{A}/\mathfrak{N}$. The assignment $\mathfrak{A} \leftrightarrow \overline{\mathfrak{A}}$ is one-to-one. Formula (1) can also be written

$$(\mathfrak{G}/\mathfrak{N})/(\mathfrak{A}/\mathfrak{N}) \sim \mathfrak{G}/\mathfrak{A}.$$

Second isomorphism theorem. Let $\mathfrak{A}$ be a subgroup and $\mathfrak{B}$ a normal divisor of $\mathfrak{G}$. Then $\mathfrak{A} \cap \mathfrak{B}$ is a normal divisor in $\mathfrak{A}$, and

$$\mathfrak{AB}/\mathfrak{B} \sim \mathfrak{A}/(\mathfrak{A} \cap \mathfrak{B}).$$

Proof. Under the homomorphism $\mathfrak{G} \sim \mathfrak{G}/\mathfrak{B}$, in particular the elements a of $\mathfrak{A}$ are assigned certain residue classes $a\mathfrak{B}$, which together make up the group $\mathfrak{AB}/\mathfrak{B}$. Thus $\mathfrak{A} \sim \mathfrak{AB}/\mathfrak{B}$, from which the assertion follows by the homomorphism theorem.

An operator-homomorphic mapping of a group $\mathfrak{G}$ onto itself or onto a subgroup is called an endomorphism of $\mathfrak{G}$. If $\mathfrak{G}$ is in particular an Abelian group (with operators), written additively, and if sum and product of homomorphisms are defined as above (ğ1, Example 6), then the operator homomorphisms of the group into itself form a ring, the automorphism ring.

The automorphism ring of a simple Abelian group (with operators) is a division ring.

Proof. Every homomorphism maps the group either onto itself or onto the zero group (since there are no other admissible subgroups). The homomorphisms that do not map everything to zero are, by what was remarked above about simple groups, isomorphisms, and the isomorphic mappings of a group onto itself form

[9] Cf. A. Châtelet, *Les Groupes Abéliens finis*, Paris, Gauthier-Villars, 1925, p. 99.

[10] One may extend the concept of operator homomorphism by allowing the groups $\mathfrak{G}, \overline{\mathfrak{G}}$ to have separate operator domains, the homomorphism then mapping not only $\mathfrak{G}$ onto $\overline{\mathfrak{G}}$ but also the operator domains onto one another, in such a way that, if a maps to $\bar{a}$ and Θ maps to $\overline{\Theta}$, then $\overline{\Theta}\bar{a}$ is the image of Θa. In this general form the concept of operator homomorphism also includes that of ring homomorphism; cf. ğ8.

a group. Thus after omitting the zero operator the ring becomes a group; hence the ring itself is a division ring.

If, in particular, $\mathfrak{G}$ is a left $\mathfrak{o}$-module, and if the operator homomorphisms are written as right operators, then $\mathfrak{G}$ becomes a *bimodule with respect to* $\mathfrak{o}$ *on the left and the automorphism ring on the right.* For the fact that the new operators Γ were chosen as homomorphisms is expressed by the formulas

$$(a+b)\Gamma = a\Gamma + b\Gamma, \qquad ra\cdot\Gamma = r\cdot a\Gamma,$$

which (together with the remaining formulas already interpreted earlier) characterize the bimodule.

Conversely, if a bimodule is given, then these same formulas express that every element of the right multiplier domain induces an operator homomorphism with respect to the left operators, and conversely.

ğ 3. Composition series

If in $\mathfrak{G}$ there is a finite sequence of admissible subgroups

$$\mathfrak{G} > \mathfrak{A}_1 > \mathfrak{A}_2 > \cdots > \mathfrak{A}_r = \mathfrak{E} \tag{2}$$

($\mathfrak{E}$ is the group consisting of the identity element e alone), such that every $\mathfrak{A}_i$ is a normal divisor in the preceding member, and it is impossible to insert between two successive members of the sequence another subgroup with the same property, then the sequence is called a composition series.

The factor groups $\mathfrak{G}/\mathfrak{A}_1,\ \mathfrak{A}_1/\mathfrak{A}_2,\ldots,\ \mathfrak{A}_{r-1}/\mathfrak{E}$ are called composition factors. They are simple groups, i.e. they possess no admissible normal divisors other than themselves and the identity group.

If among the operators one includes, in particular, all inner automorphisms, then the sequence (2) consists entirely of normal divisors, and one calls it a principal series. If one includes all automorphisms, it is called a characteristic series. In the later examples of ğ1 this would mean composition series of ideals in $\mathfrak{o}$, respectively composition series of modules or bimodules.

Jordan–Hölder theorem. If for a group $\mathfrak{G}$ *two different composition series exist,*

$$\mathfrak{G} > \mathfrak{A}_1 > \mathfrak{A}_2 > \cdots > \mathfrak{A}_r = \mathfrak{E}, \qquad \mathfrak{G} > \mathfrak{B}_1 > \mathfrak{B}_2 > \cdots > \mathfrak{B}_s = \mathfrak{E},$$

then they have the same length, $r = s$*, and the composition factors*

$$\mathfrak{G}/\mathfrak{A}_1,\ \mathfrak{A}_1/\mathfrak{A}_2,\ldots,\mathfrak{A}_{r-1}/\mathfrak{E}$$

are, in some order, isomorphic to

$$\mathfrak{G}/\mathfrak{B}_1,\ \mathfrak{B}_1/\mathfrak{B}_2,\ldots,\mathfrak{B}_{s-1}/\mathfrak{E}.$$

For the proof, see for example E. Noether, Abstrakter Aufbau usw., Math. Annalen 96 (1926), ğ10, p. 57. At the same time it is proved there that:

If in $\mathfrak{G}$ *there is a composition series, then a composition series can be drawn through every normal divisor* $\mathfrak{H}$ *of* $\mathfrak{G}$.

The existence of a composition series is clear for finite groups, more generally for those groups in which a maximal condition and a minimal condition hold:

The *maximal condition* says that in every set of subgroups there is a maximal subgroup, i.e. one that is no longer contained in another subgroup of the set. Equivalently, every ascending chain of subgroups $\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \mathfrak{A}_3 \cdots$ breaks off after finitely many members.

The *minimal condition* says that in every set of subgroups there is a minimal subgroup, one that contains no other subgroup of the set; equivalently, every descending chain $\mathfrak{A}_1 \supset \mathfrak{A}_2 \supset \mathfrak{A}_3 \cdots$ breaks off after finitely many members.

If only normal divisors are admitted as subgroups (for example for Abelian groups), *then conversely the maximal and minimal conditions follow from the existence of the composition series.*

Proof. Every normal divisor has a composition series, whose length is called the length of the normal divisor. If $\mathfrak{A} \subset \mathfrak{B}$, then the length of $\mathfrak{A}$ is smaller than that of $\mathfrak{B}$, since a composition series for $\mathfrak{B}$ can be drawn through $\mathfrak{A}$. Thus every subgroup of shortest length is at the same time minimal, and every subgroup of greatest length is at the same time maximal.

ğ 4. Direct products and intersections

A group $\mathfrak{G}$ is called the direct product of two factors, $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, if

1. $\mathfrak{A}, \mathfrak{B}$ are normal divisors in $\mathfrak{G}$,
2. $\mathfrak{A}\mathfrak{B} = \mathfrak{G}$,
3. $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{E}$.

The definition is plainly equivalent to the following: Every element g of $\mathfrak{G}$ has a unique representation as $g = ab$, with a in $\mathfrak{A}$ and b in $\mathfrak{B}$, and the elements of $\mathfrak{A}$ commute with those of $\mathfrak{B}$: $ab = ba$.

A group $\mathfrak{G}$ is called the direct product of n factors, $\mathfrak{G} = \mathfrak{A}_1 \times \cdots \times \mathfrak{A}_n$, if, putting $\mathfrak{B}_i = \mathfrak{A}_1 \cdots \mathfrak{A}_{i-1}\mathfrak{A}_{i+1} \cdots \mathfrak{A}_n$, one has $\mathfrak{G} = \mathfrak{A}_i \times \mathfrak{B}_i$ directly for every i.

The definition is again equivalent to the following: Every g of $\mathfrak{G}$ is uniquely representable as

$$g = a_1 a_2 \cdots a_n, \qquad a_i \in \mathfrak{A}_i,$$

and the elements of $\mathfrak{A}_i$ commute with those of $\mathfrak{A}_k$.

The following facts are often used:

1. If $\mathfrak{A}_1 \times \cdots \times \mathfrak{A}_n = \mathfrak{K}$ and $\mathfrak{K} \times \mathfrak{H} = \mathfrak{G}$, then $\mathfrak{A}_1 \times \cdots \times \mathfrak{A}_n \times \mathfrak{H} = \mathfrak{G}$.

2. If $\mathfrak{G} = \mathfrak{A}_1 \times \cdots \times \mathfrak{A}_n = \mathfrak{C}_1 \times \cdots \times \mathfrak{C}_n$ and $\mathfrak{C}_i \subseteq \mathfrak{A}_i$, then $\mathfrak{C}_i = \mathfrak{A}_i$. (This follows from the representation of the elements of $\mathfrak{A}_i$ by means of the $\mathfrak{C}_j$.)

3. If $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$ and $\mathfrak{K} \supseteq \mathfrak{A}$, then $\mathfrak{K} = \mathfrak{A} \times (\mathfrak{K} \cap \mathfrak{B})$. (This follows from the representation of the elements of $\mathfrak{K}$ in the form ab, where the second factor belongs both to $\mathfrak{K}$ and to $\mathfrak{B}$.)

4. If $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, then $\mathfrak{A} \simeq \mathfrak{G}/\mathfrak{B}$ and $\mathfrak{B} \simeq \mathfrak{G}/\mathfrak{A}$ (second isomorphism theorem). It follows further that:

5. If $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, and if $\mathfrak{A}$ and $\mathfrak{B}$ possess composition series of lengths m and n, then $\mathfrak{G}$ possesses a composition series of length $m + n$.

6. If $\mathfrak{A} \simeq \overline{\mathfrak{A}}$ and $\mathfrak{B} \simeq \overline{\mathfrak{B}}$, then $\mathfrak{A} \times \mathfrak{B} \simeq \overline{\mathfrak{A}} \times \overline{\mathfrak{B}}$.

A group is called directly indecomposable if it cannot be represented as a direct product of factors $\neq \mathfrak{E}$.

It is clear that *every group satisfying the minimal condition is the direct product of finitely many directly indecomposable groups.*[11]

If the groups in question are written additively, then the notions product and direct product pass into sum and direct sum. Notation: for a sum of groups, $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots)$; for a direct sum, $\mathfrak{A}_1 + \mathfrak{A}_2 + \cdots$.

The concept of "direct intersection" will not be used later, but the following theorems concerning the connection between direct intersection and direct product show how the ideal theory of the next chapters can also be formulated with intersections instead of sums, thereby restoring the connection with the familiar commutative theories.

A group $\mathfrak{D}$ is called the direct intersection of two groups $\mathfrak{R}$ and $\mathfrak{S}$ with respect to $\mathfrak{G}$ if

1. $\mathfrak{R}, \mathfrak{S}$ are normal divisors in $\mathfrak{G}$,
2. $\mathfrak{R} \cap \mathfrak{S} = \mathfrak{D}$,
3. $\mathfrak{R}\mathfrak{S} = \mathfrak{G}$.

Likewise $\mathfrak{D}$ is called the direct intersection of n groups $\mathfrak{S}_1, \ldots, \mathfrak{S}_n$ if, putting $\mathfrak{R}_i = \mathfrak{S}_1 \cap \cdots \cap \mathfrak{S}_{i-1} \cap \mathfrak{S}_{i+1} \cap \cdots \cap \mathfrak{S}_n$, the intersection $\mathfrak{D} = \mathfrak{R}_i \cap \mathfrak{S}_i$ is direct for every i.

From the definition it follows that $\mathfrak{D}$ must be a normal divisor in $\mathfrak{G}$. If $\mathfrak{D} = \mathfrak{S}_1 \cap \cdots \cap \mathfrak{S}_n$ is direct and, under the homomorphism $\mathfrak{G} \sim \mathfrak{G}/\mathfrak{D}$, the groups $\mathfrak{G}, \mathfrak{S}, \mathfrak{D}$ pass to $\overline{\mathfrak{G}}, \overline{\mathfrak{S}}, \overline{\mathfrak{E}}$, then $\overline{\mathfrak{E}} = \overline{\mathfrak{S}}_1 \cap \cdots \cap \overline{\mathfrak{S}}_n$ becomes direct. Conversely, from every such representation $\overline{\mathfrak{E}} = \overline{\mathfrak{S}}_1 \cap \cdots \cap \overline{\mathfrak{S}}_n$ one returns to a direct representation $\mathfrak{D} = \mathfrak{S}_1 \cap \cdots \cap \mathfrak{S}_n$. Through this assignment theorems on direct intersections for arbitrary $\mathfrak{D}$ are reduced to the special case $\mathfrak{D} = \mathfrak{E}$.

In the case $\mathfrak{D} = \mathfrak{E}$ and two factors, the conditions for direct product and direct intersection coincide. For n factors there is the following one-to-one relation between direct product and intersection:

[11] As W. Krull in the commutative case and O. Schmidt in general have shown (cf. note 6), under the hypothesis of the maximal and minimal conditions the representation is unique up to isomorphism. Since one can add all inner automorphisms to the operator domain without changing the concept of direct indecomposability, it is enough to require the finiteness conditions for normal divisors, or the existence of a principal series.

I. If $\mathfrak{G} = \mathfrak{A}_1 \times \cdots \times \mathfrak{A}_n = \mathfrak{A}_i \times \mathfrak{B}_i$, *then* $\mathfrak{E} = \mathfrak{B}_1 \cap \cdots \cap \mathfrak{B}_n = \mathfrak{B}_i \cap \mathfrak{C}_i$ *directly, and* $\mathfrak{C}_i = \mathfrak{A}_i$.

II. If $\mathfrak{E} = \mathfrak{S}_1 \cap \cdots \cap \mathfrak{S}_n = \mathfrak{R}_i \cap \mathfrak{S}_i$ *directly, then* $\mathfrak{G} = \mathfrak{R}_1 \times \cdots \times \mathfrak{R}_n = \mathfrak{R}_i \times \mathfrak{T}_i$, *and* $\mathfrak{T}_i = \mathfrak{S}_i$.

Proof of I. Let $\mathfrak{B} = \mathfrak{B}_1 \cap \cdots \cap \mathfrak{B}_n = \mathfrak{B}_i \cap \mathfrak{C}_i$; then $\mathfrak{C}_i \supseteq \mathfrak{A}_i$. We show $\mathfrak{C}_i \subseteq \mathfrak{A}_i$. If, for instance, c lies in $\mathfrak{C}_1$, then c lies in $\mathfrak{B}_2, \ldots, \mathfrak{B}_n$, so that the component representation with respect to the $\mathfrak{A}$ gives

$$c = a_1 a_2 \cdots a_n = a_1 e a_3 \cdots a_n = a_1 a_2 e \cdots a_n = \cdots = a_1 \cdots a_{n-1} e.$$

Since the product of all $\mathfrak{A}_i$ is direct, the representations agree; in every position except the first there is once an e, hence $c = a_1$, or $\mathfrak{C}_1 \subseteq \mathfrak{A}_1$, i.e. $\mathfrak{C}_1 = \mathfrak{A}_1$, and correspondingly $\mathfrak{C}_i = \mathfrak{A}_i$. It follows that $\mathfrak{B} = \mathfrak{B}_i \cap \mathfrak{C}_i = \mathfrak{B}_i \cap \mathfrak{A}_i = \mathfrak{E}$; moreover $\mathfrak{B}_i \mathfrak{C}_i = \mathfrak{B}_i \mathfrak{A}_i = \mathfrak{G}$, hence the intersection is direct.

Proof of II. Let $\mathfrak{H} = \mathfrak{R}_1 \cdots \mathfrak{R}_n = \mathfrak{R}_i \mathfrak{T}_i$; then $\mathfrak{T}_i \subseteq \mathfrak{S}_i$. We show $\mathfrak{S}_i \subseteq \mathfrak{T}_i$. Let, for instance, s lie in $\mathfrak{S}_1$. By means of $\mathfrak{G} = \mathfrak{S}_i \times \mathfrak{R}_i$ one obtains

$$s = s_1 e = s_2 r_2 = \cdots = s_n r_n.$$

Forming $t_1 = e r_2 \cdots r_n = t_i r_i$, and taking account of the elementwise commutativity of $\mathfrak{R}_i$ and $\mathfrak{S}_i$, one gets

$$s t_1^{-1} = s_i t_i^{-1},$$

which is therefore an element of all the $\mathfrak{S}_i$, and hence is equal to e. Thus $\mathfrak{S}_1 \subseteq \mathfrak{T}_1$, or $\mathfrak{T}_1 = \mathfrak{S}_1$, and correspondingly $\mathfrak{T}_i = \mathfrak{S}_i$. It follows that $\mathfrak{H} = \mathfrak{R}_i \mathfrak{T}_i = \mathfrak{R}_i \mathfrak{S}_i = \mathfrak{G}$ and $\mathfrak{R}_i \cap \mathfrak{T}_i = \mathfrak{R}_i \cap \mathfrak{S}_i = \mathfrak{E}$; hence $\mathfrak{G}$ is the direct product of the $\mathfrak{R}_i$.

ğ 5. Completely reducible groups

A group is called *completely reducible* if it is the direct product of finitely many simple groups:

$$\mathfrak{G} = \mathfrak{A}_1 \times \cdots \times \mathfrak{A}_n.$$

In this case the groups

$$\mathfrak{A}_1 \times \cdots \times \mathfrak{A}_n > \mathfrak{A}_1 \times \cdots \times \mathfrak{A}_{n-1} > \cdots > \mathfrak{A}_1 > \mathfrak{E}$$

form a composition series. Its length is n, and its composition factors are

$$\simeq \mathfrak{A}_n,\ \mathfrak{A}_{n-1}, \ldots, \mathfrak{A}_1.$$

If $\mathfrak{G}$ is completely reducible, then every normal divisor is a direct factor, and the other factor can be chosen as a product of such simple groups as occur in a prescribed product decomposition of $\mathfrak{G}$. The normal divisor $\mathfrak{H}$ is itself completely reducible.

Proof. We have

$$\mathfrak{G} = \mathfrak{H}\mathfrak{A}_1\mathfrak{A}_2 \cdots \mathfrak{A}_n. \tag{3}$$

Put $\mathfrak{H}_i = \mathfrak{H}\mathfrak{A}_1 \cdots \mathfrak{A}_i$. Then $\mathfrak{H}_{i+1} = \mathfrak{H}_i\mathfrak{A}_{i+1}$. Either $\mathfrak{A}_{i+1} \leq \mathfrak{H}_i$, whence $\mathfrak{H}_{i+1} = \mathfrak{H}_i$; in that case we omit the factor $\mathfrak{A}_{i+1}$ from (3). Or $\mathfrak{H}_i \cap \mathfrak{A}_{i+1}$ is a proper normal divisor of $\mathfrak{A}_{i+1}$, hence is $\mathfrak{E}$, and then $\mathfrak{H}_i \times \mathfrak{A}_{i+1}$ is direct. After the superfluous factors have been omitted, (3) becomes

$$\mathfrak{G} = \mathfrak{H} \times \mathfrak{A}_{i_1} \times \cdots \times \mathfrak{A}_{i_r},$$

so that $\mathfrak{H}$ is a direct factor. Further,

$$\mathfrak{H} \simeq \mathfrak{G}/\mathfrak{A}_{i_1} \times \cdots \times \mathfrak{A}_{i_r} \simeq \mathfrak{A}_{j_1} \times \cdots \times \mathfrak{A}_{j_\mu},$$

where $\mathfrak{A}_{j_1}, \ldots, \mathfrak{A}_{j_\mu}$ are the remaining $\mathfrak{A}_i$. Thus $\mathfrak{H}$ is completely reducible.

Corollary. Every decomposition of a completely reducible group into directly indecomposable factors is a decomposition into simple factors, and therefore gives rise to a composition series; from this follows the unique determination of the factors up to isomorphism.

ğ 6. Modules with respect to a field. Hypercomplex systems

An almost trivial example of completely reducible groups with operators is given by modules with finite basis with respect to a not necessarily commutative field.

Let $\mathfrak{G}$ be a right K-module, and let the identity element e of K be at the same time the identity operator: $ae = a$ for a in $\mathfrak{G}$. Every submodule aK derived from an a is simple, namely equal to the module derived from any one of its elements $\neq 0$. Thus if $\mathfrak{H}$ is the submodule derived from some elements, and a is an element not belonging to $\mathfrak{H}$, then $\mathfrak{H} \cap aK = \mathfrak{E}$, so $\mathfrak{H} + aK$ is direct. Starting with any basis element a_1, one can therefore keep adjoining new basis elements $a_2, a_3, \ldots$, and obtains $\mathfrak{G}$ as the direct sum

$$\mathfrak{G} = a_1K + a_2K + \cdots + a_nK.$$

Thus $\mathfrak{G}$ is completely reducible.

The number n, the length of the composition series, is called the *rank* of $\mathfrak{G}$ with respect to K. Because of the uniqueness of the representation of the elements of $\mathfrak{G}$ (and because e has been assumed to be the identity operator), the basis $a_1, \ldots, a_n$ is linearly independent.

Every submodule $\mathfrak{H}$ is a direct summand:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{R} = (h_1K + \cdots + h_sK) + (r_1K + \cdots + r_{n-s}K),$$

or: *every linearly independent basis of $\mathfrak{H}$ can be completed to a linearly independent basis of $\mathfrak{G}$.* The r_i may even be chosen from the original basis elements a_i.

Let $(a_1, \ldots, a_n)$ and $(c_1, \ldots, c_n)$ be linearly independent bases. Then

$$c_k = \sum_i a_i\pi_{ik},$$

or, written in matrices,

$$(c_1, \ldots, c_n) = (a_1, \ldots, a_n)P, \qquad P = \begin{pmatrix} \pi_{11} & \cdots & \pi_{1n} \\ \vdots & & \vdots \\ \pi_{n1} & \cdots & \pi_{nn} \end{pmatrix}.$$

Conversely,

$$(a_1, \ldots, a_n) = (c_1, \ldots, c_n)Q.$$

It follows that

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_n)PQ, \qquad (c_1, \ldots, c_n) = (c_1, \ldots, c_n)QP,$$

and, since the a_i and c_i are linearly independent,

$$PQ = QP = E.$$

Special K-modules that are also rings are the "hypercomplex systems."

A ring $\mathfrak{o}$ which is at the same time a right module with respect to a commutative field K is called a *hypercomplex system with respect to* K (also called an "algebra over K" in the literature) if:

1. its rank is finite (let a linearly independent basis be $u_1, \ldots, u_n$);
2. $ab \cdot x = a \cdot bx = ax \cdot b$. This is expressed by saying that K is joined commutatively with $\mathfrak{o}$;
3. the identity element e of K is also the identity operator: $ae = a$ for a in $\mathfrak{o}$.[12]

Since

$$\Big(\sum_i u_i\alpha_i\Big)\Big(\sum_k u_k\beta_k\Big) = \sum_{i,k}(u_iu_k)(\alpha_i\beta_k),$$

the system is uniquely determined once, in addition to K, the *multiplication table* is given, i.e. once it is known how each product u_iu_k is expressed through the u_j:

$$u_iu_k = \sum_j u_j\gamma_{ik}^j.$$

The γ_{ik}^j must satisfy the familiar relations following from the associative law.

If $\mathfrak{o}$, as we shall often assume, has an identity element e ($ea = ae = a$ for all a), then the elements x of K may be identified with ex, and K may be regarded as a subfield of $\mathfrak{o}$. The hypercomplex system may then also be described as a *ring of finite rank with respect to a field lying in the center.*

An example of a hypercomplex system is the *group ring* of a finite group: one takes the group elements as the basis elements u_i, and group multiplication as multiplication. The field K is arbitrary.

ğ 7. Matrices

The square matrices (π_{ik}), with π_{ik} from a ring $\mathfrak{o}$, form a ring under the ordinary matrix multiplication $\sum_j \pi_{ij}\rho_{jk} = \sigma_{ik}$ and addition $\pi_{ik} + \rho_{ik} = \sigma_{ik}$.

A matrix with elements from a field K for which there is both a right inverse and a left inverse is called *regular.*

We saw in ğ6: *The transition matrix between two linearly independent bases of a K-module is regular.*

For regularity a right inverse suffices. Indeed, form a right K-module with linearly independent basis $(a_1, \ldots, a_n)$ (the module of linear forms in the indeterminates $a_1, \ldots, a_n$), and put

$$(c_1, \ldots, c_n) = (a_1, \ldots, a_n)P.$$

Then

$$(c_1, \ldots, c_n)P^{-1} = (a_1, \ldots, a_n)PP^{-1} = (a_1, \ldots, a_n),$$

so $(c_1, \ldots, c_n)$ is again a basis, hence again linearly independent, and the matrix P is regular. Moreover the right inverse is equal to the left inverse.

[12] Condition 2 says that multiplication by an element of K is a homomorphism for $\mathfrak{o}$ when $\mathfrak{o}$ is regarded both as an $\mathfrak{o}$-left-module and as an $\mathfrak{o}$-right-module. By virtue of 3. these homomorphisms are even isomorphisms.

Similarly, a left inverse suffices.

If P has a left inverse, then P is not a left zero divisor. Proof. From $PA = 0$ follows $A = P^{-1}PA = 0$.

Thus P also has only one right inverse, which by ğ6 coincides with the left inverse.

If, as usual, P_x denotes the matrix $(\pi_{ik}x)$, and C_{ik} denotes the matrix which has the identity element in the ik place and zeros everywhere else, then

$$(\pi_{ik}) = \sum_{i,k} C_{ik}\pi_{ik};$$

so the matrices over K form a K-module of rank n^2. The C_{ik} satisfy the relations

$$C_{ij}C_{jk} = C_{ik}, \qquad C_{ij}C_{\bar{j}k} = 0, \quad j \neq \bar{j}.$$

Thus the matrices over K form a finite K-module and, if K is commutative, a hypercomplex system.

Chapter II. Non-commutative ideal theory

ğ 8. Homomorphism theorem for rings

If $\mathfrak{a}$ is a two-sided ideal in $\mathfrak{o}$, then the residue-class domain $\mathfrak{o}/\mathfrak{a}$ is not only an $\mathfrak{o}$-module but also a ring, as is easily seen. Every homomorphic image of $\mathfrak{o}$ is again a ring, and is isomorphic to a residue-class ring $\mathfrak{o}/\mathfrak{a}$, where $\mathfrak{a}$ is a two-sided ideal. The proof is as for groups.

In particular, if $\mathfrak{o}$ is a field, then there are no ideals other than (0) and $\mathfrak{o}$; hence here the homomorphism is either an isomorphism, or assigns zero to every element.

In particular, suppose the ring $\mathfrak{o}$ is a right K-module, where K is to be a ring elementwise commuting with $\mathfrak{o}$: $- ab\cdot x = a\cdot bx = ax\cdot b -$ (for example, in the case of a hypercomplex system with respect to a commutative field K). Then as admissible right, left, or two-sided ideals one considers only those which are at the same time K-modules, and in addition to ring homomorphism one also requires operator homomorphism with respect to multiplication by K. The admissible ideals become bimodules with respect to $\mathfrak{o}$ and K. (For hypercomplex systems, by "ideals" without further qualification one always means only those admissible with respect to the underlying coefficient field K.) In this enlarged sense too, the homomorphism theorem above remains valid.

An example of ring homomorphism is the transition from a multiplier domain $\mathfrak{o}$ to the absolute multiplier domain (ğ1, Example 4). Thus the absolute multiplier domain is isomorphic to the residue-class ring $\mathfrak{o}/\mathfrak{d}$, where $\mathfrak{d}$ is the two-sided ideal of elements of $\mathfrak{o}$ which annihilate $\mathfrak{M}$.

From the validity of the homomorphism theorem there follow, as in ğ2, the first and second isomorphism theorems for ring and operator isomorphism.

All products $\mathfrak{AB}$ of subsets of $\mathfrak{o}$ are to be understood as module products: $\mathfrak{AB}$ is the totality of all sums $\sum ab$, with a in $\mathfrak{A}$, b in $\mathfrak{B}$, and $a\mathfrak{B}$ is the totality of all sums $\sum ab$, b in $\mathfrak{B}$. If $\mathfrak{B}$ is a right module with respect to some ring as operator domain, then the product $\mathfrak{AB}$, respectively $a\mathfrak{B}$, is also a right module. In particular: a right ideal, an admissible ideal with respect to a coefficient domain K, etc. If $(\mathfrak{A}, \mathfrak{B})$ denotes the sum of the modules $\mathfrak{A}$ and $\mathfrak{B}$, then the rules of calculation are

$$\mathfrak{AB}\cdot\mathfrak{C} = \mathfrak{A}\cdot\mathfrak{BC},$$

$$\mathfrak{A}(\mathfrak{B},\mathfrak{C}) = (\mathfrak{AB},\mathfrak{AC}), \qquad (\mathfrak{A},\mathfrak{B})\mathfrak{C} = (\mathfrak{AC},\mathfrak{BC}).$$

The direct sum is denoted by $\mathfrak{A} + \mathfrak{B}$ (ğ4).

In what follows we shall often consider rings satisfying a maximal or minimal condition (ğ3) for right ideals. Hypercomplex systems in particular belong to these, since by the convention just made only K-modules are admitted as ideals, and their rank therefore remains bounded (ğ6).

ğ 9. Idempotent elements. Direct sum decomposition into right ideals

Let $\mathfrak{o}$ be a ring with identity element.

If $\mathfrak{r}$ is a right ideal, then $\mathfrak{ro} \subseteq \mathfrak{r}$, and because of the identity element even $\mathfrak{ro} = \mathfrak{r}$. Correspondingly for left ideals: $\mathfrak{ol} = \mathfrak{l}$.

An element c is called idempotent if $c^2 = c$.

If $\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_n$ *is a decomposition into right ideals, and if*

$$e = e_1 + \cdots + e_n, \qquad e_i \in \mathfrak{r}_i,$$

then

$$e_i^2 = e_i, \qquad e_i e_k = 0 \quad (i \neq k) \quad (\text{"orthogonality relations"}),$$

$$\mathfrak{r}_i = e_i \mathfrak{o}.$$

Proof. Let r be an element of $\mathfrak{r}_1$. Then

$$r = er = e_1 r + \cdots + e_n r, \qquad e_i r \in \mathfrak{r}_i,$$

but also

$$r = r + 0 + \cdots + 0,$$

so

$$e_1 r = r, \qquad e_i r = 0 \quad (i \neq 1).$$

From the first formula it follows that $\mathfrak{r}_1 \subseteq e_1 \mathfrak{o}$; on the other hand $e_1 \mathfrak{o} \subseteq \mathfrak{r}_1$, so $e_1 \mathfrak{o} = \mathfrak{r}_1$. Specializing $r = e_1$ gives

$$e_1^2 = e_1, \qquad e_i e_1 = 0 \quad (i \neq 1).$$

The same holds when the index 1 is replaced by k.

Conversely, if $e = \sum e_i$, $e_i e_k = 0$ $(i \neq k)$, $e_i^2 = e_i$, *and one puts* $\mathfrak{r}_i = e_i \mathfrak{o}$, *then* $\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_n$.

Proof. Every element r of $\mathfrak{o}$ is

$$r = er = e_1 r + \cdots + e_n r,$$

hence

$$\mathfrak{o} = (e_1 \mathfrak{o}, \ldots, e_n \mathfrak{o}).$$

But the representation is unique; for from

$$0 = e_1 a_1 + \cdots + e_n a_n$$

it follows, upon multiplication by e_i, that

$$e_i^2 a_i = e_i a_i = 0.$$[13]

From a right representation

$$\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_n = e_1 \mathfrak{o} + \cdots + e_n \mathfrak{o}$$

there accordingly follows a left representation

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n = \mathfrak{o} e_1 + \cdots + \mathfrak{o} e_n.$$

If the $\mathfrak{r}_i$ are directly indecomposable, then so are the $\mathfrak{l}_i$. For a decomposition, say of $\mathfrak{l}_1$, would mean

$$\mathfrak{l}_1 = \mathfrak{o} e_1 = \mathfrak{o} e_1' + \mathfrak{o} e_1'', \qquad \mathfrak{o} = \mathfrak{o} e_1' + \mathfrak{o} e_1'' + \mathfrak{o} e_2 + \cdots + \mathfrak{o} e_n.$$

From this would result the right decomposition

$$\mathfrak{o} = e_1' \mathfrak{o} + e_1'' \mathfrak{o} + e_2 \mathfrak{o} + \cdots + e_n \mathfrak{o} = \mathfrak{r}_1' + \mathfrak{r}_1'' + \mathfrak{r}_2 + \cdots + \mathfrak{r}_n,$$

$$\mathfrak{r}_1 \simeq \mathfrak{o}/(\mathfrak{r}_2 + \cdots + \mathfrak{r}_n) = \mathfrak{r}_1' + \mathfrak{r}_1'',$$

so $\mathfrak{r}_1$ would be decomposable.

[13] There is another converse: if $e_i e_k = 0$, $e_i^2 = e_i$, $c = \sum e_i$, then c is a left identity for the ring $e_1 \mathfrak{o} + \cdots + e_n \mathfrak{o}$. The fact that the sum is direct is seen in exactly the same way as above.

ğ 10. Decomposition into two-sided ideals

Let $\mathfrak{o}$ again be a ring with identity element, and let

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n \tag{1}$$

be a decomposition of $\mathfrak{o}$ into two-sided ideals. Then the orthogonality relations also hold for the ideals:

$$\mathfrak{a}_i\mathfrak{a}_k = 0 \quad (i \neq k), \qquad \mathfrak{a}_i^2 = \mathfrak{a}_i. \tag{2}$$

Proof. Let $\mathfrak{b}_1 = \mathfrak{a}_2 + \cdots + \mathfrak{a}_n$, $\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{b}_1$. Then $\mathfrak{a}_1\mathfrak{b}_1 \leq \mathfrak{a}_1 \cap \mathfrak{b}_1 = 0$, so $\mathfrak{a}_1\mathfrak{b}_1 = 0$, and a fortiori

$$\mathfrak{a}_1\mathfrak{a}_i = 0 \quad (i \neq 1);$$

$$\mathfrak{a}_1 = \mathfrak{a}_1\mathfrak{o} = \mathfrak{a}_1(\mathfrak{a}_1 + \mathfrak{b}_1) = (\mathfrak{a}_1^2, \mathfrak{a}_1\mathfrak{b}_1) = \mathfrak{a}_1^2.$$

Conversely: *from (1) and (2) it follows that the modules $\mathfrak{a}_i$ are two-sided ideals. Proof.*

$$\mathfrak{o}\mathfrak{a}_i = (\mathfrak{a}_1 + \cdots + \mathfrak{a}_n)\mathfrak{a}_i = \mathfrak{a}_i^2 = \mathfrak{a}_i, \qquad \mathfrak{a}_i\mathfrak{o} = \mathfrak{a}_i.$$

Right ideals in the ring $\mathfrak{a}_i$ are right ideals in $\mathfrak{o}$. Proof.

$$\mathfrak{r}\mathfrak{o} = \mathfrak{r}(\mathfrak{a}_i + \mathfrak{b}_i) = (\mathfrak{r}\mathfrak{a}_i, \mathfrak{r}\mathfrak{b}_i) = (\mathfrak{r}, 0) = \mathfrak{r}.$$

If $\mathfrak{r}$ is a right ideal in $\mathfrak{o}$, then $\mathfrak{r}$ is a direct sum of right ideals $\mathfrak{r}\mathfrak{a}_i \leq \mathfrak{a}_i$. Proof. $\mathfrak{r} = \mathfrak{r}\mathfrak{o} = (\mathfrak{r}\mathfrak{a}_1, \ldots, \mathfrak{r}\mathfrak{a}_n)$, and $\mathfrak{r}\mathfrak{a}_i\mathfrak{o} = \mathfrak{r}\mathfrak{a}_i$, so the $\mathfrak{r}\mathfrak{a}_i$ are right ideals contained in $\mathfrak{r}$. Since $\mathfrak{r}\mathfrak{a}_i \leq \mathfrak{a}_i$, the sum is direct:

$$\mathfrak{r} = \mathfrak{r}\mathfrak{a}_1 + \cdots + \mathfrak{r}\mathfrak{a}_n.$$

In particular, if $\mathfrak{r}$ is directly indecomposable, then $\mathfrak{r}$ can have only one component; hence $\mathfrak{r}$ must lie in one of the $\mathfrak{a}_i$.

By means of these theorems, ideal theory in $\mathfrak{o}$ is controlled once the ideal theory of the individual $\mathfrak{a}_i$ is known. We shall therefore mostly restrict ourselves to two-sided indecomposable rings.

Two right ideals contained in different $\mathfrak{a}_i$ can never be operator-isomorphic. Proof. An ideal lying in $\mathfrak{a}_1$ is annihilated by all the other $\mathfrak{a}_k$, but not by $\mathfrak{a}_1$. By contrast, an ideal lying in $\mathfrak{a}_2$ is annihilated by $\mathfrak{a}_1$.

Thus if it is possible to decompose the ring $\mathfrak{o}$ into two-sided indecomposable ideals $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$, and each $\mathfrak{a}_i$ again into one-sided indecomposable right ideals $\mathfrak{r}_i' + \mathfrak{r}_i'' + \cdots$, then the operator-isomorphic $\mathfrak{r}$ are to be sought among those belonging to the same $\mathfrak{a}_i$. But it may happen that there are still different classes of $\mathfrak{r}$ – that is, classes not operator-isomorphic – in the same $\mathfrak{a}_i$, as the following example shows.

Let K be the field of rational numbers,

$$\mathfrak{o} = e_1K + e_2K + uK$$

a hypercomplex system, with the e_i and u commuting with the numbers of K, and with multiplication table

	e_1	e_2	u
e_1	e_1	0	u
e_2	0	e_2	0
u	0	u	0

The identity element is $e = e_1 + e_2$. The e_i satisfy the orthogonality relations. Thus the right decomposition is

$$\mathfrak{o} = e_1\mathfrak{o} + e_2\mathfrak{o} = (e_1, u) + (e_2),$$

and the left decomposition is

$$\mathfrak{o} = \mathfrak{o}e_1 + \mathfrak{o}e_2 = (e_1) + (e_2, u).$$

Since $e_2\mathfrak{o}$ and $\mathfrak{o}e_1$ are visibly indecomposable, $\mathfrak{o}e_2$ and $e_1\mathfrak{o}$ must be indecomposable as well.

A two-sided decomposition is impossible. For then one component would have to contain $e_1\mathfrak{o}$ and the other $e_2\mathfrak{o}$; the first would then contain u, but the second would contain $ue_2 = u$ as well.

But $e_1\mathfrak{o}$ and $e_2\mathfrak{o}$ are not operator-isomorphic, since they have different rank with respect to K.

Let $\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$, with the $\mathfrak{a}_i$ two-sided indecomposable. Then they are uniquely determined.

Proof. Suppose also $\mathfrak{o} = \mathfrak{c}_1 + \cdots + \mathfrak{c}_n$. Then

$$\mathfrak{a}_i = \mathfrak{a}_i\mathfrak{o} = (\mathfrak{a}_i\mathfrak{c}_1, \ldots, \mathfrak{a}_i\mathfrak{c}_n).$$

This latter sum is direct because $\mathfrak{a}_i\mathfrak{c}_k \leq \mathfrak{c}_k$ and $\leq \mathfrak{a}_i$; since, however, the $\mathfrak{a}_i$ are indecomposable, all $\mathfrak{a}_i\mathfrak{c}_k$ must be zero except one, $\mathfrak{a}_i\mathfrak{c}_{j_i}$. Thus

$$\mathfrak{a}_i = \mathfrak{a}_i\mathfrak{c}_{j_i}.$$

Similarly,

$$\mathfrak{c}_{j_i} = \mathfrak{o}\mathfrak{c}_{j_i} = \mathfrak{a}_1\mathfrak{c}_{j_i} + \cdots + \mathfrak{a}_n\mathfrak{c}_{j_i},$$

and since $\mathfrak{a}_i\mathfrak{c}_{j_i} \neq 0$, all the remaining terms are 0. Therefore

$$\mathfrak{c}_{j_i} = \mathfrak{a}_i\mathfrak{c}_{j_i} = \mathfrak{a}_i,$$

q.e.d.

ğ 11. The center

The center $\mathfrak{Z}$ of a ring $\mathfrak{o}$ is the totality of all z commuting with all ring elements ($za = az$ for all a). $\mathfrak{Z}$ is a commutative ring.

Every one-sided ideal $\mathfrak{a}$ in $\mathfrak{o}$ has a "contraction ideal" $\mathfrak{a} \cap \mathfrak{Z}$ in $\mathfrak{Z}$. Since both $\mathfrak{a}$ and $\mathfrak{Z}$ are $\mathfrak{Z}$-modules, so is $\mathfrak{a} \cap \mathfrak{Z}$.

Every ideal $\mathfrak{A}$ in $\mathfrak{Z}$ has an extension ideal: the ideal $\mathfrak{a} = (\mathfrak{A}, \mathfrak{o}\mathfrak{A})$ generated by $\mathfrak{A}$ in $\mathfrak{o}$. This is two-sided, because

$$\mathfrak{a}\mathfrak{o} = (\mathfrak{o}\mathfrak{A}, \mathfrak{A})\mathfrak{o} = (\mathfrak{o}\mathfrak{A}\mathfrak{o}, \mathfrak{A}\mathfrak{o}) = (\mathfrak{o}^2\mathfrak{A}, \mathfrak{o}\mathfrak{A}) \subseteq \mathfrak{o}\mathfrak{A} \subseteq \mathfrak{a}.$$

If $\mathfrak{o}$ is assumed to have an identity element, one may write $\mathfrak{a} = \mathfrak{o}\mathfrak{A}$. In this case the following theorem holds:

Every two-sided decomposition of $\mathfrak{o}$ corresponds one-to-one to a decomposition of the center: from

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n, \qquad \mathfrak{A}_i = \mathfrak{a}_i \cap \mathfrak{Z} \tag{1}$$

there follows

$$\mathfrak{Z} = \mathfrak{A}_1 + \cdots + \mathfrak{A}_n, \qquad \mathfrak{o}\mathfrak{A}_i = \mathfrak{a}_i, \tag{2}$$

and conversely.

Proof. Let z be a central element, and let

$$z = z_1 + \cdots + z_n \tag{3}$$

be its decomposition according to (1). Then the z_i are central elements; for

$$za = z_1a + \cdots + z_na = az = az_1 + \cdots + az_n.$$

By directness of the sum, and since $\mathfrak{a}_i$ is two-sided, it follows that

$$z_ia = az_i.$$

Thus z_i lies in $\mathfrak{a}_i \cap \mathfrak{Z} = \mathfrak{A}_i$, so (3) gives the asserted sum decomposition. In particular, $e = \sum e_i$, hence the e_i are central elements. Finally

$$z = ze_1 + \cdots + ze_n,$$

and so

$$\mathfrak{A}_i = \mathfrak{Z}e_i, \qquad \mathfrak{o}\mathfrak{A}_i = \mathfrak{o}\mathfrak{Z}e_i = \mathfrak{o}e_i = \mathfrak{a}_i.$$

Conversely, if $\mathfrak{Z} = \mathfrak{A}_1 + \cdots + \mathfrak{A}_n$ is a decomposition of the center, then by ğ9

$$\mathfrak{A}_i = \mathfrak{Z}e_i, \qquad e_i^2 = e_i, \qquad e_ie_k = 0 \quad (i \neq k).$$

Hence, by the orthogonality relations §9,

$$\begin{aligned}\mathfrak{o} = \mathfrak{o}e &= \mathfrak{o}e_1 + \cdots + \mathfrak{o}e_n = \mathfrak{o}\mathfrak{Z}e_1 + \cdots + \mathfrak{o}\mathfrak{Z}e_n \\ &= \mathfrak{o}\mathfrak{A}_1 + \cdots + \mathfrak{o}\mathfrak{A}_n = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n.\end{aligned}$$

If now $\mathfrak{a}_i \cap \mathfrak{Z} = \mathfrak{A}_i'$, then from the first part of the assertion one knows that

$$\mathfrak{Z} = \mathfrak{A}_1' + \cdots + \mathfrak{A}_n' \quad \text{directly.}$$

But $\mathfrak{A}_i' \supseteq \mathfrak{A}_i$, hence $\mathfrak{A}_i' = \mathfrak{A}_i$ by ğ4, 2.

Corollary. $\mathfrak{a}_i$ and $\mathfrak{A}_i$ are simultaneously two-sided directly decomposable or indecomposable.

ğ 12. Nilpotent ideals

An ideal $\mathfrak{c}$ is called *nilpotent* if $\mathfrak{c}^\rho = 0$.

Example. The ideal (u) in ğ10.

If there is a nilpotent right ideal $\mathfrak{r}$ in $\mathfrak{o}$, then there is also a nilpotent left ideal, indeed a two-sided ideal.

Proof. Let $\mathfrak{r}^\rho = 0$. Then $\mathfrak{o}\mathfrak{r}$, or, if $\mathfrak{o}$ contains no identity element and $\mathfrak{o}\mathfrak{r}$ could be zero, $(\mathfrak{o}\mathfrak{r}, \mathfrak{r})$, is a left ideal, and

$$(\mathfrak{o}\mathfrak{r})^\rho = \mathfrak{o}\mathfrak{r}\mathfrak{o}\mathfrak{r}\cdots\mathfrak{o}\mathfrak{r} \subseteq \mathfrak{o}\mathfrak{r}\mathfrak{r}\cdots\mathfrak{r} = \mathfrak{o}\mathfrak{r}^\rho = 0.$$

The sum of two nilpotent right ideals is again a nilpotent right ideal.

Proof. Let $\mathfrak{c}^\rho = 0$, $\mathfrak{d}^\sigma = 0$. In

$$(\mathfrak{c}, \mathfrak{d})^{\rho+\sigma-1} = (\ldots, \mathfrak{d}\mathfrak{c}\cdots\mathfrak{d}\cdots\mathfrak{c}, \ldots)$$

every term contains either at least ρ factors $\mathfrak{c}$ or at least σ factors $\mathfrak{d}$. In the first case one has

$$\mathfrak{d}\mathfrak{c}\cdots\mathfrak{d}\cdots\mathfrak{c}\cdots \subseteq \mathfrak{d}\mathfrak{c}\mathfrak{c}\cdots\mathfrak{c} = \mathfrak{d}\mathfrak{c}^\rho = 0;$$

in the latter case the same argument applies to the factors $\mathfrak{d}$. Thus

$$(\mathfrak{c}, \mathfrak{d})^{\rho+\sigma-1} = 0.$$

If now the maximal condition for right ideals in $\mathfrak{o}$ is satisfied, then there is a maximal nilpotent right ideal. It contains all other nilpotent right ideals; otherwise one could form its sum with such an ideal. Call it $\mathfrak{c}$. Since $\mathfrak{o}\mathfrak{c}$ is also a nilpotent right ideal, $\mathfrak{o}\mathfrak{c} \subseteq \mathfrak{c}$, so $\mathfrak{c}$ is a left ideal. Every nilpotent left ideal $\mathfrak{d}$ is likewise contained in $\mathfrak{c}$, since $(\mathfrak{d}, \mathfrak{d}\mathfrak{o})$ is a nilpotent right ideal. Thus $\mathfrak{d} \subseteq \mathfrak{c}$. *There is therefore a maximal two-sided nilpotent ideal $\mathfrak{c}$, or "radical," containing all the others, right- and left-sided.*

In the example of ğ10, (u) is the maximal nilpotent ideal.

If the radical is the zero ideal, one speaks of a "ring without radical" ("semisimple ring," "Dedekind system"). The residue-class ring modulo the radical is always a ring without radical.

If $\mathfrak{Z}$ is the center of $\mathfrak{o}$, and $\mathfrak{c}$ is the radical of $\mathfrak{o}$, then $\mathfrak{C} = \mathfrak{c} \cap \mathfrak{Z}$ is the radical of $\mathfrak{Z}$.

Proof. It is clear that $\mathfrak{C}$ is nilpotent. If there were a larger nilpotent ideal $\overline{\mathfrak{C}}$ in $\mathfrak{Z}$, then it could be extended to a nilpotent ideal $\bar{\mathfrak{c}}$ not wholly contained in $\mathfrak{c}$, since $((\overline{\mathfrak{C}}\mathfrak{o})^\rho = \overline{\mathfrak{C}}^\rho\mathfrak{o}^\rho = 0)$.

Consequence. If $\mathfrak{o}$ is a ring without radical, so is $\mathfrak{Z}$. The converse is not true, however, as the example in ğ10 shows. The center of $\mathfrak{o}/\mathfrak{c}$ contains a ring isomorphic to $\mathfrak{Z}/\mathfrak{C}$, but this can be a proper subring (example in ğ10).

ğ 13. Completely reducible rings

By ğ5 a ring is called right completely reducible if it is a direct sum of finitely many simple right ideals.

A right completely reducible ring with identity element has no nilpotent ideal $\neq (0)$, hence no radical.

Proof. Every right ideal $\mathfrak{r}$ is a direct summand (ğ5):

$$\mathfrak{o} = \mathfrak{t} + \mathfrak{r} = e_1\mathfrak{o} + e_2\mathfrak{o}.$$

Since $e_2^2 = e_2$, also $e_2^\rho = e_2$. If $\mathfrak{r}$ were nilpotent, then $e_2^\rho = 0$, hence $e_2 = 0$, and so $\mathfrak{r} = 0$, q.e.d.

We now show the two converses. First: *A ring without radical satisfying the minimal condition for right ideals is completely reducible with respect to right ideals.*

Proof. Let $\mathfrak{t}$ be a minimal right ideal $\neq 0$. We shall show that $\mathfrak{t}$ contains an idempotent element.

Since $\mathfrak{t}^2 \subseteq \mathfrak{t}$ and $\mathfrak{t}^2 \neq 0$, one has $\mathfrak{t}^2 = \mathfrak{t}$, for $\mathfrak{t}^2$ is a right ideal. Hence there is an a in $\mathfrak{t}$ such that $a\mathfrak{t} \neq 0$. Then necessarily $a\mathfrak{t} = \mathfrak{t}$, because $a\mathfrak{t}$ is a right ideal.

The totality of all b in $\mathfrak{t}$ which are annihilated by a $(ab = 0)$ is a right ideal, and is not equal to $\mathfrak{t}$, hence is 0. Thus $ab = 0$ implies $b = 0$.

Because $\mathfrak{t} = a\mathfrak{t}$, a must have a representation $a = ac$, with $c \neq 0$. It follows that

$$ac = ac^2, \qquad a(c - c^2) = 0, \qquad c - c^2 = 0, \qquad c^2 = c.$$

We next show that $\mathfrak{t}$ is a direct summand. The set $c\mathfrak{o}$ is a non-zero right ideal contained in $\mathfrak{t}$, since $c^2 = c$ lies in $c\mathfrak{o}$; hence it is $\mathfrak{t}$. Every element r of $\mathfrak{o}$ has a representation

$$r = cr + (r - cr) \qquad \text{(one-sided Peirce decomposition).}$$

The elements cr form the ideal $\mathfrak{t}$; the elements $r - cr$ form another right ideal $\mathfrak{r}$, annihilated by c: $c\mathfrak{r} = 0$. Hence

$$\mathfrak{o} = (\mathfrak{t}, \mathfrak{r}).$$

Since the elements of $\mathfrak{t}$ are not annihilated by c, the sum is direct:

$$\mathfrak{o} = \mathfrak{t} + \mathfrak{r}. \tag{1}$$

Representing $\mathfrak{o}$, by the minimal condition, as a direct sum of directly indecomposable ideals,

$$\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_n,$$

the $\mathfrak{r}_i$ must be simple, i.e. minimal. For if, say, $\mathfrak{r}_1$ were not simple and $\mathfrak{t}$ were a minimal ideal in $\mathfrak{r}_1$, then (1) would give

$$\mathfrak{r}_1 = \mathfrak{t} + \mathfrak{r} \cap \mathfrak{r}_1 \qquad §4, 3,$$

so $\mathfrak{r}_1$ would be decomposable, a contradiction. Thus $\mathfrak{o}$ is completely reducible.

Second: *A ring without radical satisfying the minimal condition has an identity element.*

To show first the existence of a left identity, it is enough to prove the following: *if a right ideal $\mathfrak{a} = c_1\mathfrak{o} \neq \mathfrak{o}$ has a left identity c_1, then there is a right ideal $c\mathfrak{o}$ of greater length which likewise has a left identity c.* For, since complete reducibility, and therefore boundedness of all lengths, has already been shown, one reaches in finitely many steps a left identity for $\mathfrak{o}$ itself.

Let therefore $\mathfrak{a} = c_1\mathfrak{o}$ and $c_1^2 = c_1$. By the formula

$$r = c_1 r + (r - c_1 r)$$

we have, as above, a Peirce decomposition $\mathfrak{o} = c_1\mathfrak{o} + \mathfrak{r}$. Let c_2 be an idempotent element of $\mathfrak{r}$, as above; thus $c_2^2 = c_2$, and $c_1 c_2 = 0$ since c_1 annihilates all elements of $\mathfrak{r}$. Put $e_1 = c_1$, $e_2 = c_2 - c_2 c_1$. Then

$$e_1^2 = e_1, \quad e_1 e_2 = 0, \quad e_2 e_1 = 0, \quad e_2 c_2 = c_2, \quad e_2 \neq 0, \quad e_2^2 = e_2.$$

By the remark made in note 13), $c = e_1 + e_2$ is a left identity for the ring

$$c\mathfrak{o} = e_1\mathfrak{o} + e_2\mathfrak{o},$$

which, since $e_2^2 = e_2 \neq 0$, has greater length than $\mathfrak{a}$ as a right ideal.

To show that the constructed left identity e is also a right identity, we make the Peirce decomposition into left ideals:

$$\mathfrak{o} = \mathfrak{o}e + \mathfrak{l}.$$

We have $\mathfrak{l}e = 0$, $\mathfrak{l} = e\mathfrak{l}$, hence $\mathfrak{l}^2 = \mathfrak{l}e\mathfrak{l} = 0$. Since by hypothesis no nilpotent left ideal can exist, $\mathfrak{l} = 0$. Therefore e is also a right identity, and hence an identity altogether.

Theorem. From right-sided complete reducibility and the existence of the identity follows two-sided complete reducibility:

$$\mathfrak{o} = \mathfrak{d}_1 + \cdots + \mathfrak{d}_s, \qquad \mathfrak{d}_i \text{ two-sided simple.}$$

As in the preceding proof, it is enough to show that every minimal two-sided ideal $\mathfrak{a}$ is a direct summand. As a right ideal, $\mathfrak{a}$ is a direct summand:

$$\mathfrak{o} = \mathfrak{a} + \mathfrak{r} = e_1\mathfrak{o} + e_2\mathfrak{o}.$$

The corresponding left decomposition is

$$\mathfrak{o} = \mathfrak{c} + \mathfrak{l} = \mathfrak{o}e_1 + \mathfrak{o}e_2.$$

It follows that

$$\mathfrak{r}\mathfrak{c} \subseteq \mathfrak{r}\mathfrak{a} \leq \mathfrak{r} \cap \mathfrak{a} = 0, \qquad \mathfrak{l}\mathfrak{a} = \mathfrak{o}e_2e_1\mathfrak{o} = 0,$$
$$(\mathfrak{a}\mathfrak{l})^2 = \mathfrak{a}\mathfrak{l}\mathfrak{a}\mathfrak{l} = 0, \qquad \text{hence } \mathfrak{a}\mathfrak{l} = 0;$$
$$\mathfrak{r} = \mathfrak{r}\mathfrak{o} = (\mathfrak{r}\mathfrak{c}, \mathfrak{r}\mathfrak{l}) = \mathfrak{r}\mathfrak{l}, \qquad \mathfrak{l} = \mathfrak{o}\mathfrak{l} = (\mathfrak{a}\mathfrak{l}, \mathfrak{r}\mathfrak{l}) = \mathfrak{r}\mathfrak{l}.$$

Thus $\mathfrak{r} = \mathfrak{l}$, so $\mathfrak{r}$ is two-sided; hence $\mathfrak{a}$ is a two-sided direct summand. From here on the proof is the same as for one-sided complete reducibility.

The $\mathfrak{d}_i$ are also two-sided simple as rings, since all ideals in $\mathfrak{d}_i$ are ideals in $\mathfrak{o}$. We now investigate their structure.

ğ 14. Two-sided simple completely reducible rings with identity element

Let $\mathfrak{o}$ be such a ring:

$$\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_n = e_1\mathfrak{o} + \cdots + e_n\mathfrak{o}, \qquad \mathfrak{r}_i \text{ simple.}$$

Then

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n = \mathfrak{o}e_1 + \cdots + \mathfrak{o}e_n, \qquad \mathfrak{l}_i \text{ directly indecomposable §9.}$$

Moreover $\mathfrak{l}_i\mathfrak{r}_i$ is a non-zero two-sided ideal (since e_i^2 lies in $\mathfrak{l}_i\mathfrak{r}_i$), hence is $\mathfrak{o}$.

Put $\mathfrak{A}_{ik} = \mathfrak{r}_i\mathfrak{l}_k$. Then

$$\mathfrak{o} = (\mathfrak{r}_1, \ldots, \mathfrak{r}_n) \cdot (\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = (\ldots, \mathfrak{A}_{ij}, \ldots)$$

directly. For if $0 = \sum_{i,j} a_{ij}$, then, since a_{ij} lies in $\mathfrak{r}_i$ and $\sum \mathfrak{r}_i$ is direct,

$$0 = \sum_j a_{ij},$$

and then, because a_{ij} lies in $\mathfrak{l}_j$,

$$0 = a_{ij}.$$

Further, $\mathfrak{A}_{ij}\mathfrak{r}_j = \mathfrak{r}_i\mathfrak{l}_j\mathfrak{r}_j = \mathfrak{r}_i\mathfrak{o} = \mathfrak{r}_i$, so $\mathfrak{A}_{ij} \neq 0$. Let $a_{ij} \neq 0$ lie in $\mathfrak{A}_{ij}$. Then

$$a_{ij}\mathfrak{r}_j \subseteq \mathfrak{r}_i, \qquad a_{ij}\mathfrak{r}_j \neq 0 \text{ because } a_{ij}e_j = a_{ij},$$

and therefore

$$a_{ij}\mathfrak{r}_j = \mathfrak{r}_i.$$

If for every r_j in $\mathfrak{r}_j$ one puts

$$a_{ij}r_j = r_i,$$

then the map $r_j \mapsto r_i$ is an operator homomorphism from $\mathfrak{r}_j$ to $\mathfrak{r}_i$. The elements mapped to zero form an ideal contained in $\mathfrak{r}_j$, hence the zero ideal; therefore the map is an *isomorphism*. Thus:

Any two simple right ideals $\mathfrak{r}_i$ and $\mathfrak{r}_j$ occurring in a representation of $\mathfrak{o}$ are operator-isomorphic; the isomorphisms are mediated by the elements of $\mathfrak{A}_{ij}$. Since any two different simple right ideals $\mathfrak{r}, \mathfrak{r}'$ occur together in at least one representation of $\mathfrak{o}$, every two such ideals are isomorphic.

All homomorphisms from $\mathfrak{r}_j$ to $\mathfrak{r}_i$ are mediated by elements of $\mathfrak{A}_{ij}$.

Proof. If $e_j \mapsto a_{ij}$, then $e_j^2 \mapsto a_{ij}e_j$, so $a_{ij} = a_{ij}e_j$ lies in $\mathfrak{r}_i\mathfrak{l}_j = \mathfrak{A}_{ij}$. Further,

$$\mathfrak{r}_j = e_j\mathfrak{r}_j \mapsto a_{ij}\mathfrak{r}_j = \mathfrak{r}_i.$$

In particular, the homomorphisms of $\mathfrak{r}_i$ into itself are mediated by $\mathfrak{A}_{ii}$.

The product of two elements of $\mathfrak{A}_{ii}$ corresponds to the product of the homomorphisms, and the sum to the sum (definition: see ğ1, 6). Distinct a_{ii} give distinct automorphisms, for e_i goes to $a_{ii}e_i = a_{ii}$. Thus the ring $\mathfrak{A}_{ii}$ is isomorphic to the automorphism ring of $\mathfrak{r}_i$.

But the automorphism ring of a simple ideal is a field (ğ2), hence $\mathfrak{A}_{ii}$ is a field. Since all $\mathfrak{r}_i$ are operator-isomorphic, their automorphism rings are ring-isomorphic: $\mathfrak{A}_{ii}$ is uniquely determined by $\mathfrak{o}$ up to ring isomorphism. The possible different $\mathfrak{A}_{ii}$ are only different concrete realizations of the abstractly defined automorphism ring of the simple right ideals.

Main theorem. Every completely reducible two-sided simple ring $\mathfrak{o}$ with identity element is isomorphic to the ring of matrices of degree n over a field K. (The field K is isomorphic to the automorphism field of the right ideals of $\mathfrak{o}$.)

Proof[13a]*. Construction of the matrix units c_{ik}.* Let Γ_{11} be the identical automorphism of $\mathfrak{r}_1$, let Γ_{i1} be an arbitrary isomorphism $\Gamma_{i1}\mathfrak{r}_1 = \mathfrak{r}_i$, and finally set

$$\Gamma_{ik} = \Gamma_{i1}\Gamma_{k1}^{-1}.$$

Then in general

$$\Gamma_{ik}\Gamma_{kl} = \Gamma_{il}.$$

If Γ_{ik} is mediated by the element c_{ik} of $\mathfrak{A}_{ik}$, then further

$$c_{ik} = e_ic_{ik} = c_{ik}e_k, \qquad c_{ik}c_{kl}e_l = c_{il}e_l,$$

hence

$$c_{ik}c_{kl} = c_{il}, \qquad c_{ij}c_{kl} = c_{ij}e_je_kc_{kl} = 0 \quad (j \neq k).$$

The c_{ik} are therefore matrix units (ğ7).

Construction of K. The assignment

$$a_{ii} = c_{i1}a_{11}c_{1i}$$

assigns to every a_{11} in $\mathfrak{A}_{11}$ a "conjugate element" a_{ii} of $\mathfrak{A}_{ii}$.

This assignment is a ring isomorphism, since the isomorphisms Δ, Γ corresponding to a and c are connected by

$$\Delta_{ii} = \Gamma_{i1}\Delta_{11}\Gamma_{i1}^{-1},$$

a relation well known to represent a ring isomorphism. Now form the elements

$$\alpha = a_{11} + \cdots + a_{nn} = a_{11} + c_{21}a_{11}c_{12} + \cdots + c_{n1}a_{11}c_{1n}.$$

Each a_{11} determines exactly one α (uniquely because the sum is direct). The totality of the α is a field $K \sim \mathfrak{A}$, since from

$$\alpha = a_{11} + \cdots + a_{nn}, \qquad \beta = b_{11} + \cdots + b_{nn},$$

one obtains

$$\alpha + \beta = (a_{11} + b_{11}) + \cdots + (a_{nn} + b_{nn}), \qquad \alpha\beta = a_{11}b_{11} + \cdots + a_{nn}b_{nn};$$

so the assignment $a_{11} \mapsto \alpha$ is an isomorphism.

Further,

$$c_{ik}\alpha = c_{ik}a_{kk} = c_{ik}c_{k1}a_{11}c_{1k} = c_{i1}a_{11}c_{1k},$$

$$\alpha c_{ik} = a_{ii}c_{ik} = c_{i1}a_{11}c_{1i}c_{ik} = c_{i1}a_{11}c_{1k},$$

so every α commutes with all c_{ik}.

Finally, the same formulas give

$$c_{ik}K = c_{ik}\mathfrak{A}_{kk} = c_{ik}\mathfrak{r}_k\mathfrak{l}_k = \mathfrak{r}_i\mathfrak{l}_k = \mathfrak{A}_{ik},$$

and therefore

$$\mathfrak{o} = \sum c_{ik}K.$$

The assignment. If every element of $\mathfrak{o}$ is written in the form $\sum c_{ik}\alpha_{ik}$, and the matrix (α_{ik}) is assigned to it, the assignment is an isomorphism, as follows immediately from the definition of matrix multiplication. This proves the main theorem.

Converse. The ring of matrices of degree n over a field Λ is two-sided simple and completely reducible; Λ is isomorphic to the automorphism ring of the right ideals, and Λe is the K constructed in the preceding theorem.

Proof. Let the matrix units (ğ7) be c_{ik}. Put

$$\mathfrak{r}_i = \sum_k c_{ik}\Lambda.$$

Then plainly $\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_n$. The $\mathfrak{r}_i$ are simple right ideals, for every non-zero element $\sum c_{ik}\alpha_k$ generates the full $\mathfrak{r}_i$. Indeed, if $\alpha_j \neq 0$, then

$$\Big(\sum c_{ik}\alpha_k\Big) \cdot (c_{jl}\alpha_j^{-1}) = c_{il},$$

and $\sum c_{il}\beta_l$ runs through all elements of $\mathfrak{r}_i$.

The $\mathfrak{r}_i$ are operator-isomorphic: $\mathfrak{r}_i = c_{ik}\mathfrak{r}_k$.

It follows that $\mathfrak{o}$ is two-sided indecomposable; hence, by the theorem of ğ13 and the already proved complete reducibility, and since an identity element exists, it is two-sided simple. This is also seen from the fact that any $\sum\sum c_{ik}\alpha_{ik} \neq 0$ generates the entire two-sided ideal $\mathfrak{o}$.

Further,

$$\mathfrak{r}_i = c_{ii}\mathfrak{o}, \qquad \mathfrak{l}_i = \mathfrak{o}c_{ii},$$

$$e = \sum c_{ii}, \qquad c_{ii} = e_i,$$

[13] Recently B. L. van der Waerden found a simpler proof, operating directly with the abstract automorphism field, which is to appear in his book on algebra (Grundlehren d. Math. Wiss., Berlin: Julius Springer). [11 June 1929.]

$$\mathfrak{A}_{ii} = \mathfrak{r}_i \cap \mathfrak{l}_i = c_{ii}\Lambda \sim \Lambda.$$

Finally, putting $a_{11} = c_{11}\lambda$, one obtains

$$\alpha = a_{11} + c_{21}a_{11}c_{12} + \cdots = c_{11}\lambda + c_{22}\lambda + \cdots = e\lambda,$$

which proves everything asserted.

The center of $\mathfrak{o}$ is the center of K, hence a field.

Proof. $\mathfrak{Z}(K)$ consists of all ζ that commute with all x. But these also commute with all c_{ik}, and hence with all sums $\sum c_{ik}a_{ik}$. Thus

$$\mathfrak{Z}(K) \subseteq \mathfrak{Z}(\mathfrak{o}).$$

Conversely, let z lie in $\mathfrak{Z}(\mathfrak{o})$:

$$z = \sum_\mu \sum_\nu c_{\mu\nu}\gamma_{\mu\nu}.$$

Then

$$zc_{ik} = c_{ik}z, \qquad \sum_\mu c_{\mu k}\gamma_{\mu i} = \sum_\nu c_{i\nu}\gamma_{k\nu},$$

and so

$$\gamma_{\mu i} = 0 \ (\mu \neq i), \qquad c_{ik}\gamma_{ii} = c_{ik}\gamma_{kk}, \qquad \gamma_{ii} = \gamma_{kk} = \gamma;$$

$$z = \sum c_{ii}\gamma = e\gamma = \gamma.$$

Thus z lies in K and commutes with all x, hence z lies in $\mathfrak{Z}(K)$.

Since a matrix ring is of course also left completely reducible, and since every right completely reducible ring with identity element is a direct sum of matrix rings, it follows that:

Every right completely reducible ring with identity element is also left completely reducible, and conversely.

And: *The center of a completely reducible ring with identity element is a direct sum of commutative fields corresponding to the two-sided simple matrix rings.*

There remains the following theorem[14]:

Any two different decompositions $\mathfrak{o} = \sum c_{ik}K$, $\mathfrak{o} = \sum c'_{ik}K'$ are transformed into one another by inner automorphisms $\alpha' \mapsto x^{-1}\alpha x$, $c'_{ik} = x^{-1}c_{ik}x$.

Proof. Let

$$\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_n = \mathfrak{r}'_1 + \cdots + \mathfrak{r}'_n,$$

and let a, b be elements mediating two reciprocal isomorphisms of the ideals $\mathfrak{r}_1, \mathfrak{r}'_1$:

$$\mathfrak{r}_1 = a\mathfrak{r}'_1, \qquad \mathfrak{r}'_1 = b\mathfrak{r}_1, \qquad ab = c_{11}, \qquad ba = c'_{11}.$$

Put

$$x = \sum_i c_{i1}ac'_{1i}, \qquad y = \sum_i c'_{i1}bc_{1i}.$$

Then

$$xy = e, \qquad y = x^{-1}, \qquad x^{-1}c_{ik}x = c'_{ik}, \qquad x^{-1}\alpha x = \alpha'.$$

Chapter III. Module and representation theory

ğ 15. Representations and representation modules[15]

Let $\mathfrak{o}$ be a ring and let K be a ring with identity element. (In later applications K will always be a field.)

A representation of degree n of $\mathfrak{o}$ in K is a homomorphism

$$\mathfrak{o} \sim \mathfrak{D},$$

where $\mathfrak{D}$ is a ring of matrices of degree n over K.

By a *representation module* of $\mathfrak{o}$ with respect to K one understands a double module $\mathfrak{M}$ (ğ 1, 5) which is a left $\mathfrak{o}$-module and a right K-module,

$$\mathfrak{o}\mathfrak{M} \subseteq \mathfrak{M}, \qquad \mathfrak{M}K \subseteq \mathfrak{M},$$

[13] Cf. E. Artin, loc. cit., p. 258.

which is also a direct sum of finitely many one-membered K-modules,

$$\mathfrak{M} = x_1 K + \cdots + x_n K,$$

and in which the identity element of K is the identity operator.

Every representation module leads to a representation. Let c be in $\mathfrak{o}$ and

$$cx_k = \sum_i x_i \gamma_{ik},$$

or

$$c(x_1, \ldots, x_n) = (x_1, \ldots, x_n)C, \qquad C = (\gamma_{ik}).$$

Then the matrices C form a representation for c, for

$$(b + c)x_k = \sum_i x_i(\beta_{ik} + \gamma_{ik}),$$

and

$$\begin{aligned} bcx_k = b\sum_j x_j \gamma_{jk} = \sum_j b x_j \gamma_{jk} = \sum_j \sum_i x_i \beta_{ij} \gamma_{jk} \\ = \sum_i x_i \Big(\sum_j \beta_{ij} \gamma_{jk} \Big), \end{aligned}$$

or

$$bc(x_1, \ldots, x_n) = (x_1, \ldots, x_n)BC.$$

Conversely, every representation $\mathfrak{D}$ of $\mathfrak{o}$ belongs to a representation module, indeed to a definite basis of that module. Namely, let $\mathfrak{M}$ be the totality of the formal linear forms in $x_1, \ldots, x_n$,

$$y = \sum_i x_i \alpha_i.$$

Then $\mathfrak{M}$ is a right K-module. Define further, if the element c is assigned the matrix $C = (\gamma_{ik})$,

$$\begin{aligned} cx_k &= \sum_i x_i \gamma_{ik}, \\ c\Big(\sum_k x_k \alpha_k \Big) &= \sum_i \sum_k x_i \gamma_{ik} \alpha_k. \end{aligned} \tag{1}$$

From the homomorphism relations

$$c + d \longmapsto C + D, \qquad cd \longmapsto CD$$

it follows that

$$(c + d)x_i = cx_i + dx_i, \qquad cdx_i = c \cdot dx_i,$$

and the same is true for sums $\sum_i x_i \alpha_i$. The remaining double-module laws

$$c(y + z) = cy + cz, \qquad c(y\alpha) = (cy)\alpha$$

are trivial. Thus $\mathfrak{M}$ is a representation module which, by (1), belongs exactly to the representation $\mathfrak{o} \sim \mathfrak{D}$.

Let $(y_1, \ldots, y_n)$ be another basis for the same representation module:

$$(y_1, \ldots, y_n) = (x_1, \ldots, x_n)P, \qquad (x_1, \ldots, x_n) = (y_1, \ldots, y_n)P^{-1}.$$

If $b \sim B$ with respect to the x-basis, then

$$\begin{aligned} b(y_1, \ldots, y_n) &= b(x_1, \ldots, x_n)P = (x_1, \ldots, x_n)BP \\ &= (y_1, \ldots, y_n)P^{-1}BP. \end{aligned}$$

One calls the representations $b \sim B$ and $b \sim P^{-1}BP$ *equivalent* and counts them in the same representation class. Since every regular matrix P transforms a basis of $\mathfrak{M}$ into another basis, we have proved:

Every representation module leads uniquely to one definite representation class.[15a)]

15) Representation modules with respect to commutative fields occur first in W. Krull, *Theorie und Anwendung der verallgemeinerten Abelschen Gruppen*, Sitzungsberichte der Heidelberger Akademie, 1926, 1st treatise.

15a) Added in proof (14 April 1929). As B. L. van der Waerden informed me, one can obtain an invariant connection independent of the special choice of basis by separating the notions "linear transformation" and "matrix." A linear transformation is a homomorphism of two modules of linear forms; a matrix is the expression, or representation, of this homomorphism for a particular choice of basis. *I. Every representation module assigns to the multiplier domain $\mathfrak{o}$ a unique homomorphic system of linear transformations of the module into itself.* Indeed, by the end of ğ 2 the left multipliers of a double module $\mathfrak{M}$ generate operator homomorphisms of $\mathfrak{M}$ into itself with respect to the right operators (here multiplication by K), and the assignment is homomorphic. *II. Every system of linear transformations of a module of linear forms into itself that is homomorphic to $\mathfrak{o}$ leads to a representation module.* Indeed, again by the end of ğ 2, these homomorphisms, taken as left multipliers, yield a double module; hence the same holds with respect to the multiplier domain $\mathfrak{o}$ if, for every m in $\mathfrak{M}$ and c in $\mathfrak{o}$, one puts $cm = \Gamma m$, where $c \longmapsto \Gamma$ was the originally given ring-homomorphic assignment. Operator-isomorphic representation modules—with respect to right and left multiplication—correspond to the same transformations, and non-operator-isomorphic ones to different transformations. If, after choosing a definite basis, one expresses every transformation by a matrix, then I gives the representation $\mathfrak{o} \sim \mathfrak{D}$, while II says that every such representation leads to a representation module, indeed to a definite basis of that module. Thus one again obtains the correspondence between representation modules and representation classes, entirely without calculation.

It is clear that:

Two operator-isomorphic representation modules correspond to the same representation class.

But conversely as well:

If two representation modules $(x_1, \ldots, x_n)$ and $(\bar{x}_1, \ldots, \bar{x}_n)$ generate the same representation, then the assignment $x_i \longmapsto \bar{x}_i$, $\sum_i x_i\alpha_i \longmapsto \sum_i \bar{x}_i\alpha_i$ gives an isomorphism. For the multiplication rule is completely determined by the matrices C.

Special case: if two bases of $\mathfrak{M}$ generate the same representation, they are carried into one another by an operator isomorphism of $\mathfrak{M}$ onto itself.

Equivalently, if $C = PCP^{-1}$ for all C and one fixed P, then the assignment $y_i \longmapsto x_i$, where $y_i = \sum_k x_k\pi_{ik}$, is an isomorphism of $\mathfrak{M}$ onto itself. Conversely, every isomorphism $y_i \longmapsto x_i$ of the double module $\mathfrak{M}$ onto itself is mediated by a matrix P which commutes with all C.

One may also extend the notion of representation to rings which are commutatively connected with a commutative multiplier domain P (ğ 8). In that case one takes only such representation rings K as contain P in their center, and one demands of the representation not merely that it be a ring homomorphism $\mathfrak{o} \sim \mathfrak{D}$, but that it even be an operator homomorphism: from $a \longmapsto A$ there should follow $a\rho \longmapsto A\rho$ for ρ in P. For the representation modules this requirement means the additional rule

$$am \cdot \rho \ [= a \cdot m\rho] = a\rho \cdot m.$$

The module and the ring are then said to be "commutatively connected with P."

ğ 16. Reducible representations

If $\mathfrak{A}$ is a submodule of the representation module $\mathfrak{M}$, and if it is possible to choose a basis for $\mathfrak{M}$ consisting of a basis $z_1, \ldots, z_t$ of $\mathfrak{A}$, supplemented by $y_1, \ldots, y_r$, thus

$$\mathfrak{M} = y_1K + \cdots + y_rK + z_1K + \cdots + z_tK^{16)},$$

then the representations have the form

$$C = \begin{pmatrix} R & 0 \\ S & T \end{pmatrix},$$

where the matrices T by themselves form a representation of degree t mediated by $\mathfrak{A}$, and the matrices R form a representation of degree r mediated by $\mathfrak{M}/\mathfrak{A}$.

Proof. We have

$$(cy_1, \ldots, cy_r, cz_1, \ldots, cz_t) = (y_1, \ldots, y_r, z_1, \ldots, z_t) \cdot C.$$

Since the cz_i, as elements of $\mathfrak{A}$, are expressible through the z_i alone, the upper-right block of C is zero. If the other parts of C are named R, S, T in the order shown above, then in particular

$$(cz_1, \ldots, cz_t) = (z_1, \ldots, z_t) \cdot T;$$

hence the T form a representation mediated by $\mathfrak{A}$. Further,

$$(cy_1, \ldots, cy_r) \equiv (y_1, \ldots, y_r) \cdot R \pmod{\mathfrak{A}},$$

while the y_i form a basis linearly independent modulo $\mathfrak{A}$. Thus the R form a representation generated by $\mathfrak{M}/\mathfrak{A}$.

Conversely, if a "reducible" representation

$$C = \begin{pmatrix} R & 0 \\ S & T \end{pmatrix}$$

is given, with R and T square matrices, then in the associated representation module the products of each c with the last t basis elements $z_1, \ldots, z_t$ are expressed through those elements alone; hence $\mathfrak{A} = (z_1, \ldots, z_t)$ is a submodule.

16) In other words: if $\mathfrak{A}$ is a direct summand as a K-module. If K is a field, this hypothesis is always fulfilled.

Corollary. Let

$$\mathfrak{M} > \mathfrak{A}_1 > \mathfrak{A}_2 > \cdots > \mathfrak{A}_e = 0$$

be a composition series for $\mathfrak{M}$, and suppose that each $\mathfrak{A}_i$ is a direct summand of the preceding one as a K-module, so that one can choose a basis

$$z_{11}, \ldots, z_{1r_1}, \quad z_{21}, \ldots, z_{2r_2}, \quad \ldots \quad z_{e1}, \ldots, z_{er_e}$$

such that the z_{ik} with $i > \nu$ form a basis of $\mathfrak{A}_\nu$. The representations mediated by $\mathfrak{M}$ then have the form

$$C = \begin{pmatrix} R_{11} & 0 & \cdots & 0 \\ R_{12} & R_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ R_{1e} & R_{2e} & \cdots & R_{ee} \end{pmatrix}, \tag{2}$$

and the $R_{\nu\nu}$ form representations mediated by the composition factors $\mathfrak{A}_{\nu-1}/\mathfrak{A}_\nu$.

The individual representations $R_{\nu\nu}$ are irreducible, since the composition factors $\mathfrak{A}_{\nu-1}/\mathfrak{A}_\nu$ are simple. If K is assumed to be a field, so that every submodule is a direct summand, then conversely every representation reduced as far as possible in the form (2) leads to a composition series. By the Jordan–Hölder theorem the composition factors are uniquely determined up to operator isomorphism. Hence the $R_{\nu\nu}$ are uniquely determined up to equivalent representations and up to their order.

If $\mathfrak{M} = \mathfrak{A} + \mathfrak{B}$ is the direct sum of two representation modules $\mathfrak{A} = (y_1, \ldots, y_r)$ and $\mathfrak{B} = (z_1, \ldots, z_s)$, then the representation mediated by the basis $(y_1, \ldots, y_r, z_1, \ldots, z_s)$ plainly has the form

$$C = \begin{pmatrix} R & 0 \\ 0 & S \end{pmatrix},$$

where R denotes the representation of the element c mediated by $\mathfrak{A}$, and S the one mediated by $\mathfrak{B}$, and conversely. If one first writes $\mathfrak{M}$ as a direct sum of directly indecomposable constituents and draws composition series in these as above, then for a suitable basis the representation has the form

$$C = \begin{pmatrix} \boxed{\begin{matrix} R_{11} & 0 \\ \vdots & \ddots \\ R_{ik} & R_{rr} \end{matrix}} & & & 0 \\ & \boxed{\begin{matrix} S_{11} & 0 \\ \vdots & \ddots \\ S_{ik} & S_{ss} \end{matrix}} & & \\ & & \boxed{\begin{matrix} T_{11} & 0 \\ \vdots & \ddots \\ T_{ik} & T_{tt} \end{matrix}} & \\ 0 & & & \end{pmatrix}. \tag{3}$$

If again K is a field, every representation reduced as far as possible in the form (3) conversely leads to a representation of the module by directly indecomposable summands and composition factors within them. By the theorem of Krull and Otto Schmidt (note 11), the classes of directly indecomposable representation constituents are uniquely determined up to order.

If the module $\mathfrak{M}$ is completely reducible, all boxes in the form (3) consist of a single irreducible representation, and one calls the representation completely reducible.

ğ 17. Direct sum decompositions of representation modules for rings with identity element

Let $\mathfrak{M}$ be an $\mathfrak{o}$-module, with $\mathfrak{o}$ a ring with identity. Then

$$\mathfrak{M} = \mathfrak{M}_e + \mathfrak{M}_0,$$

where the identity is the identity operator on $\mathfrak{M}_e$ and the zero operator on $\mathfrak{M}_0$. (If $\mathfrak{M}$ is also a right K-module, then $\mathfrak{M}_e$ and $\mathfrak{M}_0$ are also right K-modules.)

Proof. Every m in $\mathfrak{M}$ can be written as

$$m = em + (m - em).$$

Let the set of the em be $\mathfrak{M}_e$, and the set of the $m - em$ be $\mathfrak{M}_0$. These are plainly additive groups, and right K-modules if $\mathfrak{M}$ is one. Moreover

$$rem = erm,$$

so $\mathfrak{M}_e$ is also an $\mathfrak{o}$-module; and

$$r(m - em) = rm - rem = rm - rm,$$

so $\mathfrak{M}_0$ is an $\mathfrak{o}$-module. For the em, e is the identity operator; for the $m - em$, it is the zero operator. Thus only zero belongs to both $\mathfrak{M}_e$ and $\mathfrak{M}_0$, and the sum $\mathfrak{M}_e + \mathfrak{M}_0$ is direct.

For representation modules, $\mathfrak{M}_0$ generates the trivial representation, in which every element is assigned zero. Splitting off the summand $\mathfrak{M}_0$, there remains the representation mediated by $\mathfrak{M}_e$, in which the identity element is assigned the identity matrix. We can and will therefore restrict ourselves henceforth to such representations.

Let $\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s$ be a direct sum of two-sided ideals, let $e = e_1 + \cdots + e_s$ be the decomposition of e, and let $\mathfrak{M}$ be an $\mathfrak{o}$-module on which e is the identity operator. Then

$$\mathfrak{M} = \mathfrak{a}_1\mathfrak{M} + \cdots + \mathfrak{a}_s\mathfrak{M}$$

directly. Plainly $\mathfrak{M} = \mathfrak{o}\mathfrak{M} = (\mathfrak{a}_1\mathfrak{M}, \ldots, \mathfrak{a}_s\mathfrak{M})$. Put $\mathfrak{b}_i = \mathfrak{a}_1 + \cdots + \widehat{\mathfrak{a}_i} + \cdots + \mathfrak{a}_s$. Then

$$\mathfrak{M} = (\mathfrak{a}_i\mathfrak{M}, \mathfrak{b}_i\mathfrak{M}),$$

and this sum is direct, since e_i is the identity operator on $\mathfrak{a}_i\mathfrak{M}$ and the zero operator on $\mathfrak{b}_i\mathfrak{M}$.

On the basis of this theorem we shall usually restrict ourselves to representations of two-sided indecomposable rings.

ğ 18. Module and representation theory of completely reducible rings

Let $\mathfrak{o}$ be completely reducible and two-sided simple, and let $\mathfrak{M}$ be a finite $\mathfrak{o}$-module for which the identity element of $\mathfrak{o}$ is the identity operator. Then $\mathfrak{M}$ is completely reducible, and its simple constituents are operator-isomorphic to the simple left ideals $\mathfrak{l}_i$.

Proof. Let

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n, \qquad \mathfrak{M} = (\mathfrak{o}m_1, \ldots, \mathfrak{o}m_k),$$

and therefore

$$\mathfrak{M} = (\ldots, \mathfrak{l}_i m_k, \ldots). \tag{4}$$

The $\mathfrak{l}_i m_k$ that are non-zero are isomorphic to $\mathfrak{l}_i$, since the assignment $a \longmapsto am_k$ is an operator isomorphism. Hence the $\mathfrak{l}_i m_k$ are simple. Omitting from (4) those $\mathfrak{l}_i m_k$ already contained in the sum of the preceding ones, the sum becomes direct.

Consequently, if in addition $\mathfrak{M}$ is directly indecomposable, then $\mathfrak{M}$ is simple and isomorphic to some $\mathfrak{l}_i$.

Let Δ be the automorphism field of this simple $\mathfrak{M}$, and let Λ be that of $\mathfrak{l}_i$. Then, by the operator isomorphism of $\mathfrak{M}$ and $\mathfrak{l}_i$, we have the ring isomorphism $\Delta \simeq \Lambda$. By ğ 1 one can regard $\mathfrak{M}$ and $\mathfrak{l}_i$ as double modules with Δ and Λ, respectively, as right domains; these double modules are also representation modules, because $\mathfrak{l}_i$, and consequently $\mathfrak{M}$, has finite rank with respect to the automorphism field (ğ 14), whose identity element is the identity operator. The representations mediated by them pass into one another under the

ring isomorphism $\Delta \simeq \Lambda$. *Thus for the study of this representation class we may restrict ourselves to the representation mediated by* $\mathfrak{l}_i$ *in its automorphism field.*

Specifically, put a basis of matrix units for $\mathfrak{l}_1$ in the form

$$\mathfrak{l}_1 = (c_{11}, \ldots, c_{n1})$$

and realize the automorphism field Λ as the subfield of $\mathfrak{o}$ denoted earlier (ğ 14) by K (in our earlier considerations right ideals must be replaced by left ideals, and the automorphisms accordingly written on the right). If

$$a = \sum c_{ik}\alpha_{ik},$$

then

$$a \longmapsto (\alpha_{ik})$$

is the representation in K mediated by $\mathfrak{l}_1$. For

$$a \cdot c_{k1} = \Big(\sum\sum c_{ij}\alpha_{ij}\Big) \cdot c_{k1} = \sum c_{i1}\alpha_{ik},$$

or

$$a(c_{11}, \ldots, c_{n1}) = (c_{11}, \ldots, c_{n1})(\alpha_{ik}).$$

Let Γ be a subfield of K such that K has finite rank t with respect to Γ:

$$K = z_1\Gamma + \cdots + z_t\Gamma.$$

Then K becomes its own representation module with respect to Γ. The elements β of K are represented by matrices B over Γ, obtained from

$$\beta z_j = \sum z_i\beta_{ij}; \qquad B = (\beta_{ij}).$$

If $\mathfrak{l}_1$ is now regarded as a representation module with respect to the subfield Γ, one obtains:

The representation of $\mathfrak{o}$ *in* Γ *mediated by* $\mathfrak{l}_1$ *is obtained by replacing, in the representation of* $\mathfrak{o}$ *in* K *given above,*

$$a \longmapsto (\alpha_{ik}),$$

the elements α_{ik} *by the matrices* A_{ik} *that correspond to them in the representation of* K *in* Γ.

Proof.

$$\mathfrak{l}_1 = \sum c_{i1}K = \sum\sum c_{i1}z_j\Gamma.$$

With respect to the basis $(\ldots, c_{i1}z_j, \ldots)$, one has

$$c_{ik} \longmapsto \begin{matrix} \\ \boxed{1} \\ \boxed{i} \\ \boxed{n} \end{matrix} \begin{matrix} \begin{matrix} \boxed{1} & & \boxed{k} & & \boxed{n} \end{matrix} \\ \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & E_t & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \end{matrix},$$

where E_t is the identity matrix and 0 the zero matrix of degree t, while

$$\alpha \longmapsto \begin{pmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{pmatrix}.$$

Consequently,

$$a = \sum c_{ik}\alpha_{ik} \longmapsto \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix}.$$

The passage to an arbitrary $\mathfrak{M}$ again amounts to a ring isomorphism for the representation. If $\mathfrak{o}$ is a direct sum of two-sided simple rings, then these rings are represented isomorphically in turn and the remaining ones by zero.

Remark. Up to isomorphism, the representations studied here, in the automorphism field of the left ideals and its finite subfields, are the only ones that can be mediated by simple $\mathfrak{o}$-modules (or left ideals). For, by a remark made earlier (ğ 2), if the $\mathfrak{o}$-module $\mathfrak{M}$ is regarded as a double module with respect to any field K, then the elements of K generate module homomorphisms; hence the field K must necessarily be homomorphically related to a subfield of the automorphism field of this $\mathfrak{o}$-module. Since the identity element is the identity operator, this homomorphism is an isomorphism, and the whole automorphism field must have finite degree over the subfield in question, since otherwise the representation module too would have infinite rank, which is impossible.

Finally, it should be mentioned that the irreducible representations studied here are not yet all of them, but only those mediated by simple $\mathfrak{o}$-modules. In general there are further representation modules (for example, a field Ω regarded as a double module with respect to a subfield Σ as left domain and itself as right domain) which are reducible as $\mathfrak{o}$-modules but irreducible as double modules, and which therefore nevertheless lead to irreducible representations.

ğ 19. The simple composition factors in modules and representation modules

Let $\mathfrak{o}$ be a ring satisfying the maximal and minimal conditions for left ideals, and let $\mathfrak{c}$ be the maximal nilpotent ideal. Then:

Every simple $\mathfrak{o}$-module $\mathfrak{M}$ is either annihilated by $\mathfrak{o}$, or it is isomorphic to a simple left ideal $\mathfrak{l}$ from the ring without radical $\mathfrak{o}/\mathfrak{c}$. In the latter case the module is annihilated by all those two-sided ideals of $\mathfrak{o}/\mathfrak{c}$ which do not contain $\mathfrak{l}$, and the absolute multiplier domain (ğ 1) is isomorphic to the two-sided simple ring which contains $\mathfrak{l}$.

Proof. Let $\mathfrak{c}^e = 0$. We must have $\mathfrak{c}\mathfrak{M} = 0$, since otherwise $\mathfrak{c}\mathfrak{M} = \mathfrak{M}$, and hence $\mathfrak{M} = \mathfrak{c}\mathfrak{M} = \mathfrak{c}^2\mathfrak{M} = \cdots = 0$ would follow. Thus $\mathfrak{M}$ can also be regarded as an $\mathfrak{o}/\mathfrak{c}$-module (all elements of a residue class modulo $\mathfrak{c}$ give the same result when multiplied by an element of $\mathfrak{M}$). As a ring without radical, $\mathfrak{o}/\mathfrak{c}$ has an identity element, and so $\mathfrak{M}$ is the direct sum of a module annihilated by $\mathfrak{o}/\mathfrak{c}$ and a module on which the identity element is the identity operator (ğ 17). Since $\mathfrak{M}$ is simple, only one of the two summands can occur. If the identity element is the identity operator, isomorphism with a simple left ideal follows as in ğ 18. Indeed, if $m \neq 0$ is an element of $\mathfrak{M}$, then $(\mathfrak{o}/\mathfrak{c}) \cdot m \neq 0$, and hence $\mathfrak{l} \cdot m \neq 0$ for at least one simple left ideal $\mathfrak{l}$ of $\mathfrak{o}/\mathfrak{c}$; it must therefore exhaust $\mathfrak{M}$. The further assertions are clear for such left ideals and carry over at once to all modules isomorphic to them.

Corollary. *If $\mathfrak{M}$ is an $\mathfrak{o}$-module possessing a composition series, then its simple composition factors are either annihilated by $\mathfrak{o}$, or are isomorphic to simple left ideals of $\mathfrak{o}/\mathfrak{c}$.*

If P is a ring commutatively connected with $\mathfrak{o}$, all the results remain valid. One need only consider, instead of modules, double modules with respect to P on the right and $\mathfrak{o}$ on the left which satisfy

$$am \cdot \rho = a \cdot m\rho = a\rho \cdot m \qquad (\text{ğ } 15).$$

The identity element of P is also to be the identity operator. As submodules one always considers only those which admit multiplication by P (as with ideals). The submodules $\mathfrak{c}\mathfrak{M}, \mathfrak{c}^2\mathfrak{M}, \ldots$ constructed in our proofs satisfy this condition.

If, in particular, P is a field and $\mathfrak{M}$ is a P-module of finite rank, then $\mathfrak{M}$ is also a representation module. The representation mediated by $\mathfrak{M}$ is not only ring-homomorphic, but also operator-homomorphic with respect to P (ğ 15). All representations in P having this property are supplied by such modules. Irreducible representations belong to simple modules, and conversely. Thus the theorems of this section can immediately be interpreted as theorems about representations of $\mathfrak{o}$ in P: *All irreducible representations (apart from the zero representations) are mediated by the simple left ideals of $\mathfrak{o}/\mathfrak{c}$. Thus, when an arbitrary representation is reduced by means of a composition series as in ğ 16, only representations equivalent to those mediated by simple left ideals of $\mathfrak{o}/\mathfrak{c}$ occur on the main diagonal, apart from zeros.*

Remark. Under the assumptions made about $\mathfrak{o}$ and P, no finiteness condition need be imposed on $\mathfrak{o}$. For all representations are at the same time isomorphic representations of the absolute multiplier domain, and this domain, as the isomorphic inverse image of a ring of matrices of finite degree, is itself a P-module of finite rank. Since, by definition, only P-modules are regarded as admissible ideals, the maximal and minimal conditions hold for this absolute multiplier domain.

This absolute multiplier domain becomes a hypercomplex system with respect to P when P is assumed to be a commutative field. This assumption is always fulfilled as soon as not only zeros occur on the main diagonal. For then, by the remark in ğ 18, P is isomorphic to a subfield of the automorphism field of $\mathfrak{l}$, which,

in the realization by the subfield K of $\mathfrak{o}/\mathfrak{c}$ (ğ 14), must—because of the commutative connection—lie in the center of K.

Chapter IV.
Representations of Groups and Hypercomplex Systems.

ğ 20.
Inclusion of Hypercomplex Systems.

We consider hypercomplex systems $\mathfrak{o}$ with respect to a commutative field P. Since, by convention, only P-modules are considered as ideals in $\mathfrak{o}$, the maximal and minimal conditions hold for left and right ideals (cf. ğ 8). Thus the whole ring theory developed in Chapter II applies.

In what follows, by *representations* of the hypercomplex system $\mathfrak{o}$ we always mean representations in the field P, and specifically representations for which $a \to A$ implies $a\rho \to A\rho$ for ρ in P (module homomorphism with respect to P). For the representation modules this means $a\rho \cdot m = a \cdot m\rho$ (cf. the end of ğ 15). The theorems of ğ 19 therefore apply to the representation modules, and they imply that *all irreducible representations are mediated by simple left ideals of* $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{c}$*, and hence that there are as many inequivalent irreducible representations as there are two-sided simple summands* $\mathfrak{a}$ *in a decomposition* $\bar{\mathfrak{o}} = \bar{\mathfrak{o}}e^{(1)} + \cdots + \bar{\mathfrak{o}}e^{(s)}$.

To determine explicitly the representation of $\mathfrak{o}$ defined by such a left ideal $\mathfrak{l}_\nu$, one first passes from the elements of $\mathfrak{o}$ to their corresponding residue classes in $\bar{\mathfrak{o}}$. Since multiplication by an element of P is an isomorphism for all ideals in $\bar{\mathfrak{o}}$, the field P is homomorphic to a subfield $e^{(\nu)}P$ of the automorphism field K_ν of every simple left ideal and, because the identity element is the identity operator, is in fact isomorphic to it. The representation in P mediated by a simple left ideal $\mathfrak{l}_\nu$ can be obtained by first examining the representation mediated by $\mathfrak{l}_\nu$ in this subfield $e^{(\nu)}P$ and then passing to P by the isomorphism $e^{(\nu)}P \simeq P$. The isomorphism field K_ν has finite rank with respect to P; thus the question is one of representation in a finite-degree subfield of the automorphism field of $\mathfrak{l}_\nu$.

To obtain the desired representation, first express each c of $\bar{\mathfrak{o}}$ by its two-sided components:

$$c = c_1 + \cdots + c_s.$$

It remains only to seek the representing matrix of c_ν, since the remaining c_i annihilate the ideal $\mathfrak{l}_\nu$ and are therefore represented by the zero matrix. By ğ 18 this matrix is found as follows. Express c_ν in terms of the matrix units $c_{ik}^{(\nu)}$ of $\mathfrak{a}_\nu$:

$$c_\nu = \sum c_{ik}^{(\nu)} \alpha_{ik}^{(\nu)},$$

and in the matrix $(\alpha_{ik}^{(\nu)})$ replace every element $\alpha_{ik}^{(\nu)}$ by the matrix $A_{ik}^{(\nu)}$ assigned to it in the representation of K_ν in P mediated by K_ν.

Remark. The field K_ν has finite rank with respect to P. Every element x satisfies an equation $f(x) = 0$ with coefficients in $e^{(\nu)}P$, since some linear dependence must hold among the powers of x. If, in particular, P is algebraically closed, this equation splits into linear factors; since K is a field, x is already a root of a linear factor and hence already belongs to $e^{(\nu)}P$, i.e. $K_\nu = e^{(\nu)}P$. In this case the matrices $(\alpha_{ik}^{(\nu)})$ themselves therefore constitute the irreducible representation.

From this remark together with the end of ğ 19 one obtains "Burnside's theorem":

Let P be algebraically closed and commutatively connected with a ring $\mathfrak{o}$. Then every irreducible representation of degree n in P – $\mathfrak{o} \sim \mathfrak{D}$ – contains exactly n^2 linearly independent matrices.[17)]

From this formulation the usual one follows at once: "A system of matrices of degree n in P which, with every two matrices, also contains their product, is irreducible if and only if there is no linear homogeneous relation

$$\sum \alpha_{ik}\rho_{ik} = 0$$

with coefficients in P that is satisfied by the entries α_{ik} of every matrix in the system." Indeed, by adjoining all linear combinations to any such system of matrices, one can derive a ring and P-module and regard this ring as its own representation.

Proof. By ğ 19, $\mathfrak{D}$ is isomorphic to a two-sided simple and completely reducible ring $\bar{\mathfrak{o}}$ with identity element. Such a ring, however, is a full matrix ring (say the ring of all matrices of degree m) over the automorphism field of its left ideals, which, by algebraic closedness, coincides with P. Every irreducible representation of $\bar{\mathfrak{o}}$, and hence also the given one, is generated by a simple left ideal. The left ideal has

rank m, while the representation has degree n; hence $m = n$, and therefore there are exactly n^2 linearly independent elements in $\bar{\mathfrak{o}}$, and thus also in $\mathfrak{D}$.

The "generalized Burnside theorem" likewise follows easily:[18)]

Under the same hypotheses, let $\mathfrak{D}$ be a completely reducible representation of $\mathfrak{o}$ which decomposes entirely into inequivalent constituents of degrees $n_1, n_2, \ldots, n_s$. Then $\mathfrak{D}$ has rank $n_1^2 + \cdots + n_s^2$ with respect to P.

Proof. Again let $\bar{\mathfrak{o}}$ be the absolute multiplier domain, which is necessarily a hypercomplex system. The different inequivalent representations are generated by left ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_s$ belonging to different two-sided simple components $\mathfrak{a}_i$ of $\bar{\mathfrak{o}}/\bar{\mathfrak{c}}$, where $\bar{\mathfrak{c}}$ is the radical. Thus the given representation is generated by $\mathfrak{l}_1 + \cdots + \mathfrak{l}_s$ and therefore has $\mathfrak{a}_1 + \cdots + \mathfrak{a}_s$ as its absolute multiplier domain. The assertion follows by the same rank considerations as above.

Now let $\mathfrak{o}$ be a hypercomplex system without radical with respect to an arbitrary field. By §§ 13, $\mathfrak{o}$ is completely reducible and has an identity element. From the theorems of §§ 17 and 18 it follows that *every representation of $\mathfrak{o}$ is completely reducible.*

Conversely, *every completely reducible representation of a ring $\mathfrak{o}$ commutatively connected with P has as its absolute multiplier domain a hypercomplex system without radical.*

Proof. The absolute multiplier domain $\bar{\mathfrak{o}}$ is isomorphic to a ring and P-module of matrices in P, and is therefore a hypercomplex system. By § 19 the elements of the radical $\bar{\mathfrak{c}}$ are represented by zero in every irreducible representation, hence also in the whole representation; thus $\bar{\mathfrak{c}} = 0$.

(If only equivalent constituents occur in the representation, all of them mediated by one left ideal $\mathfrak{l}$, then the absolute multiplier domain is two-sided simple.)

The *regular representation* of a hypercomplex system $\mathfrak{o}$ is the representation mediated by the unit ideal $\mathfrak{o}$ itself. (For the group ring one chooses specifically the basis consisting of the group elements $u_1, \ldots, u_h$; cf. § 6.) Since all left ideals of $\mathfrak{o}/\mathfrak{c}$ occur as composition factors in $\mathfrak{o}$, all irreducible representations already occur in the regular representation as diagonal matrices R_{ii} when the regular representation is transformed to a suitable basis, by means of a composition series, according to formula (2) of § 16.

A representation is known when the representing matrices of the basis elements $u_1, \ldots, u_h$ are known. In the special case of a group ring, where $u_1, \ldots, u_h$ are elements of a group, every homomorphic representation of the group by matrices also generates a representation of the group ring. Thus the problem of representing a group is a special case of representing hypercomplex systems.

17) Thus $\mathfrak{o}$ is not assumed to be a hypercomplex system and may, for example, be the group ring consisting of all linear combinations of finitely many elements of an infinite group.

18) G. Frobenius and I. Schur, Über die Äquivalenz der Gruppen linearer Substitutionen, Sitzungsber. Berlin 1906.

§ 21.
Extension of the Ground Field. Representations of the Center.

Let $\mathfrak{o} = a_1 P + \cdots + a_h P$ be a hypercomplex system, and let Ω be an extension field of the ground field P. One can form

$$\mathfrak{o}\Omega = a_1\Omega + \cdots + a_h\Omega$$

with the old multiplication rules for the basis elements a_i.[18a)] The system $\mathfrak{o}\Omega$ is again hypercomplex with respect to Ω.

Every representation of $\mathfrak{o}$ leads to a representation of $\mathfrak{o}\Omega$, since the representation of all elements is known as soon as the representations of the basis elements a_i are known.[19)]

18a) More precisely, one introduces new symbols $\bar{a}_i$ with the old multiplication rules; $\bar{a}_1\Omega + \cdots + \bar{a}_h\Omega$ then contains a subring isomorphic to $\mathfrak{o}$, so that the $\bar{a}$ may afterward be identified with the a.

19) Of course, here again only representations which are P-module homomorphisms are considered: $a \to A$ is to imply $a\rho \to A\rho$ for ρ in P, and correspondingly for Ω.

An ideal or representation module, as well as the corresponding representation, is called *absolutely irreducible* if it remains irreducible after passage to the algebraically closed field.

If $\mathfrak{o}\Omega$ is without radical, then so is $\mathfrak{o}$; for a nilpotent ideal $\mathfrak{c}$ in $\mathfrak{o}$ would lead to an extended ideal $\mathfrak{c}\Omega$ in $\mathfrak{o}\Omega$. The converse is not true, as will be seen below.

The center of $\mathfrak{o}\Omega$ is equal to the extended center $\mathfrak{Z}\Omega$. If $\mathfrak{o}$ is completely reducible, then $\mathfrak{Z}$ is a direct sum of fields:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_s.$$

If $\mathfrak{o}$ remains completely reducible upon passage to $\mathfrak{o}\Omega$ (i.e. if no nilpotent ideal is added), then the new center decomposes in Ω as

$$\mathfrak{Z}\Omega = \mathfrak{Z}_1\Omega + \cdots + \mathfrak{Z}_s\Omega$$

again into a direct sum of fields which, if Ω is algebraically closed, have rank 1 with respect to Ω (and are isomorphic to Ω), by the remark in ğ 20.

For representations of the center $\mathfrak{Z}$ the following theorems hold:

Every irreducible representation of a commutative hypercomplex system $\mathfrak{Z}$ in the algebraically closed field Ω is of degree one (or: the irreducible representations are identical with the homomorphisms from $\mathfrak{Z}$ into Ω).

Proof. Every irreducible representation of $\mathfrak{Z}$ yields one of $\mathfrak{Z}_\Omega$, and hence also one of $\mathfrak{Z}_\Omega/\mathfrak{C}$, where $\mathfrak{C}$ is the radical of $\mathfrak{Z}_\Omega$. The system $\mathfrak{Z}_\Omega/\mathfrak{C}$ is commutative and without radical, and therefore, by the end of ğ 14, is a direct sum of fields. These have degree one because Ω is assumed algebraically closed, and they generate all irreducible representations (ğ 20).

At the same time, since equivalent representations of degree one necessarily become equal ($\lambda^{-1}\alpha\lambda = \alpha$), it follows that *the number of different homomorphisms from $\mathfrak{Z}$ into Ω is equal to the rank of $\mathfrak{Z}_\Omega/\mathfrak{C}$.*

The last remark gives, for the special case in which $\mathfrak{Z}$ is a field over P, the theorem:

If $\mathfrak{Z}$ is a commutative field, then $\mathfrak{Z}$ is completely reducible (without radical) if and only if $\mathfrak{Z}$ is an extension of the first kind of P.

For in the case of a field the homomorphisms are isomorphisms; their number is equal to the rank of $\mathfrak{Z}_\Omega/\mathfrak{C}$, and hence is equal to the field degree ($\mathfrak{Z}$ being an extension of the first kind) if and only if $\mathfrak{C} = 0$.

If $\mathfrak{Z}$ is completely reducible,

$$\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_t,$$

then in every representation the individual fields $\mathfrak{Z}_\nu$ are also represented homomorphically: in an irreducible representation one of these fields is represented isomorphically and the others by zero (ğ 19).

For systems without radical, application of these theorems to hypercomplex systems gives first:

If $\mathfrak{o}_\Omega$, and hence also $\mathfrak{o}$, is a system without radical, then in every absolutely irreducible representation of $\mathfrak{o}$ the central elements z are represented by diagonal matrices $E\zeta^{(\nu)}$, and $z \to \zeta^{(\nu)}$ is a representation of degree one of $\mathfrak{Z}$ in Ω. The resulting correspondence between the absolutely irreducible representation classes of $\mathfrak{o}$ and those of $\mathfrak{Z}$ is one-to-one. Thus the number of these representation classes is equal to the rank of the center.[20)]

20) Corresponding theorems hold not only for representations in the algebraically closed field Ω, but also for representations in the individual automorphism fields, as is to be carried out elsewhere.

Proof. The decomposition into two-sided indecomposable ideals

$$\mathfrak{o}_\Omega = \mathfrak{a}_1 + \cdots + \mathfrak{a}_t$$

corresponds one-to-one to a decomposition of the center into fields:

$$\mathfrak{Z}_\Omega = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_t,$$

where $\mathfrak{Z}_\Omega$ is the center of $\mathfrak{o}_\Omega$. In an irreducible representation of $\mathfrak{o}$, one $\mathfrak{a}_\nu$ is represented isomorphically and the others by zero, and the representation class is uniquely determined by $\mathfrak{a}_\nu$. The component $\mathfrak{a}_\nu$ is represented by a full matrix ring, and the center of such a full matrix ring consists of diagonal matrices $E\zeta^{(\nu)}$. The assignment $z \to \zeta^{(\nu)}$ is a homomorphism of $\mathfrak{Z}$: one $\mathfrak{Z}_\nu$ is represented isomorphically and the others by zero. This proves everything asserted.

For the question when a system $\mathfrak{o}$ without radical gives rise to a system $\mathfrak{o}_\Omega$ likewise without radical, one obtains further:

If $\mathfrak{Z}$ has a component $\mathfrak{Z}_\nu$ which is an extension of the second kind of P, then $\mathfrak{o}_\Omega$ certainly has a radical.[21)] For in this case $\mathfrak{Z}_\Omega$ already has one.

21) If $\mathfrak{Z}$ has only components of the first kind, then $\mathfrak{o}_\Omega$ is without radical, as will likewise be proved later. In characteristic zero I. Schur already proved the equivalent theorem that irreducible representations over P remain completely reducible under every extension of the coefficient domain; see I. Schur, Beiträge zur Theorie der Gruppen linearer Substitutionen, Transact. Am. Math. Soc. 15 (1909), p. 159.

ğ 22.
Application to Abelian Groups.

Let $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \cdots \times \mathfrak{G}_r$ be a finite Abelian group, decomposed into cyclic groups $\mathfrak{G}_i$ of orders h_i. Its elements are

$$a = c_1^{\lambda_1} \cdots c_r^{\lambda_r}.$$

Let P be a field whose characteristic does not divide the group order $h = h_1 h_2 \cdots h_r$.

The group ring $\mathfrak{Z}$ consists of all sums

$$\sum a_\lambda \rho_\lambda = \sum c_1^{\lambda_1} \cdots c_r^{\lambda_r} \rho_\lambda \qquad (\rho_\lambda \text{ in } P)$$

and is a homomorphic image of the polynomial domain $P[z_1, \ldots, z_r]$ under

$$\sum \rho_\lambda z_1^{\lambda_1} \cdots z_r^{\lambda_r} \to c_1^{\lambda_1} \cdots c_r^{\lambda_r} \rho_\lambda.$$

Thus $\mathfrak{Z} \sim P[z_1, \ldots, z_r]/m$, and one readily finds

$$m = (z_1^{h_1} - e, \ldots, z_r^{h_r} - e).$$

In the extension field Ω, the $z_i^{h_i} - e$ split into distinct factors $z_i - \epsilon_i$; hence m is the product (or intersection) of distinct prime ideals

$$\mathfrak{P}^{(\nu)} = (z_1 - \epsilon_1^{(\nu)}, \ldots, z_r - \epsilon_r^{(\nu)})$$

with exactly one zero $(\epsilon_1^{(\nu)}, \ldots, \epsilon_r^{(\nu)})$ each. To the intersection corresponds a direct-sum decomposition (ğ 4):

$$\mathfrak{Z}_\Omega = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_h,$$

where in each case $\mathfrak{Z}_\nu \simeq \mathfrak{Z}_\Omega/\mathfrak{P}^{(\nu)}$ and hence mediates the representation

$$c_1^{\lambda_1} \cdots c_r^{\lambda_r} \to \epsilon_1^{(\nu)\lambda_1} \cdots \epsilon_r^{(\nu)\lambda_r} \qquad \text{or} \qquad a \to \chi^{(\nu)}(a)$$

These representations are the *characters*. Their number is $h_1 h_2 \cdots h_r = h$, as required by the general theory.

ğ 23.
Determinant of a Hypercomplex System.

Let $\mathfrak{o} = a_1 P + \cdots + a_h P$ be a hypercomplex system. I adjoin to P the h indeterminates $x_1, \ldots, x_h$ and form

$$\mathfrak{o}^* = a_1 P(x) + \cdots + a_h P(x).$$

The x_i are to commute with the a_i; this determines the rules of calculation in $\mathfrak{o}^*$.

In $\mathfrak{o}^*$ lies "the general element of $\mathfrak{o}$",

$$w = a_1 x_1 + \cdots + a_h x_h.$$

If in a representation $a_i \to A_i$, then to w is assigned

$$W = A_1 x_1 + \cdots + A_h x_h.$$

The matrix W is called the *system matrix* belonging to the representation (or, specifically, if the a_i form a group and $\mathfrak{o}$ is therefore the group ring, the *group matrix*). In the case of the regular representation one has the *regular system matrix*.

The entries w_{ik} of W are linear forms in the x. The "*system determinant*" $|W|$ is therefore of degree n when the representation has degree n. In particular, the *regular system determinant* has degree h.

The system determinant is unchanged upon passage to equivalent representations, since $|PWP^{-1}| = |P|\,|W|\,|P^{-1}| = |W|$. Upon passage from $(a_1, \ldots, a_h)$ to a new basis $(b_1, \ldots, b_h)$ and from $w = \sum a_i x_i$ to $w = \sum b_i y_i$, the new entries of W, and hence also the new determinant, are obtained by making in the old ones a substitution

$$x_i = \sum \rho_{ik} y_k$$

with regular substitution matrix.

If a composition series of the representation module is given, then, with a suitable choice of basis, the matrix W has the form

$$W = \begin{pmatrix} W_1 & & 0 \\ & W_2 & \\ & \ddots & \\ W_{ik} & & W_r \end{pmatrix}.$$

$$|W| = |W_1| \cdot |W_2| \cdots |W_r|.$$

Among the $|W_i|$ of an arbitrary representation, none occur other than those in the regular representation of $\mathfrak{o}$, or even of $\mathfrak{o}/\mathfrak{c}$, where $\mathfrak{c}$ is the radical.

If P is algebraically closed, then the determinant $|W_i|$ belonging to an irreducible representation is a prime function in the x, and inequivalent representations give different prime factors.

Proof. Since all irreducible representations of $\mathfrak{o}$ are also representations of $\mathfrak{o}/\mathfrak{c}$, we may restrict ourselves to the ring without radical $\mathfrak{o}/\mathfrak{c}$. In it we introduce the matrix units $c_{ik}^{(\nu)}$ as basis; the general element is then

$$w = \sum c_{ik}^{(\nu)} x_{ik}^{(\nu)}.$$

The matrices of the irreducible representations are $W_\nu = (x_{ik}^{(\nu)})$. The functions $|W_\nu| = |x_{ik}^{(\nu)}|$ are known to be irreducible and are plainly distinct from one another.

To calculate the $|W_\nu|$, one can factor the regular system matrix of $\mathfrak{o}/\mathfrak{c}$ into its prime factors. Each prime factor occurs as many times as the degree of the irreducible representation indicates, since the corresponding ideal $\mathfrak{l}_\nu$ occurs that many times in the composition series.

One can also take the regular system matrix of $\mathfrak{o}$ as the basis, but then each irreducible factor is obtained more often: namely, as often as the corresponding $\mathfrak{l}_\nu$ occurs as a composition factor among the left ideals. In this regular representation $\mathfrak{o}$ was regarded as a left ideal; if $\mathfrak{o}$ is regarded as a right ideal, there appears a second regular system matrix (the "antistrophic matrix" of Frobenius), which contains the same irreducible factors (namely the system determinants of all irreducible representations), though possibly with different exponents (see the example in ğ 10).

The system determinant of a commutative system splits into linear factors, since all irreducible representations have degree one. These linear factors are themselves the irreducible representations, and therefore for Abelian groups they give the characters. This fact was Dedekind's point of departure in his study of the group determinant of non-Abelian groups.

ğ 24.
Traces and Characters.

If, in a representation $\mathfrak{o} \sim \mathfrak{D}$ of a hypercomplex system $\mathfrak{o}$, the element a is assigned the matrix A, put

$$\mathrm{Sp}_{\mathfrak{D}}(a) = \mathrm{Sp}\, A.$$

Traces are linear functions:

$$\mathrm{Sp}(c+d) = \mathrm{Sp}(c) + \mathrm{Sp}(d); \qquad \mathrm{Sp}(c\alpha) = \alpha\, \mathrm{Sp}(c).$$

Equivalent representations have the same traces.

The trace in a reducible representation is the sum of the traces in the representations mediated by the composition factors.

Proof.

$$\mathrm{Sp}\begin{pmatrix} A_{11} & & 0 \\ & A_{22} & \\ & \ddots & \\ A_{ik} & & A_{rr} \end{pmatrix} = \mathrm{Sp}(A_{11}) + \mathrm{Sp}(A_{22}) + \cdots + \mathrm{Sp}(A_{rr}).$$

Principal trace = trace in the regular representation.

Reduced trace = sum of the traces in the different irreducible representations.

If c is an element of the maximal nilpotent ideal $\mathfrak{c}$, then $\mathrm{Sp}(c) = 0$ *for every representation.*

Proof. It is enough to examine the representations through the simple left ideals of $\mathfrak{o}/\mathfrak{c}$; for in every other representation only these composition factors occur, and the trace is composed additively.

But c annihilates all elements of $\mathfrak{o}/\mathfrak{c}$; hence the zero matrix is assigned to every c in $\mathfrak{c}$, and therefore $\mathrm{Sp}(c) = 0$, q.e.d.

If $\mathfrak{o}$ is two-sided simple and P algebraically closed, hence $\mathfrak{o}$ is a matrix ring, $\mathfrak{o} = \sum c_{ik} P$, then in the irreducible representation of $\mathfrak{o}$ the element $a = \sum c_{ik}\alpha_{ik}$ is assigned the matrix (α_{ik}), and therefore

$$\text{reduced trace } \mathrm{Sp}_{\mathfrak{l}}(a) = \sum_i \alpha_{ii},$$

$$\text{principal trace } \mathrm{Sp}_{\mathfrak{o}}(a) = n \cdot \text{ reduced trace } = n \sum_i \alpha_{ii}.$$

In particular,

$$\mathrm{Sp}(c_{ik}) = 0 \quad \text{for } i \neq k,$$
$$\mathrm{Sp}_{\mathfrak{l}}(c_{ii}) = e,$$
$$\mathrm{Sp}_{\mathfrak{o}}(c_{ii}) = n \cdot e.$$

Upon passage from P to the algebraically closed field Ω, the principal trace does not change, since it can be computed from the same basis. This is not true of the reduced trace.

The traces of the elements a of the system without radical in the absolutely irreducible representations are called *characters* and are denoted by $\chi(a)$, or by $\chi^{(\nu)}(a)$ when the representation intended is to be specified.

In an irreducible representation of degree n_ν, the central elements are represented, by ğ 21, by diagonal matrices $E\zeta^{(\nu)}$, where $z \to \zeta^{(\nu)}$ is a representation of degree one of the center (or a homomorphism of the center into Ω). The trace therefore has the value $n_\nu\zeta^{(\nu)}$. *Thus the homomorphisms Θ of the center are linked with the characters χ by the relation*

$$\chi(z) = n_\nu \cdot \Theta(z) \tag{1}$$

In the commutative case $n_\nu = 1$, and the characters themselves give the homomorphisms (cf. ğ 22). If the field Ω has characteristic zero, as will always be assumed in what follows, one can divide (1) by n_ν:

$$\Theta(z) = \frac{\chi(z)}{n_\nu}.$$

The homomorphism property of the $\Theta(z)$ is expressed by the formulas

$$\frac{\chi(z)}{n_\nu} + \frac{\chi(z')}{n_\nu} = \frac{\chi(z+z')}{n_\nu},$$
$$\frac{\chi(z)}{n_\nu} \cdot \frac{\chi(z')}{n_\nu} = \frac{\chi(zz')}{n_\nu}$$

A representation class is already uniquely determined by the traces of the matrices alone. (To know the traces of all matrices, it is of course enough to know the traces of the basis elements in the given representation.)

Proof. The representation module $\mathfrak{R}$ is known when one knows how often each irreducible representation module $\mathfrak{M}_\nu$ occurs in it as a direct summand. If this number is p_ν, then the trace of $e^{(\nu)}$ in the representation is equal to $p_\nu n_\nu$, where n_ν is the degree of the irreducible representation. Hence

$$p_\nu = \frac{\mathrm{Sp}\, e^{(\nu)}}{n_\nu}.$$

ğ 25.
Discriminants.

Let $\mathfrak{o} = a_1P + \cdots + a_hP$ be a hypercomplex system.

Discriminant matrix = the matrix whose entries are the principal traces $\mathrm{Sp}(a_ia_k)$.

Reduced discriminant matrix = the same matrix with reduced traces, formed in the algebraically closed field.

Determinant of the matrix = *discriminant* (respectively *reduced discriminant*).

The discriminant remains the same upon extension of the ground field.

Upon passage to another basis, the discriminant is multiplied by the square of the transformation determinant.

Proof. Let

$$(a_1, \ldots, a_h) = (b_1, \ldots, b_h)P,$$
$$(a_ia_1, \ldots, a_ia_h) = (a_ib_1, \ldots, a_ib_h)P,$$
$$(\mathrm{Sp}(a_ia_1), \ldots, \mathrm{Sp}(a_ia_h)) = (\mathrm{Sp}(a_ib_1), \ldots, \mathrm{Sp}(a_ib_h))P.$$

Or, in matrices,

$$(\mathrm{Sp}(a_ia_k)) = (\mathrm{Sp}(a_ib_k))P. \tag{1}$$

Likewise, if $\widetilde{P}$ is the transposed matrix,

$$\begin{pmatrix} a_1 \\ \vdots \\ a_h \end{pmatrix} = \widetilde{P} \begin{pmatrix} b_1 \\ \vdots \\ b_h \end{pmatrix}$$

and hence, as before,

(1a) $$(\mathrm{Sp}(a_i b_k)) = \widetilde{P}(\mathrm{Sp}(b_i b_k)).$$

From (1) and (1a),

$$(\mathrm{Sp}(a_i a_k)) = \widetilde{P} \cdot (\mathrm{Sp}(b_i b_k)) \cdot P.$$

Passing to determinants gives the assertion.

Thus the determinant is determined only up to a square from P; but its vanishing or non-vanishing is an invariant property.

From (1) it follows further that *up to a nonzero factor one can also determine the discriminant from two different bases, namely as* $|(\mathrm{Sp}(a_i b_k))|$.

The discriminant vanishes if $\mathfrak{o}$ *possesses a nilpotent ideal* $\mathfrak{c}$.

Proof. As basis elements for $\mathfrak{o}$ choose $(c_1, \ldots, c_t, d_{t+1}, \ldots, d_h)$, where $(c_1, \ldots, c_t)$ forms a basis for $\mathfrak{c}$. The discriminant becomes

$$\begin{vmatrix} \mathrm{Sp}(c_i c_k) & \mathrm{Sp}(c_i d_k) \\ \mathrm{Sp}(d_i c_k) & \mathrm{Sp}(d_i d_k) \end{vmatrix} = \begin{vmatrix} 0 & 0 \\ 0 & \mathrm{Sp}(d_i d_k) \end{vmatrix} = 0.$$

(This also holds for the reduced discriminant.)

Consequence. *The discriminant also vanishes if a nilpotent ideal appears after passage to the algebraically closed field.*

Let $\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s$ be a direct two-sided sum, and let $M, M_1, \ldots, M_s$ be the discriminant matrices of the rings $\mathfrak{o}, \mathfrak{a}_1, \ldots, \mathfrak{a}_s$. Then

$$M = \begin{pmatrix} M_1 & 0 & & 0 \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_s \end{pmatrix},$$

and hence $|M| = |M_1| \cdot |M_2| \cdots |M_s|$.

Proof. Choose a basis for $\mathfrak{o}$ composed of bases for $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$. If a lies in $\mathfrak{a}_i$, then

$$\mathrm{Sp}_{\mathfrak{o}}(a) = \mathrm{Sp}_{\mathfrak{a}_i}(a),$$

where both times principal traces are meant, but in the rings $\mathfrak{o}$ and $\mathfrak{a}_i$, respectively. Further, $a_i a_k = 0$ if a_i lies in $\mathfrak{a}_i$ and a_k in $\mathfrak{a}_k$, and hence also $\mathrm{Sp}(a_i a_k) = 0$. This proves the assertion, and the same proof applies to the reduced discriminant.

To form the *discriminant of a matrix ring* $\sum c_{ik} P$, choose two different bases, namely the c_{ik} ordered once by first indices and once by second indices. The product table has the form

	$\overbrace{c_{11} \cdots c_{1n}}^{r_1}$	$\overbrace{c_{21} \cdots c_{2n}}^{r_2}$	$\cdots$
$\left.\begin{matrix} c_{11} \\ \vdots \\ c_{n1} \end{matrix}\right\} l_1$	(c_{ik})	0	0
$\left.\begin{matrix} c_{12} \\ \vdots \\ c_{n2} \end{matrix}\right\} l_2$	0	(c_{ik})	0
$\vdots$	0	0	(c_{ik})

The discriminant is

$$D = \begin{vmatrix} \mathrm{Sp}(c_{11}) & 0 & \cdots & 0 \\ 0 & \mathrm{Sp}(c_{22}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{Sp}(c_{nn}) \end{vmatrix}^n = \begin{cases} e, & \text{for reduced traces,} \\ n^{n^2} \cdot e, & \text{for principal traces.} \end{cases}$$

Consequence. *If, over the algebraically closed extension field,* $\mathfrak{o}$ *decomposes into matrix rings of degrees* $n_1, \ldots, n_s$*, then the discriminant is*

$$D = n_1^{n_1^2} n_2^{n_2^2} \cdots n_s^{n_s^2} \cdot e$$

and the reduced discriminant is

$$D_{\text{red}} = e.$$

Thus the reduced discriminant is always nonzero for systems without radical, while the other discriminant is nonzero only when no n_i is divisible by the characteristic of the field. Hence:
Non-vanishing of the reduced discriminant is necessary and sufficient for systems without radical (after algebraic closure of the field P*).*
In characteristic zero, non-vanishing of the discriminant is necessary and sufficient for the non-appearance of a radical (after algebraic closure of the field P*).*[22)]
22) For commutative systems compare E. Noether, Diskriminantensatz für Ordnungen. . . , J. f. M. 157 (1927), pp. 82–104, §§ 4–6. The method of proof there is the same, but more complicated in detail; the passage from one basis to another (§ 4, 4.) is to be replaced by the one given here at the beginning of this paragraph, since the determinant $|(e_i e_k)|$ occurring there vanishes.

§ 26.
Placement of the Group Ring.

Let $a_1, \ldots, a_h$ *be the elements of a finite group, and form the group ring over a field whose characteristic does not divide* h*. Then the discriminant* $D \neq 0$*, and hence the group ring is a ring without radical.*

Proof. We first show (from now on Sp means principal trace):

$$\mathrm{Sp}(e) = he; \qquad \mathrm{Sp}(a_i) = 0 \quad \text{for } (a_i \neq e).$$

For in the regular representation,

$$e \longrightarrow \begin{pmatrix} e & 0 & \cdots & 0 \\ 0 & e & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e \end{pmatrix}, \qquad \mathrm{Sp}(e) = he.$$

For $a_i \neq e$,

$$a_i a_k = a_\lambda, \qquad \lambda \neq k;$$

hence the matrix by means of which the products $a_i a_1, \ldots, a_i a_h$ are expressed in terms of $a_1, \ldots, a_h$ has only zeros in the principal diagonal; therefore $\mathrm{Sp}(a_i) = 0$.

We now take the bases $a_1, \ldots, a_h$ and $a_1^{-1}, \ldots, a_h^{-1}$. The matrix $(\mathrm{Sp}(a_i a_k^{-1}))$ is

$$\begin{pmatrix} he & 0 & \cdots & 0 \\ 0 & he & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & he \end{pmatrix}.$$

Thus

$$D = h^h e \neq 0, \text{q. e. d.}$$

By the *class of a group element* a one means the sum formed in the group ring

$$K_a = \sum_s s^{-1} a s, \tag{1}$$

where the summation runs only over the distinct $s^{-1}as$. *The classes* K_a *are central elements*, since they commute with all group elements. *The classes* K_a *generate the center*; for if an element $\sum_i a_i \varrho_i$ of the group ring commutes with every s, then

$$\sum_i a_i \varrho_i = s^{-1}\Big(\sum_i a_i \varrho_i\Big) s = \sum_i (s^{-1} a_i s)\varrho_i$$
$$= \frac{1}{h}\sum_i \Big(\sum_s s^{-1} a_i s\Big)\varrho_i = \frac{1}{h}\sum_i \Big(\frac{h}{h_i} K_i\Big)\varrho_i,$$

where h is the number of group elements and h_i is the number of elements in the class K_i.

Thus the rank of the center is equal to the number of classes of conjugate group elements; hence also *the number of absolutely irreducible representations is equal to this number of classes.*

The matrices A and $S^{-1}AS$ have the same trace; hence the group elements a and $s^{-1}as$ have the same trace.

Taking the trace on both sides of (1) now gives

$$\chi(K_i) = h_i \chi(a_i),$$

or, in words:
The character of a group element is equal to the character of the class divided by the number of elements in the class.

(Eingegangen am 12. August 1928.)

35. On Maximal Domains of Integral Functions

By Emmy Noether (Göttingen).

Rec. Soc. Math. Moscou 36 (1929), pp. 65–72

The following investigations are closely connected with Hilbert's problem of relatively integral functions[13]; they go back to an occasional question of E. Hecke, who was able to dispose of one special case – needed by him as an auxiliary lemma – by direct calculation.[14]

The question is the following. By a *maximal domain* of integral functions in $x_1, \ldots, x_n$ – polynomials, power series, or quotients of such – inside a given domain $\mathfrak{Z}$, I mean one which can no longer be enlarged by adjoining integral denominators; thus, from the membership of $a \cdot g(x)$ – where $g(x)$ is in $\mathfrak{Z}$ – the membership of $g(x)$ always follows, where a denotes a nonzero rational integer. Each integral domain $\mathfrak{I}$ in $\mathfrak{Z}$ generates uniquely a maximal domain $\mathfrak{M}(\mathfrak{I})$, consisting of all functions $g(x)$ from $\mathfrak{Z}$ for which there is at least one $a \neq 0$ such that $a \cdot g(x)$ belongs to $\mathfrak{I}$.

The question is what can be said about the denominators a of this maximal $\mathfrak{M}(\mathfrak{I})$ when the original integral domain $\mathfrak{I}$ was finite, i.e. consisted of all integral polynomials in finitely many functions $f_1(x), \ldots, f_r(x)$ from $\mathfrak{Z}$. Here $\mathfrak{Z}$ is to be taken to consist of all integral polynomials or power series in $x_1, \ldots, x_n$, respectively of such quotients as contain no denominators other than those occurring in the $f(x)$ and their powers.

I show – under the additional assumption, in the case of power series or their quotients, that only algebraic dependencies occur between the $f(x)$ – that the a can then always be chosen so that only a finite number of distinct prime numbers divide them, although in general these primes may occur to arbitrary powers.

The latter point is immediately clear: if $a \cdot g(x)$ belongs to $\mathfrak{I}$, but $a^{\varrho-1} g(x)^{\varrho}$ does not for any exponent ϱ, then all powers a^{ϱ} occur; for example $\mathfrak{I} = [2x]$, where $x^{\varrho} = (2x)^{\varrho}/2^{\varrho}$.

The question of boundedness can only be formulated as follows. Can one give a, in general infinite, system of generators of $\mathfrak{M}(\mathfrak{I})$ such that in the corresponding denominators the exponents of the prime numbers remain bounded? Since only finitely many primes are involved, this question is, by familiar arguments,[15] identical with the question of the finiteness of $\mathfrak{M}(\mathfrak{I})$, hence with Hilbert's problem of relatively integral functions in its integral formulation – a question that I cannot decide by the methods used here.[16]

The proof that only finitely many distinct prime numbers p divide the denominators a rests on the fact that to every such p there corresponds at least one relation modulo p between the $f(x)$ generating $\mathfrak{I}$, a relation with integral coefficients which is not identically satisfied in x. Equivalently, if $\mathfrak{o}$ denotes the integral polynomial domain in indeterminates $u_1, \ldots, u_r$, then by the assignment $u_i \mapsto f_i(x)$ the domain $\mathfrak{I}$ becomes a homomorphic image of $\mathfrak{o}$; this homomorphism is mediated by a prime ideal $\mathfrak{a}$ of $\mathfrak{o}$, that is, $\mathfrak{I}$ becomes isomorphic to the residue-class ring $\mathfrak{o}/\mathfrak{a}$. Correspondingly, $\mathfrak{I}_p$ becomes a homomorphic image of $\mathfrak{o}_p$ – the subscript denotes passage to residue classes modulo p, which is possible with the exception of the finitely many primes occurring in the denominators of $\mathfrak{I}$. This homomorphism is again mediated by a prime ideal $\mathfrak{c}_p$ of $\mathfrak{o}_p$ which contains $\mathfrak{a}_p$. The prime p occurs in a denominator of $\mathfrak{M}(\mathfrak{I})$ if and only if $\mathfrak{c}_p$ becomes a proper over-ideal (a proper divisor in the ideal-theoretic sense) of $\mathfrak{a}_p$. This can happen only if either the transcendence degree of $\mathfrak{I}_p$ decreases relative to that of $\mathfrak{I}$, or $\mathfrak{a}_p$ loses its property of being prime.[17] That this happens only for finitely many p follows from the fact that, modulo p as well, an algebraic dependence entails the vanishing of the functional determinant (§ 1), and further from the fact that $\mathfrak{a}$ proves to be an absolute prime ideal and therefore loses its prime-ideal property only modulo finitely many p.[18]

[13] D. Hilbert, *Mathematische Probleme*, Gött. Nachr. 1900, pp. 253–297, Problem 14.

[14] E. Hecke, "Uber die Konstruktion relativ-Abelscher Zahlkörper durch Modulfunktionen von zwei Variabeln, Math. Ann. 74 (1913), pp. 465–510, § 2. In Hecke's case the finite integral domain $\mathfrak{I}$ is generated by three quotients of power series in two variables, between which there is one algebraic relation.

[15] Cf. Hilbert, loc. cit., or the more detailed account in E. Noether, Die Endlichkeit des Systems der ganzzahligen Invarianten binärer Formen, Gött. Nachr. 1919, pp. 138–156, § 1, IV.

[16] Thus, for example, in the case of the integral projective invariants of a fundamental system of forms it is shown that they can be represented by a full system of invariants in the usual sense, with only finitely many distinct prime numbers in the denominator – a result which does not follow from the usual method of the Ω-process. But nothing is asserted about integral finiteness itself, which until now is known only in the case of binary fundamental forms. Cf. the note cited under 3).

[17] By the "transcendence degree" of a system one understands, as is well known, the invariant number of algebraically independent functions on which the system depends algebraically; a system consisting of algebraically independent functions is called irreducible. By the transcendence degree, or dimension, of a prime ideal one understands that of its residue-class field. A prime ideal has no proper prime divisor of the same transcendence degree; cf. for example B. L. v. d. Waerden, Zur Nullstellentheorie der Polynomideale, Math. Ann. 96 (1926), pp. 183–208.

[18] E. Noether, Eliminationstheorie und allgemeine Idealtheorie, Math. Ann. 90 (1923), pp. 229–261, § 7. By elimination theory the theorem follows from the simpler theorem that an absolutely irreducible polynomial loses this property only modulo finitely many prime numbers (A. Ostrowski, Zur arithmetischen Theorie der algebraischen GröSSen, Gött. Nachr. 1919, pp. 279–298, there p. 296. A simpler proof is in E. Noether, Ein algebraisches Kriterium für absolute Irreduzibilität, Math. Ann. 85 (1922), pp. 26–33, § 7.) If $\mathfrak{I}$ has an integral basis containing exactly one more function than its transcendence degree – as in the case considered by Hecke (note 2) – so that $\mathfrak{a}$ becomes principal, then it is already enough to invoke this simpler theorem, avoiding elimination theory. Everywhere prime ideals of a finite algebraic number field may replace prime numbers. The theorem is evidently also valid when $\mathfrak{a}$ is the zero ideal.

It remains to note that all arguments are preserved with slight modifications when, in place of rational integers, one takes the integers of a finite algebraic number field and its prime ideals (§ 4).

§ 1. Functional determinants over coefficient domains of characteristic p.

1. Let $f_1(x_1,\dots,x_n),\dots,f_t(x_1,\dots,x_n)$ be rational functions, or more generally formally defined power series or quotients of such, with coefficients in a field P of characteristic p. The derivatives $\partial f_i/\partial x_k$ are likewise to be formally defined, with all the usual rules of calculation remaining valid. Let Ω denote an algebraically closed extension field of P.

Then, just as in characteristic zero, the following holds:

Theorem. *If there is an algebraic dependence between the $f(x)$ with coefficients in Ω, then the rank of the functional matrix $(\partial f_i/\partial x_k)$ $(i=1,\dots,t;\ k=1,\dots,n)$ is smaller than t.*[19]

Proof. In the polynomial domain $\Omega[u_1,\dots,u_t]$ let $\mathfrak{m}$ denote the prime ideal of all polynomials $G(u)$ for which $G(f)=0$ identically in x. By assumption $\mathfrak{m}$ is different from the zero ideal. Let $G(u)\neq 0$ (and hence $\neq$ const.) be a polynomial of least degree in $\mathfrak{m}$; in particular this implies that $G(u)$ is indecomposable. Then, as usual,

$$\left(\frac{\partial G}{\partial u_1}\right)_f \frac{\partial f_1}{\partial x_1}+\cdots+\left(\frac{\partial G}{\partial u_t}\right)_f \frac{\partial f_t}{\partial x_1}=0,$$

$$\vdots$$

$$\left(\frac{\partial G}{\partial u_1}\right)_f \frac{\partial f_1}{\partial x_n}+\cdots+\left(\frac{\partial G}{\partial u_t}\right)_f \frac{\partial f_t}{\partial x_n}=0,$$

and it follows that either the rank of the functional matrix is less than t, or all the $(\partial G/\partial u_i)_f$ vanish. Since $G(u)$ was chosen of least degree, the latter alternative entails the vanishing of all $\partial G/\partial u_i$.

Consequently $G(u)=H(u_1^p,\dots,u_t^p)$; and since the coefficient domain Ω was assumed algebraically closed, hence perfect, one further has $G(u)=H(u_i^p)=(T(u))^p$, contrary to the choice of $G(u)$. The proof of course also applies in characteristic zero, where the last step drops out.

2. Corollary.

Let $F_1(x_1,\dots,x_n),\dots,F_t(x_1,\dots,x_n)$ be integral functions (polynomials, power series, or quotients of such) whose functional matrix has exactly rank t. Let the prime number p be so chosen that it divides neither the denominators of the $F(x)$ nor all t-rowed determinants of the functional matrix.

Then $F_1(x),\dots,F_t(x)$ remain algebraically independent modulo p.

Proof. Let P denote the residue field modulo p, and let $f_1(x),\dots,f_t(x)$ be the functions over P obtained from $F_1(x),\dots,F_t(x)$ by replacing the integral coefficients by their residue classes modulo p. The $f_i(x)$ are defined because p did not divide the denominators of the $F_i(x)$. Their functional matrix $(\partial f_i/\partial x_k)$ is likewise obtained from $(\partial F_i/\partial x_k)$ by replacing the integral coefficients by their residue classes modulo p – no denominators other than those in the $F(x)$ occur in $(\partial F_i/\partial x_k)$. By the choice of p, $(\partial f_i/\partial x_k)$ retains rank t; the $f(x)$ are algebraically independent in Ω, and therefore all the more in P.

§ 2. Formulation of the theorem.

1. As in the introduction, let $\mathfrak{I}$ denote an integral domain (a ring without zero divisors) of integral functions in $x_1,\dots,x_n$ – polynomials or power series with rational integral coefficients, or quotients of such. In the case of power series these may be formally defined or may converge in a certain domain; what is used is only that the functions in question form an integral domain.

Let $\mathfrak{Q}$ denote the quotient field of $\mathfrak{I}$, and let $\mathfrak{Z}$ be an integral domain between $\mathfrak{I}$ and $\mathfrak{Q}$. As in the introduction, $\mathfrak{M}$ is called *maximal* in $\mathfrak{Z}$ if from the membership of $a\cdot g(x)$ – a an integer $\neq 0$, $g(x)$ in $\mathfrak{Z}$ – the membership of $g(x)$ always follows. For $\mathfrak{I}$ there exists uniquely the maximal domain $\mathfrak{M}(\mathfrak{I})$ generated by $\mathfrak{I}$ in $\mathfrak{Z}$, namely the intersection of all maximal domains in $\mathfrak{Z}$ which contain $\mathfrak{I}$; for $\mathfrak{Z}$ itself is such a domain, and with arbitrarily many such domains their intersection is again maximal and contains $\mathfrak{I}$. The domain $\mathfrak{M}(\mathfrak{I})$ consists of all functions $g(x)$ from $\mathfrak{Z}$ for which there is at least one $a\neq 0$ such that $a\cdot g(x)$ lies in $\mathfrak{I}$.

Indeed, these $g(x)$ form a maximal domain $\mathfrak{N}$ in $\mathfrak{Z}$ containing $\mathfrak{I}$, since from $b\cdot h(x)$ in $\mathfrak{I}$, with $b\neq 0$ and $h(x)$ in $\mathfrak{Z}$, it follows that $ab\cdot h(x)$ lies in $\mathfrak{I}$ and $ab\neq 0$, hence $h(x)$ lies in $\mathfrak{N}$. Conversely, every maximal domain $\mathfrak{M}$ in $\mathfrak{Z}$ containing $\mathfrak{I}$ contains $\mathfrak{N}$: if $a\cdot g(x)$ lies in $\mathfrak{I}$, then $a\cdot g(x)$ lies in $\mathfrak{M}$, since $\mathfrak{I}$ is contained in $\mathfrak{M}$; hence $g(x)$ lies in $\mathfrak{M}$.

[19] In the original version I had assumed the coefficient domain P to be a perfect field; I owe to B. L. v. d. Waerden the extension to arbitrary fields, including imperfect ones, by passing from P to Ω. That the converse in characteristic p does not hold even for perfect P is shown by the example $f=x^p$, $\partial f/\partial x=0$.

2. Now suppose $\mathfrak{I}$ is a finite integral domain with identity element, with $f_1(x), \ldots, f_r(x)$ as integral basis; that is, $\mathfrak{I}$ consists of all integral polynomials in the $f_i(x)$. Let $\mathfrak{Z}$ furthermore consist of all integral polynomials or power series in x, respectively of such quotients as contain no denominators other than those occurring in the finitely many $f_i(x)$, naturally to arbitrary powers.

Assume also that the x occur effectively in at least one of the $f_i(x)$ – in general in all of them – since otherwise $\mathfrak{I}$ and $\mathfrak{Z}$ simply consist of all integral polynomials in a rational number $1/e$, and there is nothing to prove.

If polynomials or rational functions are concerned, then the quotient field $\mathfrak{Q}$ has transcendence degree t, with $1 \leq t \leq r$, over the field K of rational numbers; and if, for instance, $f_1(x), \ldots, f_t(x)$ form an irreducible system,[20] then $\mathfrak{Q}$ is a finite algebraic extension of the purely transcendental field $K(f_1(x), \ldots, f_t(x))$. At the same time the functional matrix of $f_1(x), \ldots, f_r(x)$, and likewise that of $f_1(x), \ldots, f_t(x)$, has exactly rank t.[21]

In order that this structure of $\mathfrak{Q}$ also be preserved in the case of power series or their quotients, an additional assumption must be made. If t is the rank of the functional matrix of the $f_i(x)$ and, for instance, at the same time the rank of the functional matrix of $f_1(x), \ldots, f_t(x)$ – so that these form an irreducible system by § 1, 1 – then $\mathfrak{Q}$ is again to be a finite algebraic extension of the purely transcendental field $K(f_1(x), \ldots, f_t(x))$; i.e. $f_{t+1}(x), \ldots, f_r(x)$ are to be algebraic over $K(f_1(x), \ldots, f_t(x))$.[22] Here again $t \geq 1$, since – characteristic zero! – not all $\partial f_i / \partial x_k$ vanish.

At the same time the condition follows for every system of t functions of the integral basis whose functional matrix has exactly rank t; for these form an irreducible system, on which therefore the remaining functions algebraically depend.

3. Let $\mathfrak{o}$ now denote the integral polynomial domain in indeterminates $u_1, \ldots, u_r$. Then $\mathfrak{I}$ is a ring-homomorphic image of $\mathfrak{o}$, as is shown immediately by the assignment $u_i \mapsto f_i(x)$. Thus $\mathfrak{I}$ is ring-isomorphic to $\mathfrak{o}/\mathfrak{a}$, where $\mathfrak{a}$ is a prime ideal, since $\mathfrak{I}$ is a ring without zero divisors; $\mathfrak{a}$ consists of all polynomials $G(u)$ for which $G(f)$ vanishes identically in x.

As already mentioned in the introduction, the matter is the following theorem.

Theorem. *Under the additional assumption of 2, let $\mathfrak{o}_p$, $\mathfrak{a}_p$, $\mathfrak{I}_p$ denote the domains obtained from $\mathfrak{o}$, $\mathfrak{a}$, $\mathfrak{I}$ by replacing the integral coefficients by their residue classes modulo p. Then, again with the exception of at most finitely many prime numbers – among which are those occurring in the denominators of the $f(x)$, so that $\mathfrak{I}_p$ is defined – the homomorphism from $\mathfrak{o}_p$ to $\mathfrak{I}_p$ is mediated by $\mathfrak{a}_p$; thus $\mathfrak{I}_p$ is ring-isomorphic to $\mathfrak{o}_p/\mathfrak{a}_p$, and hence to $\mathfrak{o}/(\mathfrak{a}, p\mathfrak{o})$.*

The theorem yields the fact that only finitely many prime numbers occur in the denominators a of $\mathfrak{M}(\mathfrak{I})$ by means of the following

Corollary. *If p is so chosen that $\mathfrak{I}_p$ is isomorphic to $\mathfrak{o}_p/\mathfrak{a}_p$, then, whenever $p \cdot g(x)$ lies in $\mathfrak{I}$ and $g(x)$ lies in $\mathfrak{Z}$, one always has $g(x)$ in $\mathfrak{I}$.*

In other words, $\mathfrak{I}$ is maximal in $\mathfrak{Z}$ with respect to all prime numbers other than the finitely many exceptional primes.

One has $\mathfrak{o}_p/\mathfrak{a}_p$ isomorphic to $\mathfrak{o}/(\mathfrak{a}, p\mathfrak{o})$. For, by definition, $\mathfrak{o}_p$ is the residue-class ring $\mathfrak{o}/p\mathfrak{o}$, and correspondingly $\mathfrak{a}_p$ is $(\mathfrak{a}, p\mathfrak{o})/p\mathfrak{o}$. Thus – by the first isomorphism theorem – $\mathfrak{o}_p/\mathfrak{a}_p$, and therefore by assumption also $\mathfrak{I}_p$, is isomorphic to $\mathfrak{o}/(\mathfrak{a}, p\mathfrak{o})$.

This means: from $H(f_i(x)) \equiv 0 \pmod{p}$ in $\mathfrak{I}$ it follows that $H(u) \equiv 0 \pmod{(\mathfrak{a}, p\mathfrak{o})}$ in $\mathfrak{o}$.

This can be reformulated as follows. From $H(f_i(x)) = p \cdot g(x)$ [$H(f_i(x))$ in $\mathfrak{I}$, $g(x)$ in $\mathfrak{Z}$] it follows that $H(u_i) - pF(u_i) \equiv 0 \pmod{\mathfrak{a}}$, hence also $H(f_i(x)) = pF(f_i(x))$ and consequently $g(x) = F(f_i(x))$; thus $g(x)$ lies in $\mathfrak{I}$.

Finally, repeated application a finite number of times gives: if a is divisible by none of the exceptional primes, then from $a \cdot g(x)$ in $\mathfrak{I}$ and $g(x)$ in $\mathfrak{Z}$ it always follows that $g(x)$ lies in $\mathfrak{I}$. This proves the corollary.

§ 3. Proof of the theorem.

1. Lemma. *The prime ideal $\mathfrak{a}$ which mediates the homomorphism between $\mathfrak{I}$ and $\mathfrak{o}$ (§ 2, 3) is an absolute prime ideal.*

[20] By an "irreducible system" one means, as is well known, a system consisting of algebraically independent functions.

[21] For a purely algebraic proof of this functional-determinant theorem in characteristic zero, see B. L. v. d. Waerden, Algebraische Theorie der Differentiation, Nieuw Archief v. Wiskunde (2) 15 (1926), pp. 111–120.

[22] This additional assumption is satisfied when, as in the case considered by Hecke (note 2), analytic functions are involved and $f_1(x), \ldots, f_t(x)$ are analytically independent while $f_{t+1}(x), \ldots, f_r(x)$ depend algebraically on them. The assumption is deliberately stated formally – as the rank of a functional matrix – so that it also has a clear sense for formally defined power series. Thus all arguments remain purely formal-algebraic, and theorems about analytic functions are needed only to verify in the special case that the assumption is satisfied.

Let $\mathfrak{o}^*$ denote the polynomial domain in $u_1, \ldots, u_r$ with arbitrary algebraic numbers, including fractional ones, as coefficients, and let $\mathfrak{a}^*$ be the ideal generated by $\mathfrak{a}$ in $\mathfrak{o}^*$. Thus $\mathfrak{a}^*$ consists of all linear combinations $a_1 G_1(u) + \cdots + a_s G_s(u)$, where the a_i are arbitrary algebraic numbers and the $G_i(u)$ are polynomials in $\mathfrak{a}$. It is to be proved that $\mathfrak{a}^*$ is a prime ideal.

This will be proved once it is shown that $\mathfrak{a}^*$ mediates the homomorphism from $\mathfrak{o}^*$ to $\mathfrak{J}^*$ – where $\mathfrak{J}^*$ means the integral domain consisting of all polynomials in the $f_i(x)$ with arbitrary algebraic numbers as coefficients. In other words, one must show that $H(u)$ belongs to $\mathfrak{a}^*$, with $H(u)$ from $\mathfrak{o}^*$, whenever $H(f_i(x))$ vanishes.

Let $\omega_1, \ldots, \omega_s$ be a linearly independent basis of the finite number field generated by the finitely many coefficients of $H(u)$. Then one has

$$a \cdot H(u) = \omega_1 H_1(u) + \cdots + \omega_s H_s(u),$$

where the $H_i(u)$ lie in $\mathfrak{o}$ and $a \neq 0$ is a rational integer. From $H(f) = 0$ it follows that $\omega_1 H_1(f) + \cdots + \omega_s H_s(f) = 0$, hence $H_1(f) = 0, \ldots, H_s(f) = 0$. Therefore $H_1(u), \ldots, H_s(u)$ belong to $\mathfrak{a}$, and consequently $H(u)$ belongs to $\mathfrak{a}^*$.

2. The proof of the theorem can now be given in the following form.

If p is chosen so that

I. $\mathfrak{J}_p$ is defined,

II. $\mathfrak{a}_p$ remains a prime ideal, indeed an absolute one,

III. the transcendence degree of $\mathfrak{J}_p$ has not decreased relative to that of $\mathfrak{J}$,

then the homomorphism from $\mathfrak{o}_p$ to $\mathfrak{J}_p$ is mediated by $\mathfrak{a}_p$. Apart from at most finitely many exceptional primes, these conditions are fulfilled for all prime numbers.

That only finitely many exceptional primes occur with respect to conditions I, II, III follows immediately from the preceding discussion.

Condition I is clear: the exceptional primes are only the finitely many occurring in the denominators of the $f_i(x)$. Condition II follows from the fact that, by the lemma, $\mathfrak{a}$ is an absolute prime ideal, so that it retains this property modulo all prime numbers with at most finitely many exceptions (cf. note[6]). Finally, condition III was shown in the corollary of § 1, 2, since the functional matrix of $f_1(x), \ldots, f_t(x)$ has exactly rank t by § 2, 2.

Now choose p different from these exceptional primes. The homomorphism from $\mathfrak{o}_p$ to $\mathfrak{J}_p$ is mediated by an ideal $\mathfrak{c}_p$, which is a prime ideal – since $\mathfrak{J}_p$ is also a ring without zero divisors – and whose transcendence degree is given by that of $\mathfrak{J}_p$, hence is at least t. For, since $\mathfrak{J}_p$ is isomorphic to $\mathfrak{o}_p/\mathfrak{c}_p$, the residue-class field of $\mathfrak{c}_p$ becomes isomorphic to the quotient field of $\mathfrak{J}_p$.

Since $\mathfrak{a}_p$ is also a prime ideal and a multiple, that is a subideal, of $\mathfrak{c}_p$, $\mathfrak{a}_p$ and $\mathfrak{c}_p$ coincide if and only if their transcendence degrees coincide.[23] The transcendence degree of $\mathfrak{a}_p$, as a multiple of $\mathfrak{c}_p$, is likewise at least t; indeed the classes modulo $\mathfrak{a}_p$ of $u_1, \ldots, u_t$ form an irreducible system. It remains to show that this transcendence degree is exactly t, and then everything will be proved.

Here, in the case of power series or their quotients, the additional assumption on the structure of the quotient field $\mathfrak{Q}$ of $\mathfrak{J}$ is used (§ 2, 2). According to that assumption, the prime ideal $\mathfrak{a}$ had in every case transcendence degree t; moreover, the numbering had been chosen so that the classes modulo $\mathfrak{a}$ of $u_1, \ldots, u_t$ formed an irreducible system, on which the classes of $u_{t+1}, \ldots, u_r$ depended algebraically. Thus $\mathfrak{a}$ contained integral and primitive polynomials

$$G_1(u_{t+1}; u_1, \ldots, u_t), \ldots, G_{r-t}(u_r; u_1, \ldots, u_t) \tag{1}$$

which pass to, by primitivity nonvanishing, polynomials

$$G_1^*(u_{t+1}; u_1, \ldots, u_t), \ldots, G_{r-t}^*(u_r; u_1, \ldots, u_t) \tag{2}$$

in $\mathfrak{a}_p$. In G_λ^*, however, the variable $u_{t+\lambda}$ must actually occur; otherwise, contrary to the choice of p, there would be an algebraic dependence between the classes modulo $\mathfrak{a}_p$ of $u_1, \ldots, u_t$. Thus $\mathfrak{a}_p$ is shown to have transcendence degree t; it is therefore identical with $\mathfrak{c}_p$ and mediates the homomorphism. This proves everything.

[23] Cf. for example B. L. v. d. Waerden, Zur Nullstellentheorie der Polynomideale, Math. Ann. 96 (1926), pp. 183–208, § 3.

§ 4. Extension to algebraic integer coefficients.

As was already noted at the end of the introduction, all arguments are preserved with slight modifications if, instead of rational integers, one takes the integers of a finite algebraic number field K, and, instead of prime numbers p, the prime ideals $\mathfrak{p}$ of this number field. Section 1 remains completely unchanged, as do the considerations leading to the formulation of the theorem in § 2; in the proof (§ 3, 2) and in the corollary of § 2, 3, some additions are needed.

1. In § 3, 2, among the exceptional prime ideals one must further include the finitely many which divide the polynomials $G_1(u), \ldots, G_{r-t}(u)$, § 3, 2, (1), since these can no longer be assumed primitive. This then guarantees the nonvanishing of the polynomials $G_1^*(u), \ldots, G_{r-t}^*(u)$ (§ 3, 2, (2)); it is a strengthening of condition III. Condition II is retained, since the theorem on absolute irreducibility does not change; naturally I is retained as well.

2. The corollary which gives the final result is to be formulated, in accordance with its final form there, as follows.

Corollary. *If the integer a of K is divisible by none of the finitely many exceptional prime ideals, then from $a \cdot g(x)$ in $\mathfrak{I}$ and $g(x)$ in $\mathfrak{Z}$ it always follows that $g(x)$ lies in $\mathfrak{I}$.*

If integers $\lambda_1, \ldots, \lambda_s$ of K are chosen so that each is divisible by one exceptional prime ideal, but not by its square and not by the others, then products of powers of these λ suffice as denominators a.

Proof. Let $(a) = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_g^{\alpha_g}$ be the prime-ideal decomposition of a, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be different from the exceptional prime ideals, so that $\mathfrak{I}_{\mathfrak{p}_i}$ is isomorphic to $\mathfrak{o}_{\mathfrak{p}_i}/\mathfrak{a}_{\mathfrak{p}_i}$ for each of the $\mathfrak{p}_i$. From the ring of all integers of K one passes to the quotient ring $\mathfrak{R}$ defined by (a) by adjoining as denominators all, and only, those integers which are prime to (a), i.e. divisible by none of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$. In $\mathfrak{R}$ the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ remain prime ideals but become principal; all the others become the unit ideal; the decomposition of (a) remains the same.[24] Therefore, on passing to $\mathfrak{R}$ as coefficient domain, the corollary and its proof are preserved exactly in the form of § 2, 3.

That is: if $a \cdot g(x)$ lies in $\mathfrak{I}$, then it follows that $g(x) = F(f_i(x))$, where the polynomial $F(u)$ has coefficients in $\mathfrak{R}$. If d is a common denominator of these coefficients – hence d is prime to a – this can also be formulated as follows: from $a \cdot g(x)$ in $\mathfrak{I}$ it follows that $d \cdot g(x)$ lies in $\mathfrak{I}$ with d prime to a. Thus (d, a) is the unit ideal, and consequently from $a \cdot g(x)$ in $\mathfrak{I}$ it follows that $g(x)$ lies in $\mathfrak{I}$. This proves the first assertion of the corollary above.

To prove the second assertion, let $\mathfrak{R}^*$ be the quotient ring in K defined by the finitely many exceptional prime ideals, and let $\lambda_1, \ldots, \lambda_s$ be basis elements of these prime ideals in $\mathfrak{R}^*$, which may be taken to be integers. In $\mathfrak{R}^*$, a becomes, up to a unit of $\mathfrak{R}^*$, a product of powers of the λ. Passing back to integers, one therefore obtains $\gamma a = \beta \lambda_1^{\alpha_1} \cdots \lambda_s^{\alpha_s}$, where γ and β are divisible by none of the exceptional prime ideals. From $a \cdot g(x)$ in $\mathfrak{I}$ it follows that $\beta \cdot \lambda_1^{\alpha_1} \cdots \lambda_s^{\alpha_s} g(x)$, and hence by the first assertion of the corollary also $\lambda_1^{\alpha_1} \cdots \lambda_s^{\alpha_s} g(x)$, lies in $\mathfrak{I}$.

*) Since $\mathfrak{a}$ has coefficients of characteristic zero, the application of elimination theory in note 6 is independent of Lemma V of that paper. The proof of that lemma is not correct (everything could vanish identically under the indicated substitution); a correct proof first appears in B. L. v. d. Waerden, *Eine Verallgemeinerung des Bézoutschen Theorems*, Math. Ann. 99 (1928), pp. 497–541, note 37.

A further, readily apparent correction is needed on p. 257 of that paper (Theorem XIV is likewise not used in § 7). It is stated there that all elements of $(\mathfrak{R})$ arise as elements of $(\mathfrak{R}')$ by specializing the $t_{\mu,\nu}$ in (x_i); in fact they arise by specialization from a more general linear form

$$\sum s_{\lambda_1 \ldots \lambda_n} (y_1)^{\lambda_1} \cdots (y_n)^{\lambda_n},$$

whose exponent, however, is the same as that of (x_i).

On Maximal Domains of Integral Functions.

Emmy Noether (Göttingen).

(Abstract.)

[24] Cf. for example H. Grell, Zur Theorie der Ordnungen in algebraischen Zahl- und Funktionenkörpern, Math. Ann. 97 (1927), pp. 524–558, § 2, 1.

Every integral domain (ring without zero divisors) $\mathfrak{I}$ determines a certain maximal domain $\mathfrak{M}(\mathfrak{I})$ of the same type, consisting of all functions $g(x)$ for which there exists at least one $a \neq 0$ such that $a \cdot g(x)$ is contained in $\mathfrak{I}$.

This paper investigates the "denominators" a of this maximal domain $\mathfrak{M}(\mathfrak{I})$ under the assumption that $\mathfrak{I}$ is finite. It proves that the a can always be chosen so that, taken altogether, only finitely many prime numbers occur as factors. When the $g(x)$ are power series or quotients of such series, it is additionally assumed that the functions $f_1'(x), \ldots, f_r'(x)$ defining $\mathfrak{I}$ can be connected with one another only by algebraic relations.

The proof is based on reducing the problem to certain questions in the general theory of ideals. This reduction is effected by regarding the occurrence of the factor p in the denominator a as a relation modulo p between the functions f_i.

(Rec. Math. XXXVI:1; 1929).

36. Ideal Differentiation and the Different

J. Ber. d. DMV 39 (1930), p. 17

2. E. Noether, Göttingen: Ideal differentiation and the different.

It is shown how the different of an algebraic number field can be regarded as the *differential quotient* of a defining *ideal*. That this definition agrees with the usual one follows from structural theorems which are interesting in themselves and which, in an analogous sense, constitute a generalization of the Lagrange interpolation formula.

A detailed account is to appear in the *Mathematische Annalen*.

37. Normal Basis in Fields without Higher Ramification

Journal f. d. reine u. angew. Math. 167 (1932), pp. 147–152

By *Emmy Noether* in Göttingen.

By a normal basis of a Galois number field K/k one means a basis of the principal order $\mathfrak{O}$ of K, relative to the principal order $\mathfrak{o}$ of k, consisting of conjugate elements. A necessary condition for the existence of such a basis is, as is known,[1] that no higher ramification fields occur in K/k. This remains true even if one restricts to a place, i.e. passes to the $\mathfrak{p}$-adic extension $k_\mathfrak{p}$ of k and the corresponding $K_\mathfrak{p}$ of K. I prove below the converse:

At every place $\mathfrak{p}$ at which $\mathfrak{p}$ does not divide the degree of K/k, a normal basis exists. In particular, if K/k has no higher ramification, then at every ramified place a normal basis exists; there the discriminant is the square of a group determinant.

To this last assertion one must add that, contrary to a conjecture of E. Artin, the passage to his conductors[2] still requires further considerations: decomposing the group determinant according to irreducible characters yields generalized root numbers; a suitable grouping yields a factorization in the ground field enlarged by the characters. In the simplest cases I can identify these new factors with Artin's conductors by means of the ideal-theoretic decomposition of the root numbers.[3] I should further remark that, even in the general case where no normal basis exists, a splitting into generalized root numbers is always possible by means of a "composition series by Galois modules," and that from this one obtains, analogously to the above, a decomposition in the enlarged ground field; here ideal-theoretic questions begin again.

The proof of the existence of the normal basis under the assumptions above rests on the fact that $\mathfrak{O}/\mathfrak{o}$, regarded as a Galois module—that is, as an $\mathfrak{o}$-module with the substitutions of the Galois group as operator domain—becomes operator-isomorphic to a one-sided ideal of the integral group ring extended by $\mathfrak{o}$. At all ordinary ramified places this group ring is a maximal order, while ideals in maximal orders of $\mathfrak{p}$-adic semisimple systems are principal ideals.[4] Here they therefore arise from a single element under the substitutions of the group or of the group ring. Passing back to the Galois module, this says precisely that a normal basis exists. At the higher ramified places the integral group ring becomes a nonmaximal order and the ideal corresponding to $\mathfrak{O}/\mathfrak{o}$ becomes a nonprincipal ideal.

All these considerations plainly remain valid for function fields of one variable, provided that the characteristic of the constant field does not divide the degree of K/k.

ğ1. The $\mathfrak{p}$-adically Extended Integral Group Ring

Let $\mathfrak{o}$ and $\mathfrak{o}_\mathfrak{p}$ denote the principal orders of an algebraic number field k and of its $\mathfrak{p}$-adic extension $k_\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of k. Let $(\mathfrak{G})$ denote the rational integral group ring and $[\mathfrak{G}]$ the integral group ring of a group $\mathfrak{G}$ with n elements. By $(\mathfrak{G})_k$, respectively $(\mathfrak{G})_{k_\mathfrak{p}}$, we mean the group ring with coefficients in k, respectively $k_\mathfrak{p}$; analogously $[\mathfrak{G}]_\mathfrak{o}$ and $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ are the corresponding extensions of the integral group ring to coefficients in $\mathfrak{o}$, respectively $\mathfrak{o}_\mathfrak{p}$.

Thus $(\mathfrak{G})_k$ and $(\mathfrak{G})_{k_\mathfrak{p}}$ are systems without radical (semisimple systems), and $[\mathfrak{G}]_\mathfrak{o}$, respectively $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$, are orders in $(\mathfrak{G})_k$, respectively $(\mathfrak{G})_{k_\mathfrak{p}}$.

Theorem 1. *If the prime ideal $\mathfrak{p}$ does not divide the number n of elements of $\mathfrak{G}$, then $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ is a maximal order of $(\mathfrak{G})_{k_\mathfrak{p}}$. If $\mathfrak{p}$ divides n, then $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ is not maximal.*

The discriminant of the integral group ring, and hence that of $[\mathfrak{G}]_\mathfrak{o}$ and $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$, is a power of the number n of elements.[5] Thus if $\mathfrak{p}$ does not divide n, the discriminant of $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ is a unit. This means that, while $\mathfrak{o}_\mathfrak{p}$ is fixed, $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ cannot be enlarged to a larger order, since such an enlargement would split off a nonunit square

[1] Cf. A. Speiser, Gruppendeterminante und Körperdiskriminante, ğ 6, Math. Ann. 77 (1916), pp. 546–562.

[2] E. Artin, Über die gruppentheoretische Struktur der Diskriminante, J. f. Math. 164 (1931), pp. 1–11.

[3] [6 October 1931.] That ideal-theoretic considerations will still be necessary in general is shown by the following, arbitrarily variable example communicated to me by M. Deuring: a nonmaximal order whose discriminant can be represented as the square of the group determinant, while different ideal factors correspond to conjugate characters. Let k be the field of fifth roots of unity and $K = k(\sqrt[5]{2})$. Consider the order $[1, 2\sqrt[5]{2}, \sqrt[5]{2^2}, \sqrt[5]{2^3}, \sqrt[5]{2^4}]$, at the place (2), where by the considerations of this note it has a normal basis. Decomposition according to the characters gives precisely the displayed basis elements as the factors of the associated group determinant. The "conductors," apart from 1, therefore become $2\sqrt[5]{2}\cdot\sqrt[5]{2^4}$, $\sqrt[5]{2^2}\cdot\sqrt[5]{2^3}$, $\sqrt[5]{2^3}\cdot\sqrt[5]{2^2}$, and $\sqrt[5]{2^4}\cdot 2\sqrt[5]{2}$, that is $4, 2, 2, 4$; thus they differ for conjugate characters.

[4] Cf. H. Hasse, Über $\mathfrak{p}$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, Theorems 46 and 47, Math. Ann. 104 (1931), pp. 495–534. For commutative systems the principal-ideal property already holds on passing to the quotient ring modulo $\mathfrak{p}$ in k; thus one can restrict to this weaker extension in defining the place when Abelian groups and fields are involved.

[5] Cf., for example, E. Noether, Hyperkomplexe GröSSen und Darstellungstheorie, ğ 26, Math. Z. 30 (1929), pp. 641–692.

factor from the discriminant. But $\mathfrak{o}_\mathfrak{p}$, as a principal order, was already assumed maximal in $k_\mathfrak{p}$. This proves the first part of Theorem 1, the only part used below.

If, on the other hand, $\mathfrak{p}$ divides n, then the direct sum corresponding to the identity representation,

$$\mathfrak{C} = E^{(1)}[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}} + (1 - E^{(1)})[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}, \qquad E^{(1)} = \frac{1}{n}\sum_{S\in\mathfrak{G}} S,$$

is a proper extension of $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$. Indeed, it is a proper extension because $E^{(1)} = \frac{1}{n}\sum S$; $\mathfrak{C}$ is an order with the dependent generators $E^{(1)}$ and $(1 - E^{(1)})S$, $S \in \mathfrak{G}$, since $E^{(1)}S = E^{(1)}$.

Theorem 2. *If $\mathfrak{p}$ does not divide n, every integral or fractional ideal with respect to $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ is principal.*

Indeed, by Theorem 1, $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ is a maximal order in a $\mathfrak{p}$-adic semisimple system, and its ideals are therefore principal.[6]

§2. Galois Modules, Operator Isomorphism, Normal Basis

Let K/k be Galois with group $\mathfrak{G}$. For $z \in K$, let z^S denote the element obtained from z by the substitution $S \in \mathfrak{G}$. The substitutions in $\mathfrak{G}$ induce operator automorphisms of K/k, regarded as a k-module—that is, an additive Abelian group with k as operator domain. Thus K/k can be made into a module with respect to $(\mathfrak{G})_k$ by setting

$$z\Big(\sum_i S_i c_i\Big) = \sum_i z^{S_i} c_i, \qquad z \in K,\ S_i \in \mathfrak{G},\ c_i \in k.$$

Definition. *Every $(\mathfrak{G})_k$-module contained in K/k is called a rational Galois module. Similarly, the $[\mathfrak{G}]_\mathfrak{o}$-modules contained in K/k are called integral Galois modules; in particular, $\mathfrak{O}/\mathfrak{o}$ is an integral Galois module.*

Theorem 3. *As a rational Galois module, K/k is operator-isomorphic to $(\mathfrak{G})_k$.*

This follows from the fact that K/k always has a field normal basis, that is, a k-basis consisting of conjugate elements z^S.[7] The assignment

$$S \longmapsto z^S, \qquad \sum_i S_i c_i \longmapsto \sum_i z^{S_i} c_i \quad (c_i \in k), \quad \text{and hence } ST \longmapsto z^{ST},$$

is an operator homomorphism, and since the ranks over k are equal, it is an isomorphism.

Theorem 4. *As an integral Galois module, $\mathfrak{O}/\mathfrak{o}$ is operator-isomorphic to a $[\mathfrak{G}]_\mathfrak{o}$-module in $(\mathfrak{G})_k$ of maximum rank n. Likewise, $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$ is operator-isomorphic to a $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$-module of rank n in $(\mathfrak{G})_{k_\mathfrak{p}}$.*

The $(\mathfrak{G})_k$-isomorphism $K/k \longrightarrow (\mathfrak{G})_k$ given in Theorem 3 assigns to the $[\mathfrak{G}]_\mathfrak{o}$-module $\mathfrak{O}/\mathfrak{o}$ a $[\mathfrak{G}]_\mathfrak{o}$-module of rank n in $(\mathfrak{G})_k$. The $(\mathfrak{G})_k$-isomorphism can further be extended to a $(\mathfrak{G})_{k_\mathfrak{p}}$-isomorphism from $K_\mathfrak{p}/k_\mathfrak{p}$ to $(\mathfrak{G})_{k_\mathfrak{p}}$, simply by letting the c_i in the assignment of Theorem 3 run through all elements of $k_\mathfrak{p}$. This isomorphism then induces the $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$-isomorphism of $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$. Here $K_\mathfrak{p}/k_\mathfrak{p}$ is to be regarded as a hypercomplex system over $k_\mathfrak{p}$. It is obtained by extension of coefficients from K/k, and in general becomes a system with zero divisors, namely a sum of isomorphic fields, hence a semisimple system.

Theorem 5. *At every place $\mathfrak{p}$ which does not divide the degree n of K/k, the module $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$ has a normal basis.*[8]

By Theorem 1, $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$ is a maximal order there; the $[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$-modules of rank n in $(\mathfrak{G})_{k_\mathfrak{p}}$ are therefore integral or fractional ideals, hence principal by Theorem 2. If the ideal corresponding to $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$ is $W[\mathfrak{G}]_{\mathfrak{o}_\mathfrak{p}}$, then it has the $\mathfrak{o}_\mathfrak{p}$-basis WS_i. The operator isomorphism says that w^{S_i} is an $\mathfrak{o}_\mathfrak{p}$-basis of $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$, where w is the element corresponding to W. Thus the n conjugate elements w^{S_i} form a normal basis of $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$.

If $\mathfrak{p}$ divides n, the module corresponding to $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$ cannot be principal, since in this case no normal basis can exist.

---

[6] Hasse, loc. cit. The principal-ideal property is proved there only for simple systems, but follows by the familiar arguments for semisimple systems as well. For the components of a maximal order are again maximal, and the components of the ideal under consideration are therefore principal, say with bases a_i. Then $a = \sum a_i$ is a basis of the original ideal. For Abelian groups, see also note 3.

[7] For if $a_1, \ldots, a_n$ is a basis of K/k, and the u_i denote indeterminates, then the $\sum u_i a_i^S$ are linearly independent as S runs through the elements of $\mathfrak{G}$. Consequently the u_i can also be specialized to elements of k in such a way that linear independence is preserved.

[8] In the case of Abelian fields, the place may, by notes 3 and 5, also be defined by means of the quotient ring.

Additional remark to Theorem 3. From the operator isomorphism between $(\mathfrak{G})_k$ and K/k proved in Theorem 3[9] follow Speiser's results on Klein's problem of forms,[10] which may be formulated as follows:

Every representation of the Galois group $\mathfrak{G}$ of K/k which is irreducible over k is generated by an irreducible rational Galois module from K/k; every absolutely irreducible representation is generated by a Galois module from K_Z/Z.

Here Z denotes a splitting field containing k for the corresponding component of the group ring; K_Z/Z is to be regarded as a hypercomplex system over Z, obtained by extension of coefficients from K/k. In particular, K_Z remains a field if Z can be chosen relatively prime to K over k, so that K_Z/Z is an accessory extension (the case treated by Speiser).

The assertion itself follows by operator isomorphism from the corresponding assertion for $(\mathfrak{G})_k$, respectively $(\mathfrak{G})_Z$, where the irreducible ideals generate the representation.

If $v_1, \ldots, v_t$ is a basis of such a Galois module and $S \longmapsto \bar{S}$ is the corresponding representation, then

$$\begin{pmatrix} \vdots \\ v_i^S \\ \vdots \end{pmatrix} = \bar{S} \begin{pmatrix} \vdots \\ v_i \\ \vdots \end{pmatrix}.$$

This is precisely Klein and Speiser's formulation.

ğ3. The Discriminant as Group Determinant in Fields without Higher Ramification

For decomposing the discriminant it is enough, as is known, to consider its decomposition at the individual ramified places. In fields without higher ramification, only places with normal basis are involved.

Theorem 6. *For Galois fields K/k without higher ramification, the discriminant at every ramified place is the square of the group determinant of the Galois group after the indeterminates have been replaced by the normal basis. Corresponding to the irreducible representations, the group determinant decomposes into generalized root numbers; the discriminant decomposes into ideals of the ground field enlarged by the characters, with conjugate-complex characters corresponding to the same ideals.*

With w^S as a normal basis, the discriminant Δ is the square of

$$D = |w^{ST^{-1}}|; \qquad S, T \in \mathfrak{G}.$$

But D is the group determinant with the w^S in place of the indeterminates x_S.

The decomposition into root numbers follows from Speiser's arguments, loc. cit. Let

$$D = D_1^{f_1} \cdots D_t^{f_t}, \qquad M = f_1 M_1 + \cdots + f_t M_t$$

be the decompositions of the group determinant and the group matrix according to the absolutely irreducible representations. If $S \longmapsto \bar{S}$ denotes the representation corresponding to M_λ, with the $\bar{S}$ lying in the enlarged ground field, then

$$M_\lambda = \sum_S w^S \bar{S}, \qquad M_\lambda^{T^{-1}} = \sum_S w^{ST^{-1}} \bar{S} = \sum_R w^R \bar{R} \bar{T} = M_\lambda \bar{T},$$

and, on passing to determinants,

$$D_\lambda^{T^{-1}} = D_\lambda |\bar{T}| = D_\lambda \varepsilon_T.$$

This identifies the D_λ as generalized root numbers; ε_T, being the determinant of $\bar{T}$, is a root of unity (an irreducible representation of the quotient of $\mathfrak{G}$ by its commutator group). For cyclic groups the D_λ are simply the Lagrange root numbers $\sum w^S \chi_\lambda(S)$.

In general the D_λ lie in the hypercomplex system obtained from $K_\mathfrak{p}/k_\mathfrak{p}$ by enlarging the coefficient domain $k_\mathfrak{p}$ by the corresponding character; moreover they are *integral* quantities of this system. For the determinant formed with indeterminates x_S has, as its coefficients, algebraic integers in the character field, while the w^S are integral elements of $K_\mathfrak{p}$.

[9] The proof plainly assumes only that K is Galois of the first kind over k, and that k has infinitely many elements. This last restriction is unnecessary: M. Deuring devised a proof of Theorem 3 valid also for fields with finitely many elements, from which conversely the existence of the field normal basis follows. At the same time this gives a proof of the existence of the primitive element which proceeds uniformly for fields with finitely and infinitely many elements.

[10] Loc. cit. The notion of the Galois module is abstracted from there. If the characteristic of k divides n, one deals with composition series by Galois modules and their irreducible factors.

To pass from the factorization of the group determinant to that of the discriminant, one groups each representation with its adjoint. If $\lambda, \bar{\lambda}$ denote adjoint representations, then simultaneously

$$D_\lambda^{T^{-1}} = D_\lambda \varepsilon_T, \qquad D_{\bar{\lambda}}^{T^{-1}} = D_{\bar{\lambda}} \varepsilon_T^{-1};$$

at the same time, the determinants formed with indeterminates x_S belonging to $\lambda, \bar{\lambda}$ are complex conjugates, while in general conjugate characters correspond to conjugate determinants when the x_S are indeterminates.

Put $\Delta_\lambda = D_\lambda D_{\bar{\lambda}}$. Then only the real subfield of the λ-th character need be adjoined, and

$$\Delta_\lambda^T = \Delta_\lambda \qquad \text{for all } T \text{ in } \mathfrak{G}.$$

Consequently,[11] Δ_λ lies in the ground field enlarged by the real subfield of the λ-th character.

The discriminant factorization

$$\Delta = \Delta_1^{f_1} \cdots \Delta_t^{f_t}$$

is therefore a factorization in the ground field enlarged by the real subfields of the characters, with conjugate-complex characters corresponding to the same factors. Nothing further can be concluded directly for the remaining conjugate characters [cf. 2a)].

This proves all parts of Theorem 6. If one can show that the ideals generated by the Δ_λ in fact already lie in the base field k, and are equal for conjugate characters, then they agree with Artin's conductors, provided that to composite characters one assigns the corresponding products of powers of the Δ_λ. For both the functional equation and the fact—following directly from the normal basis (cf. Speiser, loc. cit.)—that the identity representations of subgroups correspond to the discriminants of the associated subfields hold. Agreement at every place then implies agreement of the full ideals. If one restricts to rational irreducible characters, the stated facts give the agreement. For absolutely irreducible characters the agreement will now be confirmed directly in the very simplest case.

Theorem 7. *Let k be the field of rational numbers and K/k cyclic of prime degree l, prime to the discriminant and hence without higher ramification. Then the ideals generated by the Δ_λ for the nonidentity representations are all equal and agree with the conductor of K/k.*

This follows from the known decomposition of root numbers.[12] At a ramified place $\mathfrak{p}$ of K/k, for k_ε, the field of l-th roots of unity, and K_ε (which remains a field, since k_ε is relatively prime to K, and the $\mathfrak{p}$-adic extension is unnecessary here by note 7), one has

$$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_{l-1}, \qquad \mathfrak{p}_i = \mathfrak{P}_i^l,$$

where the $\mathfrak{p}_i$ lie in k_ε and the $\mathfrak{P}_i$ in K_ε. Further, for the root numbers,

$$(\Omega_\lambda) = \mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_{l-1}^{r_{l-1}}, \qquad (\Omega_{\bar{\lambda}}) = \mathfrak{P}_1^{l-r_1} \cdots \mathfrak{P}_{l-1}^{l-r_{l-1}},$$

where $r_1, \ldots, r_{l-1}$ is a permutation of $1, \ldots, l-1$. Here the root numbers Ω_λ are identical with the factors D_λ of the group determinant; hence

$$(\Delta_\lambda) = (D_\lambda D_{\bar{\lambda}}) = (\Omega_\lambda \Omega_{\bar{\lambda}}) = \mathfrak{P}_1^l \cdots \mathfrak{P}_{l-1}^l = \mathfrak{p}_1 \cdots \mathfrak{p}_{l-1} = (p),$$

and therefore it agrees with the conductor of K/k.

Received 24 August 1931.

[11] Because this is a hypercomplex extension of the coefficients of a field, the usual argument of Galois theory must be modified. Let P be the extension field of $k_\mathfrak{p}$ in question, and let

$$(K_\mathfrak{p})_P = (K_\mathfrak{p})_P e^{S_1} + \cdots + (K_\mathfrak{p})_P e^{S_r}$$

be the direct-sum decomposition into fields. Then $(K_\mathfrak{p})_P e^{S_i} / P e^{S_i}$ is Galois (its group a subgroup of the decomposition group of a prime factor of $\mathfrak{p}$), and the e^{S_i} are conjugate with respect to the cosets. From $\Delta_\lambda^T = \Delta_\lambda$ it follows first that the i-th component of Δ_λ lies in $P e^{S_i}$, and hence is, say, $\gamma_i e^{S_i}$ with γ_i in P. From the conjugacy of the e^{S_i} it follows further that all γ_i are equal, and therefore in fact $\Delta_\lambda = \gamma \sum e^{S_i} = \gamma$ lies in P.

[12] Hilbert, Zahlbericht, ğ 108. Since by Theorem 5 the existence of the normal basis is established—the place may, by note 7, simply be defined by the quotient ring—the fact used in the Zahlbericht that absolutely cyclic fields are cyclotomic fields need no longer be invoked.

38. Jointly with R. Brauer and H. Hasse: Proof of a Main Theorem in the Theory of Algebras

Journal f. d. reine u. angew. Math. 167 (1932), pp. 399–404

Proof of a Main Theorem in the Theory of Algebras.

By *R. Brauer* in Königsberg, *H. Hasse* in Marburg, and *E. Noether* in Göttingen.[1]

At last our joint efforts have succeeded in proving the following theorem, which is of fundamental importance for the structure theory of algebras over algebraic number fields and beyond.

Main Theorem. *Every normal division algebra over an algebraic number field is cyclic (or, as one also says, of Dickson type).*

It is a special pleasure to present this result, essentially an achievement of the p-adic method, to Kurt Hensel, the founder of that method, on his seventieth birthday.

Our proof consists of three reductions, each contributed by one of us.[2]

1. H. Hasse gave the first reduction on the basis of his recently developed theory of cyclic algebras over algebraic number fields.[3]

Reduction 1. The main theorem is proved once the following is shown:

I. Every everywhere split algebra over Ω is $\sim \Omega$.

For brevity, here and below an "algebra A over Ω" always means a normal simple algebra A over the algebraic number field Ω, that is, a simple hypercomplex system with center Ω. The notation $A \sim \Omega$ means that A is a full matrix algebra over Ω, equivalently that A belongs to the special similarity class determined by Ω itself as a division algebra over Ω (equality of the associated division algebras over Ω) [H, 5]. Finally, an algebra over Ω is called everywhere split if for every prime place $\mathfrak{p}$ of Ω its $\mathfrak{p}$-adic extension—the algebra obtained by extending the coefficient field Ω to the associated $\mathfrak{p}$-adic field $\Omega_\mathfrak{p}$—is split:

$$A_\mathfrak{p} \sim \Omega_\mathfrak{p}.$$

Proof. Let D be a division algebra over Ω. Choose a cyclic field Z/Ω such that, for every prime place $\mathfrak{p}$ of Ω, the $\mathfrak{p}$-degree of Z is a multiple of the $\mathfrak{p}$-index of D [cf. the note to H, 17 Bb]. Then, for each associated prime divisor $\mathfrak{P}$ in Z, the local field $Z_\mathfrak{P}$ splits $D_\mathfrak{p}$ [H, 18.1]. Hence the algebra D_Z obtained by extending the coefficient field of D to Z is everywhere split over Z. If I is known for every Ω, then $D_Z \sim Z$. Thus D has the cyclic splitting field Z, and is therefore cyclically representable [H, 5]. It then also has such a cyclic splitting field whose degree agrees with the degree of D itself; this means that D is cyclic [H, 6, Theorem 6]. Under assumption I, the main theorem is therefore proved.

2. The decisive impulse for the second reduction was given by R. Brauer, who informed H. Hasse by letter how the related question of the exact value of the exponent of a division algebra (which is, incidentally, also solved by the main theorem; see below) can be reduced by Sylow's theorem to the case of a solvable splitting field. The same idea then gave the corresponding further reduction of the cyclicity question.

Reduction 2. Statement I is proved once the following is shown:

II. Every everywhere split algebra over Ω with a solvable splitting field is $\sim \Omega$.

[1] H. Hasse undertook the writing of this note.

[2] They are given in the order in which they arose, which is the reverse of their systematic order.

[3] H. Hasse, *Theorie der zyklischen Algebren über einem algebraischen Zahlkörper*, Gött. Nachr. 1931. A detailed presentation of the proofs, in which in particular the theory of splitting fields and crossed products developed by E. Noether in a lecture—fundamental there as here—is developed, will shortly appear in the Trans. Amer. Math. Soc. under the title *Theory of cyclic algebras over an algebraic number field.* This work is cited below as H. H, 1–6 comprise, apart from the difference in language, the former note.

Proof. Let A be everywhere split over Ω. Let K be a Galois splitting field for A, let p be any prime number, and let Σ be one of the Sylow fields of K/Ω corresponding to p, that is, the fixed field of a p-Sylow subgroup of the Galois group. Then A_Σ is likewise everywhere split over Σ, and has the solvable splitting field K. If II is known for every Ω, then $A_\Sigma \sim \Sigma$. Thus Σ is a splitting field of A, of degree prime to p. Hence the index of A, being a divisor of this degree, is prime to p. Since this holds for every prime p, the index is 1, and $A \sim \Omega$. Under assumption II, I is therefore proved.[4]

3. The third reduction, which, as H. Hasse recognized when in possession of the first two reductions, leads to the final proof, was given by E. Noether, prompted by a communication from H. Hasse. In it the main theorem was proved for the special case of an Abelian splitting field by means of the general Reduction 1 and a formulaic reduction of the associated factor system; E. Noether extracted Reduction 3 as its core. Independently of E. Noether, R. Brauer had also already considered this third reduction.

Reduction 3. Statement II is proved once the following is shown:

III. Every everywhere split algebra over Ω with a cyclic splitting field of prime degree is $\sim \Omega$.

Proof. Let A be an everywhere split algebra with a solvable splitting field K/Ω. Choose a tower

$$K = \Lambda_0 > \Lambda_1 > \cdots > \Lambda_r = \Omega$$

such that each Λ_i/Λ_{i+1} is cyclic of prime degree. Then A_{Λ_1} is likewise everywhere split over Λ_1, and has the cyclic splitting field of prime degree $K = \Lambda_0$. If III is known for every Ω, then $A_{\Lambda_1} \sim \Lambda_1$, so Λ_1 is already a splitting field of A. Starting from Λ_1 instead of Λ_0, the same argument proves $A_{\Lambda_2} \sim \Lambda_2$, and so on, until finally $A_{\Lambda_r} \sim \Lambda_r$, that is, $A \sim \Omega$. Under assumption III, II is therefore proved.

4. But III follows from the results of H. Hasse [H, 24]. Thus the validity of the main theorem follows by reversing Reductions 3, 2, and 1.

E. Noether further points out the following. The validity of III—more generally, for cyclic splitting fields of arbitrary degree—amounts to Hasse's norm theorem.[5] For Reduction 3, however, only the special case of prime degree is needed, that is, the original Hilbert–Furtwängler norm theorem.[6] Thus Reduction III supplies a new simple proof of Hasse's norm theorem. The proof would run as follows.

Let Z/Ω be cyclic and let α be a number in Ω for which the norm residue symbol

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = 1$$

for every prime place $\mathfrak{p}$ of Ω. Then every cyclic algebra

$$A = (\alpha, Z)$$

[7] is everywhere split [H, 17.7]. By Reduction 3—using only the Hilbert–Furtwängler norm theorem—it follows that $A \sim \Omega$. Hence α is the norm of an element of Z [H, 15.4].

---

[4]The idea of reducing to solvable splitting fields by Sylow's theorem had already been used by R. Brauer to show that every prime divisor of the index also occurs in the exponent (Über den Zusammenhang von arithmetischen und invariantentheoretischen Eigenschaften von Gruppen linearer Substitutionen, Berl. Akad.-Ber. 1926). More recently A. A. Albert has developed simple proofs, independent of representation theory, for this idea and for a number of general theorems in the theories of R. Brauer and E. Noether: (1) *On direct products, cyclic division algebras, and pure Riemann matrices*; (2) *On direct products*; both in Trans. Amer. Math. Soc. 33 (1931). For the reduction in question see especially Theorem 23 in (2).

Added in proof. A. A. Albert, having been informed by H. Hasse in a letter that he had proved the main theorem for Abelian algebras (see the text immediately below), independently and directly inferred from it: (a) the main theorem for degrees of the form 2^e; (b) Theorem 1 below (exponent equals index); and (c), besides the basic idea of Reduction 2, also that of the following Reduction 3, naturally without reference to Reduction 1, and consequently with the result that for division algebras D of prime-power degree p^e over Ω, there exists an extension field Ω' of degree prime to p over Ω such that $D_{\Omega'}$ is cyclic.

All three results are, of course, superseded by our proof of the main theorem, completed in the meantime. They show, however, that A. A. Albert has an independent share in the proof of the main theorem. Finally, after learning our proof of the main theorem, A. A. Albert observed that our central statement I follows in a few lines from Theorems 13, 10, and 9 of a paper of his in press (Bull. Amer. Math. Soc. 37 (1931)). The proof of these theorems rests essentially on the same arguments as our Reductions 2 and 3.

[5]Cited in H, 3.11; proved in H. Hasse, *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol*, Gött. Nachr. 1931.

[6]See H. Hasse, Bericht über neuere Untersuchungen und Probleme in der Theorie der algebraischen Zahlkörper II, Jahresber. der D. M.-V., Erg.-Bd. 6 (1930), §§ 8, and the literature cited there.

[7]In the notation of H, 1. The specification of the automorphism S of Z associated with α has been omitted here as irrelevant.

In connection with the norm theorem, we further remark that statement I is to be regarded as its proper generalization to higher, even non-Abelian cases, whereas the literal generalization, as H. Hasse showed,[5] is not true in general.

Consequences (H. Hasse).

5. The most immediate consequence of the main theorem is that the theory of cyclic algebras over algebraic number fields developed by H. Hasse now has the significance of a general structure and invariant theory of normal simple algebras (in particular, normal division algebras) over algebraic number fields. In particular, it is now proved in general that:

Theorem 1. The exponent of a normal simple algebra over an algebraic number field is equal to its index.

Statement I further gives the remarkable fact:

Theorem 2. The fundamental ideal of a proper normal division algebra over Ω is divisible by at least one prime place of Ω, and in fact by at least two.

Here the fundamental ideal may be defined as the reduced norm of the reduced different.[8] An infinite prime place is included in the fundamental ideal if and only if the algebra reduces there to the quaternion algebra rather than to the real or complex number field.

Proof. By H. Hasse's results,[9] a prime place $\mathfrak{p}$ of Ω occurs in the fundamental ideal if and only if its $\mathfrak{p}$-index differs from 1. If all $\mathfrak{p}$-indices were 1, the algebra would be everywhere split; then by I it would not be a proper division algebra. Nor can a single $\mathfrak{p}$-index alone differ from 1, because the norm residue symbols, whose orders are the $\mathfrak{p}$-indices [H, 17.7], satisfy the product theorem, or reciprocity law [H, 3.8].

6. Statement I further makes possible the determination, or arithmetic characterization, of all splitting fields K belonging to an algebra A over Ω. In exact generalization of the fact already established by H. Hasse for cyclic A, K [H, 6, Theorem 2], one obtains:

Theorem 3. For an algebra A over Ω, an algebraic number field K/Ω is a splitting field if and only if, for every prime divisor $\mathfrak{P}_i$ in K of every prime place $\mathfrak{p}$ of Ω, the $\mathfrak{P}_i$-degree $n_{\mathfrak{P}_i}$ of K is a multiple of the $\mathfrak{p}$-index $m_{\mathfrak{p}}$ of A.

Here the $\mathfrak{P}_i$-degree of K is the degree of the $\mathfrak{P}_i$-adic field $K_{\mathfrak{P}_i}$ over the $\mathfrak{p}$-adic field $\Omega_{\mathfrak{p}}$. Thus, if

$$\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_{\mathfrak{P}_i}}, \qquad N_{K/\Omega}(\mathfrak{P}_i) = \mathfrak{p}^{f_{\mathfrak{P}_i}}$$

is the decomposition of $\mathfrak{p}$ in K, it is the product of the relative degree $f_{\mathfrak{P}_i}$ and ramification order $e_{\mathfrak{P}_i}$, namely $n_{\mathfrak{P}_i} = f_{\mathfrak{P}_i} e_{\mathfrak{P}_i}$ [H, 4]. The $\mathfrak{p}$-index of A is the index $m_{\mathfrak{p}}$ of the $\mathfrak{p}$-adic extension $A_{\mathfrak{p}}$ [H, 6].

Proof. That K is a splitting field of A, that is, $A_K \sim K$, is by statement I equivalent to $A_{K_{\mathfrak{P}_i}} \sim K_{\mathfrak{P}_i}$ for every $\mathfrak{P}_i$.

For a finite prime place $\mathfrak{p}$, let

$$A_{\mathfrak{p}} \sim (\pi, W_{\mathfrak{p}})$$

be the arithmetically distinguished cyclic representation of $A_{\mathfrak{p}}$ [H, 16; also loc. cit.[9], Theorem 38], where $W_{\mathfrak{p}}$ is the unramified field of degree $m_{\mathfrak{p}}$ over $\Omega_{\mathfrak{p}}$, and π is a number in $\Omega_{\mathfrak{p}}$ exactly divisible by $\mathfrak{p}^1$. Let $K_{\mathfrak{P}_i} W_{\mathfrak{p}}$ be the composite and

$$\Delta_{\mathfrak{P}_i} = K_{\mathfrak{P}_i} \cap W_{\mathfrak{p}}$$

[8] In the special case of rational quaternion algebras, this amounts to the notion of "fundamental number" introduced by H. Brandt (Idealtheorie in Quaternionenalgebren, Math. Ann. 99 (1928)). Since here one has not a number but an ideal, "fundamental ideal" had to be used; it should not be confused with Dedekind's terminology of fundamental ideal and fundamental number for different and discriminant, which for the reason just stated proves unusable for relative fields. For the definition of the reduced different, see the following note. The reduced norm of an ideal is likewise defined by E. Noether "prime-place by prime-place": corresponding to the fact that at the individual prime places every ideal is principal, one simply takes the reduced number norms of the principal-ideal basis elements at the individual prime places.

[9] H. Hasse, *Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Math. Ann. 104 (1931), Theorems 42 and 59.

the intersection of $W_\mathfrak{p}$ and $K_{\mathfrak{P}_i}$. Since the largest unramified subfield contained in $K_{\mathfrak{P}_i}$ has degree $f_{\mathfrak{P}_i}$ over $\Omega_\mathfrak{p}$, and since for each degree there is only one unramified field over $\Omega_\mathfrak{p}$, $\Delta_{\mathfrak{P}_i}$ has

$$\text{degree } d_{\mathfrak{P}_i} = (m_\mathfrak{p}, f_{\mathfrak{P}_i}) \text{ over } \Omega_\mathfrak{p}.$$

Thus $K_{\mathfrak{P}_i} W_\mathfrak{p}$ is an unramified extension of $K_{\mathfrak{P}_i}$ of degree $m_\mathfrak{p}/d_{\mathfrak{P}_i}$.

Now

$$A_{K_{\mathfrak{P}_i}} = (A_\mathfrak{p})_{K_{\mathfrak{P}_i}} \sim (\pi, K_{\mathfrak{P}_i} W_\mathfrak{p})$$

[H, 15.5]. Hence $A_{K_{\mathfrak{P}_i}} \sim K_{\mathfrak{P}_i}$ is equivalent to π being a norm from $K_{\mathfrak{P}_i} W_\mathfrak{p}$ over $K_{\mathfrak{P}_i}$. Since this extension is unramified, that occurs if and only if the order $e_{\mathfrak{P}_i}$ of π at $\mathfrak{P}_i$ is a multiple of its degree $m_\mathfrak{p}/d_{\mathfrak{P}_i}$, or equivalently, since

$$\left(\frac{m_\mathfrak{p}}{d_{\mathfrak{P}_i}}, \frac{f_{\mathfrak{P}_i}}{d_{\mathfrak{P}_i}} \right) = 1,$$

if

$$\frac{f_{\mathfrak{P}_i}}{d_{\mathfrak{P}_i}} e_{\mathfrak{P}_i} = \frac{n_{\mathfrak{P}_i}}{d_{\mathfrak{P}_i}}$$

is a multiple of $m_\mathfrak{p}/d_{\mathfrak{P}_i}$, that is, if $n_{\mathfrak{P}_i}$ is a multiple of $m_\mathfrak{p}$, as asserted.

If $\mathfrak{p}$ is an infinite prime place and the trivial case $m_\mathfrak{p} = 1$ does not occur, then $m_\mathfrak{p} = 2$ and $A_\mathfrak{p}$ is the quaternion algebra over the real number field $\Omega_\mathfrak{p}$. The condition $A_{K_{\mathfrak{P}_i}} = (A_\mathfrak{p})_{K_{\mathfrak{P}_i}} \sim K_{\mathfrak{P}_i}$ is then equivalent to $K_{\mathfrak{P}_i}$ being the complex number field, that is, to $n_{\mathfrak{P}_i} = f_{\mathfrak{P}_i} = 2 = m_\mathfrak{p}$ (the $e_{\mathfrak{P}_i}$ do not occur here). This again gives the assertion, since both $n_{\mathfrak{P}_i}$ and $m_\mathfrak{p}$ can take only the values 1 or 2.

7. Important results arise if one reverses the question answered in Theorem 3 about all splitting fields K of a fixed algebra A: for a fixed algebraic field K/Ω, consider all algebras A over Ω split by K. These algebras form a subgroup $\mathfrak{K}$, determined by K, of R. Brauer's group $\mathfrak{A}$ of all algebras (more precisely, all classes of similar algebras) over Ω.[10] If K is assumed Galois over Ω, one obtains theorems which may be regarded as generalizations of the principal theorems of class field theory (the theory of relatively Abelian number fields) to general relatively Galois number fields.

Theorem 4. *(Decomposition theorem.)* Let K/Ω be Galois. The relative degree f of the prime divisors in K of a prime ideal $\mathfrak{p}$ of Ω not dividing the relative discriminant of K is the least exponent for which

$$A_\mathfrak{p}^f \sim \Omega_\mathfrak{p}$$

for every algebra A in the group $\mathfrak{K}$ assigned to K.

Proof. Since f is the $\mathfrak{p}$-degree of K, the same for all prime divisors of $\mathfrak{p}$ in K, while the $\mathfrak{p}$-index of A is the index, and hence the exponent, of $A_\mathfrak{p}$, Theorem 3 shows that f is in any case a multiple of that least exponent. It remains only to show that the group $\mathfrak{K}$ contains algebras A of exact $\mathfrak{p}$-index f.

By Frobenius' density theorem, there is another prime ideal $\mathfrak{p}'$ of Ω, likewise not dividing the relative discriminant of K, whose prime divisors in K have relative degree f. Let Z/Ω be cyclic with both $\mathfrak{p}$-degree and $\mathfrak{p}'$-degree equal to f. Further choose α in Ω such that the norm residue symbols

$$\left(\frac{\alpha, Z}{\mathfrak{p}} \right) \quad \text{and} \quad \left(\frac{\alpha, Z}{\mathfrak{p}'} \right)$$

have reciprocal values of order f, while for every other divisor $\mathfrak{q}$ of the conductor of Z,

$$\left(\frac{\alpha, Z}{\mathfrak{q}} \right) = 1.$$

By the generalized theorem on arithmetic progressions, α may moreover be chosen so that, apart possibly from $\mathfrak{p}, \mathfrak{p}'$, and the $\mathfrak{q}$, it contains only one further prime ideal $\mathfrak{r}$ of Ω, exactly to the first power. For this prime, the product theorem for the norm residue symbol, or reciprocity law, likewise gives

$$\left(\frac{\alpha, Z}{\mathfrak{r}} \right) = 1$$

[10] R. Brauer, Über Systeme hyperkomplexer GröSSen, Jahresber. d. D. M.-V. 38 (1929), pp. 47–48; see also H, 13.1.

[H, 3.8–10]. The algebra

$$(\alpha, Z) = A$$

then has $\mathfrak{p}$-index and $\mathfrak{p}'$-index f, but index 1 at every other prime place of Ω [H, 17.7]. By Theorem 3, in view of the assumption on $\mathfrak{p}$ and the choice of $\mathfrak{p}'$, K is a splitting field for A. Thus algebras A of $\mathfrak{p}$-index exactly f have indeed been exhibited in $\mathfrak{K}$.

Theorem 5. *(Uniqueness and ordering theorem.)* $K \leqq K'$ if and only if $\mathfrak{K} \leqq \mathfrak{K}'$.

Thus the assignment of the algebra groups $\mathfrak{K}$ to Galois fields K is one-to-one.

Proof. (a) From $K \leqq K'$ it follows trivially that $\mathfrak{K} \leqq \mathfrak{K}'$, since every algebra A split by K is a fortiori split by K'.

(b) Conversely, let $\mathfrak{K} \leqq \mathfrak{K}'$. By the decomposition theorem, for every prime $\mathfrak{p}$ not dividing the relative discriminant, $f_\mathfrak{p} \mid f'_\mathfrak{p}$. In particular, $f_\mathfrak{p} = 1$ for almost every $\mathfrak{p}$ for which $f'_\mathfrak{p} = 1$. The familiar analytic argument[11] then gives $K \leqq K'$.

8. Finally, the main theorem yields an essential advance in the question treated by I. Schur[12] concerning the number fields over which the absolutely irreducible representations of a finite group can be realized.

Theorem 6. All absolutely irreducible representations of a finite group $\mathfrak{G}$ can be realized over cyclotomic fields; in any case they can always be realized over the field of n^h-th roots of unity when n is the order of $\mathfrak{G}$ and h is sufficiently large.

Proof. Pass to the rational group ring G of $\mathfrak{G}$. The absolutely irreducible representations Γ_i of $\mathfrak{G}$ then become the absolutely irreducible representations of the simple components G_i of the semisimple algebra G, and their centers are the fields Ω_i of the corresponding characters.[13] Since $\mathfrak{G}$ is finite, these are cyclotomic fields, indeed subfields of the field of n-th roots of unity.

By Theorem 3, a cyclic field Z_i/Ω_i is a splitting field of G_i if, for every prime place $\mathfrak{p}$ of Ω_i, its $\mathfrak{p}$-degree $n_{i\mathfrak{p}}$ is a multiple of the $\mathfrak{p}$-index $m_{i\mathfrak{p}}$ of G_i. The number $m_{i\mathfrak{p}}$ differs from 1 only at the prime divisors of the fundamental ideal of G_i relative to Ω_i, and hence only at the prime divisors of the absolute discriminant of G_i. Since this discriminant divides n^n—where n^n is the discriminant of a nonmaximal order in G[14]—these are at most the prime divisors $\mathfrak{p}$ of n. To make $n_{i\mathfrak{p}}$ a multiple of $m_{i\mathfrak{p}}$ for these $\mathfrak{p}$, it is enough to require that each such $\mathfrak{p}$ ramify in Z_i with an order divisible by $m_{i\mathfrak{p}}$. As is easily seen, the field of n^h-th roots of unity does this for sufficiently large h.

In the last theorem of the cited paper, I. Schur states that in all cases known so far the field of n-th roots of unity already suffices. Whether this always holds, and whether the methods developed here suffice to decide the question, must be left to further investigation.

Received 11 November 1931.

[11] See, for example, H. Hasse [loc. cit., note 6], ğ 25, III.

[12] I. Schur, Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen, Berl. Akad.-Ber. 1906.

[13] See: (a) R. Brauer and E. Noether, Über minimale Zerfällungskörper irreduzibler Darstellungen, Berl. Akad.-Ber. 1927, ğ 1; (b) R. Brauer, Über Systeme hyperkomplexer Zahlen, Math. Z. 30 (1929), Theorem 3; (c) E. Noether, Hyperkomplexe GröSSen und Darstellungstheorie, Math. Z. 30 (1929), ğğ 21, 24, 26.

[14] See E. Noether [loc. cit., note 7(c)], ğ 26.

39. Hypercomplex Systems in Their Relations to Commutative Algebra and Number Theory

Proceedings of the International Congress of Mathematicians, Zürich 1 (1932), pp. 189–194

By Emmy Noether, Göttingen

1. The theory of hypercomplex systems, or algebras, has advanced strongly in recent years; but only very recently has the significance of this theory for commutative questions become clear. I want to report today on this significance of the noncommutative for the commutative, and I shall do so by following in detail two classical questions going back to Gauss: the principal genus theorem and the closely related norm theorem. Over time these questions have repeatedly changed their formulation. In Gauss they appear as the conclusion of his theory of quadratic forms; then they play an essential role in the characterization of relatively cyclic and abelian number fields by class field theory; finally they can be stated as theorems on automorphisms and on the splitting of algebras. This last formulation at the same time transfers the theorems to arbitrary relatively Galois number fields.

With this outline, which I shall elaborate later, I also want to explain the *principle* of applying the noncommutative to the commutative: *By means of the theory of algebras one seeks invariant and simple formulations for known facts about quadratic forms or cyclic fields, that is, formulations depending only on structural properties of algebras. Once such invariant formulations have been proved—as is the case in the examples indicated above—the transfer of these facts to arbitrary Galois fields is obtained automatically.*

2. Before going into detail, I want to give a general overview of the different methods and further results. First, it should be noted that the main difficulty lies in finding the formulation for general Galois fields, for which there was no starting point at all without the hypercomplex method. In the examples mentioned above, the underlying passage to the noncommutative is obtained by the *simultaneous consideration of field and group* through the "crossed product" and its multiplication constants, the "factor systems" (see 3). In this way one obtains a simple normal algebra over the base field, and every such algebra can essentially be generated in this way. Such crossed products were first considered by Dickson,[1] whereas the theory of factor systems was developed by Speiser, Schur, and R. Brauer[2] from a quite different starting point, namely the question of absolutely irreducible representations. Only by combining the two theories did one obtain a sufficiently simple and far-reaching structure with which commutative questions could be attacked.[3]

At the same time this gives new and transparent proofs of known facts. I should mention here a hypercomplex proof of the reciprocity law for cyclic fields, soon to appear in the Math. Ann., which H. Hasse has given[4] by means of an invariant formulation of his norm residue symbol based on the theory of the crossed product. I should also mention a hypercomplex foundation of local class field theory on the same basis, recently given by C. Chevalley, although new algebraic theorems on factor systems had still to be developed for it.[5] At the same time, however, I must add the qualification that the crossed-product method by itself apparently does *not yield the full theory of Galois number fields.* This follows from new, as yet unpublished results of Artin, which proceed from Hasse's proof above in the spirit of the stated principle, but give only numerical equalities in place of full isomorphism theorems.

Methods giving a full isomorphism—though an operator isomorphism—already exist in algebra. They continue ideas of A. Speiser,[6] namely the view of the Galois field as a "Galois module," that is, as a module over the base field which admits the substitutions of the Galois group as operators. There is an operator isomorphism between the field and the group ring (group algebra), in the sense that the elements correspond one-to-one in such a way that linear forms over the base field correspond, and the substitutions of the Galois group in the field correspond to multiplication in the group ring. This theorem, formulated by me,[7] was

[1] See his book *Algebras and Their Arithmetics*, Zürich 1927, ğ 34.

[2] See, for example, R. Brauer, *Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen*, and the literature cited there in note 2, Math. Z. 28 (1928).

[3] I first developed this structure in a lecture in the winter of 1929/30, reproduced in Chapter 2 of H. Hasse, *Theory of cyclic algebras*, Trans. Amer. Math. Soc. 34 (1932). A report by M. Deuring on hypercomplex numbers and number-theoretic applications, which is to appear in the series *Ergebnisse der Mathematik*, gives an orientation to the entire field treated in the lecture.

[4] H. Hasse, *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper (insbesondere Normenrestsymbol und Reziprozitätsgesetz).* Math. Ann. 107 (1932/33).

[5] C. Chevalley, *Sur la théorie du symbole de restes normiques*; to appear in J. f. Math. 169.

[6] A. Speiser, *Gruppendeterminante und Körperdiskriminante.* Math. Ann. 77 (1916).

[7] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, Theorem 3, J. f. Math. 167 (1932) (the proof contains a gap).

proved by M. Deuring,[8] who based on it a proof of Galois theory in which the operator isomorphism realizes the correspondence between group and field. Further structural theorems, likewise due to Deuring, run parallel to formal facts concerning Artin L-series and give a structural approach to Artin conductors. These Artin L-series and conductors,[9] formed with general group characters, constitute, alongside Speiser's work,[6)] the first connection between number theory and representation theory, a first advance beyond abelian fields. They gave a strong impetus to the whole development; in particular, the theory of Galois modules took its bearings from them.

3. I now want to follow in detail the problems placed at the outset, the norm theorem and the principal genus theorem. First, the *definition of the crossed product*. Let K/k be a Galois field of degree n, with group $\mathfrak{G}$. The crossed product means a simultaneous embedding of K and $\mathfrak{G}$ in an algebra A in such a way that the automorphisms of K become inner. Let $u_{S_1}, \ldots, u_{S_n}$ denote symbols corresponding to the n group elements. First set up A as a module of linear forms of rank n over K:

(1)
$$A = u_{S_1}K + \cdots + u_{S_n}K$$
(that is, A consists of all linear forms
$u_{S_1}a_1 + \cdots + u_{S_n}a_n$, with the a_i arbitrary in K).

By the requirement of the inner automorphism—generated by the u_S, or more generally by $u_S K^*$[10]—A becomes a ring, hence an algebra of rank n^2 over k. The requirement is expressed by

(2)
$$u_S^{-1} z u_S = z^S, \qquad \text{or} \qquad z u_S = u_S z^S$$
for every $z \in K$,[11] and by

(3)
$$u_S u_T = u_{ST} a_{S,T} \quad \text{with } a_{S,T} \text{ in } K^*$$

(4)
$$a_{ST,R}\, a_{S,T}^R = a_{S,TR}\, a_{T,R}$$
(the associative law from $[u_S u_T]u_R = u_S[u_T u_R]$).

A is called the crossed product of K with $\mathfrak{G}$ for the factor system $a_{S,T}$. One proves that A is a simple normal algebra over k, hence a matrix ring D_r of degree r over the associated division algebra D, and that K is a maximal commutative subfield, hence a splitting field (that is, extending the coefficient field k by a field isomorphic to K gives a split algebra, a full matrix ring over the center). Conversely, for any given division algebra D there are always matrix rings D_r which can be generated in the indicated way as crossed products.

If one passes from u_S to $v_S = u_S c_S$, with c_S in K^*, which generates the same automorphism, one obtains "associated" factor systems:

(5)
$$\bar{a}_{S,T} = a_{S,T} \frac{c_S^T c_T}{c_{ST}}$$

Associated factor systems are grouped into a class (a); similarly, all algebras similar to A, that is, all D_r with $r = 1, 2, \ldots$, are grouped into a class $\mathfrak{A}$. *The classes $\mathfrak{A}$ and (a) correspond one-to-one. The classes with fixed splitting field K form, under direct product, an abelian group which is isomorphic to the componentwise product of the classes of factor systems. The identity element is the split algebra class, respectively the system of all transformation quantities*
$$\frac{c_S^T c_T}{c_{ST}}.$$
This is the group of algebra classes observed by R. Brauer.

4. I now want, by *specializing* to *cyclic splitting fields*, to reach the connection with the *norm concept*, and thus the formulation of the generalized *norm theorem* according to the principle explained at the beginning.

[8] M. Deuring, *Galoissche Theorie und Darstellungstheorie*. Math. Ann. 107 (1932).

[9] E. Artin, *Über eine neue Art von L-Reihen*, Math. Sem. Hamburg 3 (1924). *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren*, ibid. 8 (1931). *Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper*, J. f. M. 164 (1931).

[10] K^* is obtained from K by omitting zero; this notation will be used throughout.

[11] z^S denotes, as usual, the element obtained from z by the substitution S.

If Z is cyclic and S is a generating substitution of its group—the associated algebra is then called cyclic—one may let the powers of u correspond to the powers of S, hence

$$(1') \qquad A = Z + uZ + \cdots + u^{n-1}Z$$
$$(2') \qquad zu = uz^S$$
$$(3') \qquad u^n = a$$
$$(4') \qquad a \text{ lies in the base field } k^*$$
$$(5') \qquad \bar{a} = a \cdot N(c), \quad \text{if } v = uc \text{ is set.}$$

Thus every factor system here consists of a single element a lying in the base field—notation $A = (a, Z)$. The identity class of the factor systems is given by the norms from Z^*, and the group of algebra classes is isomorphic to the quotient group

$$k^*/N(Z^*).$$

A cyclic algebra (a, Z) therefore splits if and only if a is the norm of an element of Z.

This connection between norm and splitting gives the formulation of the "norm theorem," namely the *theorem on split algebras: If an algebra splits at every place, then it splits absolutely.* Here a "place" is defined, as usual in number theory, by replacing the base field k with its $\mathfrak{p}$-adic extension $k_\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of k (and, correspondingly for the finitely many infinite places, by extending k and its conjugates by the field of real numbers).

Indeed, this contains the norm theorem for cyclic fields. For cyclic algebras (a, Z), by what was said above, the theorem is equivalent to the assertion: if a is a $\mathfrak{p}$-adic norm at every finite or infinite place, then a is the norm of a number in Z; or, without passing to the $\mathfrak{p}$-adic setting: *If a is a norm residue modulo every prime ideal $\mathfrak{p}$ of k (and satisfies certain sign conditions), then a is the norm of a number in Z.* This latter formulation is precisely the norm theorem proved in class field theory using the familiar analytic tools. The proof of the general theorem on split algebras can be obtained from this cyclic special case by purely algebraic-arithmetic considerations.[12] Hasse drew one first important consequence: *Every simple normal algebra over an algebraic number field is cyclic.* The general formulation arose in the search for a proof of this long-conjectured fact.

5. A second consequence of the theorem on split algebras—again by purely algebraic-arithmetic reasoning—is the principal genus theorem stated at the outset.[13] Its invariant formulation rests on the fact that the relations (2) through (5) defining the crossed product are purely multiplicative, and therefore remain meaningful when K^* is replaced by an abelian group $\mathfrak{J}$ subject only to the condition that its automorphism group contain a subgroup isomorphic to $\mathfrak{G}$. In place of (1) one then has the "extension of $\mathfrak{G}$ by $\mathfrak{J}$" in the sense of group theory. If $\mathfrak{J}$ is taken to be the group of all ideals of K, the factor systems become systems of ideals; a division into classes in $\mathfrak{J}$ induces a division into classes for the factor systems, and in general this will be a finer division into ideal classes than the original one. For the requirement that multiplication of the u_S by (absolute) ideal classes be unambiguous says only that the transformation quantities $c_S^T c_T / c_{ST}$—the identity class of the element factor systems—lie in the identity class of the ideal factor systems. In fact, as specialization to the known cases shows, a somewhat less fine division already suffices. I define: *The identity class of the factor systems consists of those elements $a_{S,T}$ which generate split algebras at all finite and infinite ramified places of K.*

Let the resulting extension of $\mathfrak{G}$ be denoted by $\mathfrak{G}^*$, and let (c) denote the absolute ideal class of c. Then the

Invariant formulation of the principal genus theorem is: *If, under the division into classes thus defined, the substitution $v_S = u_S(c_S)$ produces an automorphism of $\mathfrak{G}^*$—all these (c_S) form the principal genus—then the automorphism is inner and is generated by an ideal class $(\mathfrak{b})$.*

The known special cases follow from an equivalent, somewhat more explicit formulation: *If the transformation quantities $(c_S^T)(c_T)/(c_{ST})$ formed from the ideal classes (c_S) belong to the identity ideal class of the factor systems, then there is an ideal class $(\mathfrak{b})$ such that the (c_S) become symbolic $(1-S)$-th powers: $(c_S) = (\mathfrak{b})/(\mathfrak{b}^S)$ for every S in $\mathfrak{G}$.* For the hypothesis expresses precisely the automorphism property; that it is inner is expressed by $v_S = (\mathfrak{b})^{-1} u_S(\mathfrak{b}) = u_S(\mathfrak{b})^{1-S} = u_S(c_S)$.

Specialization to the cyclic case therefore gives (with due attention to normalization): if $N([c])$ lies in the identity ideal class of the factor systems, then (c) becomes a symbolic $(1-S)$-th power: $(c) = (\mathfrak{b})^{1-S}$.

[12] R. Brauer, H. Hasse, E. Noether, *Beweis eines Hauptsatzes in der Theorie der Algebren.* J. f. M. 167 (1932).

[13] The proof is to appear in the Math. Ann.

6. To pass from here to the familiar formulation for cyclic fields and quadratic forms, I first note that the theorem has been stated for full ideal classes, but its content remains the same if, as usual, one restricts to ideals prime to the ramified places.

With this restriction, the principal genus defined here for quadratic fields becomes Gauss's principal genus. For ideal classes correspond to quadratic forms, and the norms of the classes to the numbers represented by the forms. That the identity class generates algebras split at the ramified places of K therefore means that these represented numbers become quadratic residues at the ramified places; the associated forms thus possess the total character of the principal form and constitute Gauss's principal genus. It is known that the symbolic $(1 - S)$-th power becomes duplication.

For cyclic fields the formulation becomes the following: the principal genus consists of all ideal classes whose norms become norm residues at the finite and infinite ramified places. This is known to be equivalent to being a "norm residue modulo the conductor," and thus the usual theorem is obtained as a specialization.

Moreover, even in the general case of arbitrary Galois fields one can introduce a conductor composed only of the ramified places in such a way that, after normalizing the factor systems for each of these places, the ray contains only elements of the identity class.

This raises the question of the connection with the Artin conductors mentioned in the overview in 2, which are composed of the same prime ideals, and hence the question of the connection with the theory of Galois modules, the second hypercomplex method. The future must show how far these two methods will reach.

40. Noncommutative Algebras

Math. Zs. 37 (1933), 514–541

Noncommutative Algebra.

By

Emmy Noether in Göttingen.

The main theorems of commutative algebra are, as is known, contained in Galois theory, which is preceded by the theory of adjunction fields and splitting fields, that is, fields sufficient for a given polynomial to split off a linear factor or, respectively, to split completely into linear factors.

Here I develop the corresponding parts of algebra in the noncommutative case, especially in the hypercomplex case. In principle I work with noncommutative methods, namely representation in noncommutative fields. At the end I show how the above-mentioned theorems of commutative algebra can be proved in a completely parallel manner by means of representation in commutative fields.

The underlying representation theory—preceded by a short theory of automorphisms (ğ 1)—is a further development of the theory based on representation modules.[1] In particular, alongside direct representation I consider reciprocal representation—each can be reduced to the other—which is now generated by the reciprocal representation module. The advantage is that the reciprocal representation module—thus a bimodule—can also be regarded as a one-sided module over an extension ring (ğ 2). In this way representation in noncommutative fields is reduced to ideal theory in the extension ring; the irreducible representation classes correspond to the irreducible ideal classes of the extension ring, in exact analogy with the facts which hold for a hypercomplex system itself when represented over its commutative coefficient field (ğğ 3 and 4).

From here one obtains the structural theorems for matrix rings over noncommutative fields by observing (ğ 5) that *every subring gives a representation by this field, or respectively a reciprocal representation by the reciprocally isomorphic field*. This reciprocally isomorphic field is a first analogue of a minimal adjunction field and splitting field in the commutative case, insofar as it mediates all reciprocal representations of first degree and, when the rank over the center—not assumed finite until now—is finite, also a full decomposition into direct summands of rank 1. This gives the Galois theory for fields (ğ 6) and at the same time expresses the fact (ğ 7) that reciprocally isomorphic division algebras (fields of finite rank over the center) generate inverse classes in R. Brauer's group of algebra classes.

A second proof of the Galois theory, valid more generally for simple systems (and presented first in the text), is almost an immediate consequence of a theorem on commuting subrings, which itself connects almost directly with the preceding automorphism considerations.

Up to this point the arguments are purely noncommutative. But the question of *commutative* splitting fields is also treated noncommutatively, by representing the splitting field through the division algebra in accordance with the observation prepared in ğ 5 (ğ 7). The conclusion gives the transfer to the commutative case mentioned above (ğ 8) and the theory of splitting fields for arbitrary systems (ğ 9), thereby also establishing the connection with the usual representation theory in the commutative case.

R. Brauer based the theory of splitting fields on this representation theory in the commutative case—and on the "irrational" factor systems.[2] Because of this commutative foundation, he—and later Albert as well—had to assume that the center is a perfect field, a restriction unnecessary in the noncommutative proof. With the same restriction, and again using representation theory in the commutative case, R. Brauer and K. Shoda further developed the theory after learning of my Galois theory for noncommutative fields: R. Brauer gave the theorem on commuting subrings mentioned above, and K. Shoda independently gave the full theory also for semisimple systems.[3]

Finally, I mention that, for the case of fields, a short account is found in van der Waerden II (ğ 128), following my lecture course of summer 1928, where I first lectured on these questions. Van der Waerden's account introduced a number of simplifications relative to that course, some of which I adopted in a second course (winter 1929/30),[4] and some only here, where I have carried them further. In particular, the transfer

[1] E. Noether, *Hyperkomplexe GröSSen und Darstellungstheorie*, Math. Zeitschr. 30 (1929), pp. 641–692, cited as *Darstellungstheorie*. See the account in van der Waerden, *Moderne Algebra* II.

[2] See our joint note, *Über minimale Zerfällungskörper irreduzibler Darstellungen*, Sitz. Ber. d. PreuSS. Ak. d. Wiss. 1927, pp. 221–228. (The note on p. 222 contains an "account of the situation." The main theorems arose independently and almost simultaneously.) See further R. Brauer, *Über Systeme hyperkomplexer Zahlen*, ğ 3, Math. Zeitschr. 30 (1929), pp. 79–107. A. A. Albert later rediscovered the theorems independently.

[3] R. Brauer, *Über die algebraische Struktur von Schiefkörpern*, ğ 2, Journ. f. Math. 166 (1932), pp. 241–252. K. Shoda, *Über die galoissche Theorie der halbeinfachen hyperkomplexen Systeme*, Math. Ann. 107 (1932), pp. 252–258. J. Levitzki had also developed these results.

[4] The first course was written up by G. Köthe, the second by M. Deuring.

of the hypercomplex proof method of Galois theory to the commutative case (ğ 8) dates only from the second course, in which the noncommutative proof (ğ 6, 3) was substantially simplified relative to the first course. The theorem on commuting subrings (ğ 5) and the second proof method of noncommutative Galois theory based on it (ğ 6, 1 and 2) were added only after the second course, following R. Brauer (note 3) and van der Waerden ğ 128; but ğ 5, 3 uses substantially weaker finiteness assumptions than those accounts.

Certain arguments of the first course—the method of forming intersections of difference ideals—have the advantage, although more complicated, of carrying over to systems of infinite rank and to integral systems.[5] For commutative integral systems this leads to the connection between ideal differentiation and the different,[6] which I shall discuss in greater detail on another occasion.

The principal application of the theory of splitting fields lies in the theory of crossed products and their factor systems, which in turn provide the foundation for number-theoretic applications; this will not be pursued here.[7]

ğ 1.

Automorphisms, Modules, and Bimodules.

Representation theory based on representation modules rests, as is known (see also ğ 2), on the theory of the automorphism ring of abelian groups, with or without operators. The arguments implicitly underlying it—relations between mappings and calculation laws—will be formulated in a few simple propositions in order to avoid repetitions.

1. Multiplicative mapping. Associative law. Let $\mathfrak{G}$ first be a group without operators, and let $\mathfrak{A}$ be its absolute automorphism domain, that is, the system of all homomorphisms of $\mathfrak{G}$ into itself. $\mathfrak{A}$ is closed under multiplication, since the product $\sigma\tau$ is defined by

$$g(\sigma\tau) = (g\sigma)\tau \quad \text{with } g \text{ in } \mathfrak{G} \text{ and } \sigma, \tau \text{ in } \mathfrak{A} \tag{1}$$

and plainly satisfies the associative law.

As is known, $\mathfrak{G}$ becomes a group with operators when a set $\mathfrak{B}$ of symbols $\Theta, H, \ldots$ is given such that the combinations $g\Theta, gH, \ldots$ lead to uniquely defined elements of $\mathfrak{G}$ and generate automorphisms (homomorphisms into itself) of $\mathfrak{G}$—$(g \cdot h)\Theta = g\Theta \cdot h\Theta$. Thus there exists a unique (in general not one-to-one) mapping from $\mathfrak{B}$ onto a subset $\overline{\mathfrak{B}}$ of the absolute automorphism domain $\mathfrak{A}$. The argument mentioned above reads here as follows:

If the operator domain $\mathfrak{B}$ is multiplicatively closed, then the unique mapping of $\mathfrak{B}$ onto $\overline{\mathfrak{B}}$ is multiplicatively homomorphic if and only if the associative relation corresponding to (1)

$$g(\Theta H) = (g\Theta)H \quad \text{for } g \text{ in } \mathfrak{G} \text{ and } \Theta, H \text{ in } \mathfrak{B} \tag{1a}$$

is satisfied. Correspondingly, reciprocal homomorphism is defined when left operators are involved.

For the mapping of $\mathfrak{B}$ onto $\overline{\mathfrak{B}}$ is given by $g\Theta = g\sigma$ for all g in $\mathfrak{G}$, and hence also by

$$(g\Theta)H = (g\sigma)\tau = g(\sigma\tau),$$

so that (1a) is necessary and sufficient for multiplicative homomorphy. Left operators generate reciprocal homomorphism because automorphisms written on the left, $\sigma^* g, \tau^*\sigma^* g$, must be read from right to left: $\tau^*\sigma^* g = g\sigma\tau$, whereas operators are always read from left to right.

2. Operator-homomorphic mapping. If $\mathfrak{G}$ is a group with operators, operator homomorphy is, as is known, defined by

$$(2) \quad (g\Theta)\sigma = (g\sigma)\Theta \qquad \text{respectively} \qquad (2*) \quad (\Theta g)\sigma = \Theta(g\sigma),$$

that is, by commutative connection or by the running associative law. By the argument in 1—mapping into the automorphism domain—this gives, for two different operator domains:

[5] The method is essentially reproduced in G. Köthe, *Schiefkörper unendlichen Ranges über dem Zentrum*, ğ 5, Math. Ann. 105 (1931), pp. 15–39. See also note 10. This intersection method has now been replaced by the almost trivial fact (ğ 4, 1)—first observed by van der Waerden—that the two-sided ideals are among the invariant modules. Everything can thereby be proved through the simpler direct-sum decomposition, which, however, fails for infinite rank and in the integral case.

[6] See the lecture in Prague, Jahresber. d. Deutsch. Math. Ver. 39 (1930), p. 17 (oblique pagination).

[7] The theory of crossed products was developed in the second course; with small modifications to avoid presupposing the theory given here, it is reproduced in H. Hasse, *Theory of cyclic algebras over an algebraic numberfield*, Chapter II, Transactions of the Amer. Math. Soc. 34 (1932), pp. 171–214. An account adhering more closely to the course will appear in a report by M. Deuring in the *Ergebnisse der Mathematik*.

If two operator domains $\mathfrak{B}$ *and* $\mathfrak{C}$*, with elements* $\Theta, H, \ldots$ *and* $\bar{\Theta}, \bar{H}, \ldots$*, respectively, are given, then the* $\mathfrak{C}$*-elements generate* $\mathfrak{B}$*-automorphisms and at the same time the* $\mathfrak{B}$*-elements generate* $\mathfrak{C}$*-automorphisms if and only if the domains are commutatively connected with* $\mathfrak{G}$*, or respectively the running associative law is satisfied:*

$$(2a) \quad (g\Theta)\bar{H} \;=\; (g\bar{H})\Theta, \qquad (2a*) \quad (\Theta g)\bar{H} \;=\; \Theta(g\bar{H}).$$

3. Modules and bimodules over rings. A *right module* $\mathfrak{M}$ over a ring $\mathfrak{R}$ is, as is known, defined as an additive abelian group with the elements of $\mathfrak{R}$ as right operators, where, besides the associative relation (1a) and the relation $(g+h)\Theta = g\Theta + h\Theta$ defining the operators, the distributive relation

$$(3a) \quad g(\Theta + H) \;=\; g\Theta + gH$$

is satisfied; the corresponding statement holds for left modules.

Two kinds of *bimodules* must be distinguished. Right modules over two rings $\mathfrak{R}$ and $\mathfrak{S}$ are called bimodules when, in addition to the combinations (1a, 3a) holding separately for $\mathfrak{R}$ and $\mathfrak{S}$, $\mathfrak{R}$ and $\mathfrak{S}$ are commutatively connected with $\mathfrak{M}$ by (2a). An $\mathfrak{R}$-left, $\mathfrak{S}$-right module is called a bimodule when (2a*), the running associative law, is added to the other relations.

The significance of these relations follows from the fact that, in the case of *abelian* groups, the absolute automorphism domain forms a ring, the absolute automorphism ring.[8] In detail, the mapping argument gives:

If the operator domain $\mathfrak{R}$ *of an (additively written) abelian group* $\mathfrak{M}$ *is a ring, then the unique mapping of* $\mathfrak{R}$ *onto a subset* $\overline{\mathfrak{R}}$ *of the absolute automorphism ring is ring-homomorphic if and only if* $\mathfrak{M}$ *is a right module over* $\mathfrak{R}$*—that is, satisfies (1a) and (3a)—and is reciprocally ring-homomorphic for left modules.*

If $\mathfrak{M}$ *is a right module over the rings* $\mathfrak{R}$ *and* $\mathfrak{S}$*, then* $\mathfrak{M}$ *is a bimodule—(2a)—if and only if* $\mathfrak{R}$ *can be mapped ring-homomorphically onto a subring of the* $\mathfrak{S}$*-automorphism ring and at the same time* $\mathfrak{S}$ *onto a subring of the* $\mathfrak{R}$*-automorphism ring. If* $\mathfrak{M}$ *is a right module over* $\mathfrak{S}$ *and a left module over* $\mathfrak{R}$*, then bimodule—(2a*)—means the homomorphic mapping of* $\mathfrak{S}$ *onto a subring of the* $\mathfrak{R}$*-automorphism ring and the reciprocally homomorphic mapping of* $\mathfrak{R}$ *onto a subring of the* $\mathfrak{S}$*-automorphism ring.*

The last statement gives a more precise form of familiar consequences:

1) If $\mathfrak{R}$ *is a ring with identity, then* $\mathfrak{R}$ *is directly isomorphic—not merely homomorphic—to its automorphism ring as an* $\mathfrak{R}$*-left module, and reciprocally isomorphic to its automorphism ring as an* $\mathfrak{R}$*-right module.* For the running associative law (2a*) is satisfied, so the homomorphy assertion holds. The existence of the identity gives every automorphism in the form $e \mapsto a$ with a in $\mathfrak{R}$; hence one has isomorphism, and $\mathfrak{R}$ exhausts the $\mathfrak{R}$-automorphism ring.

2) If $\mathfrak{R}$ *is a full matrix ring over a generally noncommutative field* A*,*

$$\mathfrak{R} = \sum c_{ik} A = \sum A c_{ik},$$

then A *is reciprocally isomorphic to the automorphism field of the simple right ideals, and directly isomorphic to the automorphism field of the simple left ideals.* For every simple right ideal becomes operator-isomorphic to an A-left and $\mathfrak{R}$-right module, and A exhausts the $\mathfrak{R}$-automorphisms; correspondingly for left ideals.

4. Passage from a right bimodule to a one-sided module over a product ring. The significance of the right bimodule rests essentially on this passage.

Theorem: *If* $\mathfrak{M}$ *is a right module over a ring* $\mathfrak{T}$ *which contains two elementwise commuting subrings* $\mathfrak{R}$ *and* $\mathfrak{S}$*, then* $\mathfrak{M}$ *may also be regarded as a bimodule over* $\mathfrak{R}$ *and* $\mathfrak{S}$*. Conversely, if a bimodule over* $\mathfrak{R}$ *and* $\mathfrak{S}$ *is given and there exists a product ring* $\mathfrak{T}$ *in which* $\mathfrak{R}$ *and* $\mathfrak{S}$ *commute elementwise, then* $\mathfrak{M}$ *may also be regarded as a right module over* $\mathfrak{T}$*, in such a way that the operation by* $\mathfrak{T}$ *extends the given operations by* $\mathfrak{R}$ *and* $\mathfrak{S}$*.*

The first assertion follows because $\mathfrak{T}$, by definition, can be mapped homomorphically onto a subring $\overline{\mathfrak{T}}$ of the absolute automorphism ring, with $\mathfrak{R}, \mathfrak{S}$ going over into elementwise commuting subrings $\overline{\mathfrak{R}}, \overline{\mathfrak{S}}$. But this is precisely the relation (2a) characterizing the bimodule.

Conversely, suppose that $\mathfrak{M}$ is given as an $\mathfrak{R}, \mathfrak{S}$-bimodule (right module). Again $\mathfrak{R}, \mathfrak{S}$ can be mapped homomorphically onto elementwise commuting subrings $\overline{\mathfrak{R}}, \overline{\mathfrak{S}}$ of the absolute automorphism ring. In the absolute automorphism ring there exists for $\overline{\mathfrak{R}}, \overline{\mathfrak{S}}$ the product ring[9] $\overline{\mathfrak{T}}$, which, because of elementwise com-

[8] For nonabelian groups one has a "generalized" ring; see a paper by H. Fitting to appear in Math. Annalen. [Math. Annalen 107, pp. 514–542.]

[9] Thus "product ring" means only the ring generated by two rings with a common overring; the product need not be direct. That a product ring need not always exist when an intersection is prescribed is shown by the following example. Let $\mathfrak{o}$ be the ring of integers, and set $\mathfrak{R} = \mathfrak{o}[x]$, $\mathfrak{S} = \mathfrak{o}[y]$, with $2x - 1 = 0$, $2y - 1 = 0$, so that $\mathfrak{o}$ is the intersection of $\mathfrak{R}$ and $\mathfrak{S}$ if no relation between x and y is imposed. But if $\mathfrak{R}$ and $\mathfrak{S}$ lie in a common overring, then $(2x-1)y - x(2y-1) = 0$, hence $x = y$. Thus there is no product ring with intersection $\mathfrak{o}$.

mutativity, consists of all elements of the form

$$\sum \bar{r}_i \bar{s}_i + \bar{r} + \bar{s}$$

(if $\overline{\mathfrak{R}}, \overline{\mathfrak{S}}$ have identities, the extra terms $\bar{r}, \bar{s}$ disappear). If there also exists a product ring $\mathfrak{T}$ in which $\mathfrak{R}$ and $\mathfrak{S}$ commute elementwise, then it correspondingly consists of all elements of the form $\sum r_i s_i + r + s$. The homomorphisms

$$\mathfrak{R} \to \overline{\mathfrak{R}}, \qquad \mathfrak{S} \to \overline{\mathfrak{S}}$$

can therefore be extended by the correspondence

$$\sum r_i s_i + r + s \longmapsto \sum \bar{r}_i \bar{s}_i + \bar{r} + \bar{s}$$

to a homomorphism $\mathfrak{T} \to \overline{\mathfrak{T}}$. Thus the operation

$$m\Big(\sum r_i s_i + r + s\Big) = \sum (m r_i) s_i + mr + ms$$

is unambiguous and, by ğ 1, 3, defines a $\mathfrak{T}$-module containing the given $\mathfrak{R}, \mathfrak{S}$-module.

ğ 2.
Reciprocal and Direct Representation.

1. Modules of linear forms. The passage from the theory developed in ğ 1 to representation theory rests on specializing the modules there to modules of linear forms and considering their automorphism rings.

An $\mathfrak{S}$-right module $\mathfrak{M}$, where $\mathfrak{S}$ is a ring with identity, is called a module of linear forms in $\mathfrak{S}$ if $\mathfrak{M}$ is a direct sum of n one-term $\mathfrak{S}$-modules, $\mathfrak{M} = m_1\mathfrak{S} + \cdots + m_n\mathfrak{S}$, in such a way that $m_i\mathfrak{S}$ is operator-isomorphic to $\mathfrak{S}$, so that $m_i s = 0$ always implies $s = 0$. It follows that $\mathfrak{S}$ can be mapped not merely homomorphically but isomorphically onto a subring of the absolute automorphism ring.

Theorem 1. *If $\mathfrak{M}$ is a module of linear forms in $\mathfrak{S}$, then the $\mathfrak{S}$-automorphism ring $\mathfrak{A}$ of $\mathfrak{M}$ is reciprocally isomorphic—not merely homomorphic—to the ring $\overline{\mathfrak{A}}$ of all n-rowed matrices in $\mathfrak{S}$.*

An arbitrary $\mathfrak{S}$-automorphism α of $\mathfrak{M}$ is completely described by the correspondence $m_i \longmapsto \overline{m}_i = m_i\alpha$; for from this it follows by definition that

$$\sum m_i s_i \longmapsto \sum \overline{m}_i s_i = \sum (m_i\alpha) s_i = \sum (m_i s_i)\alpha.$$

If, in matrix notation,

$$(m_1\alpha, \ldots, m_n\alpha) = (m_1, \ldots, m_n)A,$$

then, as α runs through all automorphisms, the correspondence $\alpha \mapsto A$ gives a one-to-one relation between $\mathfrak{A}$ and $\overline{\mathfrak{A}}$. For since $\mathfrak{M}$ was assumed to be a module of linear forms, A is uniquely determined by α, and every matrix A of degree n in $\mathfrak{S}$ generates an automorphism. Moreover,

$$\alpha + \beta \mapsto A + B, \qquad \alpha\beta \mapsto BA.$$

The latter follows from

$$(m_1\alpha\beta, \ldots, m_n\alpha\beta) = (m_1, \ldots, m_n)A\beta = (m_1, \ldots, m_n)\beta A \quad [\text{since } ms\beta = m\beta s] = (m_1, \ldots, m_n)BA.$$

2. Representation and representation module. If by a reciprocal or direct representation of degree n of the ring $\mathfrak{R}$ in $\mathfrak{S}$ one means a reciprocal or direct ring homomorphism of $\mathfrak{R}$ into a subring of the ring of all n-rowed matrices in $\mathfrak{S}$, then Theorem 1 may also be stated as follows:

Theorem 1'. *The automorphism ring $\mathfrak{A}$ of a module of linear forms of degree n in $\mathfrak{S}$ admits an isomorphic (faithful) reciprocal representation by the full matrix ring $\overline{\mathfrak{A}}$ of all n-rowed matrices in $\mathfrak{S}$.*

From this point, the theorems customary for direct representations follow also for reciprocal ones.

Definition. A module of linear forms $\mathfrak{M}$ in $\mathfrak{S}$ is called a reciprocal representation module of $\mathfrak{R}$ in $\mathfrak{S}$ if $\mathfrak{M}$ is a bimodule over $\mathfrak{R}$ and $\mathfrak{S}$ and at the same time a right module over both $\mathfrak{R}$ and $\mathfrak{S}$; it is called a direct representation module if $\mathfrak{M}$ is a bimodule and at the same time an $\mathfrak{R}$-left and $\mathfrak{S}$-right module.

Theorem 2. *Every reciprocal or direct representation module generates a class of equivalent reciprocal or direct representations of $\mathfrak{R}$ in $\mathfrak{S}$, respectively, and all reciprocal or direct representations are generated in this way.*

First let $\mathfrak{M}$ be a reciprocal representation module. By ğ 1, 3, $\mathfrak{R}$ can then be mapped directly homomorphically onto a subring $\overline{\mathfrak{R}}$ of the $\mathfrak{S}$-automorphism ring of $\mathfrak{M}$; by ğ 2, Theorem 1', $\overline{\mathfrak{R}}$ admits a reciprocal (faithful) representation, which is therefore also a reciprocal representation of $\mathfrak{R}$. Conversely, if a reciprocal representation $\mathfrak{R} \to \mathfrak{R}^*$ is given, then, composed with the reciprocal isomorphism from $\mathfrak{R}^*$ to a subring $\overline{\mathfrak{R}}$ of the $\mathfrak{S}$-automorphism ring, it gives a direct homomorphism of $\mathfrak{R}$ onto $\overline{\mathfrak{R}}$. Thus $\mathfrak{M}$ becomes an $\mathfrak{R}$-module, and indeed a bimodule, hence a representation module by ğ 1, 3. Passage to other $\mathfrak{S}$-bases gives the class of equivalent representations.

For a direct representation module, $\mathfrak{R}$ is mapped reciprocally homomorphically onto $\overline{\mathfrak{R}}$. Composition with the reciprocal representation of $\overline{\mathfrak{R}}$ therefore gives a direct representation of $\mathfrak{R}$. Conversely, a direct representation gives a reciprocally homomorphic mapping onto $\overline{\mathfrak{R}}$; thereafter $\mathfrak{M}$ becomes a direct representation module by ğ 1, 3.

Remark. The two kinds of representations can of course be reduced to one another: a direct representation of $\mathfrak{R}$ is a reciprocal representation of the ring reciprocal to $\mathfrak{R}$, and conversely. Another reduction consists in passing from $\mathfrak{S}$ to a reciprocal ring and replacing the matrices by their transposes. This corresponds to passing from an $\mathfrak{R}$-left, $\mathfrak{S}$-right module to a module which is left over both $\mathfrak{R}$ and $\mathfrak{S}$.

3. Passage from a reciprocal representation module to a module over an extension ring. The advantage of the reciprocal representation module rests above all on the passage to the extension ring made possible by ğ 1, 4. In the present special case—$\mathfrak{M}$ a module of linear forms over $\mathfrak{S}$—this is the transition theorem for representation modules:

If $\mathfrak{M}$ is a right module over a ring $\mathfrak{T}$ which contains two elementwise commuting subrings $\mathfrak{R}$ and $\mathfrak{S}$, in such a way that $\mathfrak{M}$ becomes a module of linear forms over $\mathfrak{S}$, then $\mathfrak{M}$ may also be regarded as a reciprocal representation module of $\mathfrak{R}$ in $\mathfrak{S}$.

Conversely, if a reciprocal representation module of $\mathfrak{R}$ in $\mathfrak{S}$ is given and there exists a product ring $\mathfrak{T}$ in which $\mathfrak{R}$ and $\mathfrak{S}$ commute elementwise, then $\mathfrak{M}$ may also be regarded as a $\mathfrak{T}$-module in such a way that the $\mathfrak{T}$-operation extends the given $\mathfrak{R},\mathfrak{S}$-operation.

The following is used essentially in representation theory:

Corollary of the transition theorem for representation modules.
If $\mathfrak{M}$ is a reciprocal representation module of $\mathfrak{R}$ in $\mathfrak{S}$, and at the same time a $\mathfrak{T}$-module with $\mathfrak{T}$ as product ring, then $\mathfrak{R},\mathfrak{S}$-isomorphism of $\mathfrak{M}$ to a module $\mathfrak{N}$ is equivalent to $\mathfrak{T}$-isomorphism. *Thus each class of isomorphic $\mathfrak{T}$-modules corresponds to a reciprocal representation class of $\mathfrak{R}$ in $\mathfrak{S}$, and conversely.*

Combining these theorems with ğ 1, 2 and 3 gives the relation fundamental for what follows between the matrices commuting with a representation and the $\mathfrak{R},\mathfrak{S}$-automorphisms.

Theorem on commuting matrices.
If $\mathfrak{R} \to \mathfrak{R}^*$ is a reciprocal representation of degree n of $\mathfrak{R}$ in $\mathfrak{S}$, and if $\mathfrak{B}^*$ denotes the ring of all matrices of degree n in $\mathfrak{S}$ which commute elementwise with $\mathfrak{R}^*$, then $\mathfrak{B}^*$ gives a reciprocally isomorphic representation of the $\mathfrak{R},\mathfrak{S}$-automorphisms—that is, those $\mathfrak{S}$-automorphisms which are also $\mathfrak{R}$-automorphisms—of the generating representation module, or, if the product ring $\mathfrak{T}$ exists, of the $\mathfrak{T}$-automorphisms.

Let $\mathfrak{B}$ be the ring of all $\mathfrak{R},\mathfrak{S}$-automorphisms of $\mathfrak{M}$. As a subring of the $\mathfrak{S}$-automorphism ring $\mathfrak{A}$, $\mathfrak{B}$ admits a reciprocally isomorphic representation in $\mathfrak{S}$. By ğ 1, 2 and 3, $\mathfrak{B}$ consists of all those automorphisms in $\mathfrak{A}$ which are commutatively connected with $\mathfrak{R}$, hence satisfy relation (2a). Thus $\mathfrak{B}$ consists of the totality of automorphisms which commute elementwise with those in $\overline{\mathfrak{R}}$, where $\overline{\mathfrak{R}}$ denotes the image of $\mathfrak{R}$ in $\mathfrak{A}$. Since the representation of $\mathfrak{B}$ and $\overline{\mathfrak{R}}$ is a reciprocal isomorphism, not merely a homomorphism, this is the assertion to be proved.

Remark. The $\mathfrak{R},\mathfrak{S}$-automorphisms mean a correspondence $m_i \mapsto m_i'$ such that the same representation $\mathfrak{R}^*$ arises through the m_i'. The m_i' need not necessarily give an $\mathfrak{S}$-basis of $\mathfrak{M}$, corresponding to the fact that the matrices in $\mathfrak{B}^*$ need not be invertible. If the sum $\sum m_i'\mathfrak{S}$ is no longer direct, "representation" is to be understood in an extended sense:

$$(m_1', m_2', \ldots, m_n')a = (m_1', \ldots, m_n')A$$

remains correct, but A is no longer uniquely determined by a.

A further remark concerning the transition theorem is the following. The diagonal matrices $E \cdot s$ give a *directly isomorphic* representation of $\mathfrak{S}$, the "identity" representation of $\mathfrak{S}$. That this is a *direct* isomorphism follows because the $\mathfrak{S}$-automorphism ring of $\mathfrak{M}$ has a subring reciprocally isomorphic to $\mathfrak{S}$, whose reciprocal representation is in question. For every one-term summand $m_i\mathfrak{S}$ of $\mathfrak{M}$ is operator-isomorphic to $\mathfrak{S}$ as a right module, and hence its $\mathfrak{S}$-automorphism ring is reciprocally isomorphic to $\mathfrak{S}$ (ğ 1, 3, Corollary 1).

The correspondence from $\mathfrak{T}$ to matrices in $\mathfrak{S}$, uniquely defined by $\mathfrak{R}$ and $\mathfrak{S}$, is therefore *not a representation*

of the ring $\mathfrak{T}$, but the extension of the reciprocal representation of $\mathfrak{R}$ to one operator-homomorphic over $\mathfrak{S}$: $\sum r_i s_i \longmapsto \sum R_i s_i$. In particular, the reciprocal representation of $\mathfrak{R}$ is *operator-homomorphic with respect to the intersection $[\mathfrak{R}, \mathfrak{S}]$ of $\mathfrak{R}$ and $\mathfrak{S}$, which lies in the center of $\mathfrak{R}$.*

ğ 3.

Modules with Respect to a Field.

In what follows only representations in generally noncommutative fields will be involved; we therefore collect a few simple propositions on modules of linear forms over a field.

1. Normal basis of a submodule with respect to a given basis of the full module.—Let A be a field, and let $\mathfrak{N} = x_1 A + \cdots + x_n A$ be a module of linear forms of rank n; further, let $\mathfrak{L} = z_1 A + \cdots + z_\ell A$ be a submodule of rank $\ell \leq n$. *The z_i are called a normal basis with respect to x if they are of the form*

$$z_i = x_i - (x_{\ell+1}\alpha_{i,\ell+1} + \cdots + x_n \alpha_{i,n}), \qquad (i = 1, \ldots, \ell).$$

Every module $\mathfrak{L}$ has, after a suitable numbering of the x, a normal basis.

For, after a suitable numbering,

$$\mathfrak{N} = \mathfrak{L} + x_{\ell+1} A + \cdots + x_n A,$$

and hence

$$x_i \equiv x_{\ell+1}\alpha_{i,\ell+1} + \cdots + x_n \alpha_{i,n} \quad (\mathfrak{L}) \qquad (i = 1, \ldots, \ell). \tag{2}$$

Thus the ℓ elements $z_i = x_i - (x_{\ell+1}\alpha_{i,\ell+1} + \cdots)$ lie in $\mathfrak{L}$ and exhaust $\mathfrak{L}$, since together with $x_{\ell+1}, \ldots, x_n$ they form a basis of $\mathfrak{N}$.

2. Extension module. Let A again be a field and P a subfield. An A-module $\mathfrak{N}$ of rank n is called an *extension module* of a P-module $\mathfrak{M}$, written $\mathfrak{N} = \mathfrak{M}_A$, if $\mathfrak{M}$ is a submodule of $\mathfrak{N}$ of the *same rank*. If $\mathfrak{M} = y_1 P + \cdots + y_n P$, then $\mathfrak{N} = \mathfrak{M}_A = y_1 A + \cdots + y_n A$. Conversely, for every P-module $\mathfrak{M} = y_1 P + \cdots + y_n P$, the extension module $\mathfrak{M}_A$ exists uniquely up to module isomorphism. For the module $\overline{y}_1 A + \cdots + \overline{y}_n A$ contains a submodule $\overline{\mathfrak{M}}$ isomorphic to $\mathfrak{M}$, which can be identified with $\mathfrak{M}$.

Corollary a). If $z_1, \ldots, z_t$ are elements of $\mathfrak{M}$ linearly independent over P, then they are also linearly independent over A in $\mathfrak{N} = \mathfrak{M}_A$ (for they can be completed to a basis of $\mathfrak{M}$, and hence of $\mathfrak{N}$). Thus every P-module $\mathfrak{T} = z_1 P + \cdots + z_t P$ in $\mathfrak{M}$ generates an extension module $\mathfrak{T}_A = z_1 A + \cdots + z_t A$ in $\mathfrak{M}_A$.

Corollary b). Every P-module $\mathfrak{T} = z_1 P + \cdots + z_t P$ in $\mathfrak{M}$ is a contraction module, that is, the intersection of its extension module $\mathfrak{T}_A$ with $\mathfrak{M}$: $\mathfrak{T} = \mathfrak{T}_A \cap \mathfrak{M}$. For $\mathfrak{T} \subseteq \mathfrak{T}_A \cap \mathfrak{M}$. Conversely, if a lies in $\mathfrak{T}_A \cap \mathfrak{M}$, then $a = \sum z_i \alpha_i$, so the $\mathfrak{M}$-elements $a, z_1, \ldots, z_t$ are dependent over A, and hence [Corollary a)] also over P; thus a lies in $\mathfrak{T}$.

3. Theorem on invariant modules. Let $\mathfrak{N} = \mathfrak{M}_A$ again be the extension module of a P-module $\mathfrak{M}$ of rank n, and let P be the full invariant field with respect to a group $\mathfrak{G}$ of ring automorphisms of A. The group $\mathfrak{G}$ is defined as an operator domain of $\mathfrak{N} = \mathfrak{M}_A$ by setting

$$G \cdot m = m \quad \text{for } m \text{ in } \mathfrak{M} \text{ and } G \text{ in } \mathfrak{G},$$

and

$$G \cdot \sum m_i \alpha_i = \sum m_i \, G(\alpha_i) \quad \text{for } m \text{ in } \mathfrak{M} \text{ and } \alpha \text{ in } A.$$

Lemma. *Under these definitions, $\mathfrak{M}$ consists of all elements of $\mathfrak{N}$ fixed by $\mathfrak{G}$.* For if $x_1, \ldots, x_n$ is a P-basis of $\mathfrak{M}$, and thus $w = x_1\alpha_1 + \cdots + x_n\alpha_n$, then $G(w) = w$ for every G in $\mathfrak{G}$ implies $G(\alpha_i) = \alpha_i$, and therefore, by assumption, α_i lies in P.

Theorem. *The extension modules $\mathfrak{L}_A$ of the submodules $\mathfrak{L}$ of $\mathfrak{M}$, and only these, are admissible submodules with respect to $\mathfrak{G}$ as operator domain.*

The first half is clear. Conversely, let $\mathfrak{L}$ be admissible with respect to $\mathfrak{G}$, and let $z_1, \ldots, z_\ell$ be a normal basis of $\mathfrak{L}$ (see 1) with respect to x, where x is chosen as a P-basis of $\mathfrak{M}$, hence is fixed elementwise by $\mathfrak{G}$. By assumption,

$$G(z_i) = x_i - \left(x_{\ell+1} G(\alpha_{i,\ell+1}) + \cdots + x_n G(\alpha_{i,n})\right)$$

is an element of $\mathfrak{L}$ for every G in $\mathfrak{G}$, hence for fixed G is linearly expressible in terms of the z. Comparison of coefficients in $x_1, \ldots, x_\ell$ therefore gives $G(z_i) = z_i$ for every G in $\mathfrak{G}$. Thus, by the lemma, the z lie in $\mathfrak{M}$, and $\mathfrak{L}$ is the *extension* of the P-module $\mathfrak{T} = z_1 P + \cdots + z_\ell P$ in $\mathfrak{M}$, where $\mathfrak{T} = \mathfrak{L} \cap \mathfrak{M}$ (by 2).[10]

[10] The propositions of this section remain valid, by simple well-ordering arguments, even when the rank of $\mathfrak{M}$ over P is infinite; see G. Köthe, *Ein Beitrag zur Theorie der kommutativen Ringe ohne Endlichkeitsvoraussetzung*, ğ 1, Gött. Nachr. 1931, pp. 195–207.

ğ4. Hypercomplex Systems and Their Representation Classes

1. Extension theorem. We now combine the representation theorems of ğ2 with the module theorems of ğ3. Instead of arbitrary rings $\mathfrak{R}$, we consider hypercomplex systems with identity $S, T, \ldots$ over a commutative field P:

$$S = x_1 P + \cdots + x_n P.$$

Instead of arbitrary representation rings $\mathfrak{S}$, we consider only fields $A, B, \ldots$, unless otherwise stated with center P. In this case there always exists the product ring in which S and A commute elementwise, with intersection P; this is the direct product $S \times A$, which is at the same time the extension module S_A of S:

$$S_A = x_1 A + \cdots + x_n A.$$

It will therefore also be called the extension ring.

Under this specialization, the theorem on invariant modules becomes:

Extension theorem. Every two-sided ideal of S_A is the extension ideal of an ideal of S, namely the extension of its intersection with S.

Indeed, let the chosen group $\mathfrak{G}$ be the group of inner automorphisms of A. Then P, as center of A, is the full invariant field, while the elementwise commutativity of A with S says that $\mathfrak{G}$ is extended to S_A so that S is the full invariant domain. Every two-sided ideal $\mathfrak{a}$ of S_A is an admissible subgroup, since $\alpha^{-1}\mathfrak{a}\alpha \subseteq \mathfrak{a}$, and so it is the extension of its intersection module $\mathfrak{a} \cap S$, which is an ideal in S.

Addendum: If S is commutative, then S is the center of S_A. More generally, the center of S is also the center of S_A. By $A_r, B_n, \ldots$ we shall always mean matrix rings of the indicated degree over $A, B, \ldots$:

$$A_r = \sum A c_{ik} = \sum c_{ik} A.$$

We shall use essentially the extension theorem for simple systems (where, as usual, "simple" means two-sided simple):

If S is simple, then S_A is also simple:

$$S_A = \sum B c_{ik} = \sum c_{ik} B = B_t,$$

with associated field B, whose center contains P. Here A, and hence B, may have infinite rank over P; only S is assumed hypercomplex. If S and A have common center P, then P is also the center of S_A. More generally, if S is a simple hypercomplex system, then the direct product $S \times A_r$ is simple. Indeed, $S \times A_r$ agrees with $S_A \times P_r$, and is therefore B_{tr} when $S_A = B_t$.

2. Representation classes. By a reciprocal or direct representation of a hypercomplex system we mean, as usual, a representation not equal to the zero representation and operator-homomorphic with respect to the coefficient field P.

Theorem on representation classes. Let S be hypercomplex with identity and coefficient field P, and let A be a field with center P. Then the number of distinct irreducible reciprocal representation classes of S in A is equal to the number of classes of simple right ideals in the quotient ring of S_A by its radical. If S is a simple system, then it has exactly one irreducible reciprocal and one irreducible direct representation class in A.[11]

By the corollary to the transition theorem, the simple reciprocal representation classes and the simple module classes over S_A correspond one-to-one. Since S_A has finite rank over the field A, it satisfies the maximum and minimum conditions for one-sided ideals. If S is simple, then S_A is simple; hence there is only one simple one-sided ideal class, and so only one irreducible reciprocal representation class. The reciprocal system gives the corresponding assertion for direct representations.

[11] Cf. the representation theory, note 20, for the case in which A is the associated automorphism field of S.

3. Rank relation. If S is simple and

$$S_A = \sum Bc_{ik}$$

has finite rank both over A and over B, then

$$n = rt, \qquad n = (S : P), \qquad t^2 = (S_A : B), \tag{1}$$

where r is the degree of the irreducible reciprocal representation.

Indeed, S_A is itself a reciprocal representation module for S in A (the representation already lies in P). As a matrix ring over B, the ring S_A decomposes into t simple right ideals, hence into S_A-modules, whose rank over A is the degree r of the irreducible reciprocal representation. Since n is also the rank of S_A over A, the rank relation follows.

4. Sharpening of the rank relation when A has finite rank over P. In this case the three relations are

$$(S : P) = n = rt, \tag{1}$$

$$(B : P)\, t = (A : P)\, r, \tag{2}$$

$$(S : P)(B : P) = (A : P)\, r^2. \tag{3}$$

Here (2) denotes the rank over P of a simple right ideal of S_A, expressed by the ranks over B and A; (3) expresses the rank of a simple right ideal in a matrix ring over B, and follows from (2) by multiplying by r, using (1).

ğ5. Application of the Representation Theorems to Matrix Rings

The reciprocal representation of S in A considered in ğ4 can also be regarded as a direct homomorphism of S into a subring of A_r, where $\overline{A}$ denotes the field reciprocally isomorphic to A. The principle of the following paragraphs is the converse one: to reduce the investigation of matrix rings A_r to representation theory in the reciprocally isomorphic field A.

1. Reducible and irreducible embedding in A_r. Let A and $\overline{A}$ be reciprocally isomorphic fields, of finite or infinite rank over their center P.[12] The simple system S over P is called irreducibly, respectively reducibly, embeddable in A_f if S has an irreducible, respectively reducible, reciprocal representation of degree f in A. If S is irreducibly embeddable in A_r, then it is reducibly embeddable in all matrix rings A_{rs}, $s > 1$, since it has reducible representations of precisely those degrees. The isomorphism always extends the identity of P;[13] by ğ4, 3, r divides the rank n of S over P.

In this way one obtains all simple subrings containing P, of finite rank over P, in the various A_r. For every such subring is reciprocally isomorphic to a subring of $\overline{A}_r$ and therefore has a reducible or irreducible reciprocal representation in A.

2. Theorem on inner automorphisms. Let $S^{(1)}$ and $S^{(2)}$ be two simple subrings of A_f containing P, of finite rank over P. If $S^{(1)}$ and $S^{(2)}$ are isomorphic over P, then this isomorphism is induced by an inner automorphism of A_f.

Indeed, $S^{(1)}$ and $S^{(2)}$ give generally reducible embeddings of a simple system S in A_f, hence direct representations of degree f in A. They belong to the same reducible direct representation class; the transforming matrix induces the automorphism. If A itself has finite rank over P, so that it is hypercomplex, this becomes the familiar theorem: two simple subsystems of A_f containing the center P, and isomorphic over P, are carried into one another by an inner automorphism of A_f. In particular, every automorphism of A_f is inner.[14]

[12] Reciprocal fields or systems are denoted throughout by corresponding Greek and Latin letters.

[13] As with representations, all isomorphisms used below are understood to extend the identity of P, without this being repeated each time.

[14] The latter assertion no longer holds when A has infinite rank over P; cf. Köthe, in the work cited in note 5.

3. Theorem on elementwise commuting subrings. Let S be a simple system contained in A_f and containing P, and let R be the totality of all elements of A_f which commute elementwise with S. Then R is also a matrix ring:

$$R = \overline{B}_s.$$

The associated fields B of S_A and $\overline{B}$ of R are reciprocally isomorphic. The intersection of R and S is the center of S. The ring R is a field if and only if S is irreducibly embedded in A_f.

By ğ2, 3, the ring R is directly isomorphic to the automorphism ring of the reciprocal representation module $\mathfrak{M}$ of S in A. This is the automorphism ring of $\mathfrak{M}$, regarded as an S_A-module. If $\mathfrak{M}$ decomposes into s simple S_A-modules and one writes, as in ğ4, 1,

$$S_A = \sum Bc_{ik},$$

then R is isomorphic to $\sum \overline{B}c_{ik}$, where B and $\overline{B}$ are reciprocally isomorphic. Thus $R = \overline{B}$ is a field precisely when $s = 1$, i.e. when S is irreducibly embedded. By definition, $R \cap S$ is the center of S.

4. Sharpened commutation theorem for hypercomplex matrix rings. In this case the rank relations of ğ4, 4 give the sharpening:

The simple subsystems of A_f which contain P, where A has finite rank over its center P, split into pairs $S, \overline{S}$, such that $\overline{S}$ consists exactly of all elements which commute elementwise with S, and conversely. The associated fields of S_A and $\overline{S}$ are reciprocally isomorphic, as are those of S and $\overline{S}_A$. The intersection of S and $\overline{S}$ is the common center. One subring is a field if and only if the other is irreducibly embedded. The product of the ranks over P of S and $\overline{S}$ is the rank of A_f.

If $f = rs = \overline{r}\,\overline{s}$, where S is irreducibly embeddable in A_r and $\overline{S}$ in $A_{\overline{r}}$, then the associated fields of S and $\overline{S}$ become isomorphic to a pair of commuting subrings of A_g, with $f = gs\overline{s}$.

The product assertion follows directly from the rank relation. If S is irreducibly embedded, then $\overline{S}$ is a field and is reciprocally isomorphic to B, where $S_A = B_t$; the rank relation (3) of ğ4, 4 gives the assertion. If S is reducibly embedded, so $\overline{S} = \overline{B}_s$, then $f = rs$, and multiplying (3) by s^2 gives the assertion. This also shows that S is precisely the totality of the elements commuting elementwise with $\overline{S}$, and the remaining assertions follow from the theorem on commuting subrings. For the final assertion, pass twice to an irreducible embedding: in A_r, S and a system R isomorphic to B commute elementwise; reciprocity gives $S = \overline{B}_s$, so R embeds irreducibly in A_g with $r = g\overline{s}$. The commuting pair is therefore isomorphic to $B, \overline{B}$.

ğ6. Galois Theory of Simple Systems

The sharpened commutation theorem of ğ5, 4 expresses the Galois theory of simple systems with respect to the center as ground domain. We consider first division rings, and then simple systems in general.

1. Galois theory of division rings of finite rank over the center. The Galois group $\mathfrak{G}$ of A is defined as the group of all automorphisms extending the identity of the center P, hence, by ğ5, 2, as the group of all inner automorphisms. Thus

$$\mathfrak{G} \simeq A^*/P^*,$$

where A^* and P^* denote the multiplicative groups of nonzero elements of A and P. Subgroups $\mathfrak{H}$ of $\mathfrak{G}$ therefore correspond one-to-one to subgroups H^* of A^* containing P^*, by

$$\mathfrak{H} \sim H^*/P^*.$$

A subgroup $\mathfrak{H}$ of $\mathfrak{G}$ is called closed if, after adjoining zero, H^* becomes a division ring H. The fact that C admits the group $\mathfrak{H}$ is equivalent to saying that C commutes elementwise with H. Hence the commutation theorem of ğ5, 4 becomes the following.

Main theorem of the Galois theory of noncommutative division rings. The division rings C between P and A and the closed subgroups $\mathfrak{H}$ of $\mathfrak{G}$ correspond bijectively in such a way that C is the full invariant division ring of $\mathfrak{H}$, and $\mathfrak{H}$ is the full invariant group of C.

2. Galois theory of simple systems. If A_f is a simple system with center P, the Galois group $\mathfrak{G}$ is again the group of inner automorphisms, hence isomorphic to

$$A_f^*/P^*,$$

where now A_f^* denotes the multiplicative group of the regular elements of A_f. A subgroup $\mathfrak{H} \sim H^*/P^*$ of $\mathfrak{G}$ is called simple-closed if the subring H generated by H^* is a simple system and if H^* is the set of all regular elements of H. The passage from the commutation theorem to Galois theory is supplied by the following lemma.

Lemma. Every simple system in A_f containing P is generated by the group H^* of its regular elements. This is clear if P has infinitely many elements: the "general element" formed with indeterminates is regular, and by suitable specialization one obtains regular basis elements over P. The lemma holds in general by Shoda.[15]

By the lemma, commutation of S with a simple system $\overline{S}$ is again equivalent to saying that S admits the automorphisms induced by the regular elements of $\overline{S}$. Thus the commutation theorem of ğ5, 4 becomes also here the following.

Main theorem of the Galois theory of simple systems. The simple systems S in A_f containing P and the simple-closed subgroups $\mathfrak{H}$ of $\mathfrak{G}$ correspond bijectively in such a way that S is the full invariant domain of $\mathfrak{H}$, and $\mathfrak{H}$ is the full invariant group of S.

3. Proof by means of the extension principle. For the case of a division ring I give a second proof of the main theorem. It rests on the principle of extending isomorphisms, i.e. representations of first degree, and since it uses no count of ranks it makes fewer finiteness assumptions. In particular it shows in what direction a transfer to division rings S of infinite rank will be possible. The proof also does not use the fact that there is only one irreducible reciprocal representation class; it therefore applies exactly in the same way in the commutative case, ğ8, 2. I first state some lemmas.

Hypotheses. The simple system S over P is to admit a reciprocal representation of first degree in A, and is therefore a division ring. Here A may have finite or infinite rank over its center P. A decomposition of S_A into n simple operator-isomorphic right ideals, as in ğ4, 3, is given by

$$S_A = r_1 + \cdots + r_n = e_1 S_A + \cdots + e_n S_A = e_1 A + \cdots + e_n A;$$

the reciprocal representation generated by e_i is therefore defined by

$$e_i s = e_i \sigma.$$

Lemma 1. The n reciprocal representations generated by $e_1, \ldots, e_n$ are distinct, hence are distinct representations of the same representation class. Thus S has at least as many distinct representations as its rank.

To prove this, we extend the representations from S, as at the end of ğ2, to correspondences of S_A which are operator-homomorphic over A. Here these correspondences are defined by

$$e_i w = e_i \omega$$

with $\omega \in A$, for each $w \in S_A$. If e_i and e_j, $i \neq j$, generated the same representation, one would have $e_i w = e_j w$ for every $w \in S_A$. This is impossible because $e_i e_i = e_i$ and $e_j e_i = 0$.

Lemma 2. Let T be a division ring between P and S, and let s be the rank of S over T. Then every reciprocal isomorphism of T into A admits at least s different extensions.

Let the reciprocal isomorphism, i.e. the reciprocal representation of T in A, be mediated by a decomposition

$$T_A = E_1 T_A + \cdots + E_h T_A = E_1 A + \cdots + E_h A, \qquad E_i t = E_i \tau,$$

[15] Shoda, work cited in note 3); there the introduction of indeterminates is avoided.

where the E_i are idempotents. This is no restriction, since a representation generated by a basis element $E_i\alpha$ is also generated by $\alpha^{-1}E_i\alpha$, hence by an idempotent. Right multiplication by S gives

$$S_A = E_1 S_A + \cdots + E_h S_A.$$

The $E_i S_A$ all have rank s over A. Indeed the rank of $E_i S_A$ is at most s, as follows by substituting a T-basis into S, using the commutativity of S and A:

$$S = Tw_1 + \cdots + Tw_s,$$

$$E_i S_A = E_i T_A w_1 + \cdots + E_i T_A w_s = E_i w_1 A + \cdots + E_i w_s A.$$

Since the sum S_A has rank $n = hs$, every $E_i S_A$ has exactly rank s. Thus

$$E_i S_A = r_{i1} + \cdots + r_{is} = e_{i1}A + \cdots + e_{is}A,$$

where the s representations generated by $e_{i1}, \ldots, e_{is}$ are all distinct by Lemma 1. They are all extensions of the representation of T generated by E_i, since $E_i t = E_i \tau$ implies

$$(e_{i1} + \cdots + e_{is})t = (e_{i1} + \cdots + e_{is})\tau$$

and hence $e_{ij}t = e_{ij}\tau$, by the direct decomposition.

Definition. The partition $\mathfrak{I}_T$ of the reciprocal isomorphisms $\mathfrak{I}$ from S into A, induced by T, is defined as follows: precisely those isomorphisms in $\mathfrak{I}$ are regarded as equivalent which induce the same isomorphism on T.

Main theorem. If $\mathfrak{I}_T$ is the partition induced by T, then T is a maximal subfield relative to this partition.

For if L is an intermediate division ring between T and S, of degree l over T, then by Lemma 2 every class of $\mathfrak{I}_T$ splits into at least l classes of $\mathfrak{I}_L$. The transition from this form of the theorem to the usual one arises by multiplying the elements of the set $\mathfrak{I}$ by the inverse of any fixed one of them; the set then becomes the automorphism group, and a class in $\mathfrak{I}_T$ becomes the invariant group of T. The statement that closed subgroups are full invariant groups is included in this: for $\mathfrak{H} \sim H^*/P^*$, one simply puts the division ring H in place of the intermediate division ring T.

ğ7. The Class of Similar Algebras. Splitting Fields

From now on only division rings $A, \overline{A}$ and matrix rings A_r of finite rank over their center P will occur. Thus they are simple normal algebras over P, and will be called algebras over P, or simply algebras; $A, \overline{A}$ are then division algebras. All matrix rings A_r with the same associated A are collected into one class of similar algebras, $A_r \sim A_s$. Isomorphic A's are identified.

1. The group of algebra classes. If A_r, B_s are algebras over P, then the same is true of their product, the direct product over P; for by the end of ğ3,

$$A_r \times B_s = C_t,$$

where C is a uniquely determined, up to isomorphism, division algebra with center P. Multiplication of A_r, B_s by matrix rings over P shows that this multiplication is uniquely determined for the classes, which therefore form a multiplicatively closed, commutative system. Moreover R. Brauer's theorem holds: the classes of similar algebras form an abelian group under direct product. The system has an identity class, consisting of matrix rings over P, that is, of the algebras similar to P. Also each class (A) has the inverse $(\overline{A}) = (A)^{-1}$, consisting of the algebras similar to $\overline{A}$, where $\overline{A}$ is reciprocally isomorphic to A. This follows from the commutation theorem ğ5, 3 by the specialization $S = A$. For A can be embedded irreducibly in itself; one obtains $B = P$ and $A_A = P_t$.[16]

[16]The finer theorems on the group of algebra classes use the theory of factor systems; that will not be taken up here. Notice that up to this point no considerations concerning commutative fields have occurred. For example, the fact that the rank $(A : P)$ is a square has neither been used nor proved.

2. Splitting fields of an algebra class. The theory of splitting fields again rests entirely on the principle stated at the beginning of ğ5: the commutative extension fields are represented in A or in $\overline{A}$. We first need the following lemma.

Lemma. If A is a division ring with center P, and Z is a finite commutative extension field of P, then A_Z is simple with center Z. For by ğ4, 1 this holds for the system Z_A, reciprocally isomorphic to A_Z. Thus for every class (A) of algebras over P similar to A, the field Z gives an extension class $(A)_Z$ of simple algebras over Z similar to A_Z.

The associated division algebra D of an extension class follows immediately from the commutation theorem of ğ5, 3.

Theorem on the associated division algebra of an extension class. Let $(A)_Z$ be an extension class, and let Z denote an irreducible embedding, i.e. representation, of Z in A_f. Then

$$(A)_Z = (D),$$

where D is the set of all elements of A_f which commute elementwise with Z. One only has to replace the simple system S in ğ5, 3 by Z, observing that Z_A and A_Z are reciprocally isomorphic. If Z is embedded reducibly, the totality of elements commuting elementwise with Z is a matrix ring over D.

A commutative extension field Z of P is called a splitting field of the class (A) if the extension class $(A)_Z$ splits completely, that is, is equal to the identity class over Z, the class of all matrix rings over Z.

Theorem on the characterization of splitting fields. A finite commutative extension field Z of P is a splitting field of the class (A) if and only if its irreducible embedding in A_f gives a maximal commutative subfield of A_f.

Indeed, the property that Z be a splitting field of (A) is equivalent to $(D) = (Z)$. Hence, by the theorem on the associated division algebra, the irreducible embedding Z must be a maximal commutative subfield. If this condition is fulfilled, then necessarily $D = Z$, since adjoining any $a \in D$ to Z gives a commutative extension field.

Remarks. 1. It follows at the same time that a maximal commutative subfield Z, when irreducibly embedded, generates a maximal commutative subring. For the elements commuting elementwise with Z form a division ring.

2. The theorem also gives the existence of splitting fields, since the associated division algebra A certainly has maximal commutative subfields.

3. Rank relations, index, infinite commutative extensions. The rank statement from ğ5, 4 first gives the known fact that the rank of a simple algebra over its center is a square. For if Z is maximal commutative in A, then, since every embedding in A is irreducible,

$$(Z : P)(Z : P) = (A : P),$$

hence

$$(A : P) = m^2, \qquad (Z : P) = m,$$

where m is Schur's index; it is also the degree of all splitting fields embeddable in the division algebra A itself. For the degree n of a general splitting field one obtains

$$n = mr,$$

[17] for instance from $(A_r : P) = m^2 r^2$, or also from the rank relation ğ4, 3, since the index m is also the number of simple components of A_Z, which becomes a matrix ring over Z of rank m^2. More generally, if $A_\Lambda \sim D$, if L is the irreducible embedding of Λ in A_r, and if d^2 is the rank $(D : L)$ of the division algebra D over its center L, then

$$l\,d = mr.$$

[17] In general there are also "minimal" splitting fields, i.e. those for which no proper subfield is a splitting field, of all possible degrees. Compare Brauer–Noether, the work cited in note 2.

Indeed, by ğ5, 4 and the theorem on the associated division algebra from 2.,

$$(A_r : P) = (L : P)(D : P),$$

so

$$m^2 r^2 = l^2 d^2.$$

From the existence of splitting fields follow the facts for infinite commutative, algebraic or transcendental, extension fields Ω of P: the extension class $(A)_\Omega$ is a class of simple algebras with center Ω. If in particular Ω is algebraically closed, then A_Ω is a matrix ring of degree m. Thus the index is equal to the "absolute number of components." For if Z is a splitting field of A and $\overline{\Omega}$ is the compositum of Ω and Z, then $A_{\overline{\Omega}}$ is a matrix ring over $\overline{\Omega}$, hence has no radical and has center $\overline{\Omega}$. Therefore A_Ω also has no radical and its center is Ω; any element in the center of A_Ω not belonging to Ω would also lie in the center of $A_{\overline{\Omega}}$. Hence A_Ω is a simple algebra over Ω, and certainly a matrix ring over Ω if Ω is algebraically closed.

4. Existence of separable splitting fields. Every class (A) has separable splitting fields, indeed ones that can be embedded in A itself.[18]

Let the ground field P have characteristic p, and let the index be

$$m = sp^f$$

with s prime to p. If Z is a splitting field of A of degree m, and Z_0 is the extension of first kind contained in it, so that

$$(Z : Z_0) = p^f,$$

then the index of $A_{Z_0} \sim D$ is p^f. We prove the existence of a separable extension field Z_1 of Z_0 such that the index of D_{Z_1} is a proper divisor of p^f. Now D_Ω, with Ω algebraically closed, has no radical by 3.; the reduced discriminant of D therefore does not vanish. Hence there is at least one element $d \in D$ with nonzero reduced trace. This d cannot already lie in the ground field Z_0, because the trace of every element $\alpha \in Z_0$ is $p^f\alpha$, hence vanishes. Thus $Z_1 = Z_0(d)$ is a proper, indeed separable, extension field; the index of D_{Z_1} is a proper divisor of p^f. Repeating this finitely many times gives a separable splitting field of (A) whose degree m agrees with the index of A.

ğ 8.
Splitting Fields, Decomposition Fields, and Galois Theory in the Commutative Case.

In order to pass from the splitting fields of systems simple over their center to those of arbitrary simple systems, one still has to develop the splitting theory of the center; a Galois theory parallel to ğ6, 3 is to be added to it. All fields and systems occurring in this paragraph are commutative.

1. Splitting and decomposition fields of commutative simple systems. Let the commutative system Z be simple over P, hence a field, and let Ω be an algebraically closed extension field of P. The following is known (Representation Theory ğ21):

The system Z_Ω remains without radical if and only if Z is separable over P, that is, an extension of the first kind.

For only then does it have as many isomorphic maps of first degree into Ω as its rank over P, hence as many distinct representations, which in this case coincide with representation classes.

The possibility that a radical occurs in Z_Ω, so that a direct decomposition into absolutely simple components need not take place, leads to the following definitions. An extension field Λ of P is called a splitting field if Z_Λ splits into composition factors of first degree; in other words, if all absolutely irreducible representations already lie in Λ. An extension field T of P is called a decomposition field if Z_T splits off at least one composition factor of first degree; in other words, if at least one absolutely irreducible representation of Z exists in T.

Splitting and decomposition fields are characterized by the following theorem.

[18] Compare G. Köthe, Über Schiefkörper mit Unterkörpern zweiter Art über dem Zentrum, Journ. f. Math. 166 (1932), pp. 182–184. The present, much simpler proof goes back to a remark of M. Zorn.

Theorem. A field T is a decomposition field if and only if it contains a subfield Z' isomorphic to Z. A field Λ is a splitting field if and only if it contains a subfield Γ isomorphic to the Galois field belonging to Z.

This follows directly from the definitions of splitting and decomposition fields in terms of absolutely irreducible representations. In particular, in analogy with the noncommutative case, one obtains the following corollary: a field Z' is a minimal decomposition field, i.e. no proper subfield is a decomposition field, if and only if it is isomorphic to Z. A minimal decomposition field is at the same time a splitting field if and only if Z is normal, hence a Galois field over P.

This is the reason for calling a simple algebra normal over its center. In a fixed algebraically closed Ω over P, there is only one minimal splitting field, namely the Galois field belonging to Z, in contrast to the generally infinitely many nonisomorphic fields in the noncommutative case.[19] This has its source in the uniqueness of the direct decomposition in the commutative case, in contrast to the noncommutative case where uniqueness is only up to operator isomorphism; equivalently, in the finitely many different absolutely irreducible representations in the commutative case, as opposed to the infinitely many different ones in the noncommutative case, although they belong to the same class (cf. 2.).

2. Hypercomplex proof of Galois theory in the case of separable fields Z/P. In exact analogy with ğ6, 3, the theory of isomorphisms holds for arbitrary Z separable over P; if Z is Galois, one can then pass to the usual automorphism group.

Hypotheses. The simple system Z over P is a finite separable extension field, Ω denotes a finite or infinite splitting field over P, $Z' = Z^{(1)}$ a subfield isomorphic to Z, and Γ the corresponding Galois field. By 1. there is a direct decomposition

$$Z_\Omega = r^{(1)} + \cdots + r^{(n)} = e^{(1)}Z_\Omega + \cdots + e^{(n)}Z_\Omega = e^{(1)}\Omega + \cdots + e^{(n)}\Omega.$$

The representation $Z \to Z^{(i)}$ generated by $e^{(i)}$, with $Z^{(i)} \subseteq \Gamma$, is defined by

$$e^{(i)}z = e^{(i)}\zeta^{(i)}.$$

Lemma 1. The n representations generated by $e^{(1)}, \ldots, e^{(n)}$ are all distinct. The proof is as in ğ6, 3, or also follows from 1.; they belong to distinct representation classes.

Lemma 2. If T is an intermediate field between P and Z, and s is the rank of Z over T, then every isomorphism of T into Ω admits at least, and hence exactly, s extensions.

The proof is as in ğ6, 3. The strengthening of "at least" to "exactly" follows from the uniqueness of the decomposition of Z_Ω, according to which Z has not merely at least but exactly n isomorphisms in Ω.

As in ğ6, 3, one defines the partition $\mathfrak{J}_T$ induced by T of the finite set $\mathfrak{J}$ of isomorphisms of Z: precisely those isomorphisms in $\mathfrak{J}$ are regarded as equivalent in $\mathfrak{J}_T$ which induce the same isomorphism on T. One proves the following.

Main theorem. If $\mathfrak{J}_T$ is the partition induced by T, then T is a maximal subfield with respect to this partition.

From here, in the case of a Galois Z, one passes to the automorphism group and to the usual formulation exactly as in ğ6, 3 by composing with the reciprocal of an isomorphism. The corresponding assertion for subgroups follows from the consideration of idempotents, which is of interest in itself.

3. The idempotents of Z_Ω. Let S run through the n substitutions which carry $Z' = Z^{(1)}$ into the individual $Z^{(i)}$. They are obtained by composing the reciprocal of the isomorphism $Z \to Z'$ with the isomorphism $Z \to Z^{(i)}$. The field Z need not be Galois. For elements $a \in Z_{Z'}$, the substitutions S are defined as operators by stipulating that they induce the identity on Z. Thus for each a, the conjugate a^S, lying in $Z_{Z^{(i)}}$, is defined. With these conventions one has the following theorem.

[19] R. Brauer–E. Noether, work cited above.

Theorem. The n idempotents $e^{(i)}$ of Z_Ω are conjugate:

$$e^{(i)} = e^S, \qquad e = e^{(1)};$$

they lie in the n conjugate extension systems $Z_{Z^{(i)}}$.

Indeed, applying S carries the defining relations

$$ez = e\zeta^{(1)}, \qquad e^2 = e$$

to

$$e^S z = e^S \zeta^{(i)}, \qquad (e^S)^2 = e^S.$$

By uniqueness of the decomposition the idempotents are themselves uniquely determined; hence $e^S = e^{(i)}$. Since Z' is also a decomposition field, so that the representation $ez = e\zeta^{(1)}$ is already mediated, e already lies in $Z_{Z'}$, and consequently e^S lies in $Z_{Z^{(i)}}$.

If Z is Galois, the part of the main theorem of Galois theory concerning subgroups follows immediately. If $\mathfrak{H}$ is a subgroup of the Galois group $\mathfrak{G}$, then, by the uniqueness of the components of a direct sum, the element

$$\sum_{H \in \mathfrak{H}} e^H$$

admits all substitutions from $\mathfrak{H}$ and no others. Since the group $\mathfrak{G}$ was defined for Z, this is the Galois theory of Z; by isomorphism it also settles the theory for Z'.

4. Connection of the idempotents with complementary bases. Again Z is not assumed to be Galois.

Theorem. Let $a_1, \ldots, a_n$ be a basis of Z over P, and write the idempotent as

$$e = a_1\beta_1 + \cdots + a_n\beta_n,$$

so that

$$e^S = a_1\beta_1^S + \cdots + a_n\beta_n^S.$$

Then

$$\beta_1^S, \ldots, \beta_n^S$$

are the images, under the map mediated by e^S, of the complementary basis $b_1, \ldots, b_n$ to $a_1, \ldots, a_n$.

For the map mediated by e^S, $e^S z = e^S z^S$, in particular $e^S a_i = e^S \alpha_i^S$, the relations

$$e^S e^S = e^S, \qquad e^S e^R = 0 \quad (S \neq R)$$

give the assignments $e^S \mapsto 1$, $e^R \mapsto 0$. Hence

$$1 = \alpha_1^S\beta_1^S + \cdots + \alpha_n^S\beta_n^S, \qquad 0 = \alpha_1^S\beta_1^R + \cdots + \alpha_n^S\beta_n^R \quad (S \neq R).$$

Written in matrix form, this is the defining equation for the complementary bases:

$$\begin{pmatrix} \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^S & \cdots & \alpha_n^S \\ \vdots & \ddots & \vdots \end{pmatrix} \begin{pmatrix} \beta_1 & \cdots & \beta_1^R & \cdots \\ \vdots & \ddots & \vdots & \\ \beta_n & \cdots & \beta_n^R & \cdots \end{pmatrix} = E.$$

The passage to the trace definition follows because, for

$$a_i = \sum_S e^S \alpha_i^S, \qquad b_i = \sum_S e^S \beta_i^S,$$

the matrix relation, after interchanging rows, becomes

$$\delta_{ij} = \mathrm{Sp}(a_i b_j).^{20}$$

[20] Compare Representation Theory §25.

Here the a_i and b_i lie in Z, since they admit all substitutions S.[21]

The contragredience of the complementary bases follows here from the fact that the idempotents e^S are invariants of Z, independent of the basis chosen. Thus all

$$a_1\beta_1^S + \cdots + a_n\beta_n^S$$

are transformed into themselves when one passes to another basis

$$a_1', \ldots, a_n'$$

of Z/P.

ğ 9.
Splitting Fields and Decomposition Fields of Arbitrary Systems.

1. Definitions and reduction to the simple case. The definitions given in ğ8 correspond in the general case to the following. Let S be hypercomplex over P. A commutative extension field Λ of P is called a splitting field of S if, in a composition series by one-sided ideals, S_Λ splits into absolutely simple composition factors; in other words, if all irreducible representations of S in Λ are already absolutely irreducible. An extension field T of P is called a decomposition field if S_T splits off at least one absolutely simple composition factor; equivalently, if at least one representation irreducible in T is already absolutely irreducible.

These definitions plainly contain the ones given in ğ8 for the commutative case and in ğ7 for simple algebras. The latter is true because A_Λ, for every commutative extension of the center, is completely reducible, so that composition factors and components of the direct sum decomposition coincide. Full matrix rings over the center, and only these, give absolutely simple components, hence also absolutely irreducible representations. Moreover A_Λ is two-sided simple, hence decomposes into operator-isomorphic components. Therefore the splitting off of one absolutely simple component already gives complete splitting: decomposition fields and splitting fields coincide.

From the definitions the following facts follow immediately: the splitting fields of S are the composita obtained by taking one splitting field for each representation irreducible in P; a decomposition field of S is any decomposition field of a representation irreducible in P. Because of the one-to-one correspondence between the simple systems, namely the components of the residue-class ring modulo the radical, and the representations irreducible in P, it is enough to consider simple systems. The results will then follow by combining ğ7 and ğ8.

2. Splitting fields and decomposition fields of simple systems. We first consider the case of a simple system A with separable center Z over P. From ğ8, 1 and ğ8, 3 one obtains the following. The two-sided decomposition of A_Ω corresponding to the direct decomposition of Z_Ω, where Ω denotes a splitting field of Z, gives n conjugate components

$$e^S A_\Omega$$

of A_Ω, each isomorphic to A, which become simple algebras over their centers

$$e^S Z_\Omega = e^S Z.$$

The substitutions S are defined as operators for A_Ω by stipulating that they induce the identity on A.

Indeed, by ğ8, 3 the idempotents are conjugate; the same is therefore true of the components $e^S A_\Omega$, by the definition of the substitutions for A. Since A is two-sided simple, $e^S A_\Omega$ is ring-isomorphic to A. Moreover $e^S A_\Omega = e^S A_{Z^S}$, because $e^S Z_\Omega = e^S Z$; hence the center coincides with the coefficient domain, and the components are normal algebras.

The results of ğ7, 2 now further imply: if A is a simple system over P with separable center Z over P, then A_Ω too is without radical, hence completely reducible; here Ω may be any finite or infinite extension field. For by ğ7, 2, $e^S A_\Omega$ remains simple after every extension of coefficients, and therefore has no radical. Hence the same holds for the direct sum; this is A_Ω, or, if Ω is not a splitting field of Z, is obtained by coefficient extension from A_Ω.

From ğ7, 2 follows also the following characterization.

[21] Connections between complementary bases and idempotents occur first in Dedekind, Zur Theorie der aus n Haupteinheiten gebildeten komplexen GröSSen; compare vol. II of the collected works, pp. 4–5.

Characterization of decomposition fields and splitting fields. If A is a division algebra with separable center Z, then the irreducible embeddings of the decomposition fields are given by all and only the maximal commutative subfields of the A_r containing Z. The splitting fields are all and only the composita of a decomposition field with a splitting field of the center, in particular with the Galois field belonging to the center. A minimal decomposition field may be a splitting field even when the center is not Galois.

A decomposition field must contain a field isomorphic to Z; the assertion about embeddings of decomposition fields now follows from the preceding facts and from ğ7, 2. A splitting field must moreover contain a splitting field Ω of Z. But every decomposition field over Ω is at the same time a splitting field, since the components $e^S A_\Omega$ are simple and have a center isomorphic to Ω. If Z is Galois, minimal decomposition fields and splitting fields therefore coincide. But even in the non-Galois case, unlike the commutative case, there may be minimal decomposition fields which are at the same time splitting fields, namely whenever such a minimal decomposition field contains the Galois field belonging to Z. Example: a quaternion division algebra with center isomorphic to $P(\sqrt[3]{2})$, P the field of rational numbers; the Galois field belonging to $P(\sqrt[3]{2})$ is a minimal decomposition and splitting field.

Finally, if the center is inseparable, then Z_Ω, and with it A_Ω, is a system with radical. Let $\mathfrak{C}$ be the radical of Z_Ω, and let $\mathfrak{c} = \mathfrak{C}A_\Omega$ be the extension ideal in A_Ω. Then $Z_\Omega/\mathfrak{C}$ has a direct decomposition into conjugate components, in exact analogy with ğ8, 2. This gives, just as above, the direct decomposition of $A_\Omega/\mathfrak{c}$; the components determined by the idempotents $\bar{e}^{(i)}$ are isomorphic to A, with centers $\bar{e}^{(i)}Z^{(i)}$. Thus the theorems on decomposition and splitting fields remain valid. The count of ranks further shows that the composition factors corresponding to a composition series of $\mathfrak{c}$ are operator-isomorphic to $A_\Omega/\mathfrak{c}$, not merely homomorphic.

Expressed for irreducible representations, this gives the summary: if a representation of a hypercomplex system irreducible over P is given, then the representation is absolutely completely reducible if and only if the associated center is separable over P. In every case, the splitting and decomposition fields of the representation can be characterized as above by embedding into the associated simple system. In particular, the lowest degree of a decomposition field is the product of the degree of the center and the index of the associated algebra class over the center; the degree of every decomposition field is a multiple of this. The representation decomposes, in the sense of composition series, into as many distinct but conjugate absolutely irreducible representation classes as the degree of the largest separable field contained in the center. Each class occurs as many times as is given by the product of the index and the degree of the center over this separable extension.

For a perfect ground field, where only separable extension fields occur, this returns the known results of I. Schur, with the addition of the embedding characterization which already occurs in R. Brauer.

(Received 8 June 1932.)

41. The Principal Genus Theorem for Relative Galois Number Fields

By

Emmy Noether in Göttingen.

Math. Ann. 108 (1933), pp. 411–419

In recent times it has become clear that noncommutative methods, in particular the theory of algebras, make it possible to formulate and prove familiar theorems on relative cyclic and Abelian number fields for arbitrary relative Galois fields.[1] I recall above all the norm theorem, which in general can be expressed as a theorem on split algebras. In what follows I show that, correspondingly, the principal genus theorem too can be formulated hypercomplexly, as a theorem on inner automorphisms or on "crossed representations." The proof follows from the theorem on split algebras just mentioned by purely algebraic-arithmetic considerations, whereas in that former theorem the norm theorem in the cyclic case—prime degree already suffices—remains the transcendental core. For better understanding of the formulation I first put forward the "principal genus theorem in the minimal case," which is not used below,[2] an elementary algebraic theorem[3] which, in the cyclic special case, becomes the familiar Theorem 90 of Hilbert's *Zahlbericht*, according to which $N(a)$ equals one if and only if $a = b^{1-S}$.

I state even this theorem as one about inner automorphisms or crossed representations and prove it by means of the general theorems on inner automorphisms and crossed-product representations of algebras. In the actual principal genus theorem, the crossed product of the ideal-class group and the Galois group replaces the latter construction, but with a finer induced division of the factor systems into ideal classes. This captures an analogue of the ray-class division of class-field theory. Since general theorems on automorphisms and representations are still absent here—the principal genus theorem may be regarded as a first step in this direction—I give, as mentioned above, a reduction by means of the theorem on split algebras. The theorem is thereby reduced to the corresponding theorem for ideals rather than ideal classes; the Brandt theorems on the interrelation of the maximal orders of an algebra[4] may be regarded here as the equivalent of the automorphism theorems. Together with investigations of maximal orders of crossed products,[5] they indeed give a proof essentially parallel to the proof in the minimal case, though more complicated because one must pass to the individual places. I therefore prefer the almost trivial proof suggested by E. Artin, which is an even simpler analogue here of Speiser's proof.

ğ 1.

The Principal Genus Theorem in the Minimal Case

In this section k denotes an arbitrary commutative field, not necessarily a number field; K/k is a separable Galois extension of degree n, and $\mathfrak{G}$ is its Galois group.

1. I first recall the familiar facts about crossed products.[6] A crossed product means a simultaneous embedding of K and $\mathfrak{G}$ in an algebra A such that the automorphisms of K become inner. Let $u_{S_1}, \ldots, u_{S_n}$ be symbols corresponding to the n group elements. First set A, as a module of linear forms of rank n over K, equal to

$$A = u_{S_1}K + \cdots + u_{S_n}K. \tag{1}$$

[1] Cf. my Zurich lecture, *Verhandlungen des Internationalen Mathematiker-Kongresses Zürich 1932*, vol. I, "Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und Zahlentheorie," where in particular the hypercomplex formulations of the norm theorem and the principal genus theorem are discussed in detail; references are given there. For the theorem on split algebras, cf. also H. Hasse, *Die Struktur der R. Brauerschen Algebrenklassengruppe*, 6.1, Math. Ann. 107 (1932).

[2] I say "in the minimal case" because this is the algebraic analogue of the principal genus theorem over arbitrary fields, whereas "in the small" already signifies passage to a p-adic ground field.

[3] The theorem is found in A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Z. 5 (1919), pp. 1–6, p. 3. It is already stated there as a theorem on crossed representations.

[4] Brandt's theory of maximal orders is presented and re-established in detail in H. Hasse, *Über* $\mathfrak{p}$*-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Math. Ann. 104 (1931).

[5] Notes on this subject by C. Chevalley (Hamburg Reports), H. Hasse, and E. Noether will appear; the latter two are to appear in a Herbrand memorial volume.

[6] The theory, following a lecture of mine in 1929/30, is presented in H. Hasse, *Theory of cyclic algebras*, chap. 2, Trans. Amer. Math. Soc. 34 (1932). Cf. also M. Deuring's report on hypercomplex numbers, to appear in *Ergebnisse der Mathematik*. The present summary is taken from my Zurich lecture cited in note 1.

By requiring the inner automorphism generated by u_S, more generally by $u_S K^*$,[7] A becomes a ring, hence an algebra of rank n^2 over k. The requirement is expressed by

$$u_S^{-1} z u_S = z^S \qquad \text{or} \qquad z u_S = u_S z^S, \tag{2}$$

for every $z \in K$, and by

$$u_S u_T = u_{ST} a_{S,T}, \qquad a_{S,T} \in K^*. \tag{3}$$

The associative law is equivalent to

$$a_{ST,R} a_{S,T}^R = a_{S,TR} a_{T,R}, \tag{4}$$

that is, to $[u_S u_T] u_R = u_S [u_T u_R]$.

Defining the product of two arbitrary elements by

$$\Big(\sum_S u_S b_S\Big)\Big(\sum_T u_T c_T\Big) = \sum_{S,T} u_S u_T b_S^T c_T,$$

one obtains the crossed product of K with $\mathfrak{G}$ for the factor system $a_{S,T}$, written

$$A = (a_{S,T}, K, \mathfrak{G}).$$

One proves that A is a simple normal algebra over k, hence a matrix ring D_r of degree r over the associated division algebra D, and that K is a maximal commutative subfield, hence a splitting field. Conversely, for every prescribed division algebra D there are matrix rings D_r which arise in this way as crossed products.

If one passes from u_S to $v_S = u_S c_S$, with $c_S \in K^*$, which produces the same automorphism, the associated factor systems are

$$\bar{a}_{S,T} = a_{S,T} \frac{c_S^T c_T}{c_{ST}}. \tag{5}$$

In particular, by (5), the factor systems $\bar{a}_{S,T} = c_S^T c_T / c_{ST}$ are associated with one; these quantities are called transformation quantities. Associated factor systems are collected into a class (a), and the transformation quantities in particular into the class (1). Likewise, all algebras similar to A, that is, all D_r with $r = 1, 2, \ldots$, are collected into a class $\mathfrak{A}$. The classes $\mathfrak{A}$ and (a) correspond one-to-one. *The classes with fixed splitting field K form an Abelian group under direct product, isomorphic to the componentwise product of classes of factor systems. Its identity is the split algebra class, respectively the system of all transformation quantities $c_S^T c_T / c_{ST}$.* This is R. Brauer's group of algebra classes.

For cyclic algebras one obtains the following special case. If Z/k is cyclic and S is a generating substitution, the powers of u may be made to correspond to the powers of S, and

$$A = Z + uZ + \cdots + u^{n-1} Z, \tag{1'}$$

$$z u = u z^S, \tag{2'}$$

$$u^n = \alpha, \tag{3'}$$

$$\alpha \in k^*, \tag{4'}$$

$$\bar{\alpha} = \alpha\, N(c) \qquad \text{if } v = uc. \tag{5'}$$

Thus each factor system here consists of a single element α of the ground field, written $A = (\alpha, Z, S)$; the identity class of factor systems is given by the norms from Z^*, and the group of algebra classes is isomorphic to $k^*/N(Z^*)$.

2. The formulation of the *principal genus theorem in the minimal case* uses the fact that relations (2)–(5) are purely multiplicative and hence also define the extension group $\mathfrak{G}^*$ of $\mathfrak{G}$, consisting of the elements in the n complexes $u_S K^*$:

$$\mathfrak{G}^* = \{u_{S_1} K^*, \ldots, u_{S_n} K^*\}. \tag{6}$$

Here K^* is an Abelian normal subgroup of $\mathfrak{G}^*$, and $\mathfrak{G}^*/K^* \simeq \mathfrak{G}$.[8] The group $\mathfrak{G}^*$ consists of all regular elements g^* which transform K into itself, that is, $g^{*-1} K g^* = K$. Hence the ring automorphisms of K are

[7] K^* is obtained from K by omitting zero; this notation is used throughout.

[8] Relations (2)–(5) are simply the defining relations for an extension of groups. Such an extension is known to exist once there is a subgroup of the full automorphism group of K^*, regarded only as a multiplicative group, which is a homomorphic image of $\mathfrak{G}$. The special feature of the crossed product is that this homomorphism is an isomorphism and that the subgroup in question is taken to be precisely the totality of automorphisms which are both multiplicative and additive, that is, the Galois group of K. Thus the ring extension is obtained together with the group extension.

produced by all and only the elements of $\mathfrak{G}^*$. Indeed, each such g^* produces a ring automorphism of K. Conversely, every such automorphism is produced by transformation with an element $v = u_S w$, where w induces the identity on K. Thus w commutes with every element of K, and hence lies in K, indeed in K^*, since K is maximal commutative.

Principal genus theorem in the minimal case. *First form: every group automorphism of $\mathfrak{G}^*$ extending the identity automorphism of K^* is inner and is produced by an element of K^*. Second form: if the transformation quantities $c_S^T c_T / c_{ST}$ all have the value one, then the c_S are symbolic $(1-S)$-th powers; that is, there is a $b \in K^*$ such that $c_S = b^{1-S} = b/b^S$ for every $S \in \mathfrak{G}$. Third form: the group $\mathfrak{G}$ has only one crossed representation class of degree one in K^* belonging to factor system one.*

A representation $u_S \mapsto C_S$ is called crossed with factor system $a_{S,T}$ if

$$C_S^T C_T = C_{ST} a_{S,T}.$$

Two representations belong to the same class if

$$C_S = B^{-S} D_S B.$$

I prove the first form and then show its equivalence to the second and third forms. The proof rests on the fact that every group automorphism of the indicated kind extends to a ring automorphism of A, and such an automorphism is known to be inner. Let v_S be the images of the u_S under this automorphism. Then $\sum v_S K$ again forms the crossed product of $\mathfrak{G}$ with K for the same factor system, because by assumption all relations (2)–(4) remain valid. The map

$$\sum u_S b_S \longmapsto \sum v_S b_S$$

is a ring automorphism fixing all elements of K. Hence, by what was said about $\mathfrak{G}^*$, it is produced by an element of K^*.

The passage to the second form is based on the fact that, by (2), the v_S must have the form $v_S = u_S c_S$. Since the factor systems are also preserved, (5) says that the corresponding transformation quantities must all be one. Conversely, (2)–(5) show that the substitution $v_S = u_S c_S$ produces an automorphism of the required kind. The first form therefore yields

$$v_S = b^{-1} u_S b = u_S \frac{b}{b^S}, \qquad c_S = b^{1-S}.$$

In the cyclic case the hypothesis says in particular, by (5'), that $N(c) = 1$, and $c = b^{1-S}$ is the familiar theorem.[9]

The third form is immediately equivalent to the second: its hypothesis says that $u_S \mapsto c_S$ is a crossed representation of degree one with factor system one, while $c_S = b^{1-S}$ says that this representation is equivalent to the identity representation, $c_S \sim 1$.

It should be noted, however, that this third form is only a special case of the much more general theorem: *for a prescribed factor system $a_{S,T}$ there is only one irreducible crossed representation class; its degree is m, where m is the Schur index of the associated algebra, that is, the degree of the associated division algebra.*[10]

ğ 2.

The Principal Genus Theorem

1. Preliminary remarks on class divisions. In the principal genus theorem of class-field theory for cyclic relative fields, two different divisions into classes occur: absolute ideal classes in the upper field and ray classes in the lower field. In the general case this corresponds to the fact that a division of the ideals of the upper field into classes induces a finer division of the factor systems into ideal classes.

Let $\mathfrak{I}$ first denote the group of all ideals of K. Since $\mathfrak{G}$ induces automorphisms of $\mathfrak{I}$, the extension by $\mathfrak{G}$ is defined by relations (2)–(5), and consists of the n complexes $\{\ldots u_S \mathfrak{I} \ldots\}$. Passing from $\mathfrak{I}$ to the group $\overline{\mathfrak{I}}$ of absolute ideal classes by imposing equivalence, the n complexes $u_S \overline{\mathfrak{I}}$ are still defined, because $\mathfrak{G}$ also induces

[9] The proof given here remains valid when k has only finitely many elements, a case in which Hilbert's proof fails, though Speiser's remains valid.

[10] I. Schur, *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn A. Speiser*, Math. Z. 5 (1919), pp. 7–10. For a proof based on the crossed representation modules from my lecture cited in note 6, cf. M. Deuring's report cited there.

automorphisms of $\overline{\mathfrak{I}}$, the principal class being transformed into itself.[11] Thus the equivalence relation from $\mathfrak{I}$ to $\overline{\mathfrak{I}}$ transfers from $\{\dots u_S\mathfrak{I}\dots\}$ to $\{\dots u_S\overline{\mathfrak{I}}\dots\}$: equivalent ideals $\mathfrak{a},\mathfrak{b}$ yield equivalent products $u_S\mathfrak{a}, u_S\mathfrak{b}$. In particular, u_S is equivalent to every $u_S(c_S)$, where (c_S) runs through the principal ideals. Requiring the product relations (3) to be unambiguous in this equivalence sense says that all transformation quantities $(c_S)^T(c_T)/(c_{ST})$ arising from principal ideals become equivalent to the identity factor system. In other words:

In the system of the n complexes $\{\dots u_S\overline{\mathfrak{I}}\dots\}$, where $\overline{\mathfrak{I}}$ is the group of absolute ideal classes of K and H denotes the principal class, the product relations (3) for the u_SH are unambiguously defined if and only if, in the induced ideal-class division of the factor systems, the principal class contains all transformation quantities arising from principal ideals, that is, with generators $(c_S) \in H$.

As a generalization of the ray-class division, I give the following definition.

Definition. The induced ideal-class division of the factor systems is fixed by requiring the principal class to consist of all principal ideals $(a_{S,T})$ for which there is at least one system of basis elements $a_{S,T}$ such that the algebra

$$(a_{S,T}, K, \mathfrak{G})$$

splits at every ramified place of K.

These principal ideals form a group under multiplication of factor systems. This group contains the transformation quantities

$$\frac{(c_S)^T(c_T)}{(c_{ST})},$$

because the factor systems $c_S^T c_T/c_{ST}$ produce algebras which split everywhere.

2. Formulation of the principal genus theorem. I state the theorem, corresponding to the minimal theorem, in three equivalent forms.

First form: with the induced ideal-class division of the factor systems taken as basis, suppose that the substitution $v_S = u_S\bar{c}_S$,[12] produces an automorphism of the n complexes $\{\dots u_S\overline{\mathfrak{I}}\dots\}$, that is, that the same relations (3) hold for the v_S in the sense of this class division. Then this automorphism is inner and is produced by an ideal class $\bar{b}$.

Second form: if the transformation quantities $\bar{c}_S^T\bar{c}_T/\bar{c}_{ST}$ formed from the ideal classes $\bar{c}_S$ all belong to the principal class of the induced class division of the factor systems—the totality of these "vectors" $\{\dots\bar{c}_S\dots\}$ of ideal classes forms the principal genus—then the classes $\bar{c}_S$ are symbolic $(1-S)$-th powers; that is, there is an ideal class $\bar{b}$ such that $\bar{c}_S = \bar{b}^{1-S} = \bar{b}/\bar{b}^S$ for every $S \in \mathfrak{G}$.

Third form: with the induced ideal-class division for the factor systems, the group $\mathfrak{G}$ has only one crossed representation class of degree one in $\overline{\mathfrak{I}}$ which belongs to the identity class of factor systems.

The equivalence of the three forms follows as in §1. The passage from the first to the second form is even simpler here, because the automorphism is already assumed to be produced by $v_S = u_S\bar{c}_S$. This hypothesis is necessary because $\overline{\mathfrak{I}}$ need no longer be a largest commutative subgroup: all classes of $\overline{\mathfrak{I}}$ may be ambiguous. For the third form, note that because only multiplication is defined in $\overline{\mathfrak{I}}$, the representation matrices must have only one nonzero entry in every row and column; this imposes no restriction on representations of degree one.

3. Proof of the principal genus theorem. I prove the second form. The proof rests on two lemmas.

Lemma 1 (principal genus theorem for ideals). *If the transformation quantities $\mathfrak{c}_S^T\mathfrak{c}_T/\mathfrak{c}_{ST}$ formed from the ideals $\mathfrak{c}_S$ give the unit ideal, then the $\mathfrak{c}_S$ are symbolic $(1-S)$-th powers:*

$$\mathfrak{c}_S = \mathfrak{b}^{1-S} \qquad (S \in \mathfrak{G}).$$

Equivalently, the first and third forms hold again, provided in the first form, as for ideal classes, that the automorphism is assumed to be produced by $v_S = u_S\mathfrak{c}_S$.

[11] More generally, $\{\dots u_S\overline{\mathfrak{I}}\dots\}$ is defined whenever the principal class is taken to be a subgroup of $\mathfrak{I}$ admitting $\mathfrak{G}$; transformation quantities from the ideals of that subgroup then replace those from principal ideals.

[12] $\bar{c}_S$ denotes the ideal class of c_S.

Proof.[13] The module sum, or greatest common divisor,

$$\mathfrak{b} = \sum_S \mathfrak{c}_S$$

has the required property. Indeed,

$$\mathfrak{b} = \sum_S \mathfrak{c}_S, \qquad \mathfrak{b}^T = \sum_S \mathfrak{c}_S^T, \qquad \mathfrak{b}^T \mathfrak{c}_T = \sum_S \mathfrak{c}_S^T \mathfrak{c}_T = \sum_S \mathfrak{c}_{ST} = \mathfrak{b},$$

and therefore $\mathfrak{c}_T = \mathfrak{b}^{1-T}$.

Lemma 2 (the theorem on split algebras in another form). *Let the algebra $A = (a_{S,T}, K, \mathfrak{G})$ split at all finite and infinite ramified places of K, and suppose that the principal ideals $(a_{S,T})$ are transformation quantities of ideals:*

$$(a_{S,T}) = \frac{\mathfrak{c}_S^T \mathfrak{c}_T}{\mathfrak{c}_{ST}}.$$

Then A splits everywhere, absolutely. Thus the $(a_{S,T})$ are transformation quantities of principal ideals:

$$(a_{S,T}) = \frac{(d_S)^T (d_T)}{(d_{ST})}.$$

Conversely, every algebra which splits everywhere satisfies this condition.[14]

The proof rests on the known behavior of A under $\mathfrak{p}$-adic extension. Let $k_\mathfrak{p}$ be the $\mathfrak{p}$-adic extension of k, and $K_\mathfrak{P}$ the $\mathfrak{P}$-adic extension of K, where $\mathfrak{P}$ is a prime ideal above $\mathfrak{p}$. Let $A_\mathfrak{p}$ be the extension of A obtained by passing from k to $k_\mathfrak{p}$. Let $\mathfrak{Z}$ be the decomposition group of $\mathfrak{P}$, and $a_\mathfrak{Z}$ the corresponding part of the factor system, consisting of those $a_{S,T}$ for which $S, T \in \mathfrak{Z}$. Then

$$A_\mathfrak{p} \sim (a_\mathfrak{Z}, K_\mathfrak{P}/k_\mathfrak{p}, \mathfrak{Z}).$$

[15]

If $\mathfrak{p}$ is unramified, so that $\mathfrak{Z}$ is cyclic, this is the distinguished representation of $A_\mathfrak{p}$ by means of the unramified inertia field $K_\mathfrak{P}/k_\mathfrak{p}$.[16]

It remains to show that under the hypothesis of Lemma 2, $A_\mathfrak{p}$ also splits in this unramified case. At an infinite place $K_\mathfrak{P} = k_\mathfrak{p}$, so $A_\mathfrak{p}$ splits. At a finite $\mathfrak{p}$, the factor system $a_\mathfrak{Z}$ is first seen to be associated with a factor system consisting of units of $K_\mathfrak{P}$. Indeed, in $K_\mathfrak{P}$ all the ideals $\mathfrak{c}_S$ become principal, say (c_S); the hypothesis concerning $(a_{S,T})$ therefore says

$$a_{S,T} = e_{S,T} \frac{c_S^T c_T}{c_{ST}}$$

with units $e_{S,T}$. Thus $a_\mathfrak{Z}$ is associated with the factor system of units $e_{S,T}$.

This property persists on passing to the normalized cyclic representation (1')–(5'); thus α is a unit in

$$A_\mathfrak{p} = (\alpha, K_\mathfrak{P}/k_\mathfrak{p}, R),$$

where R generates $\mathfrak{Z}$. That $e_{S,T}$ is a factor system is expressed by

$$u_{R^i} u_{R^j} = u_{R^{i+j}} e_{R^i, R^j}.$$

Putting $u_R = u$ gives

$$u^i = u_{R^i} e_{R,R^{i-1}} e_{R,R^{i-2}} \cdots e_{R,R}.$$

Hence, since $u_E = e_{E,E}$, if f is the order of $\mathfrak{Z}$,

$$u^f = \alpha = e_{E,E} e_{R,R^{f-1}} \cdots e_{R,R}.$$

[13] Cf. the end of the introduction.

[14] More precisely, $a_{S,T} = d_S^T d_T / d_{ST}$. Only the weakened assertion about principal ideals is used in the proof of the principal genus theorem.

[15] Cf. Hasse, cited in note 6, ğ14. A somewhat simpler proof is as follows. Let Z be the decomposition field of $\mathfrak{P}$; then $k_\mathfrak{p}$ contains an isomorphic copy of Z, and $A_Z \sim (a_\mathfrak{Z}, K/Z, \mathfrak{Z})$. Indeed, A_Z is similar to the totality of elements of A commuting elementwise with Z (cf. van der Waerden, vol. II, p. 210, or my forthcoming paper on noncommutative algebra in Math. Z.). Extending A_Z to $A_\mathfrak{p}$ gives the result. The choice among the conjugate primes $\mathfrak{P}$ is immaterial: the resulting algebras are isomorphic and are carried into one another by transformation with u_T when $\mathfrak{G} = \sum \mathfrak{Z}T$.

[16] Cf. Hasse's work cited in note 4, ğ3.

In an unramified extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, however, every unit is a norm. It follows that $A_{\mathfrak{p}}$ splits. Thus A splits everywhere and hence, by the theorem on split algebras, splits absolutely.

Equivalently, the hypothesis implies that the $a_{S,T}$ are transformation quantities of elements,

$$a_{S,T} = \frac{d_S^T d_T}{d_{ST}}, \qquad d_S \in K^*,$$

and therefore, in weakened form, that the $(a_{S,T})$ are transformation quantities of principal ideals. Conversely, if A splits everywhere, then the principal ideals $(a_{S,T})$ are transformation quantities of ideals at every place, and A splits in particular at the ramified places. This is indeed another formulation of the hypothesis of the theorem on split algebras.

The two lemmas now immediately give the proof of the principal genus theorem. Let $\mathfrak{c}_S$ be an ideal in the class $\bar{c}_S$. By the definition of the induced class division of factor systems, the hypothesis on the classes says precisely that the transformation quantities of the $\mathfrak{c}_S$ become principal ideals $(a_{S,T})$ satisfying the hypotheses of Lemma 2. Hence there are principal ideals (d_S) such that the ideals

$$\mathfrak{d}_S = \frac{\mathfrak{c}_S}{(d_S)},$$

which lie in the same classes $\bar{c}_S$, satisfy the hypothesis of Lemma 1: their transformation quantities are the unit ideal. Thus, by Lemma 1, there is an ideal $\mathfrak{b}$ such that $\mathfrak{d}_S = \mathfrak{b}^{1-S}$. This says that the classes $\bar{c}_S$ are symbolic $(1-S)$-th powers of the class $\bar{b}$.

In the cyclic case the principal genus theorem becomes the familiar one as soon as, after normalization, the principal class of the induced class division becomes the group of principal ideals (α) for which α is a norm residue at every ramified place.

(Received 27 October 1932.)

42. Split Crossed Products and Their Maximal Orders

Actualités scientifiques et industrielles 148 (1934), pp. 5–15

In the simplest case of split crossed products[1]—that is, those which yield split algebras and hence possess factor systems associated with one—the relations can be followed rather explicitly. This remains true even for non-Galois splitting fields (maximal commutative subfields). The simple algebraic facts belonging here are developed in ğ I. In ğ II, with an algebraic number field as ground field, I give explicit representations of all maximal orders and of their ideals by means of modules and complementary modules of the underlying splitting field k.[2] I further give a division into "domains," in which all maximal orders are assigned to the same domain when they have the same intersection with k. Thus the domains correspond one-to-one to the orders in k, and the principal order is assigned the "principal domain." The maximal orders of a domain are transformed into one another by ideals formed from the modules of the corresponding order; in the principal domain these are, in particular, the extensions of ideals of k (of modules over the principal order). In ğ III I pass to arbitrary simple algebras. By refining the division into domains—requiring, besides the same intersection, agreement of the p-adic components of the maximal orders at the ramified places—one can transfer the theorems obtained in the split case. In particular, the maximal orders of a principal domain are then also transformed into one another by extensions of ideals of k.

The theorems on the principal domain are found in Chevalley[3] and Hasse.[4] Chevalley also shows that without the refined division concerning the ramified places the theorems no longer hold in general.

ğ I. — *Matrix Units of Split Crossed Products and Complementary Bases of the Splitting Fields*

1. — In this section Ω denotes an arbitrary ground field. Let k/Ω be a Galois separable extension of degree n, let $\mathfrak{G}$ be its Galois group with elements $S, T, \ldots$, and let $u_S, u_T, \ldots$ be the corresponding operators. We consider *crossed products with factor system one*, hence split algebras

$$K = \mathfrak{G} * k = u_{S_1}k + \cdots + u_{S_n}k, \qquad u_S u_T = u_{ST},$$

$$z u_S = u_S z^S \qquad \text{(for every } z \text{ in } k\text{)}.$$

Factor system one gives further relations. Set

$$E_{\mathfrak{G}} = \sum_S u_S.$$

Then

$$E_{\mathfrak{G}} u_S = u_S E_{\mathfrak{G}} = E_{\mathfrak{G}} \tag{1}$$

for every S in $\mathfrak{G}$ (that is, $E_{\mathfrak{G}}$ generates the identity representation of $\mathfrak{G}$),[5]

$$z E_{\mathfrak{G}} = \sum_S u_S z^S, \tag{2a}$$

and

$$E_{\mathfrak{G}} z E_{\mathfrak{G}} = E_{\mathfrak{G}} \cdot \sum_S u_S z^S = E_{\mathfrak{G}} \cdot \mathrm{Sp}(z), \tag{2b}$$

where $\mathrm{Sp}(z)$ denotes the trace of z as an element of k/Ω. From these relations follows the

THEOREM. — *If $a_1, \ldots, a_n$ is a basis of k/Ω, and $\widetilde{a}_1, \ldots, \widetilde{a}_n$ is the complementary basis, then*

$$c_{ik} = \widetilde{a}_i E_{\mathfrak{G}} a_k$$

[1] The theory of crossed products, following a lecture of mine, is presented in Section II of H. Hasse, *Theory of cyclic algebras over an algebraic numberfield*, Trans. Amer. Math. Soc. 34 (1932). I use here only the first basic concepts. Brandt's theory of maximal orders is presented and re-established in detail, within a broader body of results, in H. Hasse, *Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Math. Ann. 104 (1931), cited below as H.

[2] These explicit representations had long been known to me; the impetus for the ensuing considerations was provided by the communication of H. Hasse's theorem cited in note 4.

[3] C. Chevalley, "Sur certains idéaux d'une algèbre simple," Abh. Math. Sem. Hamburg, 1934.

[4] H. Hasse, "Über gewisse Ideale in einer einfachen Algebra," preceding this paper; I of the collection.

[5] If the characteristic of k does not divide n, then $\frac{1}{n}E_{\mathfrak{G}}$ is the idempotent of the identity representation. The normal form of K remains valid, however, even when the characteristic divides n; the sole hypothesis is that k/Ω be separable.

is a system of matrix units of K. Thus K can be represented as the module product

$$K = kE_{\mathfrak{G}}k = k \cdot \sum_S u_S \cdot k = \sum_{i,k} (\widetilde{a}_i E_{\mathfrak{G}} a_k)\, \Omega.$$

Indeed, by (2b),

$$\begin{aligned} c_{ij}c_{lk} &= \widetilde{a}_i E_{\mathfrak{G}} a_j \cdot \widetilde{a}_l E_{\mathfrak{G}} a_k \\ &= \widetilde{a}_i E_{\mathfrak{G}} a_k \cdot \mathrm{Sp}(a_j \widetilde{a}_l) = c_{ik} \cdot \mathrm{Sp}(a_j \widetilde{a}_l), \end{aligned}$$

which is precisely the matrix-unit property, since the complementary bases are defined by $\mathrm{Sp}(a_j \widetilde{a}_l) = \delta_{jl}$.

Remark 1. If Z is any commutative extension field of Ω, everything remains valid when a_i is a basis of k_Z/Z and K_Z becomes a direct sum of fields. The substitutions of the group are then defined by inducing the identity on Z, in agreement with the fact that u_S commutes elementwise with Z in K_Z.

Remark 2. That $K = kE_{\mathfrak{G}}k$ also follows directly from the fact that the right-hand side is a nonzero ideal of the simple system K.

2. — Now assume that the ground field Ω has *characteristic zero. The representation $K = kE_{\mathfrak{G}}k$ of the split algebra K given in 1 remains valid even when k is a non-Galois splitting field of K/Ω.* One proves this by passing to the Galois splitting field. Let $\bar{k}$ be the Galois field belonging to k, let $\bar{\mathfrak{G}}$ be its group, let $\bar{u}_S$ be the corresponding operators, and let $\bar{K} = \bar{k}E_{\bar{\mathfrak{G}}}\bar{k}$ be a split crossed product. Let the subfield k correspond to the subgroup $\mathfrak{H}$ of order h. Set

$$\bar{\mathfrak{G}} = \mathfrak{H}S_1 + \cdots + \mathfrak{H}S_n = S_1^{-1}\mathfrak{H} + \cdots + S_n^{-1}\mathfrak{H}, \qquad E_{\mathfrak{H}} = \frac{1}{h}\sum_H \bar{u}_H,$$

$$E_{\mathfrak{G}} = \frac{1}{h}E_{\bar{\mathfrak{G}}} = \sum_i u_{S_i}, \qquad \text{where} \qquad u_{S_i} = E_{\mathfrak{H}}\bar{u}_{S_i}.$$

Thus the idempotent $E_{\mathfrak{H}}$ generates the identity representation of $\mathfrak{H}$, while $E_{\mathfrak{G}}$, just like $E_{\bar{\mathfrak{G}}}$, generates the identity representation of $\bar{\mathfrak{G}}$. *For the $E_{\mathfrak{G}}$ and u_S so defined, relations (1) hold on one side and relations (2) hold in full.* Here z runs through all elements of k, and hence z^S through those of the conjugate field k^S, which, as a subfield of $\bar{k}$, is also a subfield of $\bar{K}$. First,

$$E_{\mathfrak{G}} = E_{\mathfrak{G}}E_{\mathfrak{H}} = E_{\mathfrak{H}}E_{\mathfrak{G}} = E_{\mathfrak{H}}E_{\mathfrak{G}}E_{\mathfrak{H}}, \tag{3}$$

$$zE_{\mathfrak{H}} = E_{\mathfrak{H}}z, \qquad \text{and consequently} \tag{4}$$

$$zu_{S_i} = u_{S_i}z^{S_i}. \tag{5}$$

Indeed, by the definition of $E_{\mathfrak{H}}$, relation (3) follows from (1) for $E_{\bar{\mathfrak{G}}}$, hence also for $E_{\mathfrak{G}}$, while (4) says that z, as an element of k, admits the substitutions in $\mathfrak{H}$: $z\bar{u}_H = \bar{u}_H z$. Right multiplication of (4) by $\bar{u}_{S_i}$ gives (5). Relation (1) on one side now follows:

$$E_{\mathfrak{G}}u_{S_i} = E_{\mathfrak{G}}, \quad \text{since} \quad E_{\mathfrak{G}}u_{S_i} = E_{\mathfrak{G}}E_{\mathfrak{H}}\bar{u}_{S_i} = E_{\mathfrak{G}}\bar{u}_{S_i} = E_{\mathfrak{G}}; \tag{1'}$$

(2a) follows by summing (5), and then (2b) follows from (1′).

The proof that $K = kE_{\mathfrak{G}}k$ is now exactly the same as in 1, since the proof that $\widetilde{a}_i E_{\mathfrak{G}} a_k$ are matrix units used only (2b). As a full matrix ring over Ω, K contains every field of degree n as a subfield, in particular k.

3. — With a view toward ǧ III, I also note that the passage from K to $\bar{K}$ is possible even when K does not split.[6] Besides k, the field $\bar{k}$ is also a splitting field, and hence K is similar to $\bar{K}$, the crossed product of $\bar{\mathfrak{G}}$ with $\bar{k}$. Since k is a splitting field, the subgroup $\mathfrak{H}$ corresponding to k has factor system one; the idempotent $E_{\mathfrak{H}}$ is therefore defined as in 2. It follows conversely that K is isomorphic to $E_{\mathfrak{H}}\bar{K}E_{\mathfrak{H}}$. Indeed, this algebra is isomorphic to the automorphism ring of the left ideal $\bar{K}E_{\mathfrak{H}}$, hence is similar to $\bar{K}$. Its rank agrees with that of K: $\bar{K}E_{\mathfrak{H}}$ has rank n over $\bar{k}$ (the $\bar{u}_{S_i}^{-1}E_{\mathfrak{H}}$ are independent over $\bar{k}$), while $\bar{K}$ has rank nh. Thus $\bar{K}$ decomposes into h ideals isomorphic to $\bar{K}E_{\mathfrak{H}}$, which for the automorphism ring amounts to multiplication by the full matrix algebra of degree h.

When K, and hence $\bar{K}$, splits, this recovers the result of 2, since

$$\begin{aligned} E_{\mathfrak{H}}\bar{K}E_{\mathfrak{H}} &= E_{\mathfrak{H}}\bar{k}E_{\bar{\mathfrak{G}}}\bar{k}E_{\mathfrak{H}} = (E_{\mathfrak{H}}\bar{k}E_{\mathfrak{H}})E_{\bar{\mathfrak{G}}}(E_{\mathfrak{H}}\bar{k}E_{\mathfrak{H}}) \\ &= \mathrm{Sp}(\bar{k}/k)E_{\mathfrak{H}}E_{\bar{\mathfrak{G}}}E_{\mathfrak{H}}\,\mathrm{Sp}(\bar{k}/k) = kE_{\mathfrak{G}}k. \end{aligned}$$

[6] From this one obtains the analogue of the crossed-product representation in the non-Galois case; this will probably be worked out in a dissertation.

ğ II. — *The Maximal Orders of Split Crossed Products and Their Division into Domains*

From now on let Ω be a finite algebraic number field,[7] let K be a split algebra of degree n over Ω, and let k be a Galois or non-Galois maximal commutative subfield, so that $K = kE_{\mathfrak{G}}k$ by ğ I. Let $a, \widetilde{a}$ denote a pair of complementary finite $\mathfrak{o}$-modules in k (where $\mathfrak{o}$ is the principal order of Ω and o the principal order of k). The structure of the maximal orders of K relative to k is described by the following theorems.

THEOREM 1. — *The module product*

$$\mathfrak{O}_a = \widetilde{a}E_{\mathfrak{G}}a$$

is a maximal order of K; in particular

$$\mathfrak{O} = \mathfrak{O}_o = \widetilde{o}E_{\mathfrak{G}}o$$

is a maximal order.

THEOREM 2. — *The transformation of $\mathfrak{O}$ into $\mathfrak{O}_a$ is effected by the left ideal*

$$\mathfrak{L} = \widetilde{o}E_{\mathfrak{G}}a$$

and by its reciprocal right ideal

$$\mathfrak{R} = \widetilde{a}E_{\mathfrak{G}}o$$

with respect to $\mathfrak{O}$.

Remark. The occurrence of the two complementary modules $a, \widetilde{a}$ in the product $\mathfrak{LR}$ leads to the reciprocal relation precisely because of the trace formation caused by $E_{\mathfrak{G}}$, in contrast to the mere product $a\widetilde{a}$.

THEOREM 3. — *All left and right ideals with respect to $\mathfrak{O}$ are exhausted by those described in Theorem 2; consequently the maximal orders $\mathfrak{O}_a$ exhaust all maximal orders in K. Any two maximal orders $\mathfrak{O}_a$ and $\mathfrak{O}_b$ are transformed into one another by*

$$\mathfrak{L}_a = \widetilde{a}E_{\mathfrak{G}}b, \qquad \mathfrak{R}_a = \widetilde{b}E_{\mathfrak{G}}a,$$

and these exhaust the left and right ideals with respect to $\mathfrak{O}_a$.

THEOREM 4. — *As $\mathfrak{O}_a$ runs through all maximal orders of K, the intersection $[\mathfrak{O}_a, k]$ runs through all orders of k; this intersection is in each case the order of a. If all maximal orders belonging to the same order in k are grouped into one domain, then the transformations within a domain are given by left ideals $\widetilde{a}E_{\mathfrak{G}}b$ with respect to $\mathfrak{O}_a$ and by reciprocal right ideals, where a and b are modules of the corresponding order in k.*

THEOREM 4A. — *In particular, the transformation of the maximal orders of the principal domain—that is, the domain of all maximal orders containing the principal order o of k—is effected by ideals*

$$\widetilde{a}E_{\mathfrak{G}}b,$$

where a and b are ideals of k. Equivalently: if $\mathfrak{L}$ is a left ideal of a maximal order of the principal domain and o is contained in the right order of $\mathfrak{L}$, then $\mathfrak{L}$ is the extension of an o-ideal.

The proofs rest on passage to the individual places. It is enough in each case to pass to the quotient ring at p, where p runs through all prime ideals of Ω. Let $\mathfrak{o}$ denote the principal order of Ω, and let $\mathfrak{o}_p$ denote the quotient ring at p, that is, the principal ideal ring of all p-integral numbers of Ω, those representable with denominators prime to p. If $\mathfrak{C}$ is any $\mathfrak{o}$-module in K, call the extended module $\mathfrak{C}_p = \mathfrak{C}\mathfrak{o}_p$ its component. Then we have the

Lemma. $\mathfrak{C}$ is the intersection of all extension modules $\mathfrak{C}_p$. Indeed, if $w \in \mathfrak{C}_p$, there is a $\sigma \in \mathfrak{o}$ not divisible by p such that $\sigma w \in \mathfrak{C}$. Now let w lie in the intersection of all $\mathfrak{C}_p$, and let g be the ideal of all $\sigma \in \mathfrak{o}$ such that $\sigma w \in \mathfrak{C}$. As just shown, g can be divisible by no p, and hence $g = \mathfrak{o}$.[8] Notice that the lemma imposes no hypothesis on the rank of $\mathfrak{C}$.

Consequences. Every module is determined by its components. If $\mathfrak{D}$ is a proper overmodule of $\mathfrak{C}$, at least one $\mathfrak{D}_p$ is a proper overmodule of $\mathfrak{C}_p$. In particular, if $\mathfrak{M}$ is an order in K and all its components $\mathfrak{M}_p$ are maximal orders over $\mathfrak{o}_p$, then $\mathfrak{M}$ itself is maximal.

[7] The considerations of this section remain valid when Ω is a function field in one indeterminate.

[8] If places are defined by p-adic extension, the corresponding lemma reads: the intersection of all p-adic components $\mathfrak{C}^{(p)}$ with K equals $\mathfrak{C}$. This follows because $[\mathfrak{C}^{(p)}, K] = \mathfrak{C}_p$, as one sees by using an $\mathfrak{o}_p$-basis of $\mathfrak{C}_p$ which is at the same time a basis of $\mathfrak{C}^{(p)}$. In H., Theorem 66, the lemma is stated only for ideals of maximum rank.

Proof of Theorem 1. The module $\mathfrak{O}_a$ is an order: it is a finite $\mathfrak{o}$-module, because this is true of a and $\widetilde{a}$, and it has maximum rank. Moreover,

$$\mathfrak{O}_a^2 < \mathfrak{O}_a, \quad \text{since} \quad \mathfrak{O}_a^2 = \widetilde{a}E_{\mathfrak{G}}a \cdot \widetilde{a}E_{\mathfrak{G}}a = \widetilde{a}E_{\mathfrak{G}}a \cdot \mathrm{Sp}(\widetilde{a}a),$$

where $\mathrm{Sp}(\mathfrak{c})$ denotes in general the ideal in $\mathfrak{o}$ consisting of the traces of all elements of $\mathfrak{c}$.[9] Since $\mathrm{Sp}(\widetilde{a}a) < \mathfrak{o}$, it follows that $\mathfrak{O}_a^2 < \mathfrak{O}_a$.

To prove that $\mathfrak{O}_a$ is maximal (and hence contains o), it suffices, by the consequence above, to prove that each component is maximal. Since $\mathfrak{o}_p$ is a principal ideal ring, a_p and $\widetilde{a}_p$ have independent complementary bases $a_1, \ldots, a_n$ and $\widetilde{a}_1, \ldots, \widetilde{a}_n$. The products $\widetilde{a}_i E_{\mathfrak{G}} a_k$ form matrix units by ğ I; hence

$$\widetilde{a}_p E_{\mathfrak{G}} a_p = \sum_{i,k} c_{ik}\mathfrak{o}_p$$

is maximal.

Remark. Since $\mathfrak{O}_a$ is maximal, hence $\mathfrak{O}_a^2 = \mathfrak{O}_a$, it also follows that $\mathrm{Sp}(\widetilde{a}a) = \mathfrak{o}$. This follows directly as well because the relation holds at every place, as the complementary bases show, and hence holds without qualification by the lemma.

Proof of Theorem 2. The trace rule just established gives

$$\mathfrak{O}\mathfrak{L} = \widetilde{o}E_{\mathfrak{G}}o\,\widetilde{o}E_{\mathfrak{G}}a = \widetilde{o}E_{\mathfrak{G}}a = \mathfrak{L}, \qquad \mathfrak{R}\mathfrak{O} = \widetilde{a}E_{\mathfrak{G}}o\,\widetilde{o}E_{\mathfrak{G}}o = \widetilde{a}E_{\mathfrak{G}}o = \mathfrak{R},$$
$$\mathfrak{L}\mathfrak{R} = \widetilde{o}E_{\mathfrak{G}}a\,\widetilde{a}E_{\mathfrak{G}}o = \widetilde{o}E_{\mathfrak{G}}o = \mathfrak{O}, \qquad \mathfrak{R}\mathfrak{L} = \widetilde{a}E_{\mathfrak{G}}o\,\widetilde{o}E_{\mathfrak{G}}a = \widetilde{a}E_{\mathfrak{G}}a = \mathfrak{O}_a.$$

Proof of Theorem 3. Let $\mathfrak{L}$ be a left ideal with respect to $\mathfrak{O}$. Then, in particular,

$$\mathfrak{L} = \widetilde{o}E_{\mathfrak{G}}\mathfrak{L} = (\widetilde{o}E_{\mathfrak{G}}l_1, \ldots, \widetilde{o}E_{\mathfrak{G}}l_t),$$

where $l_1, \ldots, l_t$ may be taken as an $\mathfrak{o}$-basis of $\mathfrak{L}$. Write $l_\mu = \sum_i u_{S_i} z_{\mu,i}$ with $z_{\mu,i}$ in k.[10] Then

$$E_{\mathfrak{G}}l_\mu = E_{\mathfrak{G}}\sum_i z_{\mu,i} = E_{\mathfrak{G}}a_\mu,$$

and hence $\mathfrak{L} = \widetilde{o}E_{\mathfrak{G}}a$. If $\mathfrak{L}$ is regular, a must have maximum rank n, and $\widetilde{a}E_{\mathfrak{G}}o$ is then the reciprocal right ideal. By composition, $\widetilde{a}E_{\mathfrak{G}}b$ runs through all left ideals with respect to $\mathfrak{O}_a$, and $\widetilde{b}E_{\mathfrak{G}}a$ through the reciprocal right ideals.

Proof of Theorem 4. The intersection $t = [k, \mathfrak{O}_a]$ is an order, since $\mathfrak{O}_a$ consists only of integral elements. As a subset of $\mathfrak{O}_a$, it is a right multiplier domain, and indeed the largest order in o having this property; it therefore certainly contains the order o_a of a. To prove $t = o_a$, it again suffices to prove equality componentwise. Let t be an element of t_p. Then $c_{ik}t$, for every $c_{ik} = \widetilde{a}_i E_{\mathfrak{G}} a_k$, is a linear combination of the c_{ik} with integral coefficients, that is, coefficients in $\mathfrak{o}_p$. On the other hand, $a_k t$ is a linear combination of the a_k with coefficients in Ω_p. By uniqueness of the representation through the c_{ik}, those coefficients must lie in $\mathfrak{o}_p$; hence t lies in the order of a_p. Thus t equals the order of a. That every order of k can occur as such an intersection follows because the module a in k runs, in particular, through all orders. The transformation now follows immediately from Theorem 3.

Proof of Theorem 4a. This is merely the specialization of Theorem 4 to the principal domain. For the second formulation, begin with the initial maximal order $\mathfrak{O} = \widetilde{o}E_{\mathfrak{G}}o$. If o is also contained in the right order of $\mathfrak{L} = \widetilde{o}E_{\mathfrak{G}}a$, then $\widetilde{a}E_{\mathfrak{G}}a$ also belongs to the principal domain; hence a is an ideal of k and $\mathfrak{L} = \mathfrak{O}a$. Starting from $\mathfrak{O}_a$, correspondingly $\mathfrak{L} = \widetilde{a}E_{\mathfrak{G}}b$, and b, hence also $a^{-1}b$, is an ideal of k. Therefore

$$\mathfrak{L} = \widetilde{a}E_{\mathfrak{G}}aa^{-1}b = \mathfrak{O}_a a^{-1}b.$$

[9] Thus $\mathrm{Sp}(\mathfrak{c})$ denotes the ideal in $\mathfrak{o}$ formed by the traces of all elements of $\mathfrak{c}$.

[10] For non-Galois k, z must be replaced by $\bar{z}E_{\mathfrak{H}}$, and consequently a by $\bar{a}E_{\mathfrak{H}}$. This gives

$$E_{\mathfrak{G}}l = E_{\mathfrak{G}}\bar{a}E_{\mathfrak{H}} = E_{\mathfrak{G}}a$$

with a in k. Indeed, by (3), (4), and (5),

$$kE_{\mathfrak{G}}k = kE_{\mathfrak{G}}kE_{\mathfrak{H}} = \sum_i u_{S_i}\{k^{S_i}, k\}E_{\mathfrak{H}}.$$

ğ III. — *Maximal Orders of Arbitrary Crossed Products*

The theorems derived for split crossed products remain valid in the general case once the division into domains is refined. The facts about the principal domain then hold exactly; the remaining facts must be formulated as statements about the individual places. Here a place is to be understood as a p-adic extension.

Definition. Let K be a simple normal algebra over Ω, and let k be a maximal commutative subfield. A domain relative to k consists of all maximal orders of K which have the same intersection with k and which, in addition, have the same p-adic components at the ramified places of K. If the intersection with k is the principal order, one obtains a principal domain.

For principal domains we then have:

THEOREM 1. — *The maximal orders of a principal domain are transformed into one another by transformation with extension ideals of ideals of k. Equivalently, the left ideals of the maximal orders of a principal domain which are prime to the different and contain o in their right order are extensions of ideals of k.*

THEOREM 2. — *If K has prime degree, there is only one principal domain; it is transformed into itself by extension ideals of the k-ideals. The corresponding ideals of a fixed maximal order $\mathfrak{O}$ are the ideals of k extended by the two-sided ideals of $\mathfrak{O}$.*

Proof. Two maximal orders of a principal domain differ only at finitely many places; by definition these are places where K splits. There K has the form considered in ğğ I and II. This is clear when k is Galois, for then the factor system is associated with one and may therefore be replaced by the system one; by ğ I, 2 and 3, however, it also follows in the non-Galois case. Thus at every such place, and hence globally,[11] the ideals in question are extension ideals.

If K has prime degree, it is either split (ğ II) or a division algebra. In the latter case it remains a division algebra at all ramified places and therefore has only one principal domain, so transformation by extension ideals again applies. The most general transformation is obtained by composing the extension ideals with those which transform the maximal order into itself, namely with two-sided ideals. As is known, these differ from central ideals only at the ramified places, and hence differ only by extension ideals. This proves the remaining assertions.

We also have:

THEOREM 3. — *The maximal orders of an arbitrary domain are transformed into one another by ideals prime to the different which, at every place, are composed from modules of the corresponding order as described in ğ II, Theorem 3. For a fixed ideal, the components of these modules differ from the order at only finitely many places.*

This follows directly from ğ II; one need only note that the operators u_S at the individual places must be replaced by corresponding equivalent operators.

Whether, for every order of k, there are maximal orders having that order as their intersection requires closer investigation at the ramified places. A principal domain always exists, as follows from the crossed-product, or possibly generalized crossed-product, representation: it gives an order containing o once the factor systems are taken to be integral.[12]

A further question is to what extent the arithmetic division into domains can characterize the algebraic splitting fields. In other words, do different splitting fields always produce different domain decompositions, or already different principal domains? And do the principal domains of all splitting fields perhaps exhaust all maximal orders?

That such a characterization is certainly impossible by a single maximal order is shown by the simplest examples. For instance, the maximal order

$$\left[1, i, j, \frac{1+i+j+k}{2}\right]$$

of the quaternion field contains, besides the principal order $[1, i]$, also the principal order

$$\left[1, \frac{1+i+j+k}{2}\right]$$

of the field of third roots of unity.

Göttingen, August 1932.

[11] Compare H., ğ 8, or Hasse's preceding paper cited in note 4.

[12] Another proof is given by Hasse and Chevalley, notes 4 and 3.

43. Ideal Differentiation and the Different.

Journal f. d. reine u. angew. Math. 188 (1950), pp. 1–21

By *Emmy Noether* †.[13]

Introduction.

The principal theorem of ramification theory for algebraic number fields says, as is well known, that the different, the ramification ideal, is divisible at least by the $(\varrho-1)$-st power of a prime ideal which occurs to the ϱ-th power in its rational prime p; precisely by the $(\varrho-1)$-st power when ϱ is not divisible by p, and by a higher power when ϱ is divisible by p.

This is analogous to the fact that the derivative $f'(x)$ of a polynomial $f(x)$ is divisible at least by the $(\varrho-1)$-st power of a linear factor which occurs in $f(x)$ to the ϱ-th power; precisely by that power when ϱ is not divisible by the characteristic of the coefficient domain, and by a higher power when ϱ is divisible by that characteristic.

I shall show that this is more than a formal analogy. *The different can be regarded as the differential quotient of a defining ideal of the number field K in an associated integral polynomial domain in $x_1,\dots,x_n$, the differential quotient being taken at the point $x=\omega$, that is, at $x_1=\omega_1,\dots,x_n=\omega_n$, where $\omega_1,\dots,\omega_n$ is a module basis of the system of algebraic integers of K, the principal order $\mathfrak{o}$.* The defining ideal $\mathfrak{M}$ is the totality of the relations among the ω_i, namely all integral polynomials $f(x)$ such that $f(\omega)=0$. The differential quotient $\mathfrak{M}'[x\to\omega]$ is defined as a difference quotient at $x=\omega$.

Indeed, because $f(\omega)=0$, regard $\mathfrak{M}$ as consisting of all differences $f(x)-f(\omega)$. Form the difference ideal

$$\mathfrak{B}=(x_1-\omega_1,\dots,x_n-\omega_n)$$

and the difference quotient

$$\mathfrak{A}=\mathfrak{M}:\mathfrak{B},$$

where the quotient is the usual ideal quotient, taken in the polynomial domain in the x_i with coefficients in the integers of K, hence in $\mathfrak{o}$. The different $\mathfrak{D}$ is then defined by

$$\mathfrak{D}=\mathfrak{A}[x\to\omega].$$

The extension of the coefficient domain is necessary in order for the difference ideal and the difference quotient to be defined at all. Thus this is the direct generalization of the differential quotient of a polynomial in one indeterminate x,

$$f'(\xi)=\big(f(x)-f(\xi)\big):(x-\xi),$$

taken at $x=\xi$, where here as well the polynomial domain must be enlarged by adjoining ξ so that the differences are defined. In fact, the ideal differential quotient becomes the ordinary polynomial differential quotient as soon as the basis of the ω_i consists of powers of a single element.

The definition just given therefore attaches directly to familiar facts. It introduces, however, non-invariant intermediate objects, since the ideal $\mathfrak{M}$ depends on the chosen basis. An equivalent, *completely invariant definition* is obtained by replacing the integral polynomial domain by a ring $\mathfrak{O}$ isomorphic to the principal order $\mathfrak{o}$, hence isomorphic to the residue-class ring modulo $\mathfrak{M}$, and extending its coefficient domain by $\mathfrak{o}$ to form $\mathfrak{O}_\mathfrak{o}$.[14] The difference ideal $\mathfrak{B}$ is generated by all differences $x-\xi$, where x and ξ correspond under the isomorphism from $\mathfrak{O}$ to $\mathfrak{o}$; the difference quotient $\mathfrak{A}$ is the quotient of the zero ideal by $\mathfrak{B}$; and the different is obtained from $\mathfrak{A}$ by replacing each x by its corresponding ξ.

This invariant definition is placed first below. It defines at once the different of an arbitrary commutative ring relative to a subring, subject only to hypotheses ensuring that coefficient extension is possible. These hypotheses are automatically satisfied, for example, when a module basis exists, possibly after passage to suitable quotient rings. Thus one obtains, in particular, the different of an arbitrary order in a number field, the different of a residue-class ring of an order modulo a prime-power, relative differents, and differents for algebraic functions of several indeterminates.

[13] This posthumous paper by E. Noether, written in the winter of 1927/28, was kindly made available to the editor by H. Grell. It gives a detailed account of the lecture with the same title delivered at the 1929 meeting of the German Mathematical Society in Prague; see Jahresbericht D.M.V. 39 (1930), p. 17, in italics. From §6, 3 onward, the manuscript was evidently still intended to receive a more exact revision. A knowledgeable reader will nevertheless readily understand the sketch-like exposition, which has been left unchanged here apart from minor rounding-off.

[14] The extension of the coefficient domain—direct product formation—is treated in §1 also for noncommutative rings, more generally than is required for the purposes of this paper. For those purposes §2, specialized to commutative rings and a finite basis, is sufficient.

The agreement of this differential definition with the usual definition follows from a precise structural analysis, based on direct-sum decomposition, of the Galois extension ring attached to the number field by direct product formation.[15] In the special case of a residue-class ring modulo a polynomial in one indeterminate, this analysis becomes an analysis of the Lagrange interpolation formula. More precisely, the following is meant.

Introduce a ring $\mathfrak{K}$ isomorphic to the number field K and containing $\mathfrak{O}$, and extend its coefficient field, the rational field, by the Galois closure F of K. The extended system $\mathfrak{K}_F$ is a direct sum of n simple components corresponding to the n isomorphisms of K, that is, to passage to the conjugate fields. These components are extensions of the difference quotient $\mathfrak{A}$ and of its conjugates; at the same time the zero ideal of $\mathfrak{K}_F$ is the intersection of the n ideals obtained from the difference ideal and its conjugates. The simple components are of the form $Fe^{(i)}$, where $e^{(i)}$ is the corresponding component of the identity. Since $e^{(i)}$ goes over to the identity under $x = \xi$, the difference quotient is $\mathfrak{d}e^{(i)}$, where $\mathfrak{d}$ denotes the different of $\mathfrak{o}$. Thus $\mathfrak{d}$ consists precisely of those elements of the field which, when multiplied by $e^{(i)}$, lie in $\mathfrak{O}_\mathfrak{o}$, the direct product of the order with itself. The corresponding assertions hold for the conjugates.

To recover the definition by the complementary module, observe that $e^{(i)}$ is a linear form in the basis $x_1, \ldots, x_n$ of $\mathfrak{O}$, or of $\mathfrak{K}$, corresponding to the ω_i. The coefficients of the x_i in the $e^{(i)}$ form a basis of the complementary module of $\mathfrak{o}$ and of its conjugates. Since the difference quotient $\mathfrak{A}$ has coefficients in $\mathfrak{o}$, the different is the quotient of $\mathfrak{o}$ by its complementary module. This is Dedekind's definition. The construction is not restricted to the principal order; it characterizes the different of every order as the quotient of the order by its complementary module.

In the principal-order case, the agreement with the definition by a fundamental equation follows from the fact already mentioned: the ideal differential quotient becomes the polynomial differential quotient when the basis consists of powers of one element, here the fundamental form. The conceptual relation between this latter definition and Dedekind's is thereby obtained.

With a fundamental equation in the principal-order case one obtains directly the principal ramification theorem mentioned at the start. For the exact determination of exponents one considers the different $\mathfrak{d}[p^t]$ of the residue-class ring of the principal order modulo p^t, with t sufficiently large; $t = n$ is enough, and for quadratic fields is also necessary. The crucial point is that the different $\mathfrak{d}$, reduced modulo p^t, passes exactly into $\mathfrak{d}[p^t]$. Since a direct sum of rings gives the direct sum of their differents, one may restrict to the residue-class ring modulo $\mathfrak{p}^{t\varrho}$. This ring is isomorphic to a residue-class ring modulo a polynomial in one indeterminate with coefficients modulo p^t; differentiating this polynomial gives, as Ö. Ore showed by another route,[16] the exact survey of possible exponents by means of the supplement numbers.

Finally, the structural analysis also gives the known theorem that the different of an overfield of K is the product of the relative different and the different of K. This follows from the fact that the same multiplication property holds for the identity components of the direct-sum decomposition and hence for complementary modules.

All the preceding facts hold in the same manner for relative differents after passage to suitable quotient rings, just as I carried this out for relative discriminants in the paper on discriminants. By passage to the function domain, everything also remains valid for algebraic function fields with coefficient field of characteristic zero. In characteristic p, and for integral algebraic functions, the structural properties remain—essentially even without passage to the function domain—but the ramification theory changes because inseparable extension fields can occur; this will not be developed here. The most important results are the completely invariant structural theorems sketched above (ğğ5 and 6), which also apply to algebraic functions of several indeterminates. Passage to the complementary module already amounts to resolving the result into coefficient identities and is carried out only to place known facts in their proper setting.

ğ1. Extension of the Coefficient Domain of a Ring, or Direct Product Formation. Defining Ideals[17]

In this section general rings are considered; multiplication is not assumed commutative. For simplicity, however, the existence of an identity element is assumed here and, unless the contrary is explicitly stated, throughout the paper.

[15] This continues the considerations underlying my paper on discriminants, but no knowledge of that paper is assumed. See E. Noether, "Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl- und Funktionenkörpers," J. Math. 157 (1927), 82–104.

[16] Editor's note: This citation was not completed in the manuscript. See the references in ğ7 of the paper, which survives only in sketch form.

[17] I am indebted to B. L. van der Waerden for critical comments on this section.

1. Definition of the direct product. A ring $\mathfrak{O} \times \mathfrak{o}$, or $\mathfrak{O}_\mathfrak{o}$, is called the *direct product* of the rings $\mathfrak{O}$ and $\mathfrak{o}$ relative to $\mathfrak{h}$, or the ring *obtained from* $\mathfrak{O}$ *by extending the coefficient domain* $\mathfrak{h}$ *to* $\mathfrak{o}$,[18] if the following conditions hold:

(1) $\mathfrak{O}_\mathfrak{o}$ contains $\mathfrak{O}$ and $\mathfrak{o}$ as subrings and is the product of these rings, that is, the intersection of all rings in $\mathfrak{O}_\mathfrak{o}$ which contain both $\mathfrak{O}$ and $\mathfrak{o}$.

(2) The intersection of $\mathfrak{O}$ and $\mathfrak{o}$ is $\mathfrak{h}$, and $\mathfrak{h}$ contains the identity element of $\mathfrak{O}_\mathfrak{o}$.

(3) The elements of $\mathfrak{O}$ commute elementwise with those of $\mathfrak{o}$. Thus $\mathfrak{O}_\mathfrak{o}$ consists of all finite bilinear combinations

$$x_{i_1} y_{i_1} + \cdots + x_{i_r} y_{i_r},$$

where the x's and the y's run through all finite systems of elements of $\mathfrak{O}$ and $\mathfrak{o}$, respectively; moreover, $\mathfrak{h}$ lies in the centers of $\mathfrak{O}$ and $\mathfrak{o}$, and hence in the center of $\mathfrak{O}_\mathfrak{o}$.

(4) Two elements of $\mathfrak{O}_\mathfrak{o}$ are equal only if, and of course whenever, they can be made formally equal in at least one way by means of the relations holding in $\mathfrak{O}$ on the one hand and in $\mathfrak{o}$ on the other. More precisely, if

$$x_1 y_1 + \cdots + x_n y_n = 0 \quad \text{in } \mathfrak{O}_\mathfrak{o},$$

then, by adding sums of formally vanishing expressions

$$(\gamma h)\delta - \gamma(h\delta),$$

where $h \in \mathfrak{h}$, $\gamma \in \mathfrak{O}$, and $\delta \in \mathfrak{o}$, the expression can be transformed into

$$(z_1\alpha_1 + \cdots + z_r\alpha_r) + (t_1\beta_1 + \cdots + t_s\beta_s),$$

with $z_1 = 0, \ldots, z_r = 0$ and $\beta_1 = 0, \ldots, \beta_s = 0$, where $\alpha, \beta \in \mathfrak{o}$ and $z, t \in \mathfrak{O}$. Thus the equations $z = 0$ express relations among the x, γ, h in $\mathfrak{O}$, and the equations $\beta = 0$ express relations among the y, δ, h in $\mathfrak{o}$.[19]

Two elements of $\mathfrak{O}_\mathfrak{o}$ are therefore equal only if their difference vanishes in the manner just described.

The requirement of being a direct product thus determines equality and the operations of addition and multiplication uniquely from the corresponding laws in the factors. It follows that if $\mathfrak{O}, \mathfrak{o}$, and their intersection $\mathfrak{h}$ correspond isomorphically to $\overline{\mathfrak{O}}, \overline{\mathfrak{o}}$, and $\overline{\mathfrak{h}}$, and if $\mathfrak{O} \times \mathfrak{o}$ exists, then $\overline{\mathfrak{O}} \times \overline{\mathfrak{o}}$ also exists and is isomorphic to $\mathfrak{O} \times \mathfrak{o}$.

Every ring $\mathfrak{S}$ which is the product of $\mathfrak{O}$ and $\mathfrak{o}$, with the two factors commuting elementwise, is a homomorphic image of $\mathfrak{O} \times \mathfrak{o}$, and the mappings of $\mathfrak{O}$ and $\mathfrak{o}$ remain isomorphisms. Indeed, equality in $\mathfrak{O} \times \mathfrak{o}$ is included in equality in $\mathfrak{S}$, and on $\mathfrak{O}$ and $\mathfrak{o}$ it agrees with their equality in the direct product.[20]

2. Necessary and sufficient conditions for existence of the direct product relative to a subring. Let $\mathfrak{O}$ and $\mathfrak{o}$ be rings whose intersection is the ring $\mathfrak{h}$, lying in the center of each. The direct product relative to $\mathfrak{h}$ need not exist. For example, take $\mathfrak{h}$ to be the ring of rational integers, $\mathfrak{O} = \mathfrak{h}[x]$ with the relation $1 - 2x = 0$, and $\mathfrak{o} = \mathfrak{h}[y]$ with $1 - 2y = 0$, where y is a new symbol. Then $\mathfrak{O}$ and $\mathfrak{o}$ are equivalent extensions of $\mathfrak{h}$, with set-theoretic intersection $\mathfrak{h}$, and no relations have been prescribed between x and y. There is no ring R containing $\mathfrak{O}$ and $\mathfrak{o}$ in which their intersection remains $\mathfrak{h}$, for in any such ring

$$0 = (1 - 2x)y - x(1 - 2y) = y - x,$$

even without using commutativity of x and y.[21]

The *necessary and sufficient condition for existence of the direct product* is:

There must exist at least one ring R *containing* $\mathfrak{O}$ *and* $\mathfrak{o}$ *such that their intersection is* $\mathfrak{h}$ *and they commute elementwise.*

[18] The second notation, used mostly below, is intended to recall extension of the coefficient domain; the first is the usual designation for the direct product.

[19] If the existence of an identity element is not assumed, additional linear terms occur in (3) and (4).

[20] See also ğ1, 4.

[21] The quotient ring of a commutative ring lying in a fixed overring—here the adjunction of $\frac{1}{2}$—is unique. This is analogous to the fact that two equivalent, distinct Galois field extensions cannot be embedded in a common overfield. Direct product formation nevertheless permits an embedding in a ring with zero divisors.

If the direct product exists, it is itself such a ring R. Conversely, to construct the direct product, one may assume—as will always be done below—that no relations have been prescribed between elements of $\mathfrak{O} \setminus \mathfrak{h}$ and $\mathfrak{o} \setminus \mathfrak{h}$, since this can always be achieved by passage to equivalent extensions of $\mathfrak{h}$, introducing new symbols.[22] Assume also that $\mathfrak{h}$ contains the identity e of $\mathfrak{O}$ and $\mathfrak{o}$, subject to the qualification in footnote 7.

Define $\mathfrak{T}$ as the set of all finite bilinear combinations

$$x_{i_1} y_{i_1} + \cdots + x_{i_r} y_{i_r} = y_{i_1} x_{i_1} + \cdots + y_{i_r} x_{i_r},$$

where the x's and y's run through finite systems from $\mathfrak{O}$ and $\mathfrak{o}$, respectively, and are declared to commute in $\mathfrak{T}$. Two such combinations are equal exactly when they become formally equal by the relations in $\mathfrak{O}$ and $\mathfrak{o}$, in the sense made precise in 1, (4). For

$$\alpha_{i_1} x_{i_1} + \cdots + \alpha_{i_r} x_{i_r} \quad \text{and} \quad \beta_{i_1} x_{i_1} + \cdots + \beta_{i_r} x_{i_r},$$

where some α's or β's may be zero, define their sum and product by

$$(\alpha_{i_1} + \beta_{i_1}) x_{i_1} + \cdots + (\alpha_{i_r} + \beta_{i_r}) x_{i_r}$$

and

$$\sum_{\lambda,\mu} \alpha_{i_\lambda} \beta_{i_\mu} x_{i_\lambda} x_{i_\mu},$$

respectively.

These definitions are unambiguous with respect to the equality just defined, because multiplying a zero relation of the kind in 1, (4) on either side by an element of $\mathfrak{o}$ or $\mathfrak{O}$ again gives such a relation, and the same holds for sums and differences of zero relations. The system $\mathfrak{T}$ is a ring containing $\mathfrak{O}$ and $\mathfrak{o}$ and satisfies the equality, addition, and multiplication requirements of the direct product. It also satisfies the intersection requirement, by the assumed existence of the common embedding. Indeed, let $\mathfrak{S}$ be the product of $\mathfrak{O}$ and $\mathfrak{o}$ in R. By 1, $\mathfrak{S}$ is a homomorphic image of $\mathfrak{T}$, isomorphically on $\mathfrak{O}$ and on $\mathfrak{o}$. A relation $x = y$ in $\mathfrak{T}$, with $x \in \mathfrak{O}$ and $y \in \mathfrak{o}$, therefore yields the same relation in $\mathfrak{S}$; by assumption both elements then lie in $\mathfrak{h}$, and the separate isomorphisms on $\mathfrak{O}$ and $\mathfrak{o}$ imply the same for $\mathfrak{T}$. The embedding condition is therefore necessary and sufficient.

3. Defining ideal of a ring relative to a subring. A system S of elements $\ldots, z, \ldots$ of $\mathfrak{O}$ is called a *generating system* of $\mathfrak{O}$ relative to $\mathfrak{h}$ if $\mathfrak{O}$ is the ring generated by $\mathfrak{h}$ and S, that is, the intersection of all rings in $\mathfrak{O}$ containing $\mathfrak{h}$ and S. In symbols, $\mathfrak{O} = \mathfrak{h}[S]$. Assume again that $\mathfrak{h}$ is a subring of the center of $\mathfrak{O}$. Then $\mathfrak{O}$ is a homomorphic image of the noncommutative polynomial domain $\mathfrak{h}[\ldots Z \ldots]$, where the indeterminates Z have the same cardinality as S. This polynomial domain consists of all finite sums $\sum h_i P_i = \sum P_i h_i$, where the P_i are power-products, including the identity corresponding to exponent zero:

$$P_i = Z_{i_1}^{\varrho_1} Z_{i_2}^{\varrho_2} \cdots Z_{i_n}^{\varrho_n},$$

with repetitions of indices allowed; equality is coefficientwise equality with respect to the distinct power-products.

The homomorphism gives

$$\mathfrak{O} \simeq \mathfrak{h}[\ldots Z \ldots]/\mathfrak{M},$$

where the two-sided ideal $\mathfrak{M}$ consists of all polynomials $F(Z)$ for which $F(z) = 0$ in $\mathfrak{O}$, with Z and z corresponding under the homomorphism. *The ideal $\mathfrak{M}$ is called a defining ideal relative to $\mathfrak{h}$, specifically the defining ideal corresponding to the generating system of the z's.* Isomorphic rings, with isomorphically corresponding subrings $\mathfrak{h}, \overline{\mathfrak{h}}$ and generating systems $S, \overline{S}$, have isomorphic defining ideals; if $\overline{\mathfrak{h}} = \mathfrak{h}$, the ideals may in particular be taken as identical.

Since $\mathfrak{h}$ lies in the center of $\mathfrak{O}$, the ring $\mathfrak{O}$ is certainly commutative if it has a generating system consisting of a single element z. If $\mathfrak{M}$ is then principal, an equation $G(z) = 0$, where $G(Z)$ is a basis polynomial of $\mathfrak{M}$, is called a defining equation of $\mathfrak{O}$ relative to $\mathfrak{h}$.

[22] See ğ2, 1 and footnote 12.

4. The defining ideal of a direct product. Let

$$\mathfrak{O} \simeq \mathfrak{h}[\ldots Z \ldots]/\mathfrak{M},$$

as in 3, where $\mathfrak{M}$ is a defining ideal. Alongside $\mathfrak{h}[\ldots Z \ldots]$, consider the polynomial domain $\mathfrak{o}[\ldots Z \ldots]$, consisting of all finite sums

$$\sum \gamma_i P_i = \sum P_i \gamma_i, \qquad \gamma_i \in \mathfrak{o},$$

with equality defined coefficientwise. The ring $\mathfrak{o}[\ldots Z \ldots]$ contains $\mathfrak{h}[\ldots Z \ldots]$ and is its direct product with $\mathfrak{o}$ relative to $\mathfrak{h}$; equivalently, it is obtained by extending the coefficient domain.[23]

Let $\mathfrak{M}_\mathfrak{o}$ be the extension ideal generated by $\mathfrak{M}$ in $\mathfrak{o}[\ldots Z \ldots]$, that is, the intersection of all two-sided ideals containing $\mathfrak{M}$. It consists of all linear combinations of elements of $\mathfrak{M}$ with coefficients in $\mathfrak{o}$, and because $\mathfrak{o}$ commutes with the Z's this already forms a two-sided ideal. *If the direct product* $\mathfrak{O}_\mathfrak{o}$ *relative to* $\mathfrak{h}$ *exists, then*

$$\mathfrak{O}_\mathfrak{o} \simeq \mathfrak{o}[\ldots Z \ldots]/\mathfrak{M}_\mathfrak{o}.$$

Indeed, $\mathfrak{O}_\mathfrak{o}$ is a homomorphic image of $\mathfrak{o}[\ldots Z \ldots]$, hence isomorphic to the residue-class ring modulo the defining ideal of $\mathfrak{O}_\mathfrak{o}$ relative to $\mathfrak{o}$ for the generating system of the z's. By the equality definition in 1, (4), every relation among the z's in $\mathfrak{O}_\mathfrak{o}$ is a linear combination, with coefficients in $\mathfrak{o}$, of relations already holding in $\mathfrak{O}$. Thus $\mathfrak{M}_\mathfrak{o}$ is the defining ideal.

Remark. The same argument gives a symmetric, though more cumbersome, presentation of the direct product and its defining ideal. Suppose

$$\mathfrak{o} \simeq \mathfrak{h}[\ldots Y \ldots]/\mathfrak{N},$$

where the Y's are symbols distinct from the Z's, so that $\mathfrak{h}[\ldots Y \ldots Z \ldots]$ is defined. Then

$$\mathfrak{O}_\mathfrak{o} \simeq \mathfrak{h}[\ldots Y \ldots Z \ldots]/(\mathfrak{M}, \mathfrak{N}, \ldots, YZ - ZY, \ldots),$$

where the defining ideal on the right is generated by $\mathfrak{M}$, $\mathfrak{N}$, and all expressions $YZ - ZY$. The latter express commutativity of the elements of $\mathfrak{o}$ with those of $\mathfrak{O}$; the former express that every relation in $\mathfrak{O}_\mathfrak{o}$ follows from relations holding separately in $\mathfrak{O}$ and $\mathfrak{o}$.

ğ2. Rings with Independent Module Bases. Construction of the Direct Product.

1. Construction of the direct product. A system T of elements $\ldots, t, \ldots$ of $\mathfrak{O}$ is called an $\mathfrak{h}$-module basis of $\mathfrak{O}$ if $\mathfrak{O}$ is the $\mathfrak{h}$-module generated by T in $\mathfrak{O}$. Since the identity lies in $\mathfrak{h}$, the ring $\mathfrak{O}$ then consists of all finite linear combinations $h_{i_1} t_{i_1} + \cdots + h_{i_r} t_{i_r}$. The module basis is called independent if

$$h_{i_1} t_{i_1} + \cdots + h_{i_r} t_{i_r} = 0 \quad \Longrightarrow \quad h_{i_1} = 0, \ldots, h_{i_r} = 0.$$

If $\mathfrak{O}$ *has an independent module basis containing the identity, then the direct product* $\mathfrak{O}_\mathfrak{o}$ *exists for every extension ring* $\mathfrak{o}$ *of* $\mathfrak{h}$*, provided only that* $\mathfrak{h}$ *is a subring of the center and that the set-theoretic intersection* $[\mathfrak{O}, \mathfrak{o}]$ *is* $\mathfrak{h}$.[24]

By ğ1, 2 it is enough to construct a suitable embedding ring $\mathfrak{R}$, which here will already prove to be the direct product. Define $\mathfrak{R}$ as the set of all finite linear combinations

$$\gamma_{i_1} t_{i_1} + \cdots + \gamma_{i_r} t_{i_r} = t_{i_1} \gamma_{i_1} + \cdots + t_{i_r} \gamma_{i_r},$$

where the t_{i_ν} run through finite systems from the independent basis T, and the corresponding γ's lie in $\mathfrak{o}$. Equality is coefficientwise equality in the t_{i_ν}; sums and products are defined by the usual rules, as in ğ1, 2. By the basis property, the product of any two basis elements is a finite linear combination of basis elements with coefficients in $\mathfrak{h}$, and hence $\mathfrak{R}$ is a ring. It contains $\mathfrak{O}$, since $\mathfrak{h} \subseteq \mathfrak{o}$, and it contains $\mathfrak{o}$, since T contains the identity. Since the γ's commute with the coefficients h_{i_ν} and with the t_{i_ν}, the subrings $\mathfrak{O}$ and $\mathfrak{o}$ commute elementwise in $\mathfrak{R}$.

[23] The equality and operation conditions are immediate, and the equality $\gamma = h + h_1 P_1 + \cdots + h_r P_r$ in $\mathfrak{o}[\ldots Z \ldots]$ implies $\gamma = h$. See also ğ2, 2. The fact that $\mathfrak{o}[\ldots Z \ldots]$ is a direct product is not used in this paragraph.

[24] Symmetrically, the basis assumption could instead be imposed on $\mathfrak{o}$. Without loss of generality, one assumes that no relations have been prescribed between elements of $\mathfrak{O} \setminus \mathfrak{h}$ and $\mathfrak{o} \setminus \mathfrak{h}$; see E. Noether, "Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl- oder Funktionenkörpers," J. Math. 157 (1927), 82–104, ğğ1, 2.

Finally, their intersection in $\mathfrak{R}$ is $\mathfrak{h}$. Indeed, a relation

$$\gamma = \gamma e = h_1 t_1 + \cdots + h_r t_r$$

implies, by coefficientwise equality and because e is a basis element, that one of the t's is e, that all the others have zero coefficient, and therefore that $\gamma = h$. Thus the direct product exists and equals $\mathfrak{R}$; the independence of the basis reduces the formal equality condition to coefficientwise equality. The basis T of $\mathfrak{O}$ is at the same time an $\mathfrak{o}$-basis of $\mathfrak{O}_\mathfrak{o}$.

2. Extension and contraction modules. If $\mathfrak{B}$ is an $\mathfrak{h}$-module in $\mathfrak{O}$, its extension $\mathfrak{B}_\mathfrak{o}$ is the $\mathfrak{o}$-module in $\mathfrak{O}_\mathfrak{o}$ obtained as the intersection of all $\mathfrak{o}$-modules containing $\mathfrak{B}$. If $\mathfrak{C}$ is an $\mathfrak{o}$-module in $\mathfrak{O}_\mathfrak{o}$, its contraction to $\mathfrak{O}$ is the intersection $[\mathfrak{C}, \mathfrak{O}]$. If $\mathfrak{B}$ is also an ideal in $\mathfrak{O}$, then $\mathfrak{B}_\mathfrak{o}$ is an ideal in $\mathfrak{O}_\mathfrak{o}$; if $\mathfrak{C}$ is an ideal in $\mathfrak{O}_\mathfrak{o}$, then $[\mathfrak{C}, \mathfrak{O}]$ is an ideal in $\mathfrak{O}$.

Theorem. *If a module $\mathfrak{B}$ in $\mathfrak{O}$ has an independent $\mathfrak{h}$-module basis which can be completed to an independent $\mathfrak{h}$-module basis of $\mathfrak{O}$, then $\mathfrak{B}$ is the contraction of its extension $\mathfrak{B}_\mathfrak{o}$ in $\mathfrak{O}_\mathfrak{o}$.*

Proof. Let T be an independent $\mathfrak{h}$-module basis of $\mathfrak{B}$, completed by a system $\overline{T}$ of elements $\bar{t} \in \mathfrak{O}$ to an independent $\mathfrak{h}$-module basis of $\mathfrak{O}$. Then T is also an independent $\mathfrak{o}$-basis of $\mathfrak{B}_\mathfrak{o}$, and $T, \overline{T}$ together form such a basis of $\mathfrak{O}_\mathfrak{o}$.

Certainly $\mathfrak{B} \subseteq [\mathfrak{B}_\mathfrak{o}, \mathfrak{O}]$. Conversely, let c belong to this contraction. As an element of $\mathfrak{B}_\mathfrak{o}$, it has a representation

$$c = \gamma_1 t_1 + \cdots + \gamma_r t_r, \qquad \gamma_i \in \mathfrak{o},$$

which is also a representation in the $\mathfrak{o}$-basis $T, \overline{T}$ of $\mathfrak{O}_\mathfrak{o}$. As an element of $\mathfrak{O}$, it also has a representation in the $\mathfrak{h}$-basis $T, \overline{T}$:

$$c = h_{i_1} t_{i_1} + \cdots + h_{i_r} t_{i_r} + h_{j_1} \bar{t}_{j_1} + \cdots + h_{j_s} \bar{t}_{j_s}.$$

Because $\mathfrak{O} \subseteq \mathfrak{O}_\mathfrak{o}$ and $\mathfrak{h} \subseteq \mathfrak{o}$, this too is a representation in the $\mathfrak{o}$-basis $T, \overline{T}$. Coefficientwise equality forces the coefficients of all $\bar{t}$'s to vanish and gives

$$c = h_1 t_1 + \cdots + h_r t_r,$$

so $c \in \mathfrak{B}$. Thus $\mathfrak{B}$ is the contraction.

Supplementary remark. The proof uses slightly weaker hypotheses than those stated and proves the remaining ones. In sharpened form:

The module $\mathfrak{B}$ is the contraction of its extension $\mathfrak{B}_\mathfrak{o}$ if $\mathfrak{O}$ has an independent $\mathfrak{h}$-basis $T, \overline{T}$, with $T \subseteq \mathfrak{B}$, such that T is also an independent $\mathfrak{o}$-basis of $\mathfrak{B}_\mathfrak{o}$. It then follows that T is an independent $\mathfrak{h}$-basis of $\mathfrak{B}$.

3. A sufficient criterion for existence of the direct product. It can happen, for example with the relative different, that an independent module basis exists only after extending the coefficient domain $\mathfrak{h}$. Existence of the direct product may then follow from the following sufficient criterion:

If there is an extension ring $\mathfrak{f}$ of $\mathfrak{h}$ such that the direct products $\mathfrak{O}_\mathfrak{f}$ and $\mathfrak{o}_\mathfrak{f}$ relative to $\mathfrak{h}$, and then $\mathfrak{O}_\mathfrak{f} \times \mathfrak{o}_\mathfrak{f}$ relative to $\mathfrak{f}$, exist, then $\mathfrak{O} \times \mathfrak{o}$ exists relative to $\mathfrak{h}$.

It remains to show that

$$\mathfrak{R} = \mathfrak{O}_\mathfrak{f} \times \mathfrak{o}_\mathfrak{f}$$

is an embedding ring in the sense of ğ1, 2. The subrings $\mathfrak{O}$ and $\mathfrak{o}$, contained in $\mathfrak{O}_\mathfrak{f}$ and $\mathfrak{o}_\mathfrak{f}$, commute elementwise; moreover,

$$[\mathfrak{O}, \mathfrak{o}] \subseteq [\mathfrak{O}_\mathfrak{f}, \mathfrak{o}_\mathfrak{f}] = \mathfrak{f}.$$

Also $[\mathfrak{O}, \mathfrak{o}] \subseteq \mathfrak{O}$, hence

$$[\mathfrak{O}, \mathfrak{o}] \subseteq [\mathfrak{O}, \mathfrak{f}] = \mathfrak{h}.$$

Therefore $[\mathfrak{O}, \mathfrak{o}] = \mathfrak{h}$, and $\mathfrak{R}$ is an embedding ring.

Remark. The proof uses the intersection condition only for $\mathfrak{O}_\mathfrak{f}$, not for $\mathfrak{o}_\mathfrak{f}$; the latter ring may therefore simply be the product of $\mathfrak{o}$ and $\mathfrak{f}$.

ğ3. The Different of a Ring over a Subring. Differential Quotient of a Defining Ideal.

From now on all rings under consideration are assumed commutative.[25] We also assume throughout that $\mathfrak{O}$ and $\mathfrak{o}$ are isomorphic, equivalent extensions of the subring $\mathfrak{h}$, so that the isomorphism from $\mathfrak{O}$ to $\mathfrak{o}$ extends the identity on $\mathfrak{h}$, and that the direct product $\mathfrak{O}_\mathfrak{o}$ relative to $\mathfrak{h}$ exists.

1. Definition of the different. Let x run through the elements of $\mathfrak{O}$, and let ξ denote in each case the corresponding element of $\mathfrak{o}$. Let $\mathfrak{B}$ be the two-sided *difference ideal* of $\mathfrak{O}_\mathfrak{o}$ generated by all differences $x-\xi$:

$$\mathfrak{B} = \{\ldots, (x-\xi), \ldots\}.^{26}$$

The *difference quotient* $\mathfrak{A}$ is the ideal quotient of the zero ideal by $\mathfrak{B}$; it consists of all $a \in \mathfrak{O}_\mathfrak{o}$ for which $a\mathfrak{B} = 0$:

$$\mathfrak{A} = (0) : \mathfrak{B}.$$

The *different* $\mathfrak{d}$ of $\mathfrak{o}$ relative to $\mathfrak{h}$ is defined by

$$\mathfrak{d} = \mathfrak{A}[x \to \xi].$$

Thus, in every element

$$a = \alpha_1 x_1 + \cdots + \alpha_r x_r \quad \text{of } \mathfrak{A},$$

the x's are replaced by their isomorphically corresponding ξ's. Correspondingly, the different $\mathfrak{D}$ of $\mathfrak{O}$ relative to $\mathfrak{h}$ is defined as $\mathfrak{A}[\xi \to x]$. Since $\mathfrak{A}$ is defined symmetrically in x and ξ, the ideals $\mathfrak{d}$ and $\mathfrak{D}$ correspond under the isomorphism between $\mathfrak{o}$ and $\mathfrak{O}$, being obtained from one another by interchanging ξ and x. Since $\mathfrak{A}$ is an ideal in $\mathfrak{O}_\mathfrak{o}$, and hence both an $\mathfrak{o}$-module and an $\mathfrak{O}$-module, $\mathfrak{d}$ and $\mathfrak{D}$ are ideals in $\mathfrak{o}$ and $\mathfrak{O}$, respectively.

2. Differential quotient of a defining ideal. Let $\mathfrak{M}$ be a defining ideal of $\mathfrak{O}$ relative to $\mathfrak{h}$, corresponding to the generating system of the z's (ğ1, 3). Then $\mathfrak{M}$ is also a defining ideal of $\mathfrak{o}$ relative to $\mathfrak{h}$, corresponding to the isomorphic generating system of the ξ's, and (ğ1, 4)

$$\mathfrak{O}_\mathfrak{o} \simeq \mathfrak{o}[\ldots Z \ldots]/\mathfrak{M}_\mathfrak{o}.$$

In the polynomial domain $\mathfrak{o}[\ldots Z \ldots]$, define the difference ideal and difference quotient by

$$\mathfrak{Q} = \{\ldots, (Z-\xi), \ldots\}$$

and

$$\begin{aligned}\mathfrak{C} &= \mathfrak{M}_\mathfrak{o} : \mathfrak{Q} \\ &= \{\ldots, (F(Z)-F(\xi)), \ldots\} : \{\ldots, (Z-\xi), \ldots\}.\end{aligned}$$

The *differential quotient* $\mathfrak{M}'$ is defined as $\mathfrak{C}[\xi \to Z]$. This definition is unambiguous and independent of the chosen *representation* of the elements of $\mathfrak{o}$ by the generators ξ. Indeed, since $\mathfrak{C}$ is an ideal quotient it contains $\mathfrak{M}_\mathfrak{o}$; two representations of the same element of $\mathfrak{o}$ differ by a polynomial $F(\xi)$, and after replacing ξ by Z they differ by $F(Z) \in \mathfrak{M} \subseteq \mathfrak{C}$. The ideal $\mathfrak{M}'$ is an ideal in $\mathfrak{h}[\ldots Z \ldots]$ containing $\mathfrak{M}$.

Under $Z \to \xi$, the differential quotient $\mathfrak{M}'$ goes over into the different $\mathfrak{d}$ of $\mathfrak{o}$. Under a homomorphism, ideals and their quotients correspond. Thus $\mathfrak{A}$ is the homomorphic image of $\mathfrak{C}$ under the homomorphism from $\mathfrak{o}[\ldots Z \ldots]$ to $\mathfrak{O}_\mathfrak{o}$ given by $Z \mapsto z$, because $\mathfrak{Q}$ maps to the zero ideal and $\mathfrak{M}_\mathfrak{o}$ is its defining kernel.[27] Consequently, the substitution $\xi \to Z$ in $\mathfrak{C}$ corresponds under the homomorphism to the substitution $\xi \to z$ in $\mathfrak{A}$. The different $\mathfrak{D}$ of $\mathfrak{O}$ is therefore the image of $\mathfrak{M}'$ under $Z \mapsto z$, and

$$\mathfrak{M}'[Z \to z] = \mathfrak{D}, \qquad \mathfrak{M}'[Z \to \xi] = \mathfrak{D}[z \to \xi] = \mathfrak{d}.$$

3. The different in the case of a defining equation. Suppose $\mathfrak{O}$ has a defining equation $G(z) = 0$, in the sense of the end of ğ1, 3, and assume in addition that the leading coefficient is the identity:

$$G(Z) = Z^n + h_1 Z^{n-1} + \cdots + h_n, \qquad h_i \in \mathfrak{h}.$$

The connection with the ordinary polynomial derivative is given by the following.

[25] Without this assumption one would have to define right and left differents and investigate how far they coincide with each other and, for orders in semisimple systems, with known constructions, as a generalization of the investigations in ğ4.

[26] This notation will always be used for ideals generated by entire sets.

[27] Editor's note: It is important here that $\mathfrak{M}_\mathfrak{o}$ is the full inverse image of (0), in order to conclude that the quotients correspond.

Theorem. *The differents of* $\mathfrak{o}$ *and* $\mathfrak{O}$ *relative to* $\mathfrak{h}$ *are defined—that is, the direct product* $\mathfrak{O}_\mathfrak{o}$ *exists—and are principal ideals generated by* $G'(\xi)$ *and* $G'(z)$*, respectively, where* $G'(Z)$ *denotes the ordinary polynomial derivative. The ideal differential quotient is*

$$\mathfrak{M}' = (G'(Z), G(Z)).$$

Proof. First, the elements

$$e, z, \ldots, z^{n-1}$$

form an independent module basis of $\mathfrak{O}$. Since the leading coefficient of G is the identity, these powers span $\mathfrak{O}$ over $\mathfrak{h}$; they are independent because $\mathfrak{M}$ contains no polynomial of degree less than n. Indeed, the degree of $K(Z)G(Z)$ is the sum of the degrees of the factors, again because of the hypothesis on the leading coefficient. The direct product $\mathfrak{O}_\mathfrak{o}$ therefore exists, so the different is defined.

It remains to examine the difference quotient $\mathfrak{C}$ in $\mathfrak{o}[Z]$. It is principal, with generator

$$\begin{aligned} C(Z,\xi) = (&Z^{n-1} + Z^{n-2}\xi + \cdots + \xi^{n-1}) \\ &+ h_1(Z^{n-2} + \cdots + \xi^{n-2}) + \cdots + h_{n-1}. \end{aligned}$$

The polynomial C is obtained by formal division of $G(Z) - G(\xi)$ by $Z - \xi$, so it belongs to $\mathfrak{C}$, since $Z - \xi$ generates $\mathfrak{Q}$. Every polynomial can be reduced modulo C to a polynomial D of degree less than $n-1$ in Z. Then $D(Z-\xi)$ has degree less than n, and can belong to $\mathfrak{M}$ only if it vanishes. But $D(Z-\xi) = 0$ implies $D = 0$, because the coefficient of Z in $Z - \xi$ is the identity. Thus C generates $\mathfrak{C}$.

Replacing ξ by Z in C and its multiples, and observing that $G(Z) = C(Z-\xi)$, gives

$$\mathfrak{M}' = (G'(Z), G(Z)),$$

and hence

$$\mathfrak{d} = (G'(\xi)), \qquad \mathfrak{D} = (G'(z)).$$

ğ4. The Different of a Direct Sum.

We impose the following hypotheses on $\mathfrak{O}$:

(1) $\mathfrak{O}$ is a direct sum of ideals,

$$\mathfrak{O} = \mathfrak{R}_1 + \cdots + \mathfrak{R}_r = \mathfrak{R}_i + \mathfrak{S}_i = \mathfrak{O}e_1 + \cdots + \mathfrak{O}e_r,$$

where the e_i are the components of the identity.

(2) Each $\mathfrak{R}_i$ has an independent $\mathfrak{h}_i$-module basis T_i, where $\mathfrak{h}_i$ is the component of $\mathfrak{h}$ in $\mathfrak{R}_i$, so $\mathfrak{h}_i = \mathfrak{h}e_i$. The basis T_i contains the identity e_i of $\mathfrak{R}_i$.

(3) Every intersection $[\mathfrak{h}, \mathfrak{S}_i]$ is zero; thus $\mathfrak{S}_i$ contains no constants.

By isomorphism, the same hypotheses hold for $\mathfrak{o}$.

Theorem. *Under these hypotheses, the different of* $\mathfrak{O}$ *relative to* $\mathfrak{h}$ *is the direct sum of the differents of the* $\mathfrak{R}_i$ *relative to the* $\mathfrak{h}_i$*.*

The proof rests on a sequence of individual facts.

I. First, $\mathfrak{O}$ itself has an independent $\mathfrak{h}$-module basis containing e; hence the differents of $\mathfrak{O}$ and $\mathfrak{o}$ relative to $\mathfrak{h}$ are defined. This basis is obtained from the union T of the bases T_i of the $\mathfrak{R}_i$. Indeed,

$$x = xe_1 + \cdots + xe_r,$$

and

$$\begin{aligned} xe_i &= (h_1 e_i)t_{1i}e_i + \cdots + (h_\lambda e_i)t_{\lambda i}e_i \\ &= h_1(t_{1i}e_i) + \cdots + h_\lambda(t_{\lambda i}e_i), \end{aligned}$$

so T is an $\mathfrak{h}$-basis of $\mathfrak{O}$. It is independent: a relation among elements of T yields, by directness of the sum, separate relations among the elements of each T_i, and hence $he_i = 0$ for every coefficient h. But

$$h \equiv he_i \pmod{\mathfrak{S}_i},$$

so $he_i = 0$ implies $h \in [\mathfrak{h}, \mathfrak{S}_i] = 0$. Finally, T contains the identities e_i, whose sum is e. Replacing one e_i in T by e gives a basis $\overline{T}$ satisfying all requirements. Hence $\mathfrak{O}_\mathfrak{o}$, and therefore the different of $\mathfrak{O}$ relative to $\mathfrak{h}$, exists.

II. The intersection condition (3) implies the sharper condition

$$[\mathfrak{o}, \mathfrak{S}_{i(\mathfrak{o})}] = 0,$$

where $\mathfrak{S}_{i(\mathfrak{o})}$ denotes the ideal of $\mathfrak{O}_\mathfrak{o}$ generated by $\mathfrak{S}_i$. Suppose

$$\alpha = \alpha e_i = \beta_1 t_1 + \cdots + \beta_\lambda t_\lambda,$$

where $t_1, \ldots, t_\lambda$ belong to the basis obtained from T by omitting T_i, and $\alpha, \beta_j \in \mathfrak{o}$. Form $\overline{T}$ by replacing e_i by e. Then $e, t_1, \ldots, t_\lambda$ are distinct elements of the $\mathfrak{h}$-basis $\overline{T}$ of $\mathfrak{O}$. Equality in $\mathfrak{O}_\mathfrak{o}$ is coefficientwise equality in every such basis, so the displayed relation gives $\alpha = 0$. This proves the *sharpened intersection property.* In particular,

$$\alpha \in \mathfrak{o}, \quad \alpha \neq 0 \quad \Longrightarrow \quad \alpha e_i \neq 0.$$

III. It follows immediately that $\mathfrak{o}$ is *ring-isomorphic* to each of its *components* $\mathfrak{o}e_i$ determined by the decomposition of $\mathfrak{O}$, and the isomorphism includes

$$\mathfrak{h} \simeq \mathfrak{h}_i = \mathfrak{h}e_i.$$

Since $e_i^2 = e_i$, and e_i commutes with every element of $\mathfrak{o}$, the ring $\mathfrak{o}e_i$ is a homomorphic image of $\mathfrak{o}$; the relation is one-to-one because $\alpha \neq 0$ implies $\alpha e_i \neq 0$. The subring $\mathfrak{h}$ corresponds to $\mathfrak{h}_i = \mathfrak{h}e_i$.

IV. Further isomorphisms follow when we also use the corresponding decomposition of $\mathfrak{o}$:

$$\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_r = \mathfrak{r}_i + \mathfrak{s}_i = \mathfrak{o}\varepsilon_1 + \cdots + \mathfrak{o}\varepsilon_r.$$

Then

$$\begin{aligned} \mathfrak{o} &\simeq \mathfrak{o}e_i, \qquad \mathfrak{O} \simeq \mathfrak{O}\varepsilon_i, \\ \mathfrak{r}_i &\simeq \mathfrak{r}_i e_i, \qquad \mathfrak{R}_i \simeq \mathfrak{R}_i \varepsilon_i, \\ \mathfrak{h} &\simeq \mathfrak{h}e_i \simeq \mathfrak{h}\varepsilon_i \simeq \mathfrak{h}e_i\varepsilon_i. \end{aligned}$$

The relation $\mathfrak{O} \simeq \mathfrak{O}\varepsilon_i$ corresponds exactly to $\mathfrak{o} \simeq \mathfrak{o}e_i$, with the roles of $\mathfrak{O}$ and $\mathfrak{o}$ interchanged. The next two relations correspond in the same way; the first follows because under $\mathfrak{o} \simeq \mathfrak{o}e_i$, the subring $\mathfrak{r}_i$ corresponds to $\mathfrak{r}_i e_i$. Likewise,

$$\mathfrak{h} \simeq \mathfrak{h}e_i \simeq \mathfrak{h}\varepsilon_i.$$

Since $\mathfrak{h}\varepsilon_i$ is a subring of $\mathfrak{o}$, and of $\mathfrak{r}_i$, one also has

$$\mathfrak{h}\varepsilon_i \simeq \mathfrak{h}e_i\varepsilon_i.$$

V. The direct-sum decomposition of $\mathfrak{O}$ implies: *if $\mathfrak{C} = (0) : \mathfrak{B}$ is the quotient of the zero ideal by $\mathfrak{B}$ in $\mathfrak{O}$, then each component $\mathfrak{C}_i$ is the quotient of the zero ideal of $\mathfrak{R}_i$ by the component $\mathfrak{B}_i$.* From

$$\mathfrak{B}\mathfrak{C} = (\mathfrak{B}e_1)(\mathfrak{C}e_1) + \cdots + (\mathfrak{B}e_r)(\mathfrak{C}e_r) = 0$$

one obtains separately, because the sum is direct,

$$(\mathfrak{B}e_i)(\mathfrak{C}e_i) = 0.$$

Conversely, if $re_i \in \mathfrak{R}_i$ satisfies

$$(\mathfrak{B}e_i)(re_i) = 0,$$

then $(\mathfrak{B}e_k)(re_i) = 0$ also holds for $k \neq i$. Thus $re_i \in \mathfrak{C} \cap \mathfrak{R}_i = \mathfrak{C}_i = \mathfrak{C}e_i$. Hence $\mathfrak{C}_i$ is the quotient of the zero ideal by $\mathfrak{B}_i$, and equally the quotient of the zero ideal of $\mathfrak{R}_i$ by $\mathfrak{B}_i$; for

$$re_i\mathfrak{B}_i = 0 \pmod{\mathfrak{S}_i}$$

already implies $re_i\mathfrak{B}_i = 0$.[28] Since

$$\mathfrak{O}_\mathfrak{o} = \mathfrak{O}_\mathfrak{o}e_1 + \cdots + \mathfrak{O}_\mathfrak{o}e_r$$

is also a direct sum, the assertion holds for ideals in $\mathfrak{O}_\mathfrak{o}$ as well.

VI. Component representation of the different. By definition (ğ3, 1), $\mathfrak{D} = \mathfrak{A}[\xi \to x]$. Therefore

$$\begin{aligned}\mathfrak{D} &= \mathfrak{D}e_1 + \cdots + \mathfrak{D}e_r \\ &= \mathfrak{A}[\xi \to x]e_1 + \cdots + \mathfrak{A}[\xi \to x]e_r.\end{aligned}$$

The element e_i lies in $\mathfrak{O}$ and corresponds to itself; under the isomorphism ε_i goes over to e_i, and $e_i\varepsilon_i = e_i$. Hence

$$\begin{aligned}\mathfrak{A}[\xi \to x]e_i &= \mathfrak{A}e_i[\xi \to x] \\ &= \mathfrak{A}e_i\varepsilon_i[\xi \to x].\end{aligned}$$

By V, $\mathfrak{A}e_i\varepsilon_i$ is the quotient

$$(0) : \mathfrak{B}e_i\varepsilon_i,$$

and also the quotient of the zero ideal of $\mathfrak{R}_i\mathfrak{r}_i$ by $\mathfrak{B}e_i\varepsilon_i$. Indeed, multiplying the decompositions of $\mathfrak{O}$ and $\mathfrak{o}$ gives the direct decomposition

$$\mathfrak{O}_\mathfrak{o} = \sum_{i,k} \mathfrak{O}_\mathfrak{o}e_i\varepsilon_k = \sum_{i,k} \mathfrak{R}_i\mathfrak{r}_k,$$

because the $e_i\varepsilon_k$ sum to the identity and satisfy the orthogonality relations.

VII. We now show that

$$\mathfrak{D}e_i = \mathfrak{A}e_i\varepsilon_i[\xi \to x] = (0) : \mathfrak{B}e_i\varepsilon_i$$

is the different of $\mathfrak{R}_i$ relative to $\mathfrak{h}_i$. The proof rests on these facts: $\mathfrak{R}_i\mathfrak{r}_i$ is the direct product

$$\mathfrak{R}_i\varepsilon_i \times \mathfrak{r}_ie_i$$

relative to $\mathfrak{h}e_i\varepsilon_i$; its difference ideal is $\mathfrak{B}e_i\varepsilon_i$, and its difference quotient is $\mathfrak{A}e_i\varepsilon_i$. The ideal $\mathfrak{D}e_i\varepsilon_i$ is the different of $\mathfrak{R}_i\varepsilon_i$, and correspondingly $\mathfrak{d}e_i\varepsilon_i$ is the different of $\mathfrak{r}_ie_i$. The isomorphisms

$$\mathfrak{R}_i\varepsilon_i \simeq \mathfrak{R}_i, \qquad \mathfrak{r}_ie_i \simeq \mathfrak{r}_i$$

then identify $\mathfrak{D}e_i$ and $\mathfrak{d}\varepsilon_i$ as the differents of $\mathfrak{R}_i$ relative to $\mathfrak{h}e_i$ and of $\mathfrak{r}_i$ relative to $\mathfrak{h}\varepsilon_i$, respectively.

VIII. *The ring $\mathfrak{R}_i\mathfrak{r}_i$ is the direct product $\mathfrak{R}_i\varepsilon_i \times \mathfrak{r}_ie_i$ relative to $\mathfrak{h}e_i\varepsilon_i$.* Since $\mathfrak{R}_i$ has the $\mathfrak{h}_i$-module basis T_i, the isomorphism $\mathfrak{R}_i \simeq \mathfrak{R}_i\varepsilon_i$ from IV shows that $T_i\varepsilon_i$ is an $\mathfrak{h}e_i\varepsilon_i$-module basis of $\mathfrak{R}_i\varepsilon_i$. The ring $\mathfrak{r}_ie_i$ is isomorphic to $\mathfrak{R}_i\varepsilon_i$, because $\mathfrak{r}_i \simeq \mathfrak{R}_i$ under $\mathfrak{o} \simeq \mathfrak{O}$, and is an extension ring of $\mathfrak{h}e_i\varepsilon_i$. The direct product therefore consists of all linear forms in the elements of $T_i\varepsilon_i$ with coefficients in $\mathfrak{r}_ie_i$, equality being coefficientwise. Under $\mathfrak{O} \times \mathfrak{o}$, this is exactly $\mathfrak{R}_i\mathfrak{r}_i$, since $T_i = T_ie_i$, $\mathfrak{r}_i = \mathfrak{r}_i\varepsilon_i$, and T_i belongs to a module basis of $\mathfrak{O}$.

IX. *The difference ideal of $\mathfrak{R}_i\varepsilon_i \times \mathfrak{r}_ie_i$ is $\mathfrak{B}e_i\varepsilon_i$, and its difference quotient is $\mathfrak{A}e_i\varepsilon_i$.* Write

$$\mathfrak{B} = \{\ldots, xe_1 - \xi\varepsilon_1, \ldots, xe_r - \xi\varepsilon_r, \ldots\}.$$

Then

$$\mathfrak{B}e_i\varepsilon_i = \{\ldots, xe_i\varepsilon_i - \xi e_i\varepsilon_i, \ldots\},$$

which is precisely the difference ideal of $\mathfrak{R}_i\varepsilon_i \times \mathfrak{r}_ie_i$. By VI, $\mathfrak{A}e_i\varepsilon_i$ is the quotient of the zero ideal of this ring by $\mathfrak{B}e_i\varepsilon_i$, and hence is its difference quotient.

[28] This also follows directly from the theorem used in ğ3, 2: under a homomorphism, not only ideals but their quotients correspond.

X. *The different of* $\mathfrak{R}_i\varepsilon_i$ *is* $\mathfrak{D}e_i\varepsilon_i$. It is obtained from $\mathfrak{A}e_i\varepsilon_i$ by replacing each element of $\mathfrak{r}_ie_i$ by its isomorphic correspondent: $(\xi\varepsilon_i)e_i$ is replaced by $(xe_i)\varepsilon_i$. Equivalently, replace ξ by x in $\mathfrak{A}e_i\varepsilon_i$, carrying $(\xi\varepsilon_i)e_i$ to $(xe_i)e_i = xe_i$, and then multiply by ε_i. By VI,

$$\mathfrak{A}e_i\varepsilon_i[\xi \to x] = \mathfrak{D}e_i.$$

Thus the different of $\mathfrak{R}_i\varepsilon_i$ relative to $\mathfrak{h}e_i\varepsilon_i$ is $\mathfrak{D}e_i\varepsilon_i$, and symmetrically the different of $\mathfrak{r}_ie_i$ is $\mathfrak{d}e_i\varepsilon_i$.

XI. *The different of* $\mathfrak{R}_i$ *is* $\mathfrak{D}e_i$. Under the isomorphism, the different of $\mathfrak{R}_i$ goes over into the different of $\mathfrak{R}_i\varepsilon_i$ by multiplication by ε_i. Since the latter is $\mathfrak{D}e_i\varepsilon_i$, the former is $\mathfrak{D}e_i$. Therefore

$$\mathfrak{D} = \mathfrak{D}e_1 + \cdots + \mathfrak{D}e_r,$$

and $\mathfrak{D}e_i$ *is the different of* $\mathfrak{R}_i$. Symmetrically,

$$\mathfrak{d} = \mathfrak{d}\varepsilon_1 + \cdots + \mathfrak{d}\varepsilon_r,$$

and $\mathfrak{d}\varepsilon_i$ *is the different of* $\mathfrak{r}_i$. This proves the theorem.

§5. Galois Extension Ring of a Field. Structure Theorems.

1. The underlying rings. Let K be a *field of degree* n *over a ground field* P, and suppose that K is a separable extension. Let Γ be an associated Galois field—uniquely determined up to isomorphism—which therefore contains the n conjugates $K^{(i)}$ and is their product, with $K = K^{(1)}$. Let $\mathfrak{K}$ denote an extension of P, isomorphic to K and hence equivalent to all the $K^{(i)}$ over P, such that the intersection $[\mathfrak{K}, \Gamma]$ is P (so that there is no common enveloping field of Γ and $\mathfrak{K}$).[29] Since $\mathfrak{K}$ has an independent finite P-module basis containing the identity, the direct products

$$\mathfrak{K}_\Gamma, \qquad \mathfrak{K}_K, \qquad \mathfrak{K}_{K^{(i)}}$$

exist by §2, 1. The ring $\mathfrak{K}_\Gamma$ is the product of its n subrings $\mathfrak{K}_{K^{(i)}}$ and is called the *Galois extension ring* of $\mathfrak{K}$. At the same time, $\mathfrak{K}_\Gamma$ is the direct product of $\mathfrak{K}_K$ and Γ relative to K, since every independent P-basis of $\mathfrak{K}$ is also an independent K-basis of $\mathfrak{K}_K$, and similarly for the conjugates.[30] For the ideals of these rings one has the following.

Theorem. *Every ideal of* $\mathfrak{K}$ *is the contraction of its extension in* $\mathfrak{K}_K$ *or* $\mathfrak{K}_\Gamma$*; every ideal of* $\mathfrak{K}_K$ *is the contraction of its extension in* $\mathfrak{K}_\Gamma$.

Proof. Since P and K are fields, every P-module in $\mathfrak{K}$, respectively every K-module in $\mathfrak{K}_K$, has an independent finite P-module, respectively K-module, basis which can be completed to such a basis of $\mathfrak{K}$, respectively $\mathfrak{K}_K$. The theorem now follows from the theorem in §2, 2.

Let $\mathfrak{B}^{(i)}_{K^{(i)}}$ denote the difference ideal of $\mathfrak{K}_{K^{(i)}}$, thus

$$\mathfrak{B}^{(i)}_{K^{(i)}} = \{\ldots, x - \xi^{(i)}, \ldots\},$$

and in particular

$$\mathfrak{B}_K = \{\ldots, x - \xi, \ldots\}.$$

Since ξ, respectively $\xi^{(i)}$, is the element of K, respectively $K^{(i)}$, corresponding to x under the isomorphism, these n difference ideals are conjugate to one another.

Let $\mathfrak{A}_K$, respectively $\mathfrak{A}^{(i)}_{K^{(i)}}$, denote the difference quotients $(0) : \mathfrak{B}_K$ in $\mathfrak{K}_K$ and their conjugates. Denote the extension ideals in $\mathfrak{K}_\Gamma$ by $\mathfrak{B}_\Gamma$ and $\mathfrak{A}_\Gamma$. The theorem of this number on extensions and contractions then gives in particular:

The difference ideal $\mathfrak{B}_K$ *and the difference quotient* $\mathfrak{A}_K$ *are the contractions of their extensions* $\mathfrak{B}_\Gamma$ *and* $\mathfrak{A}_\Gamma$.

[29] It is of course assumed—which is no restriction on generality—that there are no relations between the elements of K and $\mathfrak{K}$ which do not belong to P; compare §1, 2, §2, 1, and footnote 11.

[30] Statements holding uniformly for all conjugates will usually be stated only for $\mathfrak{K}_K$, with the indices omitted.

2. Direct-sum decomposition of the Galois extension ring. The connection between the difference ideal and difference quotient and the structure of the Galois extension ring is given by the following.

Structure theorem. *The zero ideal of the Galois extension ring $\mathfrak{K}_\Gamma$ is the intersection of the extensions of the n conjugate difference ideals; $\mathfrak{K}_\Gamma$ itself is the direct sum of the extensions of the n conjugate difference quotients. Each $\mathfrak{K}_{K^{(i)}}$ is the direct sum, and its zero ideal the intersection, of the corresponding difference ideal and difference quotient.*

Proof. The residue-class ring modulo each $\mathfrak{B}_\Gamma^{(i)}$ has rank one relative to Γ, since every element is congruent modulo $\mathfrak{B}_\Gamma^{(i)}$ to an element of Γ, while $\mathfrak{B}_\Gamma^{(i)}$ can contain no nonzero element of Γ (for $\mathfrak{B}_\Gamma^{(i)}$ vanishes under $x \to \xi^{(i)}$). By separability the ideals $\mathfrak{B}_\Gamma^{(i)}$ are all distinct and hence pairwise coprime. Consequently the rank of the ideals

$$\mathfrak{B}_\Gamma^{(1)}, \quad [\mathfrak{B}_\Gamma^{(1)}, \mathfrak{B}_\Gamma^{(2)}], \quad \ldots, \quad [\mathfrak{B}_\Gamma^{(1)}, \ldots, \mathfrak{B}_\Gamma^{(n)}]$$

decreases by at least one at each step. The intersection of all of them is the zero ideal, whereas the intersection of fewer than all the conjugates must differ from the zero ideal because they are pairwise coprime; hence the rank has decreased by exactly one at each step. The familiar theorems now give the following uniquely determined direct-sum representation of $\mathfrak{K}_\Gamma$:[31]

$$\begin{aligned} \mathfrak{K}_\Gamma &= \mathfrak{C}_\Gamma^{(1)} + \cdots + \mathfrak{C}_\Gamma^{(n)} = \Gamma e^{(1)} + \cdots + \Gamma e^{(n)} = \mathfrak{C}_\Gamma^{(i)} + \mathfrak{B}_\Gamma^{(i)}, \\ e &= e^{(1)} + \cdots + e^{(n)}, \qquad \mathfrak{C}_\Gamma^{(i)} = [\mathfrak{B}_\Gamma^{(1)}, \ldots, \mathfrak{B}_\Gamma^{(i-1)}, \mathfrak{B}_\Gamma^{(i+1)}, \ldots, \mathfrak{B}_\Gamma^{(n)}]. \end{aligned} \tag{1}$$

It remains to show that $\mathfrak{C}_\Gamma$ is equal to $\mathfrak{A}_\Gamma$. This will follow once the corresponding equality has been established in $\mathfrak{K}_K$. Here one has the decomposition

$$\mathfrak{K}_K = \mathfrak{C}_K + \mathfrak{B}_K = \mathfrak{K}_K e^{(1)} + \mathfrak{K}_K (e - e^{(1)}). \tag{2}$$

Indeed, $e^{(1)}$ lies in $\mathfrak{K}_K$. For $\mathfrak{C}_\Gamma^{(1)}$ is invariant under all permutations of $\mathfrak{B}_\Gamma^{(2)}, \ldots, \mathfrak{B}_\Gamma^{(n)}$, and hence the same is true of $e^{(1)}$, as the component of the identity in $\mathfrak{C}_\Gamma^{(1)}$. If, therefore, $e^{(1)}$ is expressed in an independent K-basis of $\mathfrak{K}_K$—which is possible because this is at the same time an independent Γ-basis of $\mathfrak{K}_\Gamma$—then the individual coefficients are invariant under all permutations of $K^{(2)}, \ldots, K^{(n)}$, and hence lie in K. Since $(e^{(1)})^2 = e^{(1)}$, the sum

$$\mathfrak{K}_K = \mathfrak{K}_K e^{(1)} + \mathfrak{K}_K (e - e^{(1)})$$

is direct. Its extension in $\mathfrak{K}_\Gamma$ is again direct and therefore, by (1), yields $\mathfrak{K}_\Gamma = \mathfrak{C}_\Gamma^{(1)} + \mathfrak{B}_\Gamma^{(1)}$. Thus, by the conclusion of §2, 2,

$$\begin{aligned} \mathfrak{K}_K e^{(1)} &= [\mathfrak{C}_\Gamma, \mathfrak{K}_K] = [\Gamma e^{(1)}, \mathfrak{K}_K] = K e^{(1)} = \mathfrak{C}_K; \\ \mathfrak{K}_K (e - e^{(1)}) &= [\mathfrak{B}_\Gamma, \mathfrak{K}_K] = \mathfrak{B}_K, \end{aligned}$$

which proves (2).

But (2) implies $\mathfrak{C}_K = \mathfrak{A}_K$, and consequently $\mathfrak{C}_\Gamma = \mathfrak{A}_\Gamma$. For $e^{(1)}(e - e^{(1)}) = 0$ gives $\mathfrak{C}_K \mathfrak{B}_K = 0$. Conversely, $b\mathfrak{B}_K = 0$ also gives $b(e - e^{(1)}) = 0$, so that $b = be = be^{(1)}$, and hence

$$\mathfrak{C}_K = (0) : \mathfrak{B}_K = \mathfrak{A}_K,$$

and, after extension, $\mathfrak{C}_\Gamma = \mathfrak{A}_\Gamma$. Therefore

$$\begin{aligned} \mathfrak{K}_\Gamma &= \mathfrak{A}_\Gamma^{(1)} + \cdots + \mathfrak{A}_\Gamma^{(n)} = \Gamma e^{(1)} + \cdots + \Gamma e^{(n)}; & 0 &= [\mathfrak{B}_\Gamma^{(1)}, \ldots, \mathfrak{B}_\Gamma^{(n)}]; \\ \mathfrak{K}_{K^{(i)}} &= \mathfrak{A}_{K^{(i)}}^{(i)} + \mathfrak{B}_{K^{(i)}}^{(i)} = K^{(i)} e^{(i)} + \mathfrak{B}_{K^{(i)}}^{(i)}; & 0 &= [\mathfrak{A}_{K^{(i)}}^{(i)}, \mathfrak{B}_{K^{(i)}}^{(i)}]. \end{aligned} \tag{3}$$

This proves the theorem in all its parts. It should also be emphasized that this is a *completely invariant structure theorem*, since all the constructions that occur ($\mathfrak{K}_K$, $\mathfrak{K}_\Gamma$, $\mathfrak{B}_K$, $\mathfrak{A}_K$) are defined without reference to a basis.[32]

[31] Compare E. Noether, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96 (1927), 26–61, §4, 5.

[32] A formulation possible here by means of a defining equation and the factorization of the corresponding polynomial into linear factors would not be invariant.

3. Component representation of $\mathfrak{K}$ by conjugate elements. The conjugate difference ideals and difference quotients correspond to a representation of the elements of $\mathfrak{K}$ by conjugate components:

Theorem. *If*

$$x = \xi^{(1)}e^{(1)} + \cdots + \xi^{(n)}e^{(n)}$$

is the $\mathfrak{K}$-component representation of an element x of $\mathfrak{K}$, then the n components are conjugate to one another. In particular, $\xi^{(1)}, \ldots, \xi^{(n)}$ are the n conjugate values corresponding to x under the isomorphisms of $\mathfrak{K}$ with $K^{(1)}, \ldots, K^{(n)}$.

That $e^{(1)}, \ldots, e^{(n)}$ are conjugate to one another follows from the relations (3) in 2: the automorphisms of Γ which carry $\mathfrak{B}_K$ into $\mathfrak{B}^{(i)}_{K^{(i)}}$ simultaneously carry $e^{(1)}$ into $e^{(i)}$, the latter being an element of $\mathfrak{K}_{K^{(i)}}$. The same relations give $xe^{(i)} = \xi^{(i)}e^{(i)}$, because $\mathfrak{B}^{(i)}_{K^{(i)}}e^{(i)} = 0$, and hence

$$(x - \xi^{(i)})e^{(i)} = 0$$

(alternatively, this follows from the fact that $\mathfrak{K}$, as a field, is isomorphic to its component, which is therefore given by $K^{(i)}e^{(i)}$, with x corresponding isomorphically to $\xi^{(i)}e^{(i)}$).

The theorem yields:

Corollary. *If $\mathfrak{B}$ is an absolute module in $\mathfrak{K}$ (that is, together with any two elements it also contains their difference), and if $\mathfrak{B}^{(1)}, \ldots, \mathfrak{B}^{(n)}$ are its components in $\mathfrak{K}_\Gamma$, then $\mathfrak{B}$ is equal to the intersection $[\mathfrak{K}, \mathfrak{B}^{(1)} + \cdots + \mathfrak{B}^{(n)}]$.*

Indeed, $\mathfrak{B}$ is contained in this intersection. Conversely, if an element of $\mathfrak{B}^{(1)} + \cdots + \mathfrak{B}^{(n)}$ is to belong to $\mathfrak{K}$, then by the theorem it must be a sum of conjugates and therefore is an element of $\mathfrak{B}$.

4. Complementary bases of $\mathfrak{K}$ and their connection with the components of the identity. On passing from the invariant structure to a representation by a basis, this structure groups the bases into complementary pairs:

Theorem. *To every P-basis $t_1, \ldots, t_n$ of $\mathfrak{K}$ there corresponds a complementary basis $T_1, \ldots, T_n$ in $\mathfrak{K}$, whose complementary basis is again the original basis of the t's. The bases $A^{(i)}_1, \ldots, A^{(i)}_n$ of $K^{(i)}$, isomorphic to the complementary basis $T_1, \ldots, T_n$, are defined as the coefficients of the identity components $e^{(i)}$ in the basis representation determined by the t's,*

$$e^{(i)} = A^{(i)}_1 t_1 + \cdots + A^{(i)}_n t_n.$$

If $\alpha^{(i)}_1, \ldots, \alpha^{(i)}_n$ are the bases corresponding to the t_i, then the matrices of the α's and the A's are reciprocal. If two bases (s) and (t) of $\mathfrak{K}$ are related by a transformation

$$(s) = (t)P,$$

then their complementary bases satisfy the contragredient relation

$$(S) = P^{-1}(T).$$

Proof. Let

$$e^{(i)} = A^{(i)}_1 t_1 + \cdots + A^{(i)}_n t_n$$

be the basis representations of the n components $e^{(i)}$ of the identity, relative to a P-basis $t_1, \ldots, t_n$ of $\mathfrak{K}$, which consequently becomes a Γ-basis of $\mathfrak{K}_\Gamma$. By 2 and 3, $A^{(i)}_1, \ldots, A^{(i)}_n$ lie in $K^{(i)}$, and conjugate coefficient systems A correspond to the different $e^{(i)}$. If $\alpha^{(i)}_1, \ldots, \alpha^{(i)}_n$ denotes the basis in $K^{(i)}$ assigned isomorphically to $t_1, \ldots, t_n$, then the following further relations hold:

$$e^{(i)}[t \to \alpha^{(i)}] = e; \qquad e^{(i)}[t \to \alpha^{(j)}] = 0 \quad \text{for } i \neq j. \tag{1}$$

Indeed, $\mathfrak{B}^{(i)}_{K^{(i)}}$ contains the elements $t_1 - \alpha^{(i)}_1, \ldots, t_n - \alpha^{(i)}_n$—which form a dependent P-module basis of $\mathfrak{B}^{(i)}_{K^{(i)}}$—and therefore vanishes under the substitution $t = \alpha^{(i)}$. Thus

$$e \equiv e^{(i)} \pmod{\mathfrak{B}^{(i)}_{K^{(i)}}}$$

gives the first relation (1), while the second follows from the fact that $e^{(i)}$ is an element of every $\mathfrak{B}^{(j)}_{K^{(j)}}$ for $i \neq j$. Written out in coefficients, the relations (1) take the matrix form

$$\begin{pmatrix} \alpha_1^{(1)} & \cdots & \alpha_n^{(1)} \\ \vdots & & \vdots \\ \alpha_1^{(n)} & \cdots & \alpha_n^{(n)} \end{pmatrix} \begin{pmatrix} A_1^{(1)} & \cdots & A_1^{(n)} \\ \vdots & & \vdots \\ A_n^{(1)} & \cdots & A_n^{(n)} \end{pmatrix} = E_n. \tag{2}$$

Here E_n denotes the identity matrix; the A's are therefore already uniquely determined by the α's. Relation (2) shows that the determinants of both matrices are nonzero. It further shows that $A_1^{(i)}, \ldots, A_n^{(i)}$ are linearly independent over P: a linear dependence would also hold for the conjugate systems and would therefore lower the rank of the A-matrix, contrary to the fact that the rank of E_n is n. Hence each $A_1^{(i)}, \ldots, A_n^{(i)}$ is a basis of $K^{(i)}$. Since these bases are conjugate, they are all isomorphic to the same basis $T_1, \ldots, T_n$ of $\mathfrak{K}$, where, by 3, T_λ is determined by

$$T_\lambda = A_\lambda^{(1)} e^{(1)} + \cdots + A_\lambda^{(n)} e^{(n)}.$$

The basis $T_1, \ldots, T_n$ is called complementary to $t_1, \ldots, t_n$, and correspondingly $A_1^{(i)}, \ldots, A_n^{(i)}$ is called complementary to $\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}$. Since the A's are uniquely determined by (2), and since this same relation—on passing to the transposed matrix—determines the α's from the basis of the T's, that is, from the A's, the original basis of the t's is complementary to the T's. Thus, under the correspondence effected by the components of the identity, all bases fall into complementary pairs.

Let s, S be another pair of complementary bases, with

$$e^{(i)} = B_1^{(i)} s_1 + \cdots + B_n^{(i)} s_n \qquad \text{and} \qquad (s) = (t)P.$$

Then

$$A_1 t_1 + \cdots + A_n t_n = B_1 s_1 + \cdots + B_n s_n$$

is an identity in t after the substitution $(s) = (t)P$, and therefore B, A transform contragrediently to s, t. By isomorphism, the same consequently holds for S and T. This proves every part of the theorem.

Remark. If $c = C_1 t_1 + \cdots + C_n t_n$ is the representation of an element of $\mathfrak{K}$ relative to a P-basis, and $c = c_1 T_1 + \cdots + c_n T_n$ is the representation of the same element relative to the complementary basis, then

$$C_\lambda = \mathrm{Sp}(cT_\lambda), \qquad c_\lambda = \mathrm{Sp}(ct_\lambda),$$

where, as usual, $\mathrm{Sp}(x)$ means the sum of the conjugates,

$$\mathrm{Sp}(x) = \xi^{(1)} + \xi^{(2)} + \cdots + \xi^{(n)},$$

for arbitrary x in $\mathfrak{K}$. Indeed,

$$c = \gamma^{(1)} e^{(1)} + \cdots + \gamma^{(n)} e^{(n)} = \sum_\lambda \gamma^{(1)} A_\lambda^{(1)} t_\lambda + \cdots + \sum_\lambda \gamma^{(n)} A_\lambda^{(n)} t_\lambda,$$

and comparison of coefficients gives $C_\lambda = \mathrm{Sp}(cT_\lambda)$. The second relation follows correspondingly by interchanging t and T.[19)]

5. Taking a defining equation as basis. Lagrange's interpolation formula. [Editorial note: This number was left uncompleted in the manuscript.]

§ 6. The Different of an Order.

The structure theorems that concern only fields and their Galois extension rings are now to be sharpened in the sense of integrality by distinguishing certain subrings of P, together with the elements of $\mathfrak{K}$ and K integral with respect to them: the orders. All notation from § 5 is retained.[20)]

[19)] The considerations of this number show that the invariant structural theorems are essentially simpler than the noninvariant basis theorems. The latter were needed only to exhibit the connection with what was already known. In fact, the decomposition of the Galois extension ring and the use of the components of the identity accomplish everything accomplished by the complementary bases (or by the complementary module in the next paragraph). There too, the connection between the different and the complementary module is given only for purposes of classification. The same holds for the consideration of Lagrange's interpolation formula under 5.

[20)] For the concepts *integral with respect to a ring* and *integrally closed*, cf. § 1 of the paper cited in footnote 17.

1. The underlying rings. Let $\mathfrak{h}$ be a subring of P such that P is the quotient field of $\mathfrak{h}$; suppose further that $\mathfrak{h}$ is *integrally closed in* P (every element of P that is integral with respect to $\mathfrak{h}$ belongs to $\mathfrak{h}$). Let $\mathfrak{O}$ denote an $\mathfrak{h}$-order in $\mathfrak{K}$, that is, a subring of $\mathfrak{K}$ containing $\mathfrak{h}$, whose quotient field is $\mathfrak{K}$, and which possesses a finite, not necessarily independent, $\mathfrak{h}$-module basis. All elements of $\mathfrak{O}$ are then integral (with respect to $\mathfrak{h}$); the $\mathfrak{h}$-module basis is at the same time a—generally dependent—P-module basis of $\mathfrak{K}$. Let $\mathfrak{o}$ denote the order in K isomorphic to $\mathfrak{O}$, and $\mathfrak{o}^{(i)}$ the conjugate orders in $K^{(i)}$. Let $\mathfrak{g}$ be the ring generated in Γ by the n conjugate orders; then $\mathfrak{g}$ too is an order. Indeed, $\mathfrak{g}$ contains $\mathfrak{h}$. The products of all elements of the $\mathfrak{h}$-bases of the $\mathfrak{o}^{(i)}$ form an $\mathfrak{h}$-basis of $\mathfrak{g}$ and at the same time a P-basis of Γ.

The direct products $\mathfrak{O}_\mathfrak{o}$ *and* $\mathfrak{O}_\mathfrak{g}$ *exist*, as is shown by the sufficient criterion in § 2, 3 (the ring $\mathfrak{f}$ there is to be replaced by P). In $\mathfrak{K}_\Gamma$, the direct product $\mathfrak{O}_P = \mathfrak{K}$, relative to $\mathfrak{h}$, exists first of all. Indeed, $\mathfrak{h}$ lies in the intersection $[\mathfrak{O}, P]$; conversely, every element of this intersection is integral as an element of $\mathfrak{O}$, hence, as an element of P, belongs to $\mathfrak{h}$ because $\mathfrak{h}$ is integrally closed. The linear combinations, with coefficients in P, of any n linearly independent elements of $\mathfrak{O}$ now give $\mathfrak{K}$ as a direct product. Likewise,

$$\mathfrak{o}_P = K \qquad \text{and} \qquad \mathfrak{g}_P = \Gamma;$$

from the direct product $\mathfrak{K}_\Gamma = \mathfrak{O}_P \times \mathfrak{o}_P$, relative to $\mathfrak{h}$, the criterion in § 2, 3 gives the existence of $\mathfrak{O}_\mathfrak{o}$ relative to $\mathfrak{h}$; likewise, $\mathfrak{K}_\Gamma = \mathfrak{O}_P \times \mathfrak{g}_P$ gives the existence of $\mathfrak{O}_\mathfrak{g}$. Along with $\mathfrak{O}_\mathfrak{o}$, the conjugate rings $\mathfrak{O}_{\mathfrak{o}^{(i)}}$ also exist. The ring $\mathfrak{O}_\mathfrak{g}$ is called the *Galois extension ring of the order* $\mathfrak{O}$.

The different of $\mathfrak{O}$, respectively of $\mathfrak{o}$, relative to $\mathfrak{h}$ is therefore defined, as are the conjugate differents. Let

$$\mathfrak{B} = \{\ldots, y - \eta, \ldots\}$$

denote the difference ideal of $\mathfrak{O}_\mathfrak{o}$, and

$$\mathfrak{B}^{(i)} = \{\ldots, y - \eta^{(i)}, \ldots\}$$

the conjugate difference ideals of $\mathfrak{O}_{\mathfrak{o}^{(i)}}$; likewise let

$$\mathfrak{A}^{(i)} = (0) : \mathfrak{B}^{(i)} \quad \text{—the quotient being taken in } \mathfrak{O}_{\mathfrak{o}^{(i)}}\text{—}$$

denote the conjugate *difference quotients*, and in particular

$$\mathfrak{A} = (0) : \mathfrak{B} \quad \text{in } \mathfrak{O}_\mathfrak{o}.$$

Further, let

$$\mathfrak{D} = \mathfrak{A}[\eta \to y]$$

denote the different of $\mathfrak{O}$, and

$$\mathfrak{d}^{(i)} = \mathfrak{A}^{(i)}[y \to \eta^{(i)}]$$

the differents of the n conjugate orders $\mathfrak{o}^{(i)}$, in particular

$$\mathfrak{d} = \mathfrak{A}[y \to \eta]$$

the different of $\mathfrak{o}$.[21)]

2. Structure theorems. Corresponding to the structure theorem for Galois extension rings of fields (§ 5, 2) is the following.

Structure theorem for the Galois extension ring of orders. *The difference ideal and difference quotient relative to the order and to the field are related as follows:* $\mathfrak{B}_K$ *is the extension of the difference ideal* $\mathfrak{B}$ *of* $\mathfrak{O}_\mathfrak{o}$*, and likewise* $\mathfrak{A}_K$ *is the extension of the difference quotient* $\mathfrak{A}$ *of* $\mathfrak{O}_\mathfrak{o}$*, while* $\mathfrak{A}$ *is the contraction of* $\mathfrak{A}_K$*. Between the difference quotient, the different, and the components of the identity there are the relations*

$$\mathfrak{A} = \mathfrak{d}e^{(1)}, \qquad \mathfrak{A}^{(i)} = \mathfrak{d}^{(i)}e^{(i)},$$

[21)] The hypothesis that $\mathfrak{h}$ is integrally closed in P is satisfied, for example, when $\mathfrak{h}$ is the principal order of a number field, and in particular when $\mathfrak{h}$ is the system of rational integers; thus the different and relative different of arbitrary orders, including orders in relative fields, are defined. Further, $\mathfrak{h}$ may be the polynomial domain in n indeterminates, which gives the different in algebraic function fields of n indeterminates.

and hence

$$\mathfrak{d} = [\mathfrak{o}, \mathfrak{A}^{(1)} + \cdots + \mathfrak{A}^{(n)}].$$

Thus the different $\mathfrak{d}$ *of* $\mathfrak{o}$ *consists of all elements* x *of* K *such that* $xe^{(1)}$ *lies in* $\mathfrak{O}_\mathfrak{o}$*; it differs from the zero ideal.*

That $\mathfrak{B}_K$ is the extension of $\mathfrak{B}$ follows from the fact that $\mathfrak{K} = \mathfrak{O}_P$, and likewise $K = \mathfrak{o}_P$, so that every $x - \xi$ in $\mathfrak{B}_K$ can be expressed linearly, with coefficients in K, in terms of the $y - \eta$ in $\mathfrak{B}$. It follows further that $\mathfrak{A}_K = (0) : \mathfrak{B}_K$ is also defined as the quotient $(0) : \mathfrak{B}$ in $\mathfrak{K}_K$. Hence $\mathfrak{A} = (0) : \mathfrak{B}$ in $\mathfrak{O}_\mathfrak{o}$ consists of all elements of $\mathfrak{O}_\mathfrak{o}$ belonging to $\mathfrak{A}_K$:

$$\mathfrak{A} = [\mathfrak{O}_\mathfrak{o}, \mathfrak{A}_K],$$

so it is the contraction of $\mathfrak{A}_K$. Since $\mathfrak{A}_K = Ke^{(1)}$, it follows that $\mathfrak{A} = \mathfrak{z}e^{(1)}$, where $\mathfrak{z}$ is an $\mathfrak{o}$-module in K, because $\mathfrak{A}$ too is an $\mathfrak{o}$-module. But by the definition of the different,

$$\mathfrak{d} = \mathfrak{A}[x \to \xi] = (\mathfrak{z}e^{(1)})[x \to \xi] = \mathfrak{z}(e^{(1)}[x \to \xi]) = \mathfrak{z}e = \mathfrak{z}$$

(cf. § 5, 4, (1)). Thus $\mathfrak{z} = \mathfrak{d}$; the difference quotient $\mathfrak{A}$ is the component in K of the different $\mathfrak{d}$ of $\mathfrak{o}$, and correspondingly for the conjugates. By the corollary in § 5, 3, this entails the relation for $\mathfrak{d}$ displayed above. And

$$\mathfrak{A} = \mathfrak{d}e^{(1)} = [Ke^{(1)}, \mathfrak{O}_\mathfrak{o}]$$

shows that $\mathfrak{d}$ consists of all elements x of K for which $xe^{(1)}$ lies in $\mathfrak{O}_\mathfrak{o}$. It follows that $\mathfrak{d}$ differs from the zero ideal; for $e^{(1)}$, as an element of $\mathfrak{K}_K = \mathfrak{O}_P \times \mathfrak{o}_P$, is a linear combination of finitely many elements of $\mathfrak{O}$ with coefficients in K, hence a quotient of an element of $\mathfrak{O}_\mathfrak{o}$ by an element of $\mathfrak{o}$ (indeed, by an element of $\mathfrak{h}$). This denominator gives a nonzero element of $\mathfrak{d}$. Consequently, $\mathfrak{d}$ has rank n relative to P, or $\mathfrak{d}_P = K$, and therefore $\mathfrak{A}_K$ is the extension of $\mathfrak{A}$.

From here on, a sketch.

3. Relation to the complementary module when an independent basis exists. If $t_1, \ldots, t_n$ is an independent $\mathfrak{h}$-basis of $\mathfrak{O}$, then every basis $(s) = (t)P$ of $\mathfrak{K}$ is also such a basis, provided the matrix P has entries in $\mathfrak{h}$ and is unimodular. But $(S) = P^{-1}(T)$ then shows that, along with T, S too is a basis of one and the same $\mathfrak{h}$-module, called the complementary module of $\mathfrak{O}$.

The last part of the structure theorem in 2 now says that $\mathfrak{d}$ is equal to the quotient

$$\mathfrak{o} : \mathfrak{c}$$

in K, where $\mathfrak{c}$ denotes the complementary module. Indeed, let

$$e^{(1)} = A_1 t_1 + \cdots + A_n t_n,$$

where the A_i form a basis of $\mathfrak{c}$; then $\mathfrak{d}$ consists of all elements δ for which $\delta e^{(1)}$ lies in $\mathfrak{O}_\mathfrak{o}$, that is, for which δA_i lies in $\mathfrak{o}$. Hence $\mathfrak{d} = \mathfrak{o} : \mathfrak{c}$.

Special case. A regular order with $e, z, \ldots, z^{n-1}$ as module basis:

$$\mathfrak{d} = \{f'(z)\}.$$

Remark. The remark to § 5, 4 gives the further familiar definition of the complementary module $\mathfrak{C}$ of $\mathfrak{O}$. *It consists of all elements* c *of* $\mathfrak{K}$ *for which the traces* $\mathrm{Sp}(ct)$*, that is, the traces* $\mathrm{Sp}(co)$ *with arbitrary* o *in* $\mathfrak{O}$*, are integral, that is, lie in* $\mathfrak{h}$; correspondingly for $\mathfrak{c}$ relative to $\mathfrak{o}$ and K.

Indeed, let $c = c_1 T_1 + \cdots + c_n T_n$, with the c_i in $\mathfrak{h}$, be an expression of an element c of $\mathfrak{C}$ in terms of the basis of $\mathfrak{K}$ complementary to t. Then $c_i = \mathrm{Sp}(ct_i)$, and hence belongs to $\mathfrak{h}$; conversely, if $\mathrm{Sp}(ct_i)$ belongs to $\mathfrak{h}$, then c_i belongs to $\mathfrak{h}$, and therefore c belongs to $\mathfrak{C}$.

Supplement. *If an independent $\mathfrak{h}$-module basis exists in the order, then the difference quotient $\mathfrak{A}^{(i)}$ is the intersection of all difference ideals other than $\mathfrak{B}^{(i)}$; more precisely,*

$$\mathfrak{A}^{(i)} = [\mathfrak{O}_{\mathfrak{o}^{(i)}}, \mathfrak{B}_{\mathfrak{g}}^{(1)}, \ldots, \mathfrak{B}_{\mathfrak{g}}^{(i-1)}, \mathfrak{B}_{\mathfrak{g}}^{(i+1)}, \ldots, \mathfrak{B}_{\mathfrak{g}}^{(n)}].$$

Indeed, by the sharpened formulation in § 2, 2, $\mathfrak{B}$ is then also the contraction ideal of $\mathfrak{B}_K$. For let $e, t_2, \ldots, t_n$ be a module basis of $\mathfrak{O}$, and hence of $\mathfrak{O}_{\mathfrak{o}}$; then so is

$$e, t_2 - \alpha_2, \ldots, t_n - \alpha_n;$$

but $t_2 - \alpha_2, \ldots, t_n - \alpha_n$ is at the same time a K-module basis of $\mathfrak{B}_K$. Thus the hypotheses of § 2, 2 (Supplement) are satisfied. Now

$$\mathfrak{A}_\Gamma = [\mathfrak{B}_\Gamma^{(2)}, \ldots, \mathfrak{B}_\Gamma^{(n)}]; \qquad \mathfrak{A}_{\mathfrak{g}} = [\mathfrak{A}_\Gamma, \mathfrak{O}_{\mathfrak{g}}] = [\ldots, [\mathfrak{B}_\Gamma^{(i)}, \mathfrak{O}_{\mathfrak{g}}], \ldots] = [\mathfrak{B}_{\mathfrak{g}}^{(2)}, \ldots, \mathfrak{B}_{\mathfrak{g}}^{(n)}].$$

But $\mathfrak{A} = [\mathfrak{A}_{\mathfrak{g}}, \mathfrak{O}_{\mathfrak{o}}]$; hence

$$\mathfrak{A} = [\mathfrak{O}_{\mathfrak{o}}, \mathfrak{B}_{\mathfrak{g}}^{(2)}, \ldots, \mathfrak{B}_{\mathfrak{g}}^{(n)}].$$

4. Relation to the differential quotient of a fundamental equation, when such an equation exists. Extend the order $\mathfrak{O}$ by n indeterminates $u_1, \ldots, u_n$, thus forming the direct product $\mathfrak{O}_U$, where U denotes the polynomial domain $\mathfrak{h}[u_1, \ldots, u_n]$, so that $\mathfrak{O}_U = \mathfrak{O}[u_1, \ldots, u_n]$. Then the extension $\mathfrak{C}_U$ of every ideal $\mathfrak{C}$ of $\mathfrak{O}$ consists of all polynomials in u with coefficients in $\mathfrak{C}$; conversely, $\mathfrak{C}$ is characterized as the system of all coefficients of $\mathfrak{C}_U$.

Suppose now that a fundamental equation exists; that is, $e, U, \ldots, U^{n-1}$ are to form an $\mathfrak{h}$-module basis upon passage to the quotient ring by one or more primitive polynomials $H(u)$ in $\mathfrak{h}[u]$. The ideals $\mathfrak{C}_U$ then pass into systems obtained from $\mathfrak{C}_U$ by multiplication by units ($H(u)$ and its negative and positive powers). Thus, in order to recover $\mathfrak{C}$, one may first reach $\mathfrak{C}_U$ (integral in u) by multiplication by these units, and then pass from it to $\mathfrak{C}$. In particular, let the different $\mathfrak{D}$ of $\mathfrak{O}$ pass into $\mathfrak{D}_U$, so that $\mathfrak{D}_U$ is the different of $\mathfrak{O}_U$. But in $\mathfrak{O}_U$—by taking the quotient by primitive $H(u)$—there exists a defining equation $G(U) = 0$. Thus $G'(U)$ becomes a basis polynomial of the different; that is, the different is derived from the coefficients of $G'(U)$. (It remains to be shown more precisely that $(G'(U))$ really contains only $\mathfrak{D}_U$ and nothing further; perhaps this is valid only when $\mathfrak{o}$ is integrally closed in K. Multiplication by divisors of $H(u)$ could produce, from elements lying in $\mathfrak{D}_U$, further elements besides those of $\mathfrak{D}_U$. Under integral closure (five axioms), it follows from the theorem that coefficient ideals (contents) multiply. This makes possible a ramification theory by consideration of the fundamental equation modulo p.)

§ 7. Ramification Theory of the Principal Order modulo p^t.

Let a number field be given, with $\mathfrak{h}$ its ring of integers; or also a relative field with respect to the quotient ring of the principal order by a prime ideal, where p denotes the basis element of the prime ideal of this quotient ring. Suppose that the indeterminates $u_1, \ldots, u_n$ have been adjoined. Then both the principal order and the residue class ring modulo p^t possess the $\mathfrak{h}$-module basis $e, U, \ldots, U^{n-1}$; hence in both cases the different is given by $G'(u)$. *The different of the principal order passes modulo p^t into that of the residue class ring modulo p^t* (does this hold for arbitrary orders or not?). If, however,

$$p = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r},$$

then the residue class ring $\mathfrak{R}$ modulo p^t is a direct sum whose components are isomorphic to the residue class rings modulo $\mathfrak{p}_i^{t\varrho_i}$, thus

$$\mathfrak{R} = \mathfrak{R}e_1 + \cdots + \mathfrak{R}e_r;$$

here, for $i \neq k$, e_k is divisible by $\mathfrak{p}_i^{t\varrho_i}$. If, therefore,

$$\mathfrak{d}[p^t] = \mathfrak{d}[p^t]e_1 + \cdots + \mathfrak{d}[p^t]e_r = \mathfrak{d}_1 + \cdots + \mathfrak{d}_r$$

and t is sufficiently large, then $\mathfrak{p}_i$ occurs in $\mathfrak{d}_i$ to the same power as in $\mathfrak{d}[p^t]$, hence as in $\mathfrak{d}$. But by § 4, $\mathfrak{d}_i$ is the different of $\mathfrak{R}_i$; it is therefore enough to consider the different of the residue class ring modulo $\mathfrak{p}^{\varrho t}$. Choose ξ (Zahlbericht, Theorems 29 and 30) so that ξ is an algebraic integer and

$$\varphi(\xi) \equiv 0(p), \qquad \not\equiv 0(p^2),$$

where $\varphi(x)$ is a prime function modulo p of degree f. If (for $t \geq 2$) this ξ is replaced by $\xi^* = \xi e_1$, where e_1 is the first idempotent occurring in the decomposition of the residue class ring $\mathfrak{R}$ modulo p^t, then, in addition to $\varphi(\xi^*) \equiv 0(p)$, $\not\equiv 0(p^2)$, one even has $\mathfrak{p}_1 = (p, \varphi(\xi^*))$. A basis with respect to the rational integers modulo p^t then consists of the elements $\xi^\mu \varphi(\xi)^\nu$ with $\mu = 0, 1, \ldots, f-1$ and $\nu = 0, 1, \ldots, t-1$. An independent $\mathfrak{h}$-basis (residue classes modulo p^t) is given by

$$\xi^{\mu_0} \varphi(\xi)^{\nu_0} \quad \text{with} \quad \mu_0 = 0, 1, \ldots, f-1; \quad \nu_0 = 0, 1, \ldots, \varrho - 1. \tag{1}$$

For $(\varphi(\xi), p^{\varrho t}) = \mathfrak{p}$; hence, because $(p) = \mathfrak{p}^\varrho$ in the residue class ring, passage from principal ideals to elements gives $\varphi(\xi) = pM(\xi)$, where $M(\xi)$ is a unit in the residue class ring, that is, $M(\xi) \not\equiv 0(p)$. Thus (because $p^t = 0$) one may successively express $\xi^{\varrho t}$ in terms of lower powers, first in $M(\xi)$ and then in the residue class ring; consequently (1) is indeed a basis. The defining equation with respect to this basis is

$$F(x) = \varphi(x)^\varrho + pM(x),$$

where $M(x)$ modulo p is not divisible by $\varphi(x)$ (Ö. Ore, Math. Ann. 96, p. 348), and hence

$$M(\xi) \not\equiv 0(p).$$

The basis is also independent. Indeed, from

$$a_0(\xi) + a_1(\xi)\varphi(\xi) + \cdots + a_{\varrho-1}(\xi)\varphi(\xi)^{\varrho-1} \equiv 0(p^{t\varrho})$$

it follows that the left-hand side is $\equiv 0(p)$; hence $a_0(\xi) \equiv 0(p)$, and therefore

$$a_0(x) \equiv 0(p);$$

successive division by p gives

$$a_0(x) \equiv 0(p), \ldots, a_{\varrho-1}(x) \equiv 0(p)$$

and, after division by p once more,

$$a_0(x) \equiv 0(p^2), \ldots, a_{\varrho-1}(x) \equiv 0(p^2)$$

and so on, until

$$a_0(x) \equiv 0(p^t), \ldots, a_{\varrho-1}(x) \equiv 0(p^t).$$

The different of the residue class ring is therefore given by the polynomial derivative $F'(\xi)$—everything has been reduced to Ore, p. 345, § 3. Ore's Theorem 10 (cf. Dedekind–Hensel) shows that $p^t = p^n$ suffices for every $\mathfrak{p}$; Ore's supplement numbers follow as well.

By passage to the quotient ring, all of this also holds for relative differents, so that Ore, Math. Ann. 97, p. 594, § 4 follows directly from Ore, Math. Ann. 96. One need only add the statements concerning the expression of the different of the overfield as the product of the different of the base field and the relative different (cf. the Introduction to this paper).

Received 25 October 1949.

RA10: scan-visible apparatus for Papers 40–43

This appendix records source-visible scholarly apparatus restored during the scan-first recursive audit. It is appended as endnote apparatus so the cumulative branch contains the omitted details while the main mathematical text remains undisturbed.

Paper 40

1. E. Noether, *Hypercomplex quantities and representation theory*, Math. Z. 30 (1929), 641–692; cf. van der Waerden, *Modern Algebra II.*

2. Brauer–Noether, *On minimal splitting fields of irreducible representations*, Sitzungsberichte Preuss. Akad. Wiss. 1927, 221–228; the note on p. 222 gives a report on priority. The main theorems arose independently and almost simultaneously. See also R. Brauer, *Systems of hypercomplex numbers*, Math. Z. 30 (1929), 79–107; A. A. Albert later rediscovered the theorems independently.

3. R. Brauer, *On the algebraic structure of division rings*, J. reine angew. Math. 166 (1932), 241–252; K. Shoda, *On the Galois theory of semisimple hypercomplex systems*, Math. Ann. 107 (1932), 252–258; J. Levitzki had also developed these results.

4. The first lecture was written up by G. Koethe, the second by M. Deuring.

5. The method is essentially reproduced by G. Koethe, *Division rings of infinite rank over the center*, Math. Ann. 105 (1931), 15–39, especially section 5. The intersection method is replaced here by the observation that two-sided ideals belong to invariant modules; this permits direct-sum decomposition but fails for infinite rank and in the integral case.

6. See Noether's Prague lecture, Jahresbericht DMV 39 (1930), p. 17, in oblique pagination.

7. The theory of crossed products was developed in the second lecture and reproduced, with small modifications, in H. Hasse, *Theory of cyclic algebras over an algebraic number field*, Trans. Amer. Math. Soc. 34 (1932), 171–214. A version closer to the lecture was announced in a report by M. Deuring.

8. For non-abelian groups the object is a generalized ring; cf. H. Fitting, Math. Ann. 107, 514–542.

9. A product ring here means only the ring generated by two rings inside a common overring; the product need not be direct. The scan gives the integer-ring example with $R = o[x]$, $S = o[y]$, $2x - 1 = 0$, $2y - 1 = 0$ to show that a product ring need not exist for a prescribed intersection.

10. The theorems of that paragraph remain valid for infinite rank of M over P by simple well-ordering arguments; cf. G. Koethe, Goettingen Nachrichten 1931, 195–207.

11. A simple system means, as usual, two-sided simple.

12. Cf. Representation theory, note 20, for the case in which A is the associated automorphism division ring of S.

13. Reciprocal fields or systems are generally denoted by corresponding Greek and Latin letters.

14. The isomorphisms below always extend the identity of P, unless explicitly noted.

15. This no longer holds when A has infinite rank over P; cf. Koethe.

16. Shoda, work cited in note 3; the introduction of indeterminates is avoided there.

17. The finer theorems on the group of algebra classes use factor systems; up to that point no arguments about commutative fields have entered, and it has not been used or proved that $(A : P)$ is a square.

18. There are minimal splitting fields of all degrees; cf. Brauer–Noether, note 2.

19. Cf. G. Koethe, *On division rings with subfields of the second kind over the center*, J. reine angew. Math. 166 (1932), 182–184. The simpler proof used here is due to a remark of M. Zorn.

20. R. Brauer–E. Noether, loc. cit.

21. Cf. Representation theory, section 25.

22. Relations between complementary bases and idempotents occur first in Dedekind, *On the theory of complex quantities formed from n principal units*, Collected Works, vol. II, 4–5.

Papers 41–42

1. The scan apparatus cites Noether's Zurich lecture of 1932 on hypercomplex systems, commutative algebra and number theory, and Hasse's account of the R. Brauer algebra-class group.

2. "In the minimal sense" designates the algebraic analogue of the principal genus theorem over arbitrary fields; "in the small" already concerns passage to the p-adic ground field.

3. A. Speiser, Math. Z. 5 (1919), 1–6; the theorem is already stated there as one on crossed representations.

4. Brandt's theory of maximal orders is presented and newly grounded in H. Hasse, Math. Ann. 104 (1931).

5. Notes by C. Chevalley, H. Hasse and E. Noether are announced, the latter two in a Herbrand memorial volume.

6. Crossed products are tied to Noether's 1929/30 lecture and to Hasse, *Theory of cyclic algebras*, Trans. Amer. Math. Soc. 34 (1932), chapter 2, with M. Deuring's report on hypercomplex numbers.

7. K^* denotes K with zero removed.

8. The crossed-product relations are the defining relations for a group extension; the special feature is that the relevant automorphism subgroup is exactly the Galois group of K, producing a ring extension as well.

9. The proof given in the scan also holds when k has only finitely many elements.

10. I. Schur, Math. Z. 5 (1919), 7–10; for a proof by crossed representation modules, cf. Deuring.

11. The construction is defined whenever the principal class is replaced by a group-stable subgroup; transformation quantities from its ideals replace those from principal ideals.

12. c_s denotes the ideal class of $\mathfrak{c}_s$.

13. Cf. the close of the introduction.

14. In the proof only the weakened assertion about principal ideals is used.

15. The scan gives the alternative proof via Hasse and the decomposition field; extension to A_p gives the result independently of the chosen conjugate prime.

16. Cf. Hasse, work cited in note 1, section 3.

17. Paper 42, note 1: the theory of crossed products follows Noether's lecture as reproduced in H. Hasse, *Theory of cyclic algebras over an algebraic numberfield*, Trans. Amer. Math. Soc. 34 (1932), Section II; Brandt's theory of maximal orders is given in Hasse, *On p-adic division rings*, Math. Ann. 104 (1931).

18. Paper 42, note 2: Noether had long known the explicit representations; the immediate stimulus for the following considerations was Hasse's communication of the theorem cited in note 4.

19. Paper 42, note 3: C. Chevalley, *Sur certains idéaux d'une algèbre simple*, Abh. Math. Sem. Hamburg, 1934.

20. Paper 42, note 4: H. Hasse, *Ueber gewisse Ideale in einer einfachen Algebra*, the paper immediately preceding this one in the same collection.

21. Paper 42, note 5: if the characteristic does not divide n, then $\frac{1}{n}E_1$ is the idempotent of the identity representation; the normal form also holds when the characteristic divides n, provided that k/Q is separable.

22. Paper 42, note 6: in the non-Galois case this leads to the analogue of the crossed-product representation; Noether records that this will probably be carried out in a dissertation.

23. Paper 42, note 7: the considerations of this section remain valid when the ground field is a function field in one indeterminate.

24. Paper 42, note 8: when places are defined by p-adic extension, the corresponding lemma says that the intersection of all p-adic components with K is the original module; in Hasse's Theorem 66 the lemma is stated only for ideals of maximal rank.

25. Paper 42, note 9: $\mathrm{Sp}(\mathfrak{c})$ denotes, in general, the ideal in $\mathfrak{o}$ consisting of the traces of all elements of $\mathfrak{c}$.

26. Paper 42, note 10: for non-Galois k, z must be replaced by zE_1 and the corresponding modules by products with E_1; the scan gives the formula $E_1aE_1 = E_1a$ with $a \in k$ and the subsequent computation.

27. Paper 42, note 11: compare Hasse, Section 8, or Hasse's preceding paper cited in note 4.

28. Paper 42, note 12: another proof is in Hasse and Chevalley, notes 4 and 3.

Paper 43

1. The editor's note states that this posthumous Noether paper was written in winter 1927/28 and gives a detailed form of the Prague 1929 lecture; from section 6.3 on the manuscript was evidently still to be revised.

2. Extension of the coefficient domain is treated in section 1 also for noncommutative rings, more generally than needed; section 2 for commutative rings with finite basis suffices for this paper.

3. This continues Noether's discriminant paper, J. reine angew. Math. 157 (1927), 82–104.

4. Editor's note: the intended manuscript citation was left blank; see the references in the sketched section 7.

5. Noether thanks B. L. van der Waerden for critical remarks on the relevant section.

6. The second notation recalls extension of the coefficient domain; the first is the usual notation for a direct product.

7. Without a unit element, formulas (3) and (4) receive additional linear terms.

8. Cf. section 1.4.

9. Cf. section 2.1 and footnote 12.

10. The scan justifies equality and composition conditions for the direct product; equality in $O[Z]$ gives the stated identification.

11. Without the stated hypothesis one would have to define right and left differents and compare them.

12. The scan fixes the notation for ideals derived from totalities.

13. Editor's note: it is important that the inverse image of (0) is the relevant set in order to infer correspondence of quotients.

14. The theorem also follows directly from the homomorphism theorem used earlier: under a homomorphic image, ideals and quotients correspond.

15. It is assumed, without loss of generality, that no products are imposed between elements of K not in P and elements of S.

16. Statements holding uniformly for all conjugates are usually stated for one K, omitting indices.

17. Cf. Noether, *Abstract construction of ideal theory in algebraic number and function fields*, Math. Ann. 96 (1927), sections 4–5.

18. A formulation by a defining equation and factorization into linear factors would not be invariant.

19. The considerations show that invariant structure theorems are much simpler than non-invariant basis theorems.

20. For the notions integral with respect to a ring and integrally closed, cf. section 1 of the paper cited in note 17.

21. The hypothesis on the base ring integrally closed in P is satisfied, for example, for the principal order of a number field and for polynomial rings; hence differents and relative differents of arbitrary orders, also in relative fields, are defined.

Algebra of Hypercomplex Quantities

Lectures by Prof. E. Noether
Winter Semester 1929/30

Written up by Prof. M. Deuring

Contents

Introduction ... 3

Chapter I: Representations ... 3
§ 1. Definition of Direct Representation — Definition of Reciprocal Representation ... 3
§ 2. Representation Classes ... 4
§ 3. Representation Modules ... 4
§ 4. The Connection between Representation Modules and Representations ... 5

Chapter II: Galois Theory of Commutative Fields ... 7
§ 5. Extension of the Coefficient Domain of Hypercomplex Systems ... 7
§ 6. The Irreducible Representations of Commutative Systems ... 8
§ 7. The Isomorphisms of a Field ... 8
§ 8. The Splitting Field ... 9
§ 9. The Isomorphisms from Z_1 onto the Z_i ... 9
§ 10. The Galois Group ... 9
§ 11. The Fundamental Theorem of Galois Theory ... 9
§ 12. The Formal Significance of the Components e_i ... 11
§ 13. The General Extension Theorem ... 12

Chapter III: Abelian Groups ... 13
§ 14. The Group Ring ... 13
§ 15. The Group Rings of Abelian Groups ... 14
§ 16. The Character Relations ... 15
§ 17. The Galois Theory of Abelian Groups ... 15

Chapter IV: Two-Sided Simple Rings ... 18
§ 18. An Auxiliary Theorem ... 18
§ 19. Representations of Two-Sided Simple Hypercomplex Systems in Noncommutative Extension Fields of Their Coefficient Fields ... 19
§ 20. Noncommutative Fields ... 22
§ 21. The Galois Theory of Noncommutative Fields ... 26

Chapter V: Factor Systems 29
§ 22. The Group of Fields with Given Center 29
§ 23. Factor Systems 30
§ 24. Multiplication of Factor Systems 33
§ 25. Normal Representation of $\mathfrak{R}_r$ with a Galois Maximal Commutative Subfield 39
§ 26. Multiplication of Crossed Representations 43

Chapter VI: Theory of Crossed Products 44
§ 27. Representations of the $\mathfrak{R}_r$ as Crossed Products 44
§ 28. Product Theorem for Factor Systems 47
§ 29. The Principal Genus Theorem in the Minimal Case 50
§ 30. Specialization to Cyclic Splitting Fields 50
§ 31. Applications of the Cyclic Special Case 52

Introduction

These lectures treat the general representation theory of rings, which grew, on the one hand, out of the theory of representations of finite groups and, on the other, out of the algebraic and arithmetic theory of hypercomplex number systems. This more general conception of representation theory has the following advantages over the theory hitherto developed (Frobenius, Schur):

Because one considers not the group but the group ring, or, more generally, a hypercomplex system or an arbitrary ring, one can use the theory of rings and ideals; this frees the theory from many unwieldy computations. The use of general ring and ideal theory, however, not only simplifies the theory but also carries it further—for example, in the question of the relations between a group and its subgroups—and opens up new fields of application. General representation theory provides a new and very elegant foundation for Galois theory and—what is perhaps still more important—makes it possible to establish a Galois theory of noncommutative fields.

The fundamental concepts of group, ring, and ideal theory and the general theorems of representation theory are found in Miss Noether's paper, *Hypercomplex Quantities and Representation Theory*, *Mathematische Zeitschrift* 30, p. 641. That paper, cited as M.Z., is to be regarded as a supplement to these notes. The same material as in M.Z. is also found in the notes from Miss Noether's lectures on *Hypercomplex Quantities and Group Characters*, winter semester 1927/28.

The concepts of representation and representation module are briefly explained here in order to introduce reciprocal representation modules and reciprocal representations, which are new only in a formal sense.

Chapter I. Representations

Let $\mathfrak{o}$ be a ring—the ring to be represented—and T another ring—the ring in which it is to be represented.

ğ 1. Definition of Direct Representation

A *direct representation* of degree n of $\mathfrak{o}$ in T is a subring $\mathfrak{D}$ of the ring T_n of matrices of degree n with entries in T, onto which $\mathfrak{o}$ is mapped ring-homomorphically. In symbols,

$$\mathfrak{o} \to \mathfrak{D} \subseteq \mathsf{T}_n.$$

Definition of Reciprocal Representation

A *reciprocal representation* of degree n of $\mathfrak{o}$ in T^* is a subring $\mathfrak{D}^*$ of the ring T_n^* of matrices of degree n with entries in T^*, onto which $\mathfrak{o}$ is mapped reciprocal-ring-homomorphically. Reciprocal ring homomorphy means the following: if the elements c, d of $\mathfrak{o}$ correspond to the elements c^*, d^* of $\mathfrak{D}^*$, then the element cd of $\mathfrak{o}$ is to correspond to the element $d^* \cdot c^*$ of $\mathfrak{D}^*$, and the element $c + d$ of $\mathfrak{o}$ to the element $c^* + d^*$ of $\mathfrak{D}^*$. In symbols,

$$\mathfrak{o} \mapsto \mathfrak{D}^* \subseteq \mathsf{T}_n^*.$$

For an example of reciprocal homomorphy, assign to each n-rowed matrix over a commutative field its transpose. This assignment is a reciprocal ring isomorphism.

In general, a ring T^* reciprocally isomorphic to any given ring T can be constructed as follows.

Assign a symbol c^* to every element c of T, and define addition of these symbols by $c^* + d^* = (c + d)^*$ and multiplication by

$$c^* \cdot d^* = (dc)^*.$$

The set of symbols c^* is a ring T^* reciprocally isomorphic to T.

ğ 2. Representation Classes

A direct representation $\mathfrak{D}$ of $\mathfrak{o}$ in T can be transformed into an isomorphic representation $\mathfrak{D}'$ by transforming it elementwise with a regular matrix P; that is, one assigns to an element c of $\mathfrak{o}$, in place of $C \subseteq \mathfrak{D}$, the element $P^{-1}CP \subseteq P^{-1}\mathfrak{D}P$.

Two representations that can be transformed into one another in this way are called *equivalent*.

All representations equivalent to a given representation form a *representation class* (direct representation class, d.r.c.).

Equivalence of reciprocal representations is defined in the same way: two reciprocal representations are called equivalent if one can be obtained from the other by transformation with a regular matrix. All representations equivalent to a fixed reciprocal representation form a *class of reciprocal representations.*

ğ 3. Representation Modules

Definition of the *direct representation module* (d.r.m.).

A direct representation module of $\mathfrak{o}$ with respect to T is any $\mathfrak{o},\mathsf{T}$-bimodule $\mathfrak{M}$ (that is, an additively written Abelian group which is a left module with respect to $\mathfrak{o}$, a right module with respect to T, and satisfies the mixed associative law: if $c \in \mathfrak{o}$, $m \in \mathfrak{M}$, $\tau \in \mathsf{T}$, then $(cm)\tau = c(m\tau)$) that can be written as the direct sum of finitely many one-generator T-modules—with $x_i\tau = 0$ implying $\tau = 0$—

$$\mathfrak{M} = x_1 \cdot \mathsf{T} + x_2 \cdot \mathsf{T} + \cdots + x_n \cdot \mathsf{T}.$$

Definition of the *reciprocal representation module* (r.r.m.).

A reciprocal representation module of $\mathfrak{o}$ with respect to T^* is any $\mathfrak{o}$-left and T^*-left module $\mathfrak{M}^*$ which satisfies the commutative law (if $c \in \mathfrak{o}$, $m \in \mathfrak{M}^*$, $\tau \in \mathsf{T}^*$, then $c(\tau^* m^*) = \tau^*(cm)$) and can be written as the direct sum of finitely many simple T^*-modules—with $\tau^* \cdot x_i^* = 0$ implying $\tau^* = 0$—

$$\mathfrak{M}^* = \mathsf{T}^* \cdot x_1 + \cdots + \mathsf{T}^* \cdot x_n.$$

ğ 4. The Connection between Representation Modules and Representations

1. *Every representation module determines a representation class uniquely (a d.r.m. determines a d.r.c., and an r.r.m. an r.r.c.).*

The construction is as follows.

Multiplication of the d.r.m. $\mathfrak{M}$ by an element c of $\mathfrak{o}$ defines a homomorphism of $\mathfrak{M}$ onto itself which, by virtue of the associative law $(cm)\tau = c(m\tau)$, admits the elements of T as operators. It is therefore a *linear transformation* of $\mathfrak{M}$ into itself; that is, the assignment $m \mapsto cm = m'$ has the property

$$\text{if } y_i \mapsto y_i' (= cy_i), \text{ then also } \sum y_i\tau_i \mapsto \sum y_i'\tau_i \left(= c\sum y_i\tau_i\right).$$

Define the sum $\mathfrak{T}_1 + \mathfrak{T}_2$ of two linear transformations

$$\mathfrak{T}_1 : \ m \mapsto m' (= c_1 m) \quad \text{and} \quad \mathfrak{T}_2 : \ m \mapsto m'' (= c_2 m)$$

to be the transformation $m \mapsto m' + m'' (= (c_1 + c_2)m)$, and their product $\mathfrak{T}_1 \cdot \mathfrak{T}_2$ to be the composite transformation $m \mapsto (m'')' = c_1 c_2 m$. Then the set of distinct linear transformations of $\mathfrak{M}$ generated by the elements of $\mathfrak{o}$ is a ring-homomorphic image $\overline{\mathfrak{D}}$ of $\mathfrak{o}$.

Now choose any basis $x_1, \ldots, x_n$ of $\mathfrak{M}$. The linear transformation of $\mathfrak{M}$ generated by c is plainly determined once it is known how the basis elements x_i are transformed, hence once the matrix $(\gamma_{ij}) = C$ of the system of equations

$$x_j' = cx_j = \sum x_i \gamma_{ij}$$

is known; for any other element $x = \sum x_j\tau_j$, one simply has $x' = \sum x_j'\tau_j$. These matrices C correspond uniquely to the distinct linear transformations (for they determine one another) and form, as is immediately seen, a ring isomorphic to $\overline{\mathfrak{D}}$, hence a ring-homomorphic image of $\mathfrak{o}$: a representation of degree n of $\mathfrak{o}$.

The isomorphism between $\overline{\mathfrak{D}}$ and the representation is embodied in the following formulas. If the matrix C corresponds to the linear transformation generated by $c \in \mathfrak{o}$, so that

$$c(x_1, \ldots, x_n) = (x_1, \ldots, x_n)C,$$

and if, in the same way, $d \in \mathfrak{o}$ and $D \in \mathsf{T}_n$ correspond,

$$d(x_1, \ldots, x_n) = (x_1, \ldots, x_n)D,$$

then plainly

$$(c+d)(x_1,\dots,x_n) = (cx_1+dx_1,\dots,cx_n+dx_n)$$
$$= (x_1,\dots,x_n)(C+D)$$

and

$$cd(x_1,\dots,x_n) = c(dx_1,\dots,dx_n) = c((x_1,\dots,x_n)D)$$
$$= (cx_1,\dots,cx_n)D = (x_1,\dots,x_n)CD.$$

Thus, when realized by means of a specified basis x_ν of $\mathfrak{M}$, the linear transformations of $\mathfrak{M}$ into itself generated by $\mathfrak{o}$ give a representation of degree n of $\mathfrak{o}$ in T.

If $(y_1,\dots,y_n)$ is another basis of $\mathfrak{M}$, it is obtained from $x_1,\dots,x_n$ by multiplication by a regular matrix,

$$(y_1,\dots,y_n) = (x_1,\dots,x_n)P.$$

If a linear transformation of $\mathfrak{M}$ is realized by the matrix C with respect to the basis x_ν, then it is realized by $P^{-1}CP$ with respect to the basis y_ν. For if

$$c(x_1,\dots,x_n) = (x_1,\dots,x_n)C$$

then

$$c(y_1,\dots,y_n) = c(x_1,\dots,x_n)P = ((x_1,\dots,x_n)C)P$$
$$= (x_1,\dots,x_n)CP = ((y_1,\dots,y_n)P^{-1})CP$$
$$= (y_1,\dots,y_n)P^{-1}CP.$$

It follows immediately that $\mathfrak{M}$ gives all the representations in one representation class when all bases of $\mathfrak{M}$ are used to realize the linear transformations of $\mathfrak{M}$ induced by $\mathfrak{o}$.

2. Every representation class is generated by a representation module in the manner specified under 1. (We again restrict ourselves to direct representations.)

Proof. Choose a specified representation in the class, given by the homomorphic assignment $c \mapsto C$. If n is the degree of the representation, form, with n indeterminates $x_1,\dots,x_n$, a right T-module

$$\mathfrak{M} = x_1\mathsf{T} + \cdots + x_n\mathsf{T}$$

(with the usual rules of calculation $\sum x_i\tau_i + \sum x_i\overline{\tau}_i = \sum x_i(\tau_i+\overline{\tau}_i)$, $\sum x_i\tau_i = \sum x_i\overline{\tau}_i$ if and only if $\tau_i = \overline{\tau}_i$ for all i, and $(\sum x_i\tau_i)\varrho = \sum x_i\tau_i\varrho$), and make it a left $\mathfrak{o}$-module by stipulating that $c\sum x_i\tau_i = \sum x_i'\tau_i$ if $(x_1',\dots,x_n') = (x_1,\dots,x_n)C$, where C denotes the matrix in the representation assigned to the element c of $\mathfrak{o}$.

This stipulation makes $\mathfrak{M}$ into an $\mathfrak{o},\mathsf{T}$-bimodule. First, the homomorphy relations

$$c+d \mapsto C+D \quad \text{and} \quad cd \mapsto CD$$

imply

$$(c+d)x_i = cx_i + dx_i$$

and

$$cd\cdot x_i = c\cdot dx_i, \quad \text{and furthermore} \quad c\left(\sum x_i\tau_i + \sum x_i\overline{\tau}_i\right) = c\sum x_i\tau_i + c\sum x_i\overline{\tau}_i;$$

these are the left-module properties. Second, plainly

$$c(\sum x_i\,\tau_i\,\varrho) = (c\sum x_i\,\tau_i)\cdot\varrho\,;$$

this is the mixed associative law.

Thus $\mathfrak{M}$ is a representation module, and the representation used is generated from it in the manner specified under 1 when the basis $x_1,\dots,x_n$ is used to realize its linear transformations. The other bases give the remaining representations in the class.

Everything proceeds in the same way for reciprocal representations and representation modules. One obtains the result that the module

$$\mathfrak{M}^* = \mathsf{T}^* x_1^* + \cdots + \mathsf{T}^* x_n^*$$

generates a reciprocal representation of $\mathfrak{o}$ in T^* by assigning to the element c of $\mathfrak{o}$ the matrix C in the equation

$$c \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} cx_1 \\ \vdots \\ cx_n \end{pmatrix} = C \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

The different bases again give the different representations in one class.

Chapter II. Galois Theory of Commutative Fields

The representation theory developed thus far suffices to provide a foundation for Galois theory which has the advantage over the usual foundation that it need not resort to special systems of generating elements and theorems about polynomials in indeterminates.[1]

ğ 5. Extension of the Coefficient Domain of Hypercomplex Systems

We formulate the following general theorem, whose proof may be omitted because it is almost self-evident. Let $\mathfrak{o} = c_1\mathsf{P} + \cdots + c_n\mathsf{P}$ be a hypercomplex system over the commutative field P. Let Ω be an extension ring of P whose center contains P. We define the *extended system* $\mathfrak{o}_\Omega$ as the set of all formal sums $\sum c_i\omega_i$, $\omega_i \in \Omega$. This set is first made into an Ω-module commuting with Ω by the stipulations

$$\begin{aligned}
&\textstyle\sum c_i\omega_i = \sum c_i\omega_i' \quad \text{if and only if } \omega_i = \omega_i' \text{ for every } i;\\
&\textstyle\sum c_i\omega_i + \sum c_i\omega_i' = \sum c_i(\omega_i + \omega_i');\\
&\textstyle\omega \sum c_i\omega_i = \sum c_i\omega\omega_i; \quad \sum c_i\omega_i \cdot \omega = \sum c_i\omega_i\omega;\\
&\textstyle\sum c_i\omega_i = \sum \omega_i c_i,
\end{aligned}$$

and is then made into an extension ring of $\mathfrak{o}$ by the further stipulation

$$\sum c_i\omega_i \cdot \sum c_i\omega_i = \sum_i \sum_j c_i c_j \omega_i \omega_j$$

—where c_ic_j is already defined as an element of $\mathfrak{o}$. The system $\mathfrak{o}_\Omega$ has rank n over Ω and can be written in the form

$$\mathfrak{o}_\Omega = c_1\Omega + \cdots + c_n\Omega.$$

The definition of $\mathfrak{o}_\Omega$ is independent of the basis $c_1, \ldots, c_n$. If Ω is a commutative field, then $\mathfrak{o}_\Omega$ is a hypercomplex system over Ω.

ğ 6. The Irreducible Representations of Commutative Systems

Let $\mathfrak{Z} = z_1\mathsf{P} + \cdots + z_n\mathsf{P}$ be a commutative system over P. We wish to determine all irreducible representations of $\mathfrak{Z}$ in an algebraically closed extension field Ω of P. Every representation of $\mathfrak{Z}$ in Ω gives a representation of $\mathfrak{Z}_\Omega = z_1\Omega + \cdots + z_n\Omega$—for the representations of the basis elements already contained in P suffice to determine the entire representation—and, conversely, every representation of $\mathfrak{Z}_\Omega$ contains a representation of $\mathfrak{Z}$. We may therefore ask instead for the representations of $\mathfrak{Z}_\Omega$. By M.Z. § 20, these are contained in the regular representation of $\mathfrak{Z}_\Omega$, that is, in the representation of $\mathfrak{Z}_\Omega$ obtained by using $\mathfrak{Z}_\Omega$ itself as a representation module. It even suffices to restrict oneself to $\mathfrak{Z}_\Omega/\mathfrak{C}$ as representation module, where $\mathfrak{C}$ denotes the radical of $\mathfrak{Z}_\Omega$ (see M.Z. § 19).

But $\mathfrak{Z}_\Omega/\mathfrak{C}$ is a completely reducible system, hence a direct sum of fields of finite degree over Ω. Since Ω is algebraically closed, these summands are isomorphic to Ω:

[1] For what follows, compare M.Z. §§ 15–20. M.Z. § 21 contains the first theorems of the following section on Galois theory. For the definition of hypercomplex systems, see M.Z. § 6.

$$\mathfrak{Z}_\Omega/\mathfrak{C} = e_1\Omega + \cdots + e_t\Omega.$$

The e_ν are the components of the identity. Thus:

The system $\mathfrak{Z}_\Omega$ has exactly t distinct irreducible representation classes in Ω, all of degree one. Here t is the rank of $\mathfrak{Z}_\Omega/\mathfrak{C}$, and is therefore at most n.

Each of these representation classes contains only one representation, for transforming a representation of degree one in a commutative field does not alter the representation: $\pi^{-1} \cdot \alpha \cdot \pi = \alpha$.

There are therefore exactly t distinct homomorphic mappings $\Theta_1, \ldots, \Theta_t$ of $\mathfrak{Z}_\Omega$ onto subrings of Ω.

ğ 7. The Isomorphisms of a Field

Now let $\mathfrak{Z}$ be a field. Every homomorphism Θ_i from $\mathfrak{Z}_\Omega$ onto a subring of Ω must map $\mathfrak{Z}$ isomorphically onto a subfield Z_i of Ω. For either $Z_i = 0$—which is not the case here, because the identity of $\mathfrak{Z}$ corresponds to the identity of Ω—or Z_i is an isomorphic image of $\mathfrak{Z}$. Hence:

If $\mathfrak{Z}$ is a finite field extension of degree n of P, then Ω contains as many distinct fields Z_i isomorphic to $\mathfrak{Z}$ as the rank t of $\mathfrak{Z}_\Omega/\mathfrak{C}$. The number of the Z_i is therefore at most n.

One calls $\mathfrak{Z}$ of the first kind over P if the number of the Z_i equals n, and of the second kind if this number is less than n.

The field $\mathfrak{Z}$ is of the first kind over P if and only if $\mathfrak{Z}_\Omega$ is completely reducible.

Here one sees the advantage of this foundation of Galois theory over the usual one. In the usual Galois theory one considers the isomorphisms of one of the Z_i onto the others. That asymmetry is avoided here. To show that a field has no more conjugate fields than its degree, one ordinarily uses a primitive element. Here the fact follows simply because all irreducible representations of $\mathfrak{Z}_\Omega$ are contained in the regular representation.

ğ 8. The Splitting Field

The Z_i are the irreducible representations of $\mathfrak{Z}$ in Ω. Thus, if the field Γ between P and Ω, $\mathsf{P} \subseteq \Gamma \subseteq \Omega$, contains every Z_i, then $\mathfrak{Z}_\Gamma/\mathfrak{C}$ must already decompose into t fields of degree one over Γ. Conversely, in order that $\mathfrak{Z}_\Gamma/\mathfrak{C}$ decompose into t fields, which are then the irreducible representations of degree one of $\mathfrak{Z}_\Gamma$, the Z_i must be contained in Γ. If one calls a field Γ a splitting field of $\mathfrak{Z}$ when it has the property that $\mathfrak{Z}_\Gamma/\mathfrak{C}$ becomes a direct sum of t fields, then we have:

The Galois field of the Z_i isomorphic to $\mathfrak{Z}$, that is, their compositum, is the minimal splitting field of $\mathfrak{Z}$.

ğ 9. The Isomorphisms from Z_1 onto the Z_i

When restricted to $\mathfrak{Z}$, Θ_i is an isomorphic mapping of $\mathfrak{Z}$ onto Z_i. Thus $S_i = \Theta_i\Theta_1^{-1}$ is an isomorphic mapping of Z_1 onto Z_i. Since the Θ_i are distinct, so are the S_i. These S_i are the isomorphisms of a field Z_1 onto its conjugates ordinarily considered in Galois theory. There are no others, because there are no other Θ_i.

ğ 10. The Galois Group

If $\mathfrak{Z}$ is a Galois field, so that the Z_i coincide as sets of elements, then the S_i form the group of all isomorphisms of Z onto itself that leave P fixed. For every product S_iS_j is an automorphism of Z, and, since there are none other than the S_i, S_iS_j is equal to some S_k. Thus the S_i form the group of all automorphisms of Z that leave every element of P fixed; this is the Galois group of Z relative to P.

ğ 11. The Fundamental Theorem of Galois Theory

Let $\mathfrak{Z}$ now be a Galois extension of the first kind of P. We prove the fundamental theorem of Galois theory:

The fields Γ between P and $\mathfrak{Z}$ can be placed in one-to-one correspondence with the subgroups $\mathfrak{H}$ of the Galois group $\mathfrak{G}$ of Z relative to P, in such a way that the group $\mathfrak{H}$ assigned to the field Γ consists of all automorphisms of Z which leave Γ elementwise fixed, while Γ is the set of all elements of Z fixed by every automorphism contained in $\mathfrak{H}$.

We formulate this briefly as follows:

1. If $\mathfrak{H}$ is the invariant group of Γ, then Γ is the invariant field of $\mathfrak{H}$.

2. If Γ is the invariant field of $\mathfrak{H}$, then $\mathfrak{H}$ is the invariant group of Γ.

1. can be reduced to the auxiliary theorem: *If* $\mathsf{P} \subseteq \Sigma \subseteq \mathsf{T} \subseteq \mathsf{Z}$, *and* T *has degree* t *over* Σ, *then every isomorphism from* Σ *onto a conjugate field (necessarily contained in* Z*) can be extended to* t *distinct isomorphisms from* T *onto conjugate fields.*

Suppose that $\mathfrak{H}$ is the invariant group of Σ, and that T is the invariant field of $\mathfrak{H}$. We can then argue as follows. The elements of $\mathfrak{H}$ are the extensions to all of Z of the identity isomorphism of Σ. If these extensions are applied only to T, the auxiliary theorem shows that they fall into t classes, such that isomorphisms in the same class are identical on T, while isomorphisms in different classes are distinct on T. But because T is the invariant field of $\mathfrak{H}$, one must have $t = 1$, hence $\mathsf{T} = \Sigma$, as was to be proved.

To prove the auxiliary theorem, return to the fields $\mathfrak{S}, \mathfrak{T}$ between P and Z that correspond under Θ_1 to Σ and T. We must then prove:

Every isomorphism H_i *from* $\mathfrak{S}$ *onto a field* Σ_i *can be extended in exactly* t *distinct ways to isomorphisms from* $\mathfrak{T}$ *onto subfields* T_i *of* Z.

Because $\mathfrak{Z}$ is assumed to be of the first kind over P, $\mathfrak{Z}_\Omega/\mathfrak{C}$ is identical with $\mathfrak{Z}_\Omega$; hence $\mathfrak{S}_\Omega$ decomposes into as many fields as its degree s indicates:

$$\mathfrak{S}_\Omega = E_1\Omega + \cdots + E_s\Omega.$$

As representation modules, the $E_\nu\Omega$ generate the s isomorphisms of $\mathfrak{S}$ onto s subfields $\Sigma_1, \ldots, \Sigma_s$. To find the isomorphisms of $\mathfrak{T}$, we require $\mathfrak{T}_\Omega$. Because the $E_\nu\Omega$ are ideals of $\mathfrak{S}_\Omega$, one has $E_\nu\Omega = \mathfrak{S}_\Omega E_\nu$. Moreover, plainly,

$$\mathfrak{T}_\Omega = \mathfrak{T} \cdot \Omega = \mathfrak{T} \cdot \mathfrak{S}_\Omega.$$

Therefore

$$\mathfrak{T}_\Omega = E_1\mathfrak{S}_\Omega \cdot \mathfrak{T} + \cdots + E_s\mathfrak{S}_\Omega \cdot \mathfrak{T} = E_1\mathfrak{T}_\Omega + \cdots + E_s\mathfrak{T}_\Omega.$$

This is a decomposition of $\mathfrak{T}_\Omega$ into ideals. The ideal $E_\nu \cdot \mathfrak{T}_\Omega$ decomposes into t simple ideals. Indeed, the degree relations

$$[\mathfrak{T}_\Omega \cdot E_\nu : \mathfrak{S}_\Omega E_\nu] \leqq [\mathfrak{T}_\Omega : \mathfrak{S}_\Omega] = [\mathfrak{T} : \mathfrak{S}] = t$$

hold; therefore, since $\mathfrak{S}_\Omega E_\nu = \Omega E_\nu \simeq \Omega$,

$$[\mathfrak{T}_\Omega \cdot E_\nu : \Omega] = [\mathfrak{T}_\Omega E_\nu : \mathfrak{S}_\Omega E_\nu] \leqq t,$$

and, because the sum of all the degrees $[\mathfrak{T}_\Omega E_\nu : \Omega]$ must equal $s \cdot t$,

$$[\mathfrak{T}_\Omega \cdot E_\nu : \Omega] = t, \qquad E_\nu\mathfrak{T}_\Omega = e_\nu^{(1)} \cdot \Omega + \cdots + e_\nu^{(t)}\Omega.$$

Each $e_\nu^{(i)}\Omega$ gives an irreducible representation of $\mathfrak{T}_\Omega$. It remains only to show that all these representations, when restricted to $\mathfrak{S}_\Omega$, coincide with the representation generated by $E_\nu \cdot \Omega$. This is clear, for

$$s \cdot E_\nu = E_\nu\sigma_\nu \quad (s \in \mathfrak{S}_\Omega \text{ is represented by } \sigma_\nu)$$

implies

$$\sum s \cdot e_\nu^{(i)} = \sum e_\nu^{(i)}\sigma_\nu,$$

and hence, by the uniqueness of the direct-sum representation,

$$s \cdot e_\nu^{(i)} = e_\nu^{(i)}\sigma_\nu;$$

thus the new representations too assign to the element s the element σ_ν.

2. Let T **be the invariant field of** $\mathfrak{H}$**.** We wish to recognize $\mathfrak{H}$ as the invariant group of T. For this it suffices to exhibit an element of T which is not fixed by any given automorphism not belonging to $\mathfrak{H}$.

The elements S_i of the Galois group $\mathfrak{G}$ of Z are the automorphisms of Z that leave P fixed. We make them automorphisms of $\mathfrak{Z}_\mathsf{Z}$ by stipulating

$$S_i z = z, \quad \text{if } z \text{ is in } \mathfrak{Z}.$$

Application of S_i to

$$\mathfrak{Z}_\mathsf{Z} = e_1\mathsf{Z} + \cdots + e_n\mathsf{Z}$$

must permute the direct summands $e_\nu \mathsf{Z}$, since they are uniquely determined. In particular,

$$S_i e_\nu = e_{\nu'}, \qquad \text{and} \qquad S_i e_\nu \neq S_k e_\nu \quad \text{for } i \neq k.$$

If $S_1, \ldots, S_h$ are the elements of $\mathfrak{H}$, choose any one e_ν, say e', and consider all the e_ν generated from it by the S_i, $i \leqq h$:

$$e_1 = S_1 e', \ldots, e_h = S_h e'.$$

Since, for $i \leqq h$, $j \leqq h$,

$$S_i e_j = S_i S_j e' = S_k e' = e_k \quad \text{with} \quad k \leqq h,$$

every S_i in $\mathfrak{H}$ permutes $e_1, \ldots, e_h$ among themselves. Consequently,

$$E_1 = e_1 + \cdots + e_h$$

is an element of $\mathfrak{Z}$ invariant under every $S_i \in \mathfrak{H}$. If E_1 is expressed in terms of a basis of $\mathfrak{Z}$, its coefficients must be elements of Z invariant under $\mathfrak{H}$; they therefore belong to T.

The element E_1 is not invariant under any S_i not belonging to $\mathfrak{H}$. For, for such an S_i,

$$S_i E_1 = e_i + \cdots$$

contains the component e_i, which does not occur among $e_1, \ldots, e_h$, while the direct-sum representation of E_1 is unique.

ğ 12. The Formal Significance of the Components e_i

Fix a basis $z_1, \ldots, z_n$ of $\mathfrak{Z}$:

$$\mathfrak{Z} = z_1 \mathsf{P} + \cdots + z_n \mathsf{P}.$$

(We now assume of $\mathfrak{Z}$ only that it is of the first kind.) The isomorphism Θ_i maps the system $z_1, \ldots, z_n$ onto a basis $\zeta_1^{(i)}, \ldots, \zeta_n^{(i)}$ of Z_i, by the relations

$$z_\nu e_i = e_i \zeta_\nu^{(i)}.$$

Conversely, the component e_j of the identity must be expressible in terms of the z_ν with coefficients from Z:

$$e_j = \sum_\nu \varrho_\nu^{(j)} z_\nu.$$

Hence

$$e_j = e_j^2 = \sum \varrho_\nu^{(j)} z_\nu e_j = \sum \varrho_\nu^{(j)} \cdot \zeta_\nu^{(j)} \cdot e_j$$

and

$$0 = e_j e_k = \sum \varrho_\nu^{(j)} \cdot z_\nu \cdot e_k = \sum \varrho_\nu^{(j)} \cdot \zeta_\nu^{(k)} \cdot e_k;$$

therefore,

$$\sum_\nu \varrho_\nu^{(j)} \cdot \zeta_\nu^{(j)} = 1; \qquad \sum_\nu \varrho_\nu^{(j)} \cdot \zeta_\nu^{(k)} = 0, \quad \text{if } j \neq k.$$

That is, the matrices

$$\begin{pmatrix} \zeta_1^{(1)} & \cdots & \zeta_n^{(1)} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \zeta_1^{(n)} & \cdots & \zeta_n^{(n)} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \varrho_1^{(1)} & \cdots & \varrho_1^{(n)} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \varrho_n^{(1)} & \cdots & \varrho_n^{(n)} \end{pmatrix}$$

are inverse to one another. This is also expressed by saying that $\varrho_1^{(i)}, \ldots, \varrho_n^{(i)}$ is the basis complementary to $\zeta_1^{(i)}, \ldots, \zeta_n^{(i)}$. It plays a role in the theory of the different of a number field.

ğ 13. The General Extension Theorem

The theorem proved on p. 10 concerning the extension of the H_i can be generalized.

Let $\mathfrak{Z} = z_1\mathsf{P} + \cdots + z_n\mathsf{P}$ be a commutative, hypercomplex, completely reducible system. Let $\mathfrak{S}$ and $\mathfrak{T}$ be—necessarily also completely reducible—subsystems of $\mathfrak{Z}$, situated as follows:

$$\mathsf{P} \subseteq \mathfrak{S} \subseteq \mathfrak{T} \subseteq \mathfrak{Z}.$$

By M.Z. § 13, each of the three systems has an identity. These three identities need by no means be the same. (They certainly are not if $\mathfrak{S}$ and $\mathfrak{T}$ are ideals of $\mathfrak{Z}$ different from $\mathfrak{Z}$.) Let E be the identity of $\mathfrak{S}$. The system $\mathfrak{T} \cdot E$ is an $\mathfrak{S}$-module of finite rank:

$$E\mathfrak{T} = a_1\mathfrak{S} + \cdots + a_t\mathfrak{S}$$

(whereas $\mathfrak{T}$ in general is not).

Proof. The system $\mathfrak{S}$ is a direct sum of fields: $\mathfrak{S} = \mathfrak{R}_1 + \cdots + \mathfrak{R}_r$. This gives a corresponding direct-sum decomposition of $\mathfrak{T}E$. Every summand of $\mathfrak{T}E$ must contain one of the fields $\mathfrak{R}_i$; otherwise it would be annihilated by E, whereas E is the identity of $\mathfrak{T}E$. Thus $\mathfrak{T}E$ is a direct sum of extension rings of the $\mathfrak{R}_i$, that is, a direct sum of the form

$$\mathfrak{T}E = a_{11}\mathfrak{R}_1 + \cdots + a_{1p_1}\mathfrak{R}_1 + \cdots + a_{rp_r}\mathfrak{R}_r,$$

or $E\mathfrak{T} = a_{11}\mathfrak{S} + \cdots + a_{rp_r}\mathfrak{S}$, as was to be proved.

General Extension Theorem.

Every irreducible representation of $\mathfrak{S}$ in Ω, given by a homomorphism H_i, can be extended in exactly t distinct ways to representations of $\mathfrak{T}$.

The proof is analogous to that on pp. 10–11. One has

$$\mathfrak{S}_\Omega = E_1\Omega + \cdots + E_s\Omega, \qquad E_\nu\Omega = \mathfrak{S}_\Omega E_\nu,$$

$$\mathfrak{T}_\Omega \cdot E = \mathfrak{T} \cdot E\Omega = \mathfrak{T}\mathfrak{S}\Omega = \mathfrak{T}\mathfrak{S}_\Omega,$$

$$\mathfrak{T}_\Omega \cdot E = \mathfrak{T}(E_1\mathfrak{S}_\Omega + \cdots + E_s\mathfrak{S}_\Omega) = E_1\mathfrak{T}_\Omega + \cdots + E_s\mathfrak{T}_\Omega,$$

$$[\mathfrak{T}_\Omega E_\nu : \Omega] = [\mathfrak{T}_\Omega E_\nu : \Omega E_\nu] = [\mathfrak{T}_\Omega E_\nu : E_\nu\mathfrak{S}_\Omega] \leqq [\mathfrak{T}_\Omega \cdot E : \mathfrak{S}_\Omega] = [\mathfrak{T} \cdot E : \mathfrak{S}] = t,$$

$$\sum [\mathfrak{T}_\Omega \cdot E_\nu : \Omega] = st;$$

hence

$$[\mathfrak{T}_\Omega E_\nu : \Omega] = t.$$

Accordingly, $\mathfrak{T}_\Omega E_\nu$ decomposes into t ideals, each of which, being a summand of $\mathfrak{T}_\Omega E$ and hence also of $\mathfrak{T}_\Omega$, gives a representation of $\mathfrak{T}_\Omega$ which proves, just as on pp. 10–11, to be an extension of the representation given by H_ν. The remaining irreducible representations of $\mathfrak{T}_\Omega$—generated by the summands of $\mathfrak{T}_\Omega$ not contained in $\mathfrak{T}_\Omega \cdot E_\nu$—cannot be extensions of the representations of $\mathfrak{S}_\Omega$ generated by the H_ν, because these ideals are annihilated by $\mathfrak{T}_\Omega \cdot E_\nu$, and therefore all the more by $\mathfrak{S}_\Omega$.

Chapter III. Abelian Groups

ğ 14. The Group Ring

Let $\mathfrak{G}$ be a finite group with elements $a_1, \ldots, a_h$, and let P be a commutative field. Using group multiplication as multiplication, we form a hypercomplex system

$$\mathfrak{o}[\mathfrak{G}] = a_1\mathsf{P} + \cdots + a_h\mathsf{P},$$

the group ring of $\mathfrak{G}$ in P. (M.Z. § 6; Speiser, *Theorie der Gruppen endlicher Ordnung*, § 48.)

We ask for the representations of $\mathfrak{o}[\mathfrak{G}]$ in P, or in an algebraically closed field Ω over P. As already mentioned, the irreducible representations are generated by the simple left ideals of $\mathfrak{o}[\mathfrak{G}]/\mathfrak{C}$. Thus, as in Galois theory, the question of when $\mathfrak{o}[\mathfrak{G}]$ has a radical is of interest. The following general theorem holds:

The group ring $\mathfrak{o}[\mathfrak{G}]$ is completely reducible if and only if the order h of $\mathfrak{G}$ is not divisible by the characteristic p of P.

We first prove:

$$\text{From } h = 0(p) \text{ it follows that } \mathfrak{C} \neq 0.$$

The set

$$\mathfrak{a} = \mathsf{P}(a_1 + \cdots + a_h)$$

is a two-sided ideal of $\mathfrak{o}$. Indeed,

$$\mathsf{P} \cdot (a_1 + \cdots + a_h)a = \mathsf{P} \cdot (a_1 a + \cdots + a_h a) = \mathsf{P}(a_1 + \cdots + a_h) = \mathfrak{a}$$

and

$$a \cdot \mathsf{P}(a_1 + \cdots + a_h) = \mathsf{P}(aa_1 + \cdots + aa_h) = \mathsf{P}(a_1 + \cdots + a_h) = \mathfrak{a}$$

by the group property of the a_i. The ideal $\mathfrak{a}$ is of course nonzero, but it is nilpotent:

$$\left(\sum_i a_i\right)^2 = \sum_i \sum_j a_i a_j = h \sum_j a_j = 0.$$

The converse,

$$\text{from } h \neq 0(p) \text{ it follows that } \mathfrak{C} = 0,$$

will now be proved only for Abelian groups. (In M.Z. § 26 this part of the theorem is proved in general.)

ğ 15. The Group Rings of Abelian Groups

Let $\mathfrak{A} = \{a_1, \ldots, a_h\}$ denote an Abelian group. Then $\mathfrak{o}$ is commutative, so we may apply the general theorems on commutative hypercomplex systems.

If h is not divisible by the characteristic p of P, then $\mathfrak{o}[\mathfrak{A}]$ has exactly h distinct irreducible representations in Ω. (They are of degree one because $\mathfrak{o}$ is commutative.)

It then follows that $\mathfrak{o}[\mathfrak{A}]/\mathfrak{C}$ has the same rank as $\mathfrak{o}$, and hence that $\mathfrak{C} = 0$. This proves, for Abelian groups, the second part of the theorem just left unproved.

Proof. The group $\mathfrak{A}$ is a direct product of cyclic groups $\mathfrak{Z}_i$ of orders h_i:

$$\mathfrak{A} = \mathfrak{Z}_1 \times \cdots \times \mathfrak{Z}_t, \qquad h = h_1 h_2 \cdots h_t.$$

If z_i is a generating element of $\mathfrak{Z}_i$, then the element corresponding to it in an irreducible representation (of degree one) must be an h_i-th root of unity $\varepsilon_\nu^{(h_i)}$. Conversely, assigning an h_i-th root of unity $\varepsilon_\nu^{(h_i)}$ to each z_i gives an irreducible representation of $\mathfrak{o}$ in Ω. Since $h \neq 0(p)$, and therefore all the more $h_i \neq 0(p)$, there are exactly $h_1 h_2 \cdots h_t = h$ distinct representations of $\mathfrak{o}$, as was to be proved.

(One also sees easily that if $h = 0(p)$, so that $h_i = 0(p)$ for at least one h_i, there are at most h_i/p distinct $\varepsilon_\nu^{(h_i)}$, hence fewer than h representations. Thus $\mathfrak{o}_\Omega$ must contain a nonzero radical. But nothing follows immediately from this about the radical of $\mathfrak{o}$.)

Denote the h distinct homomorphic mappings from $\mathfrak{o}_\Omega$ onto subrings of Ω by $\Theta_1, \ldots, \Theta_h$. To each Θ_i there corresponds a summand $e_i\Omega$ of $\mathfrak{o}_\Omega$ as representation module. At times we apply Θ_i only to $\mathfrak{A}$, and then speak of a representation of $\mathfrak{A}$. These mappings of $\mathfrak{A}$ onto groups of roots of unity are the h characters of $\mathfrak{A}$. One special character is the principal character, which assigns 1 to every element of $\mathfrak{A}$. Let the corresponding Θ_i be Θ_1.

Representation by the principal character is possible for every group, not only for Abelian groups. Since this representation already lies in P, if $\mathfrak{o}$ is completely reducible it must split off a simple summand $E \cdot \mathfrak{o}$ which gives this representation. We can calculate E directly. It must be $E = \sum x_i a_i$. First,

$$aE = E \cdot 1 \quad \text{or} \quad \sum x_i a a_i = \sum x_i a_i,$$

from which, for $a = a_j a_i^{-1}$,

$$x_1 a_j a_i^{-1} a_1 + \cdots + x_i a_j + \cdots + x_h a_j a_i^{-1} a_h = x_1 a_1 + \cdots + x_h a_h,$$

and therefore

$$x_i = x_j,$$

follows.

Second,

$$E = E^2 = x^2 \left(\sum a_i\right)^2 = x^2 h \sum a_i = xhE.$$

If $h = 0(p)$, it follows that $E = 0$; that is, $\mathfrak{o}$ does not contain the representation module for the principal character, and therefore cannot have been completely reducible. This again proves one half of the theorem on p. 13.

If, however, $h \neq 0(p)$, so that $\mathfrak{o}$ is completely reducible, then it follows immediately that

$$x = \frac{1}{h}, \qquad E = \frac{1}{h}(a_1 + \cdots + a_h).$$

ğ 16. The Character Relations

The fact that $E = (1/h) \cdot \sum a_i$ gives the principal character leads immediately to the character relations. One must have

$$a \cdot e_i = e_i \cdot \Theta_i a,$$

and hence

$$e_i \cdot \Theta_i e_j = \begin{cases} e_i & i = j \\ 0 & i \neq j. \end{cases}$$

or

$$\Theta_i e_j = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

In particular,

$$\Theta_i e_1 = \begin{cases} 1 & i = 1 \\ 0 & i \neq 1. \end{cases}$$

or, since $e_1 = (1/h) \sum a_i$,

$$\sum_\nu \Theta_i a_\nu = \begin{cases} h & i = 1, \\ 0 & i \neq 1. \end{cases}$$

These are the familiar character relations:

The sum of a character over all group elements is zero, except for the principal character, for which it is h.

ğ 17. The Galois Theory of Abelian Groups

For the group rings of Abelian groups one can establish theorems similar to those proved for commutative fields in Galois theory. In Galois theory the $\Theta_i \Theta_1^{-1}$ formed a group $\mathfrak{G}$. The fundamental theorem expresses a one-to-one correspondence, based on certain invariance properties, between the subgroups of $\mathfrak{G}$ and the subfields of Z.

The homomorphisms Θ_i of $\mathfrak{o}[\mathfrak{A}]$ can be combined into a group A whose subgroups stand in a similar relation to the subgroups of $\mathfrak{A}$.

Define the product $\Theta_i \Theta_k = \Theta$ by

$$\Theta a = \Theta_i a \cdot \Theta_k a.$$

Then the totality of the Θ_i is a group A isomorphic to $\mathfrak{A}$.

Proof. Since

$$\begin{aligned}\Theta a \cdot \Theta b &= \Theta_i a \cdot \Theta_k a \cdot \Theta_i b \cdot \Theta_k b \\ &= \Theta_i a \cdot \Theta_i b \cdot \Theta_k a \cdot \Theta_k b \\ &= \Theta_i ab \cdot \Theta_k ab = \Theta ab,\end{aligned}$$

$\Theta = \Theta_i \cdot \Theta_k$ is a homomorphism from $\mathfrak{A}$ onto A; and since there are no homomorphisms of $\mathfrak{A}$ other than the Θ_i, Θ is equal to some Θ_j. Thus the Θ_i do indeed form a group of h elements.

Let ε_{h_ν} now denote a primitive h_ν-th root of unity. Then Θ_i maps the generating element z_ν of the cyclic factor $\mathfrak{Z}_\nu$ of $\mathfrak{A}$ onto a power of ε_{h_ν}:

$$\Theta_i z_\nu = \varepsilon_{h_\nu}^{\varrho_\nu^{(i)}}.$$

Assign to the homomorphism Θ_i the element $\prod_\nu z_\nu^{\varrho_\nu^{(i)}}$ of $\mathfrak{A}$. This is a one-to-one mapping of A onto $\mathfrak{A}$, for Θ_i is determined by the $\varrho_\nu^{(i)}$, and therefore distinct Θ_i correspond to distinct $\prod_\nu z_\nu^{\varrho_\nu^{(i)}}$. The mapping is isomorphic. Indeed, on the one hand,

$$\Theta_i \Theta_j z_\nu = \Theta_i z_\nu \cdot \Theta_j z_\nu = \varepsilon_{h_\nu}^{\varrho_\nu^{(i)} + \varrho_\nu^{(j)}},$$

while, on the other hand,

$$\prod_\nu z_\nu^{\varrho_\nu^{(i)}} \cdot \prod_\nu z_\nu^{\varrho_\nu^{(j)}} = \prod_\nu z_\nu^{\varrho_\nu^{(i)} + \varrho_\nu^{(j)}}, \quad \text{as was to be proved.}$$

We now define:

Invariant domain of a subgroup B *of* A*:*

The subgroup $\mathfrak{B}$ consisting of the elements of $\mathfrak{A}$ which are mapped onto 1 by every $\Theta \in \mathsf{B}$.

Invariant group of a subgroup $\mathfrak{B}$ *of* $\mathfrak{A}$*:*

The subgroup B consisting of the elements of A which map every $a \in \mathfrak{B}$ onto 1.

We formulate the fundamental theorem:

The subgroups $\mathfrak{B}$ of $\mathfrak{A}$ and the subgroups B of A can be placed in one-to-one correspondence in such a way that, if $\mathfrak{B}$ and B correspond, B is the invariant group of $\mathfrak{B}$, while $\mathfrak{B}$ is the invariant domain of B.

We must therefore prove:

1. If B is the invariant group of $\mathfrak{B}$, then $\mathfrak{B}$ is the invariant domain of B.

2. If $\mathfrak{B}$ is the invariant domain of B, then B is the invariant group of $\mathfrak{B}$.

1. This follows, as on p. 10, from the general extension theorem. Suppose that B is the invariant group of $\mathfrak{B}$, and let $\mathfrak{B}'$ be the invariant domain of B; then $\mathfrak{B}'$ contains $\mathfrak{B}$. The elements of B are the extensions to all of $\mathfrak{A}$ of the one homomorphism of $\mathfrak{B}$ which maps $\mathfrak{B}$ onto 1. If these extensions are applied only to $\mathfrak{B}'$, it follows from the general extension theorem that they fall into t classes, such that homomorphisms in the same class are identical, and homomorphisms in different classes are distinct, on $\mathfrak{B}'$. Here t is the degree of $\mathfrak{o}[\mathfrak{B}']$ over $\mathfrak{o}[\mathfrak{B}]$, hence the index of $\mathfrak{B}$ in $\mathfrak{B}'$, since $\mathfrak{o}[\mathfrak{B}]$ and $\mathfrak{o}[\mathfrak{B}']$ have the same identity element, namely the identity element of all of $\mathfrak{A}$. Because $\mathfrak{B}'$ is the invariant domain of B, one must have $t = 1$, hence $\mathfrak{B}' = \mathfrak{B}$, as was to be proved.

2. We reduce this to 1. Regard the elements a of $\mathfrak{A}$ as homomorphisms of A. Namely, set $a\Theta$ equal to the root of unity Θa, briefly $a\Theta = \Theta a$. This does indeed define a as a homomorphism of A, for

$$a\Theta \cdot a\Theta' = \Theta a \cdot \Theta' a = \Theta\Theta' a = a\Theta\Theta'.$$

The product of two homomorphisms a, b is the usual group product:

$$\begin{array}{ccccc} ab\Theta & = & a\Theta \cdot b\Theta & = & \Theta a \cdot \Theta b = \Theta ab \quad = ab\Theta \\ & & \text{product of homomorphisms} & & \text{group product} \end{array}$$

Elements a, b distinct as group elements are also distinct as homomorphisms. From $a\Theta = b\Theta$ for every Θ, it follows that $\Theta a = \Theta b$ for every Θ, or $\Theta ab^{-1} = 1$ for every Θ. Thus the Θ are the extensions to all of $\mathfrak{A}$

of the identity homomorphism of the cyclic subgroup $\mathfrak{Z}$ of $\mathfrak{A}$ generated by ab^{-1}. By the extension theorem, the index of $\mathfrak{Z}$ in $\mathfrak{A}$ is therefore h; that is, $\mathfrak{Z} = e$, and $a = b$.

We now translate the statements made under the new interpretation,

a) $\mathfrak{B}$ is the invariant group of B.
b) B is the invariant domain of $\mathfrak{B}$,

into the old interpretation.

For a), $\mathfrak{B}$ consists of all $a \in \mathfrak{A}$ with $a\Theta = 1$ for every $\Theta \in \mathsf{B}$; that is, $\mathfrak{B}$ consists of all $a \in \mathfrak{A}$ with $\Theta \cdot a = 1$ for every $\Theta \in \mathsf{B}$. Thus the translation of a) is

a') $\mathfrak{B}$ is the invariant domain of B.

Correspondingly, the translation of b) is

b') B is the invariant group of $\mathfrak{B}$.

Hence the translation of the assertion already proved under 1,
If $\mathfrak{B}$ is the invariant group of B, then B is the invariant domain of $\mathfrak{B}$,
is precisely the assertion to be proved:
If $\mathfrak{B}$ is the invariant domain of B, then B is the invariant group of $\mathfrak{B}$.
Writing down the character relations of p. 15 for A in place of $\mathfrak{A}$, one obtains the equations

$$\sum_{i=1}^{h} \Theta_i a_\nu = \begin{cases} h & \nu = 1, \\ 0 & \nu \neq 1. \end{cases}$$

The sum of all characters at a group element is zero, except at the identity element, where it is h.

Chapter IV. Two-Sided Simple Rings

ğ 18. An Auxiliary Theorem

By K we mean a division ring, and by $\mathfrak{G}$ a group of automorphisms (isomorphic mappings onto itself) of K. The set of those elements of K that remain unchanged under every automorphism belonging to $\mathfrak{G}$ is a division subring P of K, the *invariant division ring of* $\mathfrak{G}$.

If $\tau \neq 0$ is any element of K, then an automorphism of K is obtained by assigning to an element α of K the element $\tau^{-1}\alpha\tau$. Following the corresponding terminology of group theory, we call such an automorphism an *inner automorphism*. The invariant division ring P of the group of all inner automorphisms of a division ring K is its center.

Now let a division ring K, an automorphism group $\mathfrak{G}$ of K, and its invariant division ring P be given. Let

$$\mathfrak{M} = x_1\mathsf{P} + \cdots + x_n\mathsf{P}$$

be a P-module of rank n. We define the action of an element γ of $\mathfrak{G}$ on the elements of $\mathfrak{M}$ by

$$\gamma \cdot x_i = x_i, \qquad \text{and hence} \qquad \gamma \sum \varrho_i x_i = \sum \varrho_i x_i.$$

It follows that $\mathfrak{G}$ has become an automorphism group of the extended module

$$\mathfrak{M}_\mathsf{K} = x_1\mathsf{K} + \cdots + x_n\mathsf{K};$$

the invariant domain of $\mathfrak{G}$ in $\mathfrak{M}_\mathsf{K}$ is then $\mathfrak{M}$. Under these assumptions the following theorem holds:
If

$$\mathfrak{C} = z_1\mathsf{K} + \cdots + z_r\mathsf{K}$$

is a submodule of $\mathfrak{M}_\mathsf{K}$ that is mapped into itself (not necessarily elementwise) by every element γ of $\mathfrak{G}$, then $\mathfrak{C}$ is the extension module, formed with K, of a submodule $\mathfrak{c}$ of $\mathfrak{M}$:

$$\mathfrak{C} = \mathfrak{c}_\mathsf{K}.$$

Proof. 1. Preliminary observation: We must have $\mathfrak{c} = \mathfrak{C} \cap \mathfrak{M}$. For in general

$$\mathfrak{c} = \mathfrak{c}_{\mathsf{K}} \cap \mathfrak{M}.$$

The inclusion $\mathfrak{c} \subseteq \mathfrak{c}_{\mathsf{K}} \cap \mathfrak{M}$ is clear. To prove $\mathfrak{c}_{\mathsf{K}} \cap \mathfrak{M} \subseteq \mathfrak{c}$, take a basis $y_1, \ldots, y_r$ of $\mathfrak{c}$,

$$\mathfrak{c} = y_1\mathsf{P} + \cdots + y_r\mathsf{P};$$

then

$$\mathfrak{c}_{\mathsf{K}} = y_1\mathsf{K} + \cdots + y_r\mathsf{K}.$$

Every element c of $\mathfrak{c}_{\mathsf{K}} \cap \mathfrak{M}$ admits a basis representation as an element of $\mathfrak{c}_{\mathsf{K}}$,

$$c = \sum_{i=1}^{r} y_i\chi_i,$$

and a basis representation as an element of $\mathfrak{M}$,

$$c = \sum_{i=1}^{r} y_i\varrho_i + \sum_{j=r+1}^{n} y_j\varrho_j,$$

where $y_{r+1}, \ldots, y_n$ denotes a system of elements of $\mathfrak{M}$ that completes $y_1, \ldots, y_r$ to a basis of $\mathfrak{M}$ (M.Z. ğ 6).

Since both representations may be regarded as basis representations in $\mathfrak{M}_{\mathsf{K}}$, they are identical: $\chi_i = \varrho_i$ $(i = 1, \ldots, r)$, $\varrho_j = 0$ $(j = r+1, \ldots, n)$. Hence

$$c = \sum_{i=1}^{r} y_i\varrho_i, \qquad \text{q.e.d.}$$

2. To prove the theorem in question, we construct a basis $z_1, \ldots, z_r$ of $\mathfrak{C}$ whose elements z_i belong to $\mathfrak{M}$. Then, on setting

$$\mathfrak{c} = z_1\mathsf{P} + \cdots + z_r\mathsf{P},$$

we do indeed have

$$\mathfrak{C} = \mathfrak{c}_{\mathsf{K}}.$$

Take any basis $y_1, \ldots, y_r$ of $\mathfrak{C}$, and complete it to a basis of $\mathfrak{M}_{\mathsf{K}}$ by suitable elements $x_{r+1}, \ldots, x_n$ of a basis $x_1, \ldots, x_n$ of $\mathfrak{M}$, which is therefore also a basis of $\mathfrak{M}_{\mathsf{K}}$. This is possible by M.Z. ğ 5.

$$\mathfrak{M}_{\mathsf{K}} = \mathfrak{C} + x_{r+1}\mathsf{K} + \cdots + x_n\mathsf{K}.$$

For the first r elements $x_1, \ldots, x_r$ of the basis of $\mathfrak{M}$, this gives equations

$$x_i = z_i - \sum_{j=r+1}^{n} x_j\chi_j^{(i)}, \qquad z_i \in \mathfrak{C}, \quad \chi_j^{(i)} \in \mathsf{K}.$$

Since the z_i, together with $x_{r+1}, \ldots, x_n$, plainly form a basis of $\mathfrak{M}_{\mathsf{K}}$, they are linearly independent; hence $z_1, \ldots, z_r$ is a basis of $\mathfrak{C}$. It is a basis of the form we seek: the z_i belong to $\mathfrak{M}$.

Let γ be an element of $\mathfrak{G}$. On the one hand,

$$(1) \qquad \gamma z_i = \gamma x_i + \sum_{j=r+1}^{n} \gamma x_j \cdot \gamma\chi_j^{(i)} = x_i + \sum_{j=r+1}^{n} x_j\gamma\chi_j^{(i)}.$$

On the other hand,

$$(2) \qquad \gamma z_i = \sum_{\mu=1}^{r} z_\mu\sigma_\mu^{(i)}, \qquad \sigma_\mu^{(i)} \in \mathsf{K},$$

because $\mathfrak{C}$ is invariant under every $\gamma \in \mathfrak{G}$. Equation (2) may then also be written in the form

$$(3) \qquad \gamma z_i \;=\; \sum_{\mu=1}^{r} x_\mu \sigma_\mu^{(i)} + \sum_{j=r+1}^{n} x_j \sum_{\mu=1}^{r} \chi_j^{(\mu)} \sigma_\mu^{(i)}.$$

Comparison of the coefficients in (1) and (3) gives

$$\sigma_j^{(i)} = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$$

Therefore

$$\gamma \cdot z_i = z_i.$$

Thus the z_i belong to the invariant domain of $\mathfrak{G}$, i.e. to $\mathfrak{M}$, q.e.d.

ğ 19. Representations of Two-Sided Simple Hypercomplex Systems in Noncommutative Extension Division Rings of Their Coefficient Fields

Let

$$\mathfrak{S} = x_1 \mathsf{P} + \cdots + x_n \mathsf{P}$$

be a two-sided simple, and hence completely reducible, hypercomplex system, and let K be a division ring with center P.

Theorem 1. $\mathfrak{S}_\mathsf{K}$ is two-sided simple (and hence also completely reducible).

Proof. 1. Every two-sided $\mathfrak{S}_\mathsf{K}$-ideal $\mathfrak{a}$ is invariant under the group $\mathfrak{G}$ of inner automorphisms of K. Indeed, if, for a nonzero element χ of K, we put $\chi^{-1}\mathfrak{a}\chi = \bar{\mathfrak{a}}$, then $\bar{\mathfrak{a}} \subseteq \mathfrak{a}$ by the ideal property of $\mathfrak{a}$; but since $\bar{\mathfrak{a}}$, regarded as a K-module, has the same rank over K as $\mathfrak{a}$, we must have $\bar{\mathfrak{a}} = \mathfrak{a}$.

2. By the auxiliary theorem just established, a two-sided $\mathfrak{S}_\mathsf{K}$-ideal $\mathfrak{a}$ must therefore be the extension ideal of a submodule $\mathfrak{A}$ of $\mathfrak{S}$, $\mathfrak{a} = \mathfrak{A}_\mathsf{K}$. The module $\mathfrak{A}$ is a two-sided $\mathfrak{S}$-ideal, for $\mathfrak{A} = \mathfrak{S} \cap \mathfrak{a}$ gives

$$\mathfrak{S}\mathfrak{A} \subseteq \mathfrak{S}\mathfrak{S} \cap \mathfrak{S}\mathfrak{a} \subseteq \mathfrak{S} \cap \mathfrak{a} = \mathfrak{A}$$

and

$$\mathfrak{A}\mathfrak{S} \subseteq \mathfrak{S}\mathfrak{S} \cap \mathfrak{a}\mathfrak{S} \subseteq \mathfrak{S} \cap \mathfrak{a} = \mathfrak{A}.$$

But since $\mathfrak{S}$ contains only the two-sided ideals 0 and $\mathfrak{S}$, $\mathfrak{S}_\mathsf{K}$ likewise contains only the two two-sided ideals 0 and $\mathfrak{S}_\mathsf{K}$, q.e.d.

We now seek the irreducible representations of $\mathfrak{S}$ in K. We shall set up the reciprocal representations, which has a formal advantage. Ultimately, of course, it makes no difference whether one takes direct or reciprocal representations, since they correspond bijectively.

Let $\mathfrak{M}$ be a reciprocal representation module of $\mathfrak{S}$ in K, that is, an $\mathfrak{S}$-left and K-left module of finite rank,

$$\mathfrak{M} = \mathsf{K} \cdot y_1 + \cdots + \mathsf{K} \cdot y_r,$$

with the commutation law

$$s(xm) = x(sm).$$

We prove that $\mathfrak{M}$ may also be regarded as an $\mathfrak{S}_\mathsf{K}$-left module. First the multiplication of an element of $\mathfrak{S}_\mathsf{K}$ by an element of $\mathfrak{M}$ must be defined. If $s \in \mathfrak{S},\ x \in \mathsf{K},\ m \in \mathfrak{M}$, put

$$sx \cdot m = s \cdot (x \cdot m),$$

and correspondingly, for a general element $\sum s_i x_i$ of $\mathfrak{S}_\mathsf{K}$, put

$$\sum s_i x_i \cdot m = \sum s_i \cdot (x_i \cdot m).$$

We verify that this definition is unambiguous and does not depend on the manner in which an element of $\mathfrak{S}_\mathsf{K}$ is represented as a sum of products $s_i x_i$.

Thus it is a matter of inferring from

$$(1) \qquad \sum_{i=1}^{p} s_i x_i \;=\; 0$$

that

$$\sum_{i=1}^{p} s_i(x_i m) = 0.$$

Assume that $s_1, \ldots, s_q$ are linearly independent and that $s_{q+1}, \ldots, s_p$ can be expressed in terms of $s_1, \ldots, s_q$:

$$s_j = \sum_{i=1}^{q} s_i \varrho_i^{(j)}, \qquad j = q+1, \ldots, p.$$

The coefficients must lie in P, because s_j can be expressed in only one way, while the representation is already possible in $\mathfrak{S}$. Equation (1) gives

$$x_i + \sum_{j=q+1}^{p} \varrho_i^{(j)} x_j = 0, \qquad i = 1, \ldots, q.$$

Consequently,

$$\begin{aligned}
\sum_{i=1}^{p} s_i(x_i m) &= s_1(x_1 m) + \cdots + s_q(x_q m) + \left(\sum_i s_i \varrho_i^{(q+1)}\right)(x_{q+1} m) \\
&\quad + \cdots + \left(\sum_i s_i \varrho_i^{(p)}\right)(x_p m) \\
&= s_1(x_1 m) + \cdots + s_q(x_q m) \\
&\quad + s_1 \varrho_1^{(q+1)}(x_{q+1} m) + \cdots + s_q \varrho_q^{(q+1)}(x_{q+1} m) \qquad \text{by the module property} \\
&\quad + \cdots \\
&\quad \cdots \\
&\quad + s_1 \varrho_1^{(p)}(x_p m) + \cdots + s_q \varrho_q^{(p)}(x_p m) \\
&= s_1(x_1 m) + \cdots + s_q(x_q m) \\
&\quad + s_1(\varrho_1^{(q+1)} x_{q+1} m) + \cdots + s_q(\varrho_q^{(q+1)} x_{q+1} m) \\
&\quad + \cdots \\
&\quad \cdots \\
&\quad \qquad \text{by the associative laws} \\
&\quad + s_1(\varrho_1^{(p)} x_p m) + \cdots + s_q(\varrho_q^{(p)} x_p m) \qquad s'(sm) = s's \cdot m \text{ and} \\
&\quad \qquad x'(xm) = x'x \cdot m \\
&= s_1\left(x_1 m + \varrho_1^{(q+1)} x_{q+1} \cdot m + \cdots + \varrho_1^{(p)} x_p \cdot m\right) + \cdots \\
&= s_1\left(\left(x_1 + \varrho_1^{(q+1)} x_{q+1} + \cdots + \varrho_1^{(p)} x_p\right) m\right) + \cdots \\
&= 0.
\end{aligned}$$

Of the $\mathfrak{S}_{\mathsf{K}}$-module properties of $\mathfrak{M}$, the distributive laws $(S+S')m = Sm + S'm,\ S(m+m') = Sm + Sm'$ are clear. The associative law $S(S'm) = SS' \cdot m$ still deserves attention. Since the distributive laws hold, we may restrict ourselves to the case

$$sx \cdot (s'x'm) = sx(s'x' \cdot m).$$

On the one hand, by the definition of $sx \cdot m$,

$$sx \cdot (s'x' \cdot m) = s \cdot (x \cdot (s' \cdot (x' \cdot m)));$$

on the other hand,

$$sxs'x' \cdot m = ss'xx' \cdot m = ss' \cdot (xx' \cdot m) = s \cdot (s' \cdot (x \cdot (x' \cdot m))),$$

which, by the two commutation relations

$$x \cdot s' = s' \cdot x$$

and

$$s' \cdot (x \cdot m) = x \cdot (s' \cdot m),$$

equals $s \cdot (x \cdot (s' \cdot (x' \cdot m)))$.

Thus $\mathfrak{M}$ is indeed an $\mathfrak{S}_\mathsf{K}$-left module, and of course a finite one. Conversely, every finite $\mathfrak{S}_\mathsf{K}$-left module is a reciprocal representation module of $\mathfrak{S}$ in K, for it is plainly a finite K-module and, because

$$s(x \cdot m) = sx \cdot m = xs \cdot m = x(s \cdot m),$$

it also satisfies the commutation condition. (See also the simpler proof in ğ 24.)

Now, by M.Z. ğ 18, every finite $\mathfrak{S}_\mathsf{K}$-module is a sum of simple modules that are $\mathfrak{S}_\mathsf{K}$-operator-isomorphic to the simple left ideals of $\mathfrak{S}_\mathsf{K}$. Conversely, every left ideal of $\mathfrak{S}_\mathsf{K}$ is a representation module of $\mathfrak{S}$ in K; and since all $\mathfrak{S}_\mathsf{K}$-left ideals are operator-isomorphic, we obtain:

Theorem 2. *The unique irreducible reciprocal representation class of $\mathfrak{S}$ in K is the one generated by a simple left ideal of $\mathfrak{S}_\mathsf{K}$.*

If this irreducible representation has degree r, then the degree of any representation is a multiple of r. Conversely, by adjoining irreducible representations, one may construct a representation of degree rs for any given multiple rs of r; this corresponds to forming a representation module that is the direct sum of s simple modules.

We already know one representation of $\mathfrak{S}$ in K, namely that generated by $\mathfrak{S}$ itself as representation module (the principal representation, M.Z. ğ 20); it already lies in P. Its degree is n, and therefore n is divisible by r:

$$n = rt.$$

The quotient t is readily determined. Since r is the rank of a single left ideal over K, while n is the rank of all of $\mathfrak{S}_\mathsf{K}$, t is the number of left ideals of $\mathfrak{S}_\mathsf{K}$; hence t^2 is the rank of $\mathfrak{S}_\mathsf{K}$ over the automorphism division ring of its simple ideals.

We specialize our considerations to the case in which $\mathfrak{S}$ is a commutative field.

Theorem 3. *If $\mathfrak{S}$ is a commutative field, then $\mathfrak{S}$ is the center of $\mathfrak{S}_\mathsf{K}$.*

Proof. Since every element of $\mathfrak{S}$ commutes with every element of $\mathfrak{S}$ and with every element of K, and hence also with every element of $\mathfrak{S}_\mathsf{K}$, $\mathfrak{S}$ belongs to the center of $\mathfrak{S}_\mathsf{K}$. An element of $\mathfrak{S}_\mathsf{K}$ commutes with every element of $\mathfrak{S}_\mathsf{K}$ only if it commutes at least with every element of K, that is, only if its coefficients belong to the center of K, which is P, and hence only if it lies in $\mathfrak{S}$, q.e.d.

For commutative rings there is no distinction between reciprocal and direct isomorphy, so every reciprocal representation may also be regarded as direct. The irreducible representation of $\mathfrak{S}$ in K must therefore also be furnished by a direct representation module. This direct representation module is a simple right ideal of $\mathfrak{S}_\mathsf{K}$. Indeed, $\mathfrak{r}$ is a finite K-right module of rank r, and because $\mathfrak{r}\mathfrak{S} = \mathfrak{S}\mathfrak{r}$, it is also an $\mathfrak{S}$-left module (with the associative law holding throughout, of course); hence it is a direct representation module of rank r. Since there is only one irreducible representation class, it must generate the given representation.

ğ 20. Noncommutative Division Rings

We now let

$$\mathfrak{K} = y_1\mathsf{P} + \cdots + y_m\mathsf{P}$$

denote a noncommutative division ring with center P. We shall develop for $\mathfrak{K}$ a series of theorems analogous to those of the theory of finite algebraic extensions of commutative fields.

If $Z = \xi_1\mathsf{P} + \cdots + \xi_n\mathsf{P}$ denotes a hypercomplex system over P, the two extended systems $\mathfrak{K}_Z$ and $Z_\mathfrak{K}$ are identical. Indeed, we may write

$$\mathfrak{K}_Z = y_1\xi_1\mathsf{P} + \cdots + y_m\xi_n\mathsf{P}$$

for $\mathfrak{K}_Z$, and

$$Z_\mathfrak{K} = \xi_1 y_1\mathsf{P} + \cdots + \xi_n y_m\mathsf{P}$$

for $Z_\mathfrak{K}$; the two expressions are identical because $y_i\xi_j = \xi_j y_i$.

In what follows, Z will always be a commutative field, so the theorems of ğ 19 may be applied. By Theorem 1 of ğ 19, $\mathfrak{K}_Z$ is always two-sided simple.

Theorem 1. *Let Ω be an algebraically closed extension field of P. Then the center of $\mathfrak{K}_\Omega$ is Ω.*

Proof. We invoke the corresponding Theorem 3 of ğ 19. It is clear that Ω lies in the center of $\mathfrak{K}_\Omega$. If α is any element of the center of $\mathfrak{K}_\Omega$, its coefficients belong to a finite algebraic extension field Z of P (namely, the field they generate). Plainly, α must also belong to the center of $\mathfrak{K}_Z$. But that center is Z; hence α belongs to Z, and thus also to Ω, q.e.d.

In a completely similar manner we prove:

Theorem 2. *$\mathfrak{K}_\Omega$ is two-sided simple.*

Proof. Let $\mathfrak{a} = z_1\Omega + \cdots + z_r\Omega$ be a two-sided ideal. The coefficients of $z_1, \ldots, z_r$ belong to a finite extension field Z of P, and $\mathfrak{a}' = z_1 Z + \cdots + z_r Z$ is a two-sided ideal in $\mathfrak{K}_Z$. Since $\mathfrak{K}_Z$ is two-sided simple, $\mathfrak{a}'$ is either zero or equal to $\mathfrak{K}_Z$, and therefore $\mathfrak{a}$ is either zero or equal to $\mathfrak{K}_\Omega$. Thus $\mathfrak{K}_\Omega$ is two-sided simple, q.e.d.

By this theorem, $\mathfrak{K}_\Omega$ is a matrix ring over an extension field of its center Ω. As a subring of all of $\mathfrak{K}_\Omega$, this field must have finite degree over Ω, and hence must be equal to Ω:

Theorem 3. *$\mathfrak{K}_\Omega$ is a matrix ring over Ω,*

$$\mathfrak{K}_\Omega = \sum \Omega c_{ik},$$

and therefore the degree of $\mathfrak{K}$ over its center P is a square, $m = t^2$.

The number t of right (or left) ideals into which $\mathfrak{K}_\Omega$ decomposes will be called, for short, the absolute number of components of $\mathfrak{K}$.

The property of Ω that $\mathfrak{K}_\Omega$ decomposes into t simple ideals is of course already possessed by finite extensions Z of P, for example by fields Z obtained by adjoining to P the coefficients of the c_{ik}. We now investigate these splitting fields.

Definition. A finite algebraic extension field Z of P is called a *splitting field* of $\mathfrak{K}$ if the number of simple right ideals into which $\mathfrak{K}_Z$ decomposes is already equal to the absolute number of components t[1].

Theorem 4. *If Z is a splitting field of $\mathfrak{K}$, then Z is the automorphism division ring of the right ideals of $\mathfrak{K}_Z$. Conversely, if the automorphism division ring of the right ideals of $\mathfrak{K}_Z$ is equal to Z, then Z is a splitting field.*

Proof. 1. Let Z be a splitting field, and let $\mathfrak{T}$ be the automorphism division ring of the right ideals of $\mathfrak{K}_Z$, so that

$$\mathfrak{K}_Z = \sum \mathfrak{T} c_{ik}.$$

It follows that

$$\mathfrak{K}_\Omega = \sum \mathfrak{T}_\Omega c_{ik}.$$

The rank of $\mathfrak{K}_\Omega$ over Ω is therefore the product of t^2 and the rank of $\mathfrak{T}_\Omega$. On the other hand, it is equal to t^2; hence the rank of $\mathfrak{T}_\Omega$, and therefore also that of $\mathfrak{T}$, is equal to 1. Thus $\mathfrak{T} = Z$, q.e.d.

2. If Z is the automorphism division ring of the simple ideals of $\mathfrak{K}_Z$, then

$$\mathfrak{K}_Z = \sum Z c_{ik},$$

and hence

$$\mathfrak{K}_\Omega = \sum \Omega c_{ik}.$$

The number of the c_{ik} must therefore be equal to t^2, q.e.d.

Theorem 5. *The irreducible representation $\mathfrak{Z}$ of a splitting field Z of $\mathfrak{K}$ in $\mathfrak{K}$—by Theorem 2 on page 22 there is only one irreducible representation class—is a maximal commutative subfield of the matrix ring $\mathfrak{K}_r$ (where r is the degree of the irreducible representation of Z).*

Conversely, if the irreducible representation $\mathfrak{Z}$ of a commutative extension field Z of P is a maximal commutative subfield of $\mathfrak{K}_r$, then Z is a splitting field.

Proof. 1. If n is the degree of the splitting field Z over P, then the degree r of the irreducible representation $\mathfrak{Z}$ of Z is equal to n/t (page 22). Let $\mathfrak{Z} \subseteq \mathfrak{Z}^* \subseteq \mathfrak{K}_r$, where $\mathfrak{Z}^*$ is a maximal commutative field of degree $n^* \geq n$ over P. We must prove $\mathfrak{Z}^* = \mathfrak{Z}$. It suffices instead to prove $n^* = n$. If r^* denotes the degree of the irreducible

[1] Compare the notion of splitting field on page 9

representation of an extension field Z^* of Z isomorphic to $\mathfrak{Z}^*$, then again $n^* = r^*t$. On the other hand, r is divisible by r^*, because $\mathfrak{Z}^*$ contains a representation of Z^* of degree r; hence $r^* \leq r$. From

$$n \leq n^* = r^*t \leq rt = n \qquad \text{it follows that} \qquad n^* = n.$$

2. Let the irreducible representation $\mathfrak{Z}$ of degree r of the commutative extension field Z of P in $\mathfrak{K}$ be a maximal commutative subfield of $\mathfrak{K}_r$. Let $\mathfrak{T}$ be the automorphism division ring of the simple ideals of $\mathfrak{K}_Z$, so that

$$\mathfrak{K}_Z = \sum_1^{t'} \mathfrak{T} c_{ik}.$$

The division ring $\mathfrak{T}$ contains Z. We must prove $\mathfrak{T} = Z$. A simple right ideal $\mathfrak{r}$ of $\mathfrak{K}_r$ is not only a representation module of Z in $\mathfrak{K}$, but also a representation module of $\mathfrak{T}$, for

$$\mathfrak{r} = \mathfrak{T} c_{i1} + \cdots + \mathfrak{T} c_{ik};$$

hence $\mathfrak{T}\mathfrak{r} = \mathfrak{r}$, and $\mathfrak{r}$ is a $\mathfrak{T}$-left module and, of course, a $\mathfrak{K}$-right module.

There is therefore a sub-division-ring $\overline{\mathfrak{T}}$ of $\mathfrak{K}_r$, isomorphic to $\mathfrak{T}$, that contains $\mathfrak{Z}$. If $\mathfrak{T}$ differed from Z, and hence $\overline{\mathfrak{T}}$ from $\mathfrak{Z}$, then adjoining to $\mathfrak{Z}$ an element α of $\overline{\mathfrak{T}}$ not belonging to $\mathfrak{Z}$ would yield a proper commutative extension field of $\mathfrak{Z}$ in $\mathfrak{K}_r$, contradicting the maximality of $\mathfrak{Z}$, q.e.d.

Theorem 5 immediately gives:

Theorem 6. *The maximal commutative subfields of $\mathfrak{K}$ have degree t over P and are splitting fields*[1]*.*

We now develop a theorem on the isomorphy of subrings of a $\mathfrak{K}_r$, on which rests the more precise knowledge of the structure of the Galois group of a $\mathfrak{K}$ and related facts.

Theorem 7. *Let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be two-sided simple subrings, containing P, of the matrix ring $\mathfrak{K}_r$ over $\mathfrak{K}$, and suppose there is between them an isomorphism $\mathfrak{S}_1 \cong \mathfrak{S}_2$ that fixes P elementwise. Then this isomorphism is transformation by a regular element τ of $\mathfrak{K}_r$.*

If $\sigma_1 \in \mathfrak{S}_1$ and $\sigma_2 \in \mathfrak{S}_2$ correspond to one another, then

$$\tau^{-1}\sigma_1\tau = \sigma_2.$$

Proof. We construct a ring Σ reciprocally isomorphic to $\mathfrak{S}_1$ and $\mathfrak{S}_2$, and identify its subfield isomorphic to P with P. Then $\mathfrak{S}_1, \mathfrak{S}_2$ are two reciprocal representations of the same degree r of Σ in $\mathfrak{K}$. By Theorem 2 on page 22 there is only one irreducible reciprocal representation class, and hence only one representation class of a given degree, of Σ in $\mathfrak{K}$ (a multiple of the irreducible class). Thus $\mathfrak{S}_1$ and $\mathfrak{S}_2$ must belong to the same class, and consequently are obtained from one another by transformation, q.e.d.

Theorem 7 immediately gives:

Theorem 8. *The group of automorphisms of $\mathfrak{K}$ fixing P elementwise—that is, the Galois group $\mathfrak{G}$ of $\mathfrak{K}$ with respect to its center—is the group of inner automorphisms of $\mathfrak{K}$.*

One need only put $r = 1$ and $\mathfrak{S}_1 = \mathfrak{S}_2 = \mathfrak{K}$ in Theorem 7.

The next two theorems demonstrate the usefulness of the general theory developed thus far in treating special questions.

Theorem 9. *The only noncommutative division ring of finite degree whose center is the field R of real numbers is the quaternion division ring.*

Proof. Let $\mathfrak{K}$ be a noncommutative division ring with center R (of finite rank over R). By Theorem 6, the degree of $\mathfrak{K}$ over R is the square of the degree t of a maximal commutative subfield of $\mathfrak{K}$; since the latter can only be a field isomorphic to the field of complex numbers, $t = 2$, and $\mathfrak{K}$ has degree 4 over R. Let $\mathfrak{Z}_1$ be a maximal commutative subfield of $\mathfrak{K}$; we may then put $\mathfrak{Z}_1 = R(i)$, where $i^2 = -1$. But $\mathfrak{Z}_2 = R(-i)$ is also a field isomorphic to $\mathfrak{Z}_1$—and, as a set, coincident with it—the isomorphism being given by $i \mapsto -i$. By Theorem 7 there is therefore an element $j^* \in \mathfrak{K}$ such that

$$j^{*-1} i j^* = -i.$$

The rank of $\mathfrak{Z}_1(j^*)$ over $\mathfrak{Z}_1$ is at least 2, since j^* cannot belong to $\mathfrak{Z}_1$. Thus $\mathfrak{Z}_1(j^*)$ has rank 4 over R, and so is equal to $\mathfrak{K}$; we may therefore write

[1] The conjecture that every splitting field must then also contain a maximal commutative subfield of $\mathfrak{K}$ is false. There can be splitting fields that do not have this property; the corresponding r is certainly greater than 1. See R. Brauer and E. Noether, "Über minimale Zerfällungskörper irreduzibler Darstellungen," *Sitzungsberichte d. preuss. Akademie der Wisssch.* 1927 XXXII, p. 221.

$$\mathfrak{K} = R + Ri + Rj^* + Rij^*.$$

Since

$$\begin{aligned} j^{*-2}1j^{*2} &= 1, \\ j^{*-2}ij^{*2} &= i, \\ j^{*-2}j^*j^{*2} &= j^*, \\ j^{*-2}ij^*j^{*2} &= ij^*, \end{aligned}$$

the element j^{*2} commutes with all elements of $\mathfrak{K}$, and hence belongs to the center R; thus j^{*2} is a real number r. The number r cannot be positive, for otherwise the polynomial $x^2 - r$ in the commutative field $R(j^*)$ would have the four roots $+\sqrt{r}, -\sqrt{r}, +j^*$, and $-j^*$. Thus $j^{*2} = -m^2,\ m \in R$. Put $j = j^*m^{-1}$; then $j^2 = -1$, and $1, i, j, k = ij$ are the quaternion units, q.e.d.

The proof plainly holds with any real closed field in place of R.

Theorem 10 (Wedderburn's theorem). *Every finite division ring is commutative.*

Proof. Let $\mathfrak{K}$ be a division ring with finitely many elements and let P be its center. Let t^2 be the degree of $\mathfrak{K}$ over P. All maximal commutative subfields of $\mathfrak{K}$ have degree t over P, and hence have the same number of elements. By a familiar theorem from the theory of Galois fields (Moore's theorem), they are therefore isomorphic; and because every Galois field is a Galois extension of its prime field, these isomorphisms can be chosen so that every element of P corresponds to itself. By Theorem 7, all maximal commutative subfields of $\mathfrak{K}$ are therefore obtained from one such field $\mathfrak{Z}$ by transformation. But $\mathfrak{K}$ is the union of all its maximal commutative subfields. (Adjoining an element to P generates a commutative field.) Now consider only the multiplicative group $\mathfrak{K}^*$ of $\mathfrak{K}$ ($\mathfrak{K}$ without zero). We have shown that $\mathfrak{K}^*$ is the union of the subgroups conjugate to the subgroup $\mathfrak{Z}^*$. If $t > 1$, however, this is a contradiction. Indeed, if $\mathfrak{K}^*$ has M elements, $\mathfrak{Z}^*$ has N elements, and L is the index of $\mathfrak{Z}^*$ in $\mathfrak{K}^*$, then $M = NL$, and the number of distinct conjugate subgroups is at most L. Even if this number were equal to L, in order for all the conjugate subgroups together to exhaust the entire group, no two of them could have an element in common. Yet they all have the identity element in common.

ğ 21. The Galois Theory of Noncommutative Division Rings

Let G denote the Galois group of $\mathfrak{K}$ with respect to its center P. By Theorem 8, G is isomorphic to $\overline{G} = \mathfrak{K}^*/\mathsf{P}^*$; we regard this isomorphism as fixed. We call a subgroup H of G closed if the subgroup $\mathfrak{H}^*$ of $\mathfrak{K}^*$ assigned to it by the isomorphism $G \simeq \mathfrak{K}^*/\mathsf{P}^*$ becomes a division ring upon adjoining zero.

Theorem 11. Fundamental theorem of Galois theory. *The closed subgroups H of G and the division rings $\mathfrak{S}$ between P and $\mathfrak{K}$ can be placed in one-to-one correspondence in such a way that, when H and $\mathfrak{S}$ correspond, H is the invariant group of $\mathfrak{S}$ and $\mathfrak{S}$ is the invariant division ring of H.*

Proof. We split our theorem into three partial assertions:

1. The invariant group H of a division ring $\mathfrak{S}$ is closed.
2. If $\mathfrak{S}$ has invariant group H, then $\mathfrak{S}$ is the invariant division ring of H.
3. If H has invariant division ring $\mathfrak{S}$, then H is the invariant group of $\mathfrak{S}$.

1. Under the isomorphism $G \simeq \mathfrak{K}^*/\mathsf{P}^*$, the invariant group H of a division ring $\mathfrak{S}$ corresponds to the set $\mathfrak{H}^*$ of all nonzero elements of $\mathfrak{K}$ that commute elementwise with $\mathfrak{S}$. Together with 0 these plainly form a division ring; that is, H is closed.

2. We reduce the third partial assertion to the second. The division ring $\mathfrak{S}$ is assigned a subgroup S of G, namely the subgroup of G corresponding to $\mathfrak{S}^*/\mathsf{P}^*$. Likewise, the group H corresponds to a sub-division-ring $\mathfrak{H}$ of $\mathfrak{K}$, with $H \simeq \mathfrak{H}^*/\mathsf{P}^*$. If $\mathfrak{S}$ is the invariant division ring of H, then $\mathfrak{S}$ consists of all elements of $\mathfrak{K}$ that commute elementwise with $\mathfrak{H}$; equivalently, S is the invariant group of $\mathfrak{H}$. Correspondingly, if H is the invariant group of $\mathfrak{S}$, then $\mathfrak{H}$ is the invariant division ring of S. Thus the third partial assertion may also be formulated as follows:

3′. If $\mathfrak{H}$ has invariant group S, then $\mathfrak{H}$ is the invariant division ring of S. This is precisely the second partial assertion, which now remains to be proved.

3. Apart from a few minor differences, this proof proceeds as in the commutative case:

Form a division ring K reciprocally isomorphic to $\mathfrak{K}$, and identify its center with P. In place of the automorphisms of $\mathfrak{K}$, we may consider the reciprocal isomorphisms of $\mathfrak{S}$ with sub-division-rings of K.

We shall again prove an auxiliary theorem analogous to the extension theorem used in the commutative case.

Let $\mathfrak{S}$ and $\mathfrak{T}$ be division rings between P and $\mathfrak{K}$,

$$\mathsf{P} \subseteq \mathfrak{S} \subseteq \mathfrak{T} \subseteq \mathfrak{K}.$$

We claim that every reciprocal isomorphism of $\mathfrak{S}$ onto a sub-division-ring of K (a reciprocal representation of degree one of $\mathfrak{S}$ in K) can be extended to reciprocal isomorphisms of $\mathfrak{T}$ in at least as many ways as are given by the degree s of $\mathfrak{T}$ over $\mathfrak{S}$.

The division rings P, $\mathfrak{S}$, $\mathfrak{T}$, and $\mathfrak{K}$ are extended by K:

$$K \subseteq \mathfrak{S}_K \subseteq \mathfrak{T}_K \subseteq \mathfrak{K}_K.$$

By Theorem 1 on page 20, every $\mathfrak{S}_K$ is two-sided simple and completely reducible, and its simple left ideals—which are operator-isomorphic to one another—are representation modules for the unique irreducible representation class of $\mathfrak{S}$ in K. Since this representation class has degree 1—by construction of K, there are in K division rings reciprocally isomorphic to $\mathfrak{S}$—the simple left ideals all have rank 1. Thus $\mathfrak{S}_K$ is a sum of as many left ideals as its degree over P:

$$\mathfrak{S}_K = KE_1 + \cdots + KE_p, \qquad KE_\nu = \mathfrak{S}_K E_\nu.$$

Then

$$\mathfrak{T}_K = \mathfrak{T} \cdot K = \mathfrak{T} \cdot \mathfrak{S}_K,$$
$$\mathfrak{T}_K = \mathfrak{T}\mathfrak{S}_K E_1 + \cdots + \mathfrak{T}\mathfrak{S}_K E_p = \mathfrak{T}_K E_1 + \cdots + \mathfrak{T}_K E_p.$$

Every ideal $\mathfrak{T}_K \cdot E_\nu$ decomposes into s simple ideals, for

$$[\mathfrak{T}_K E_\nu : K] = [\mathfrak{T}_K E_\nu : KE_\nu] = [\mathfrak{T}_K E_\nu : \mathfrak{S}_K E_\nu] \leqq [\mathfrak{T}_K : \mathfrak{S}_K] = [\mathfrak{T} : \mathfrak{S}] = s$$

and

$$\sum [\mathfrak{T}_K E_\nu : K] = sp;$$

hence

$$[\mathfrak{T}_K E_\nu : K] = s, \qquad \mathfrak{T}_K E_\nu = Ke_1^{(\nu)} + \cdots + Ke_s^{(\nu)}.$$

The representation of $\mathfrak{T}$ furnished by $Ke_i^{(\nu)}$ is an extension of the representation of $\mathfrak{S}$ given by KE_ν. Indeed, if $\alpha \in \mathfrak{S}$, then

$$\alpha E_\nu = \sigma E_\nu, \qquad \sum \alpha e_i^{(\nu)} = \sigma \sum e_i^{(\nu)}, \qquad \alpha e_i^{(\nu)} = \sigma e_i^{(\nu)}.$$

It remains only to prove that the representations furnished by the $Ke_i^{(\nu)}$ are all distinct. In the commutative case this was clear because they belonged to different representation classes. Here, on the contrary, they all belong to the same representation class, so we must examine the representations themselves. To this end, consider the K-homomorphic mappings of all of $\mathfrak{T}_K$ furnished by the $Ke_i^{(\nu)}$. These mappings are already completely determined once the representations of $\mathfrak{T}$ are known, because to construct the entire mapping it is enough to know how the basis elements are represented. We may therefore restrict ourselves to showing that the mappings of $\mathfrak{T}_K$ thus furnished by the $Ke_i^{(\nu)}$ are all distinct. If we represent $e_i^{(\nu)}$ once by means of the representation module $Ke_i^{(\nu)}$, and a second time by means of $Ke_j^{(\nu)}$, then, because

$$e_i^{(\nu)2} = e_i^{(\nu)},$$

we obtain 1 the first time, while because

$$e_i^{(\nu)} e_j^{(\nu)} = 0,$$

we obtain 0 the second time as the element representing $e_i^{(\nu)}$. Thus the two representations are indeed distinct. (Exactly the same arguments may also be used in the commutative case, but there they are unnecessary.)

From this point onward we argue exactly as on page 10 and on page 16. Let H be the invariant group of $\mathfrak{S}$, and let $\mathfrak{T}$ be the invariant division ring of H. The elements of H are all the extensions of the identity automorphism of $\mathfrak{S}$ to all of $\mathfrak{K}$. Since, by the auxiliary theorem just proved, among them there are at least s that are distinct on $\mathfrak{T}$, we must have $s = 1$, and $\mathfrak{T} = \mathfrak{S}$, q.e.d.

Chapter V. Factor Systems

ğ 22. The Group of Division Rings with Given Center

We take a fixed commutative field P as the basis of our investigations. The totality of all matrix rings $\mathfrak{K}_r$ whose automorphism division rings $\mathfrak{K}$ are division rings of finite rank over P, with P itself as center, is a multiplicatively closed system with respect to "direct product formation." The direct product of two such rings $\mathfrak{K}_r$ and $\mathfrak{L}_s$ is simply the ring $\mathfrak{K}_r \cdot \mathfrak{L}_s$ obtained from $\mathfrak{K}_r$ by extending the ground field to $\mathfrak{L}_s$:

$$\mathfrak{K}_r \times \mathfrak{L}_s = \mathfrak{K}_r \cdot \mathfrak{L}_s.$$

By the remark on page 22, this direct product formation is commutative:

$$\mathfrak{K}_r \times \mathfrak{L}_s = \mathfrak{L}_s \times \mathfrak{K}_r.$$

The assertion that the system of all $\mathfrak{K}_r$ is multiplicatively closed means nothing more than that $\mathfrak{K}_r \times \mathfrak{L}_s = \mathfrak{K}_r \mathfrak{L}_s$ is always again a matrix ring whose automorphism division ring $\mathfrak{M}$ has center P—finite rank with respect to P being self-evident. By Theorem 1 on page 20, $\mathfrak{K}_r \times \mathfrak{L}_s$ is two-sided simple and completely reducible, and is therefore a matrix ring over an extension division ring $\mathfrak{M}$ of P. That the center of $\mathfrak{M}$ is equal to P follows immediately from the facts that, first, P is certainly contained in the center and, second, the center must be contained in the center P of $\mathfrak{K}$ (or of $\mathfrak{L}$). The multiplication $\mathfrak{K}_r \times \mathfrak{L}_s$ is plainly associative. The $\mathfrak{K}_r$ form a multiplicatively closed system, but not a group: if $\mathfrak{K}_r \times \mathfrak{L}_s = \mathfrak{M}_m$, then certainly $m \geq rs$, so no $\mathfrak{L}_s$ satisfying $\mathfrak{K}_r \times \mathfrak{L}_s = \mathfrak{M}_m$ can be found when $r > m$.

We now combine all $\mathfrak{K}_r$ having the same $\mathfrak{K}$ into a class $\{\mathfrak{K}\}$. Then the following holds: if $\mathfrak{K}_r$ and $\mathfrak{K}_{r'}$ belong to the same class $\{\mathfrak{K}\}$, and $\mathfrak{L}_s$ and $\mathfrak{L}_{s'}$ to the same class $\{\mathfrak{L}\}$, then $\mathfrak{K}_r \times \mathfrak{L}_s$ and $\mathfrak{K}_{r'} \times \mathfrak{L}_{s'}$ likewise belong to the same class. It is enough to show that $\mathfrak{K}_r \times \mathfrak{L}_s$ belongs to the same class as $\mathfrak{K} \times \mathfrak{L}$, that is, that if $\mathfrak{K} \times \mathfrak{L} = \mathfrak{M}_m$, then $\mathfrak{K}_r \times \mathfrak{L}_s$ is also a matrix ring over $\mathfrak{M}$. This is easy to see. We have

$$\mathfrak{K}_r \times \mathfrak{L} = \left(\sum_1^r \mathfrak{K} c_{ik} \right) \mathfrak{L} = \sum_1^r \mathfrak{K}_{\mathfrak{L}} c_{ik} = \sum_1^r \mathfrak{M}_m c_{ik}.$$

This is a matrix ring of degree r over $\mathfrak{M}_m$, and hence, of course, a matrix ring of degree mr over $\mathfrak{M}$. Continuing in exactly the same way, we obtain

$$\mathfrak{K}_r \times \mathfrak{L}_s = \left(\sum_1^s \mathfrak{L} d_{ik} \right)_{\mathfrak{K}_r} = \sum_1^s \mathfrak{L}_{\mathfrak{K}_r} d_{ik} = \sum_1^s \mathfrak{M}_{mr} d_{ik} = \mathfrak{M}_{mrs},$$

which proves our assertion. We record that $\mathfrak{L} \times \mathfrak{K} = \mathfrak{M}_m$ implies $\mathfrak{K}_r \times \mathfrak{L}_s = \mathfrak{M}_{mrs}$.

It follows from what has been proved that, if the product of two classes $\{\mathfrak{K}\}$ and $\{\mathfrak{L}\}$ is defined as the class of the product of a representative of $\{\mathfrak{K}\}$ with a representative of $\{\mathfrak{L}\}$, this definition is independent of the choice of representatives.

Thus the mapping $\mathfrak{K}_r \mapsto \{\mathfrak{K}\}$ is a homomorphism of the system of all $\mathfrak{K}_r$ onto the set of all classes $\{\mathfrak{K}\}$; consequently, the set $\mathscr{K}$ of the classes $\{\mathfrak{K}\}$ is a multiplicatively closed system. We prove that $\mathscr{K}$ is a group. As is immediately seen, the identity element is the class $\{\mathsf{P}\}$, since $\mathfrak{K}_r \times \mathsf{P} = \mathfrak{K}_r$.

It therefore remains only to prove, for each class $\{\mathfrak{K}\}$, the existence of a class $\{\mathfrak{K}\}^{-1}$. We find that we must put $\{\mathfrak{K}\}^{-1} = \{\overline{\mathfrak{K}}\}$, where $\{\overline{\mathfrak{K}}\}$ denotes the division ring reciprocally isomorphic to $\mathfrak{K}$. In other words, $\mathfrak{K} \times \overline{\mathfrak{K}}$ must be a matrix ring over P; or, if $\mathfrak{K}$ has rank t^2, and hence $\mathfrak{K} \times \overline{\mathfrak{K}}$ has rank t^4 over P, then $\mathfrak{K} \times \overline{\mathfrak{K}}$ must decompose into t^2 simple left ideals. This follows because a simple left ideal of $\mathfrak{K} \times \overline{\mathfrak{K}}$, as the representation module of an irreducible reciprocal representation of $\overline{\mathfrak{K}}$ in $\mathfrak{K}$—which has degree 1—has rank 1 over $\mathfrak{K}$, and hence rank t^2 over P.

We shall call $\mathfrak{K}$ a *simple division ring* if there is no division ring between P and $\mathfrak{K}$ whose center is also P.

Theorem. *Every division ring $\mathfrak{K}$ is the direct product of simple sub-division-rings $\mathfrak{K}^{(i)}$,*

$$\mathfrak{K} = \mathfrak{K}^{(1)} \times \cdots \times \mathfrak{K}^{(p)}.$$

Proof. It suffices to show that, if $\mathfrak{K}^{(1)}$ is a sub-division-ring of $\mathfrak{K}$ with center P, there is a sub-division-ring $\mathfrak{S}$ of $\mathfrak{K}$, with center P, satisfying the equation

$$\mathfrak{K}^{(1)} \times \mathfrak{S} = \mathfrak{K}.$$

In any event, there exists a class $\{\mathfrak{S}\}$ with the property

$$\{\mathfrak{K}^{(1)}\} \times \{\mathfrak{S}\} = \{\mathfrak{K}\},$$

namely

$$\{\mathfrak{S}\} = \{\overline{\mathfrak{K}^{(1)}}\} \times \{\mathfrak{K}\}. \qquad \text{Let} \qquad \overline{\mathfrak{K}^{(1)}} \times \mathfrak{K} = \mathfrak{S}_\lambda.$$

Then

$$\mathfrak{K}^{(1)} \times \mathfrak{S}_\lambda = \mathfrak{K}^{(1)} \times \overline{\mathfrak{K}^{(1)}} \times \mathfrak{K} = \mathsf{P}_{t^2} \times \mathfrak{K} = \mathfrak{K}_{t^2}, \qquad t^2 = \text{rank of } \mathfrak{K}^{(1)}.$$

But $\mathfrak{K}^{(1)} \times \mathfrak{S}_\lambda$ is a matrix ring of a degree at least λ, and so $\lambda \leq t^2$. The ring $\mathfrak{S}_\lambda = \overline{\mathfrak{K}^{(1)}} \times \mathfrak{K}$ must decompose into simple ideals of rank 1 over $\mathfrak{K}$, because $\overline{\mathfrak{K}^{(1)}}$ admits reciprocal representations of degree one in $\mathfrak{K}$; hence $\lambda \geq t^2$, and $\lambda = t^2$:

$$\mathfrak{K}_{t^2} = \mathfrak{K}^{(1)} \times \mathfrak{S}_{t^2}.$$

Thus $\mathfrak{K}^{(1)} \times \mathfrak{S}$ itself must be a division ring, and

$$\mathfrak{K}^{(1)} \times \mathfrak{S}_{t^2} = \big(\mathfrak{K}^{(1)} \times \mathfrak{S}\big)_{t^2} = \mathfrak{K}_{t^2}.$$

The division ring $\mathfrak{K}^{(1)} \times \mathfrak{S}$ is the automorphism division ring of the simple left ideals in one decomposition of $\mathfrak{K}_{t^2}$, while $\mathfrak{K}$ is the automorphism division ring of the simple left ideals in another decomposition of $\mathfrak{K}_{t^2}$. Since any two different left ideals of $\mathfrak{K}_{t^2}$ can be included in one decomposition, $\mathfrak{K}$ and $\mathfrak{K}^{(1)} \times \mathfrak{S}$ are isomorphic, and this isomorphism may be chosen to fix P elementwise. By Theorem 7 on page 25, this isomorphism is therefore generated by an inner automorphism of $\mathfrak{K}_{t^2}$:

$$\mathfrak{K} = \lambda^{-1}\big(\mathfrak{K}^{(1)} \times \mathfrak{S}\big)\lambda = \lambda^{-1}\mathfrak{K}^{(1)}\lambda \times \lambda^{-1}\mathfrak{S}\lambda, \qquad \lambda \in \mathfrak{K}_{t^2}.$$

The division ring $\lambda^{-1}\mathfrak{K}^{(1)}\lambda$ is a sub-division-ring of $\mathfrak{K}$ isomorphic to $\mathfrak{K}^{(1)}$; hence, by Theorem 7 on page 25, with a suitable μ from $\mathfrak{K}$,

$$\mu^{-1}\lambda^{-1}\mathfrak{K}^{(1)}\lambda\mu = \mathfrak{K}^{(1)},$$

and therefore

$$\mu^{-1}\mathfrak{K}\mu = \mathfrak{K} = \mathfrak{K}^{(1)} \times \mu^{-1}\lambda^{-1}\mathfrak{S}\lambda\mu,$$

which proves the assertion.

ğ 23. Factor Systems

In the following investigations the ground field P is assumed to be perfect. In place of this one may make the more general assumption that only those noncommutative division rings $\mathfrak{K}$ with center P are considered which have the property that every $\mathfrak{K}_r$ contains a maximal commutative subfield of the first kind over P. (As Köthe has since shown, this holds for every $\mathfrak{K}$.)

Let Z be a splitting field of the noncommutative division ring $\mathfrak{K}$ with center P. Let the irreducible representation $\mathfrak{Z}$ of Z in $\mathfrak{K}$ have degree r; it is then a maximal commutative subfield of $\mathfrak{K}_r$. Let Γ be the Galois field of Z, so that

$$\mathfrak{Z}_\Gamma = e_1\Gamma + \cdots + e_n\Gamma \qquad \text{(page 9)}.$$

Here n is the degree of Z over P. The ring $\mathfrak{K}_r$, when extended by Γ, then likewise has a decomposition

$$\mathfrak{K}_{r\Gamma} = \mathfrak{K}_{r\Gamma}e_1 + \cdots + \mathfrak{K}_{r\Gamma}e_n,$$

$$\mathfrak{K}_{r\Gamma} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n, \qquad \mathfrak{l}_i = \mathfrak{K}_{r\Gamma}e_i.$$

The $\mathfrak{l}_i$ are plainly left ideals. They are in fact simple left ideals, because, since Z is a splitting field, $\mathfrak{K}_{r\Gamma}$ is a matrix ring of degree $r \cdot t = n$ over Γ. (Theorem 4, page 23; $n = rt$ on page 22.) The decomposition of $\mathfrak{K}_{r\Gamma}$ into simple left ideals thus obtained is especially well adapted to the algebraic properties of $\mathfrak{K}$ and Z. Indeed, define, as on page 18, the action of a substitution S of the Galois group $\mathfrak{G}$ of Γ/P on all elements of $\mathfrak{K}_{r\Gamma}$ by putting, for every element z of $\mathfrak{K}_r$,

$$S(z) = z.$$

Then the ideals $\mathfrak{l}_i$ are conjugate; that is, applying an S to an $\mathfrak{l}_j$ gives another one,

$$S(\mathfrak{l}_j) = \mathfrak{l}_i,$$

because every indecomposable component e_j of the identity must pass into another e_i. (See also page 11.)

The representation module $e_i\Gamma$ maps $\mathfrak{Z}$ onto a subfield Z_i of Γ. The element e_i already lies in $\mathfrak{Z}_{Z_i}$, because the representation Z_i of $\mathfrak{Z}$ is already contained in Z_i, and thus $\mathfrak{Z}_{Z_i}$ must split off the representation module e_iZ_i. Let $\{Z_i, Z_k\}$ be the compositum of Z_i and Z_k. The ring $\mathfrak{K}_{r\{Z_i,Z_k\}}$ splits off the two left ideals

$$\bar{\mathfrak{l}}_i = \mathfrak{K}_{r\{Z_i,Z_k\}}e_i, \qquad \bar{\mathfrak{l}}_k = \mathfrak{K}_{r\{Z_i,Z_k\}}e_k,$$

which are simple because $\mathfrak{l}_i = \mathfrak{K}_{r\Gamma}\bar{\mathfrak{l}}_i$. Thus

$$\bar{\mathfrak{l}}_i = \sum_{\lambda=1}^{m}\{Z_i, Z_k\}c_{\lambda i}^{(ik)}, \qquad \bar{\mathfrak{l}}_k = \sum_{\lambda}\{Z_i, Z_k\}c_{\lambda k}^{(ik)}.$$

The $c_{\lambda\rho}^{(ik)}$ form a system of matrix units of $\mathfrak{K}_{r\{Z_i,Z_k\}}$.

Every isomorphism $a_i \mapsto a_k$ of $\bar{\mathfrak{l}}_i$ onto $\bar{\mathfrak{l}}_k$, with $\mathfrak{K}_{r\{Z_i,Z_k\}}$ as operator domain, is characterized by the element p_{ik} with $e_i \mapsto p_{ik}$, because then $a_i = a_ie_i \mapsto a_ip_{ik}$, and hence $\bar{\mathfrak{l}}_i \cdot p_{ik} = \bar{\mathfrak{l}}_k$. All possible such p_{ik} are plainly

$$p_{ik} = c_{ik}^{(ik)}\gamma_{ik}, \qquad \gamma_{ik} \neq 0 \quad \text{from} \quad \{Z_i, Z_k\}.$$

The mapping $a_i \mapsto a_ip_{ik}$ then also gives an operator isomorphism of $\mathfrak{l}_i$ onto $\mathfrak{l}_k$. We now select particular systems of such p_{ik} by imposing a conjugacy condition on them.

Define the action of an S on an index i by

$$S(i) = k, \qquad \text{if} \qquad S(Z_i) = Z_k.$$

For every pair of indices (ν, μ) there is at least one conjugate pair $S(\nu, \mu)$ of the form $S(\nu, \mu) = (1, k)$. From each class of conjugate index pairs choose a fixed pair $(1, k)$, and for this $(1, k)$ put

$$p_{1k} = c_{1k}^{(1k)}\gamma_{1k}, \qquad \gamma_{1k} \neq 0 \quad \text{from} \quad \{Z_1, Z_k\},$$

otherwise arbitrarily; then, if $S(1, k) = (\nu, \mu)$, put

$$p_{\nu\mu} = S(p_{1k}).$$

The element $p_{\nu\mu}$ then actually has the form

$$p_{\nu\mu} = c_{\nu\mu}^{(\nu\mu)}\gamma_{\nu\mu}, \qquad \gamma_{\nu\mu} \neq 0 \quad \text{from} \quad \{Z_\nu, Z_\mu\}.$$

Indeed, applying S to the isomorphism

$$a_1 \mapsto a_1p_{1k}, \qquad \text{in particular} \qquad e_1 \mapsto p_{1k} \quad \text{from } \bar{\mathfrak{l}}_1 \text{ onto } \bar{\mathfrak{l}}_k$$

gives an isomorphism

$$a_\nu \mapsto a_\nu p_{\nu\mu}, \qquad \text{in particular} \qquad e_\nu \mapsto p_{\nu\mu} \quad \text{from } \bar{\mathfrak{l}}_\nu \text{ onto } \bar{\mathfrak{l}}_\mu.$$

If $c_{\lambda\rho}$ denotes a system of matrix units of $\mathfrak{K}_{r\Gamma}$, it is clear that $p_{\nu\mu}$ may also be written in the form

$$p_{\nu\mu} = c_{\nu\mu}\bar{\gamma}_{\nu\mu}.$$

The relations

$$c_{ij}c_{1k} = 0, \quad \text{if} \quad j \neq 1, \qquad c_{ij}c_{jk} = c_{ik}$$

therefore imply the relations

$$\begin{aligned} &p_{ij}p_{1k} = 0, && \text{if } j \neq 1, \\ &p_{ij}p_{jk} = \alpha_{ik}^{(j)}p_{ik}, && \alpha_{ik}^{(j)} \text{ from } \Gamma \text{ (more precisely from } \{Z_i, Z_j, Z_k\}). \end{aligned}$$

The n^3 quantities α form the *factor system of* $\mathfrak{K}$ *relative to* Z belonging to the system p_{ik} of "pseudo-matrix units."

The α are conjugate: $S(i,k,j) = (\nu,\mu,\tau)$ implies

$$S(\alpha_{ik}^{(j)}) = \alpha_{\nu\mu}^{\tau}.$$

Every system p_{ik}^* of pseudo-matrix units is obtained from a system p_{ik} by multiplying the initial p_{ik} by arbitrary $\delta_{ik} \neq 0$ from $\{Z_i, Z_k\}$:

$$p_{1k}^* = p_{1k}\delta_{1k},$$

and then again, if $S(1,k) = (\nu,\mu)$, by putting

$$p_{\nu\mu}^* = S(p_{1k}^*).$$

Thus

$$p_{\nu\mu}^* = p_{\nu\mu}\delta_{\nu\mu},$$

where $\delta_{\nu\mu}$ is from $\{Z_\nu, Z_\mu\}$. The $\delta_{\nu\mu}$ are conjugate: $S(i,k) = (\nu,\mu)$ implies $S(\delta_{ik}) = \delta_{\nu\mu}$. If α^* is the factor system belonging to p_{ik}^*, then

$$\alpha_{ik}^{(j)*} = \frac{\delta_{ij}\delta_{jk}}{\delta_{ik}}\alpha_{ik}^{(j)}.$$

The factor systems α^* and α are called associated (as are p_{ik}^* and p_{ik}); all factor systems of $\mathfrak{K}$ relative to Z form a class $\{\alpha\}$ of associated factor systems.

The class $\{\alpha\}$ does not depend on which representation $\mathfrak{Z}$ of Z in $\mathfrak{K}_r$ is used as the basis of its definition. Indeed, the passage from one $\mathfrak{Z}$ to another may be effected by transformation with an element λ from $\mathfrak{K}_r$, which is therefore $\mathfrak{G}$-invariant. Thus a system p_{ik} belonging to $\mathfrak{Z}$ gives rise to a system

$$p'_{ik} = \lambda^{-1}p_{ik}\lambda$$

belonging to $\mathfrak{Z}'$; but the factor systems of p_{ik} and p'_{ik} are identical.

A factor system is nothing more than a multiplication table of $\mathfrak{K}_{n\Gamma}$, but one adapted to the special algebraic properties of $\mathfrak{K}$.

ğ 24. Multiplication of Factor Systems

Instead of speaking of a splitting field of a noncommutative division ring $\mathfrak{K}$, we also speak of a splitting field of $\{\mathfrak{K}\}$. This is meaningful because, together with $\mathfrak{K}_Z$, every ring $\mathfrak{K}_{rZ}$ decomposes into absolutely irreducible components, and conversely.

Any two division rings $\mathfrak{K}$, $\mathfrak{S}$ with center P have common splitting fields; for example, the compositum of a splitting field of $\mathfrak{K}$ and a splitting field of $\mathfrak{S}$.

Theorem 1. *The $\{\mathfrak{K}\}$ that have a field Z as splitting field form a subgroup $\mathscr{K}_Z$ of the group $\mathscr{K}$ of all $\{\mathfrak{K}\}$.*

Proof. If $\mathfrak{K}$ and $\mathfrak{S}$ have Z as splitting field, then $\mathfrak{K}_Z$ and $\mathfrak{S}_Z$, and hence also $(\mathfrak{K}\times\mathfrak{S})_Z$, decompose into absolutely irreducible components; that is, Z is a splitting field of $\{\mathfrak{K}\times\mathfrak{S}\}$ (Theorem 4, page 23).

Reciprocally isomorphic division rings have all their splitting fields in common.

An auxiliary consideration. Let

$$\mathfrak{K}_r = \mathfrak{L}_1 + \cdots + \mathfrak{L}_r, \qquad \mathsf{P}_m = \mathfrak{z}_1 + \cdots + \mathfrak{z}_m$$

be decompositions of $\mathfrak{K}_r$, P_m into simple left ideals. Then

$$\mathfrak{K}_{rm} = \mathfrak{K}_r \times \mathsf{P}_m = \mathfrak{L}_1\mathfrak{z}_1 + \cdots + \mathfrak{L}_i\mathfrak{z}_j + \cdots + \mathfrak{L}_r\mathfrak{z}_m$$

is a decomposition of $\mathfrak{K}_{rm}$ into rm nonzero, and hence simple, left ideals. Consequently every r-component left ideal A of $\mathfrak{K}_{rm}$ is connected by an inner automorphism of $\mathfrak{K}_r$ with the r-component left ideal

$$\mathfrak{L}_1\mathfrak{z}_1 + \cdots + \mathfrak{L}_r\mathfrak{z}_1 = \mathfrak{K}_r\mathfrak{z}_1 :$$

$$A = \tau^{-1}\mathfrak{K}_r\tau\cdot\tau^{-1}\mathfrak{z}_1\tau = \mathfrak{K}'_r\cdot\mathfrak{z}'_1.$$

Let $\mathfrak{K}_{r\Gamma} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n$ be a decomposition of $\mathfrak{K}_{r\Gamma}$ into conjugate left ideals belonging to a $\mathfrak{Z}$ in $\mathfrak{K}_r$, with $\mathfrak{l}_i = \mathfrak{K}_r e_i$. Since

$$S(\tau^{-1}\mathfrak{l}_i\tau\cdot\mathfrak{z}'_1) = S(\tau^{-1}\mathfrak{l}_i\tau)\,\mathfrak{z}'_1 = \tau^{-1}(S\mathfrak{l}_i)\tau\cdot\mathfrak{z}'_1 = \tau^{-1}\mathfrak{l}_k\tau\cdot\mathfrak{z}'_1,$$

we have in

$$A_\Gamma = \mathfrak{l}'_1\mathfrak{z}'_1 + \cdots + \mathfrak{l}'_n\mathfrak{z}'_1 \tag{1}$$

a decomposition of A_Γ into conjugate left ideals. Here

$$\mathfrak{l}'_i\mathfrak{z}'_1 = \mathfrak{K}_{rm\Gamma} \cdot e'_i E',$$

where $\tau^{-1}e_i\tau = e'_i$, and E' denotes the identity of $\mathfrak{z}'_1$.

Every other decomposition

$$A_\Gamma = \mathfrak{q}_1 + \cdots + \mathfrak{q}_n, \qquad S\mathfrak{q}_i = \mathfrak{q}_k \quad \text{if} \quad S\mathfrak{l}'_i\mathfrak{z}'_1 = \mathfrak{l}'_k\mathfrak{z}'_1 \tag{2}$$

into conjugate left ideals is obtained from (1) by transformation with an element λ of $\mathfrak{K}_{rm}$:

$$\mathfrak{q}_i = \lambda^{-1}\mathfrak{l}'_i\mathfrak{z}'_1\lambda, \qquad \text{hence, if } e_i^* \text{ is the identity of } \mathfrak{q}_i, \quad e_i^* = \lambda^{-1}e'_iE'\lambda.$$

The proof is an immediate consequence of the following auxiliary theorem.

Auxiliary theorem. *Let A be a left ideal of $\mathfrak{K}_n$, and let*

$$A = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n = \mathfrak{K}_{n\Gamma}e_1 + \cdots + \mathfrak{K}_{n\Gamma}e_n$$

be a decomposition—assumed to exist—into conjugate left ideals; without loss of generality, the $\mathfrak{l}_i$ may here be assumed conjugate.

Let $\mathfrak{z}$ be operator-isomorphic to A, and suppose the same assumptions hold:

$$\mathfrak{z} = \mathfrak{q}_1 + \cdots + \mathfrak{q}_n = \mathfrak{K}_{n\Gamma}e_1^* + \cdots + \mathfrak{K}_{n\Gamma}e_n^*$$

(thus the $\mathfrak{q}_i$, and the e_i^*, are conjugate). Then there is a regular element λ of $\mathfrak{K}_n$ such that $\mathfrak{q}_i = \lambda^{-1}\mathfrak{l}_i\lambda$.

Proof. 1. That the e_i may be assumed conjugate follows as follows. If e_1 is any generating idempotent of $\mathfrak{l}_1$, so that $\mathfrak{l}_1 = \mathfrak{K}_{n\Gamma}e_1$, then applying an automorphism of Γ gives $\mathfrak{l}_i = \mathfrak{K}_{n\Gamma}e_i$, where e_i is conjugate to e_1 and is again a generating idempotent.

2. Every $\mathfrak{l}$ is isomorphic to every $\mathfrak{q}$: the $\mathfrak{l}$, being conjugate, all have the same (absolute) length; the numbers of the $\mathfrak{l}$ and the $\mathfrak{q}$ agree; and $\mathfrak{z}$ and A are assumed isomorphic.

3. Let an isomorphism between $\mathfrak{l}_1$ and $\mathfrak{q}_1$, and its inverse, be fixed by the assignments

$$e_1 \mapsto s_1 = e_1s_1; \qquad e_1^* \mapsto t_1 = e_1^*t_1; \qquad s_1t_1 = e_1; \qquad t_1s_1 = e_1^*. \tag{3}$$

Applying all automorphisms transforms (3) into

$$e_i \mapsto s_i = e_is_i; \qquad e_i^* \mapsto t_i = e_i^*t_i; \qquad s_it_i = e_i; \qquad t_is_i = e_i^*,$$

thereby fixing the isomorphisms $\mathfrak{q}_i = \mathfrak{l}_is_i$ and $\mathfrak{l}_i = \mathfrak{q}_it_i$.

4. Put

$$s = s_1 + \cdots + s_n; \qquad t = t_1 + \cdots + t_n.$$

Then

$$\mathfrak{q}_i = \mathfrak{l}_is; \qquad \mathfrak{l}_i = \mathfrak{q}_it; \qquad st = e_1 + \cdots + e_n = \xi; \qquad ts = e_1^* + \cdots + e_n^* = \xi^*.$$

Here ξ and ξ^* lie in $\mathfrak{K}_n$, and

$$A\xi = A, \qquad \mathfrak{z}\xi^* = \mathfrak{z} \quad (\text{because } \mathfrak{l}_i\xi = \mathfrak{l}_i\mathfrak{l}_i = \mathfrak{l}_i),$$

$$\xi^2 = \xi, \qquad \xi^{*2} = \xi^*.$$

Now put $e = \overline{E} + E = \overline{E}^* + E^*$, and accordingly

$$\mathfrak{K}_n = \overline{A} + A = \mathfrak{K}_n\overline{\xi} + \mathfrak{K}_n\xi = \overline{\mathfrak{z}} + \mathfrak{z} = \mathfrak{K}_n\overline{\xi}^* + \mathfrak{K}_n\xi^*.$$

Then $\overline{A}$ and $\overline{\mathfrak{z}}$ are also isomorphic. Let

$$\overline{E} \mapsto \overline{s} = \overline{E}\,\overline{s} \qquad \text{and} \qquad \overline{E}^* \mapsto \overline{t} = \overline{E}^*\overline{t}$$

be reciprocal isomorphisms, and put

$$\lambda = s + \bar{s}, \qquad \mu = t + \bar{t}.$$

Then

$$\lambda\mu = \mu\lambda = e, \qquad \mathfrak{l}_i\lambda = \mathfrak{q}_i, \qquad \lambda^{-1}\mathfrak{q}_i = \mathfrak{q}_i \quad (\lambda^{-1}\mathfrak{q}_i \subseteq \mathfrak{q}_i = \lambda\cdot\lambda^{-1}\mathfrak{q}_i \subseteq \lambda^{-1}\mathfrak{q}_i),$$

and hence

$$\lambda^{-1}\mathfrak{l}_i\lambda = \mathfrak{q}_i, \qquad \text{q.e.d.}$$

For the decomposition (1), elements

$$r_{ik} = c_{ik}^{\prime(ik)}\gamma_{ik}, \qquad \gamma_{ik} \in \{Z_i, Z_k\},$$

may again be determined which, by $e_i'E' \mapsto r_{ik}$, furnish operator isomorphisms between the ideals $\mathfrak{l}_i'\mathfrak{z}_1'$ and $\mathfrak{l}_k'\mathfrak{z}_1'$, and which also satisfy the conjugacy condition $S(r_{ik}) = r_{\nu\mu}$ if $S(i,k) = (\nu,\mu)$. By

$$r_{ij}r_{jk} = \alpha_{ik}^{(j)}r_{ik}$$

they determine a factor system α of A_Γ. It is important that the arbitrary decomposition (2) can be used just as well to determine the factor systems of A_Γ. Indeed, if a system r_{ik} belonging to (1) is replaced by $r_{ik}' = \lambda^{-1}r_{ik}\lambda$, then $e_i^* \mapsto r_{ik}'$ gives an operator isomorphism of $\mathfrak{q}_i$ onto $\mathfrak{q}_k$; the r_{ik}' satisfy the conjugacy condition because λ is $\mathfrak{q}$-invariant; and the r_{ik}' have the same factor system as the r_{ik}.

If one takes a system of pseudo-matrix units p_{ik} of $\mathfrak{K}$, then

$$r_{ik} = \tau^{-1}p_{ik}\tau\cdot E'$$

is an r_{ik}-system of A_Γ with the same factor system. We have therefore proved the auxiliary theorem:

Theorem. *The factor systems of A_Γ formed with the aid of any decomposition*

$$A_\Gamma = \mathfrak{q}_1 + \cdots + \mathfrak{q}_n$$

of A_Γ into conjugate left ideals are the same as those of $\mathfrak{K}_r$.

The following theorem shows that if $\alpha_{ik}^{(j)}$, $\beta_{ik}^{(j)}$ are factor systems of $\{\mathfrak{K}\}$, $\{\mathfrak{S}\}$, respectively, relative to Z, then $\varepsilon_{ik}^{(j)} = \alpha_{ik}^{(j)}\cdot\beta_{ik}^{(j)}$ is a factor system of $\{\mathfrak{K}\times\mathfrak{S}\}$ relative to Z. It is therefore meaningful to define the product $\{\alpha\}\times\{\beta\}$ of two classes $\{\alpha\}$, $\{\beta\}$ of associated factor systems as the class $\{\alpha_{ik}^{(j)}\beta_{ik}^{(j)}\}$.

Theorem 2. *Let $\{\mathfrak{K}\}$, relative to Z, have the class $\{\alpha\}$ of associated factor systems. The $\{\alpha\}$ of all $\{\mathfrak{K}\}$ having splitting field Z form a group which is mapped isomorphically onto $\mathscr{K}_Z$ by $\{\mathfrak{K}\}\mapsto\{\alpha\}$.*

Two things must be shown in the proof:

1. If $\{\mathfrak{K}\}$ has factor system $\alpha_{ik}^{(j)}$, and $\{\mathfrak{S}\}$ has factor system $\beta_{ik}^{(j)}$, then $\varepsilon_{ik}^{(j)} = \alpha_{ik}^{(j)}\beta_{ik}^{(j)}$ is a factor system of $\{\mathfrak{K}\times\mathfrak{S}\}$.

2. If $\{\mathfrak{K}\}$ has factor system $\alpha_{ik}^{(j)} = 1$, then $\mathfrak{K} = \mathsf{P}$.

1. Let the degrees of the irreducible representations of Z in $\mathfrak{K}$, $\mathfrak{S}$ be r, s, and let

$$\mathfrak{K}_{r\Gamma} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n, \qquad \mathfrak{S}_{s\Gamma} = \mathfrak{m}_1 + \cdots + \mathfrak{m}_n$$

be decompositions into conjugate ideals, where $\mathfrak{l}_i$ and $\mathfrak{m}_i$ are to be corresponding ideals (derived from corresponding components of $\mathfrak{Z}_r$ and $\mathfrak{Z}_r'$, respectively). Then

$$(\mathfrak{K}_r\times\mathfrak{S}_s)_\Gamma = \mathfrak{l}_1\mathfrak{m}_1 + \cdots + \mathfrak{l}_i\mathfrak{m}_j + \cdots + \mathfrak{l}_n\mathfrak{m}_n$$

is a decomposition into n^2 nonzero, and hence simple, ideals. Thus

$$A_1 = \mathfrak{l}_1\mathfrak{m}_1 + \mathfrak{l}_2\mathfrak{m}_2 + \cdots + \mathfrak{l}_n\mathfrak{m}_n$$

is an ideal of absolute length n. The ideal A_1 is invariant under every S, because the $\mathfrak{m}_i$ transform in the same way as the $\mathfrak{l}_i$; hence there is a $\mathfrak{K}_r\times\mathfrak{S}_s$-ideal A with

$$A_1 = A_\Gamma$$

(auxiliary theorem, page 18).

If u is the degree of the irreducible representation of $\mathfrak{Z}$ in the automorphism division ring $\mathfrak{M}$ of the simple ideals of $\mathfrak{K} \times \mathfrak{S}$, then A decomposes into u simple ideals (because its absolute length is n). Our auxiliary theorem therefore shows that the factor systems of A are also those of $\mathfrak{M}$.

A decomposition of A_Γ into conjugate ideals is, however, the one used for the definition:

$$A_\Gamma = \mathfrak{l}_1\mathfrak{m}_1 + \mathfrak{l}_2\mathfrak{m}_2 + \cdots + \mathfrak{l}_n\mathfrak{m}_n. \tag{3}$$

If $\alpha_{ik}^{(j)}$, $\beta_{ik}^{(j)}$ belong to the pseudo-matrix units p_{ik}, q_{ik} of $\mathfrak{K}$, $\mathfrak{S}$, then plainly $r_{ik} = p_{ik}q_{ik}$ is a system of pseudo-matrix units of A_Γ for the decomposition (3). The corresponding factor system $\varepsilon_{ik}^{(j)} = \alpha_{ik}^{(j)}\beta_{ik}^{(j)}$ is then also one of $\mathfrak{M}$.

2. Let $\{\mathfrak{K}\}$ have the factor system $\alpha_{ik}^{(j)} = 1$, with p_{ik} as the corresponding pseudo-matrix units and with the decomposition

$$\mathfrak{K}_{r\Gamma} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n$$

into conjugate ideals. We must prove $\mathfrak{K} = \mathsf{P}$, or $\mathfrak{K}_r = \mathsf{P}_r$, or the existence of an n-component left ideal $\mathfrak{l}$ of $\mathfrak{K}_r$—because a simple $\mathfrak{K}_r$-left ideal has rank t^2r, and hence $n = t^2rh$ with integral h, or else $t = 1$.

The $\mathfrak{K}_{r\Gamma}$-ideal

$$\Omega = \mathfrak{l}_1(p_{11} + \cdots + p_{1n})$$

is nonzero—$e_1 \sum_i p_{1i} \neq 0$—and simple, and therefore has rank n. The ideal Ω is $\mathfrak{G}$-invariant:

$$S\Omega = \mathfrak{l}_i \sum_\nu Sp_{1\nu} = \mathfrak{l}_i \sum_\mu p_{i\mu} = \mathfrak{l}_i \sum_\mu p_{i1}p_{1\mu},$$

because $\alpha_{ik}^{(j)} = 1$. Hence

$$S\Omega = \mathfrak{l}_i p_{i1} \sum_\mu p_{1\mu} = \mathfrak{l}_1 \sum_\mu p_{1\mu} = \Omega.$$

Consequently $\Omega = \mathfrak{l}_\Gamma$, where $\mathfrak{l}$ denotes a $\mathfrak{K}_r$-ideal of rank n.

Theorem 3. *Every element $\{\mathfrak{K}\}$ of the group $\mathscr{K}$ has finite order λ, which divides the absolute number of components t of $\mathfrak{K}$.*

First proof (Brauer). Take two decompositions of $\mathfrak{K}_{r\Gamma}$ into conjugate left ideals,

$$\mathfrak{K}_{r\Gamma} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n = \mathfrak{z}_1 + \cdots + \mathfrak{z}_n, \qquad \mathfrak{l}_i = \mathfrak{K}_{r\Gamma}e_i, \quad \mathfrak{z}_i = \mathfrak{K}_{r\Gamma}e_i^*.$$

Let an operator isomorphism of $\mathfrak{l}_i$ onto $\mathfrak{z}_k$ be given by $a_i \mapsto a_i r_{ik}$, and in particular by $e_i \mapsto r_{ik}$. Under its inverse, e_k^* passes into an s_{ki} from $\mathfrak{l}_i$, with $s_{ki} \cdot r_{ik} = e_k^*$. If we choose the r_{ik} conjugate,

$$S(r_{ik}) = r_{\nu\mu} \quad \text{if} \quad S(i,k) = (\nu,\mu),$$

then the s_{ik} are also conjugate:

$$S(s_{ki})S(r_{ik}) = S(s_{ki}r_{ik}) = S(e_k^*) = e_\mu^* = s_{\mu\nu}r_{\nu\mu} = s_{\mu\nu}S(r_{ik}),$$

and hence $S(s_{ki}) = s_{\mu\nu}$. Since $e_i \mapsto e_i r_{ij} s_{jk}$ gives an operator isomorphism of $\mathfrak{l}_i$ onto $\mathfrak{l}_k$, we must have

$$r_{ij}s_{jk} = p_{ik}\xi_{ik}^{(j)}, \qquad \xi_{ik}^{(j)} \neq 0 \in \Gamma.$$

Because the r, the s, and the p are conjugate, the ξ are also conjugate: $S(i,j,k) = (\nu,\tau,\mu)$ implies

$$S(\xi_{ik}^{(j)}) = \xi_{\nu\mu}^{\tau}.$$

From

$$r_{i\lambda}s_{\lambda j}r_{j\lambda}s_{\lambda k} = r_{i\lambda}e_\lambda^* s_{\lambda k} = r_{i\lambda}s_{\lambda k}$$

it follows that

$$p_{ij}\xi_{ij}^{(\lambda)} \cdot p_{jk}\xi_{jk}^{(\lambda)} = p_{ik}\xi_{ik}^{(\lambda)},$$

or, since $p_{ij}p_{jk} = p_{ik}\alpha_{ik}^{(j)}$,

$$\alpha_{ik}^{(j)} = \frac{\xi_{ik}^{(\lambda)}}{\xi_{ij}^{(\lambda)}\xi_{jk}^{(\lambda)}}.$$

Put $\delta_{\nu\mu} = \prod_\lambda \xi_{\nu\mu}^{(\lambda)}$. Then $\delta_{\nu\mu}$ is invariant under every S fixing ν and μ, and hence lies in $\{Z_\nu, Z_\mu\}$; moreover, the $\delta_{\nu\mu}$ are conjugate because the $\xi_{\nu\mu}^{(j)}$ are. Since

$$\alpha_{ik}^{(j)n} = \frac{\prod_\lambda \xi_{ik}^{(\lambda)}}{\prod_\lambda \xi_{ij}^{(\lambda)} \prod_\lambda \xi_{jk}^{(\lambda)}} = \frac{\delta_{ik}}{\delta_{ij}\delta_{jk}},$$

the formula for associated factor systems (page 32) shows that $\alpha_{ik}^{(j)n}$ is associated with the system $\beta_{ik}^{(j)} = 1$. Since the order of $\{\mathfrak{K}\}$ is equal to the order of $\{\alpha\}$, it follows that the order of $\{\mathfrak{K}\}$ divides n. If $\mathfrak{Z}$ is chosen in particular as a maximal commutative subfield of $\mathfrak{K}$, then $n = t$, and hence λ divides t.

Second proof (Schur). This proof is based on representing the p_{ik} by regular n-rowed matrices P_{ik} in Γ that satisfy the same conjugacy conditions as the p_{ik}. The matrix P_{ik} lies in $\{Z_i, Z_k\}$; if p_{ik} corresponds to P_{ik}, then $S(p_{ik})$ corresponds to $S(P_{ik})$. This representation is homomorphic: that is, if P_{ik} corresponds to p_{ik}, and P_{kj} to p_{kj}, then $P_{ik}P_{kj}$ corresponds to $p_{ik}p_{kj}$, or

$$P_{ik}P_{kj} = \alpha_{ij}^{(k)} P_{ij}.$$

The relation $P_{ik_1}P_{k_2 j} = 0$ for $k_1 \neq k_2$ cannot hold. Once this representation of the p_{ik} is available, one argues as follows. Passing to determinants gives

$$|P_{ik}| \cdot |P_{kj}| = \alpha_{ij}^{(k)n} \cdot |P_{ij}|,$$

and therefore, since the matrices P_{ik} are regular, $|P_{\nu\mu}| \neq 0$,

$$\alpha_{ij}^{(k)n} = \frac{\delta_{ik}\delta_{kj}}{\delta_{ik}},$$

where $|P_{\nu\mu}| = \delta_{\nu\mu}$. One then continues as in Brauer's proof.

The representation of the p_{ik} by matrices P_{ik}:

The ideals $\mathfrak{l}_i$ of the decomposition

$$\mathfrak{K}_{r\Gamma} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n$$

are reciprocal representation modules of $\mathfrak{K}_r$ in Γ (Theorem 2, page 32). If a fixed basis $k_1, \ldots, k_n$ of $\mathfrak{K}_r$ with respect to $\mathfrak{Z}$ is taken as basis, then

$$\mathfrak{K}_{r\Gamma} = k_1\mathfrak{Z}_r + \cdots + k_n\mathfrak{Z}_r,$$

and hence

$$\mathfrak{l}_i = \mathfrak{K}_{r\Gamma}e_i = k_1\mathfrak{Z}_r e_i + \cdots + k_n\mathfrak{Z}_r e_i = k_1 e_i\Gamma + \cdots + k_n e_i\Gamma.$$

It follows that

$$\mathfrak{l}_k = \mathfrak{l}_i p_{ik} = k_1 p_{ik}\Gamma + \cdots + k_n p_{ik}\Gamma.$$

The two bases $(k_1e_i, \ldots, k_ne_i)$ and $(k_1p_{ik}, \ldots, k_np_{ik})$ of $\mathfrak{l}_k$ can be transformed into one another by multiplication by a regular matrix P_{ik}:

$$P_{ik} \cdot \begin{pmatrix} k_1e_i \\ \vdots \\ k_ne_i \end{pmatrix} = \begin{pmatrix} k_1p_{ik} \\ \vdots \\ k_np_{ik} \end{pmatrix}, \qquad \text{or briefly} \quad P_{ik}(k_\varrho e_i) = (k_\varrho p_{ik}).$$

The conjugacy of the P_{ik} follows:

$$S(P_{ik})(k_\varrho S(e_k)) = (k_\varrho S(p_{ik})) \quad \text{or} \quad S(P_{ik})(k_\varrho e_\mu) = (k_\varrho p_{\nu\mu}) = P_{\nu\mu}(k_\varrho e_\mu),$$

that is,

$$S(P_{ik}) = P_{\nu\mu} \quad \text{if} \quad S(i,k) = (\nu,\mu).$$

It follows in turn that P_{ik} lies in $\{Z_i, Z_k\}$, namely in the invariant field of those S that fix i and k. The homomorphy is also easy to see:

$$\begin{aligned} P_{ik}P_{kj}(k_\varrho e_j) &= P_{ik}(k_\varrho p_{kj}) = (k_\varrho p_{ik}p_{kj}) \\ &= \alpha_{ij}^{(k)}(k_\varrho p_{ij}) = \alpha_{ij}P_{ij}(k_\varrho e_j), \quad \text{and hence} \\ &\cdot\ P_{ik}P_{kj} = \alpha_{ij}^{(k)}P_{ij}, \quad \text{q.e.d.} \end{aligned}$$

Theorem 3 can be sharpened:

Theorem 4. *If p is a prime factor of the absolute number of components t of $\mathfrak{K}$, then p also divides the order λ of $\{\mathfrak{K}\}$. (Brauer)*

Proof. Let p^σ be the highest power of p contained in the degree n of the splitting field Z, let $\mathfrak{H}$ be a subgroup of order p^σ of $\mathfrak{G}$ (which exists by *Sylow's theorem*, Speiser, 1st ed., §19, p. 42, Theorem 43), and let T be the invariant field of $\mathfrak{H}$.

Then $[\Gamma : T] = p^\sigma$, and $[T : \mathsf{P}] = n/p^\sigma$ is not divisible by p, and still less by t. Thus T is not a splitting field, and the automorphism division ring $\mathfrak{S}$ of $\mathfrak{K}_T = \mathfrak{S}_m$ differs from P. But $\mathfrak{S}$ has splitting field Γ, whose degree over the center T of $\mathfrak{S}$ is p^σ; hence the absolute number of components of $\mathfrak{S}$ is a power $p^\beta > 1$, and consequently, by Theorem 3, the order of $\{\mathfrak{S}\}$ is a power $p^\alpha > 1$ of p. Since

$$\{\mathfrak{K}\}^\lambda = \{\mathsf{P}\}, \qquad \{\mathfrak{K}_T\}^\lambda = \{T\},$$

it follows that $\lambda \equiv 0 \pmod{p^\alpha}$, q.e.d. (Brauer has given examples showing that one need not have $\lambda = t$[1]).

Theorem 5. *Let t, decomposed into prime factors, be $t = \prod_i p_i^{\varrho_i}$, where $\varrho_i \geq 1$, and $p_i \neq p_j$ if $i \neq j$. Then $\mathfrak{K} = \mathfrak{K}^{(1)} \times \mathfrak{K}^{(2)} \times \cdots$, where $\mathfrak{K}^{(i)}$ is a division ring with absolute number of components $p_i^{\varrho_i}$.*

Proof. By Theorems 3 and 4, the order λ of $\{\mathfrak{K}\}$ is

$$\lambda = \prod_i p_i^{\alpha_i}, \qquad 1 \leq \alpha_i \leq \varrho_i.$$

The cyclic subgroup $\mathfrak{Z}$ of $\mathscr{K}$ generated by $\{\mathfrak{K}\}$ is the direct product of subgroups $\mathfrak{Z}_i$ of orders $p_i^{\alpha_i}$; hence

$$\{\mathfrak{K}\} = \prod_i \{\mathfrak{K}^{(i)}\}.$$

It follows that every splitting field Z of $\mathfrak{K}$ is also a splitting field of $\mathfrak{K}^{(i)}$. Thus the absolute number of components $p_i^{\sigma_i}$ of $\mathfrak{K}^{(i)}$ divides t, and $\sigma_i \leq \varrho_i$. Let $\prod_i \mathfrak{K}^{(i)} = \mathfrak{K}_m$; then

$$\prod_i p_i^{\varrho_i} = \prod_i p_i^{\sigma_i} \cdot m, \qquad \sigma_i \geq \varrho_i,$$

and consequently

$$\sigma_i = \varrho_i, \qquad m = 1, \qquad \mathfrak{K} = \prod_i \mathfrak{K}^{(i)}, \quad \text{q.e.d.}$$

§25. Normal Representation of $\mathfrak{K}_r$ with a Galois Maximal Commutative Subfield[33]

Let the maximal commutative subfield $\mathfrak{Z}$ of $\mathfrak{K}_r$ be Galois. By Theorem 7, page 25, the n automorphisms H_i of $\mathfrak{Z}/\mathsf{P}$ are inner automorphisms of $\mathfrak{K}_r$; that is, there are elements u_i such that

$$H_i z = u_i^{-1} z u_i \quad \text{for every } z \text{ from } \mathfrak{Z}.$$

Each u_i is determined up to a nonzero factor y from $\mathfrak{Z}$. Indeed, if $u^{-1}zu = u'^{-1}zu'$ for every z from $\mathfrak{Z}$, then $(u^{-1}u')^{-1}z(u^{-1}u') = z$ for every $z \in \mathfrak{Z}$. Adjoining $u^{-1}u'$ to $\mathfrak{Z}$ therefore gives a commutative subfield of $\mathfrak{K}_r$, which, by the maximality of $\mathfrak{Z}$, coincides with $\mathfrak{Z}$. Thus $u^{-1}u'$ lies in $\mathfrak{Z}$.

We prove the following theorem:

$$\mathfrak{K}_r = u_1\mathfrak{Z} + \cdots + u_n\mathfrak{Z}.$$

For this it is plainly sufficient to establish the linear independence of the u_i with respect to $\mathfrak{Z}$. The proof is given by specifying the u_i directly. Let

$$\mathfrak{Z}_Z = e_1 Z + \cdots + e_n Z, \qquad \mathfrak{K}_{rZ} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n, \quad \mathfrak{l}_i = \mathfrak{K}_{rZ} e_i,$$

and let p_{ik} be a system of pseudo-matrix units for this decomposition. On page 8 we denoted by Θ_i the isomorphism of $\mathfrak{Z}$ onto Z furnished by the representation module $e_i Z$, so that

$$S_i = \Theta_i \Theta_1^{-1}$$

[1] Brauer, "Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen II," *Math. Zeitschr.* 31, p. 733, §5 (1930).

[33] A simpler justification beginning with §27.

are the n automorphisms of Z (but only insofar as they are applied to Z itself, and no longer for the application of the S_i to all of $\mathfrak{K}_{rZ}$, which is always understood here!). For simplicity, in $S_i = \Theta_i\Theta_1^{-1}$ we shall write Θ_{S_i} in place of Θ_i, and then also replace the indices i, k of the p_{ik} by the corresponding automorphisms S:

$$p_{ik} = p_{S_iS_k}.$$

The n automorphisms of $\mathfrak{Z}$ are (with E the identity substitution)

$$H = \Theta_E^{-1}\Theta.$$

The H's are now numbered as follows:

$$H_S = \Theta_E^{-1}\Theta_{S^{-1}}.$$

Under these circumstances we may put

$$u_T = \sum_S p_{S,ST} = \sum_S S(p_{E,T}).$$

Indeed:
1. u_T^{-1} exists:

$$u_T^{-1} = \sum_S p_{ST,S}\frac{1}{\alpha_{S,S}^{ST}\overline{\gamma}_{S,ST}\overline{\gamma}_{ST,S}}.$$

(For the meaning of $\bar{\gamma}$, see page 32.)
2. u_T is an element of $\mathfrak{K}_r$, because it is $\mathfrak{G}$-invariant:

$$R(u_T) = \sum_S RS(p_{E,T}) = \sum_{S'} S'(p_{E,T}) = u_T.$$

3. u_T generates H_T; that is, if $z \in \mathfrak{Z}$, then $u_T^{-1}zu_T = H_T(z)$, or

$$zu_T = u_TH_T(z).$$

Indeed,

$$z = \sum_S \Theta_S(z)e_S, \qquad u_T = \sum_S S(e_Ep_{E,T}) = \sum_S e_SS(p_{E,T}),$$

and hence

$$zu_T = \sum_{S,S'} \Theta_S(z)e_Se_{S'}S(p_{E,T}) = \sum_S \Theta_S(z)S(p_{E,T}).$$

On the other hand,

$$u_T = \sum_S S(p_{E,T}e_T) = \sum_S S(p_{E,T})e_{ST},$$

and the following equation holds when applied to elements of $\mathfrak{Z}$:

$$\Theta_SH_T = \Theta_S\Theta_E^{-1}\Theta_{T^{-1}} = S\Theta_{T^{-1}} = ST^{-1}\Theta_E = \Theta_{ST^{-1}}.$$

Thus

$$H_T(z) = \sum_S e_S\Theta_SH_T(z) = \sum_S e_S\Theta_{ST^{-1}}(z),$$

that is,

$$\begin{aligned} u_TH_T(z) &= \sum_{S,S'} S(p_{E,T})e_{ST}\cdot e_{S'}\Theta_{S'T^{-1}}(z) \\ &= \sum_S S(p_{E,T})\Theta_S(z), \end{aligned}$$

and hence

$$z \cdot u_T = u_T \cdot H_T(z).$$

4. The u_S are linearly independent with respect to $\mathfrak{Z}$.

From

$$\sum_T z_T u_T = 0$$

and $z = \sum_S \Theta_S(z) e_S$, it follows that

$$\sum_{T,S,L} \Theta_S(z_T) e_S p_{L,LT} = \sum_{S,T} \Theta_S(z_T) p_{S,ST} \quad \text{and hence} \quad \Theta_S(z_T) = 0,$$

and therefore $z_T = 0$.

From now on we write z^S, a "symbolic power," in place of $H_S(z)$. Relations of the following kind must hold for the u_S:

$$u_R u_T = u_{RT} a_{R,T}, \qquad a_{R,T} \neq 0 \quad \text{from } \mathfrak{Z}.$$

Since

$$\begin{aligned} u_R u_T &= \sum_{S,S'} S(p_{E,R}) S'(p_{E,T}) = \sum_S p_{S,SR} p_{SR,SRT} \\ &= \sum_S p_{S,SRT} \alpha^{(SR)}_{S,SRT} = \sum_S p_{S,SRT} \alpha^{(SR)}_{S,SRT} e_{SRT}, \end{aligned}$$

and

$$a_{R,T} = \sum_S e_{SRT}\, \Theta_{SRT}\left(a_{R,T}\right),$$

and therefore

$$u_{RT} a_{R,T} = \sum_S p_{S,SRT} \Theta_{SRT}(a_{R,T}),$$

it follows that

$$\Theta_{SRT}(a_{R,T}) = \alpha^{(SR)}_{S,SRT}, \quad a_{R,T} = \sum_S e_{SRT} \alpha^{(SR)}_{S,SRT} = \sum_L e_L \alpha^{(LT^{-1})}_{LT^{-1}R^{-1},L}.$$

We shall call the system of the $a_{R,T}$ a small factor system of $\mathfrak{K}_r$. A large factor system $\alpha^{(A)}_{BC}$ and a small factor system $a_{R,T}$ determine one another. To the product $\varepsilon^{(A)}_{BC} = \alpha^{(A)}_{BC} \beta^{(A)}_{BC}$ of two large factor systems belongs the product $f_{R,T} = a_{R,T} b_{R,T}$ of the small factor systems $a_{R,T}$, $b_{R,T}$ assigned to $\alpha^{(A)}_{BC}$, $\beta^{(A)}_{BC}$; this follows immediately from the preceding formulas. The large identity factor system $\alpha^{(A)}_{BC} = 1$ corresponds to the small identity factor system $a_{R,T} = 1$, and conversely.

One may replace u_S by $u'_S = u_S r_S$, where $r_S \neq 0$ is chosen arbitrarily from $\mathfrak{Z}$. A small factor system $a'_{R,T}$ belongs to the u'_S:

$$(1) \qquad u'_R u'_T = u'_{RT} a'_{R,T}.$$

The factor system $a'_{R,T}$ is to be called associated with $a_{R,T}$. We have

$$u_R r_R u_T r_T = u_{RT} r_{RT} a'_{R,T} = u_R u_T r_R^T r_T = u_{RT} a_{R,T} r_R^T r_T,$$

from which

$$(2) \qquad a'_{R,T} = a_{R,T} \frac{r_R^T r_T}{r_{RT}}$$

follows.

The following system of pseudo-matrix units belongs to $u'_S = u_S r_S$:

$$p'_{S,ST} = p_{S,ST} r_T.$$

The small factor system $a'_{R,T}$ therefore belongs to a large factor system $\alpha^{(A)\prime}_{BC}$ that is associated with the factor system $\alpha^{(A)}_{BC}$ belonging to $a_{R,T}$. Associated small factor systems correspond to associated large factor systems, and conversely. The assignment of the classes $\{\alpha\}$ of associated large factor systems to the corresponding classes $\{a\}$ of associated small factor systems is a group isomorphism.

We now come to a representation of the u_S by n-rowed matrices in $\mathfrak{Z}$, which differs essentially from the representations considered thus far.

If the $\mathfrak{Z}$-basis

$$\text{(I)} \qquad k_{S_1}, \ldots, k_{S_n}$$

of $\mathfrak{K}_r$ is multiplied on the right by u_S, one obtains

$$\text{(II)} \qquad k_{S_1}u_S, \ldots, k_{S_n}u_S.$$

The (regular) matrix A_S that transforms (I) into (II),

$$\text{(III)} \qquad (k_{S_1}u_S, \ldots, k_{S_n}u_S) = (k_{S_1}, \ldots, k_{S_n})A_S,$$

is to be the matrix representing u_S. The representation is to apply to all elements of $\mathfrak{K}_r$ that, like the u_S, generate an automorphism of $\mathfrak{Z}/P$, that is, to all elements $u_S r_S$, where $r_S \neq 0$ is arbitrary in $\mathfrak{Z}$. All these elements form a group $\mathfrak{G}^*$, which contains as a normal subgroup the multiplicative group $\mathfrak{Z}^*$ of $\mathfrak{Z}$. The quotient group $\mathfrak{G}^*/\mathfrak{Z}^*$ is thereby isomorphic to the Galois group $\mathfrak{G}$ of $\mathfrak{Z}/P$: every element of a residue class of $\mathfrak{G}^*$ modulo $\mathfrak{Z}^*$ generates the corresponding automorphism of $\mathfrak{Z}$. The group $\mathfrak{G}^*$ is represented in the manner just indicated:

$u_S \mapsto A_S$.

But this representation is not homomorphic, nor even reciprocally homomorphic. From

$u_S \mapsto A_S$, $u_T \mapsto A_T$

it does not follow that $u_S u_T \mapsto A_S A_T$; rather, because

$$\begin{aligned}(k_{S_1}, \ldots, k_{S_n})u_S u_T &= (k_{S_1}, \ldots, k_{S_n})A_S u_T = (k_{S_1}, \ldots, k_{S_n})u_T A_S^T \\ &= (k_{S_1}, \ldots, k_{S_n})A_T A_S^T : \ u_S u_T \mapsto A_T A_S^T.\end{aligned}$$

This representation of $\mathfrak{G}^*$ will be called the crossed representation. If $h_{S_1}, \ldots, h_{S_n}$ is another basis of $\mathfrak{K}_r$ with respect to $\mathfrak{Z}$, and

$$\text{(IV)} \qquad (h_{S_1}, \ldots, h_{S_n}) = (k_{S_1}, \ldots, k_{S_n})M,$$

then (III) and (IV) give

$$(h_{S_1}, \ldots, h_{S_n})\, u_S = (h_{S_1}, \ldots, h_{S_n})\, M^{-1} A_S\, M^S.$$

That is: if u_S is represented by A_S with respect to the k-basis, then it is represented by $M^{-1}A_S M^S$ with respect to the h-basis, where M is the matrix that transforms the k-basis into the h-basis.

Formula (III), defining the crossed representation, shows that the crossed representation stands in a relation to the ring $\mathfrak{K}_r$ similar to that in which an ordinary reciprocal representation (written from the right rather than from the left) stands to its representation module. The difference arises because, in place of the commutation relation

$$(m^*\tau^*)c = (m^*c)\tau^*$$

(see page 5)

for a reciprocal representation module, here one has

$$(kz)u_S = (ku_S)z^S \qquad k \text{ in } \mathfrak{K}_r, \quad z \text{ in } \mathfrak{Z}.$$

A crossed representation of $\mathfrak{G}^*$ may also be formed by means of a basis of a right ideal $\mathfrak{r}$ of $\mathfrak{K}_r$. In this way every right ideal of $\mathfrak{K}_r$ generates a class of equivalent representations. Here the representations $u_S \mapsto A_S$, $u_S \mapsto B_S$ are called equivalent if there is a matrix M such that $B_S = M^{-1}A_S M^S$.

Instead of restricting ourselves to the representations of $\mathfrak{G}^*$ in $\mathfrak{Z}$ generated by right ideals of $\mathfrak{K}_r$, we may now define a crossed representation of degree m of $\mathfrak{G}^*$ in $\mathfrak{Z}$ in general as follows:

1. To every u_S there corresponds an m-rowed $\mathfrak{Z}$-matrix A_S.

2. From $u_S \mapsto A_S$, $u_T \mapsto A_T$ it follows that $u_S u_T \mapsto A_T A_S^T$.

Take a $\mathfrak{Z}$-right module of rank m,

$$\mathfrak{M} = x_1\mathfrak{Z} + \cdots + x_m\mathfrak{Z},$$

and make it a $\mathfrak{G}^*$-right module by setting

$$(x_1 u_S, \ldots, x_m u_S) = (x_1, \ldots, x_m)A_S,$$

with the commutation relation

$$(mz)u_S = (mu_S)z^S,$$

entirely analogously to the construction on page 5 of the representation module corresponding to a given representation. We now show, as on page 20, that $\mathfrak{M}$ becomes a finite $\mathfrak{K}_r$-right module by setting

$$m \cdot zu_S = mz \cdot u_S = mu_S \cdot z^S,$$

and, in general,

$$m \cdot \sum z_S u_S = \sum mz_S \cdot u_S = \sum mu_S \cdot z_S^S.$$

Nothing corresponding to the calculation on page 20 is needed here, because in making our definition we used a particular basis.

By M.Z. ğ 18, however, every finite simple $\mathfrak{K}_r$-module $\mathfrak{M}$ is operator-isomorphic to a simple right ideal of $\mathfrak{K}_r$. Correspondingly to Theorem 2, page 22, we conclude that there is only *one* irreducible crossed representation class of $\mathfrak{G}^*$ in $\mathfrak{Z}$, namely the one belonging to the simple right ideals.

The degree of this irreducible representation is t, where t is the index (absolute exponent number) of $\mathfrak{K}$. This follows by a simple count of ranks. For the degree is equal to the $\mathfrak{Z}$-rank $(\mathfrak{r} : \mathfrak{Z})$ of a simple right ideal. On page 22 we have

$$(\mathfrak{Z} : P) = n = rt; \qquad (\mathfrak{K}_r : P) = n^2; \qquad (\mathfrak{r} : P) = n \cdot t,$$

the last because $\mathfrak{K}_r = \mathfrak{r}_1 + \cdots + \mathfrak{r}_r$.

From

$$(\mathfrak{r} : P) = (\mathfrak{r} : \mathfrak{Z}) \cdot (\mathfrak{Z} : P)$$

or $n \cdot t = (\mathfrak{r} : \mathfrak{Z}) \cdot n$, it therefore follows that $(\mathfrak{r} : \mathfrak{Z}) = t$.

ğ 26. Multiplication of Crossed Representations

Thus far we have always regarded a crossed representation as a representation of $\mathfrak{G}^*$. But we may also regard it as a representation of the Galois group $\mathfrak{G}$ of $\mathfrak{Z}/P$, by assigning to every element S of $\mathfrak{G}$ the matrix A_S that represents an element u_S of $\mathfrak{K}_r$ which generates the automorphism S by transformation—$u_S^{-1} z u_S = z^S$.

To characterize such a representation $S \mapsto A_S$[1], one must specify in which $\mathfrak{K}_r$ it is taken, which u_S, and which $k_{S_1}, \ldots, k_{S_n}$ of $\mathfrak{K}$ over $\mathfrak{Z}$, are used. A change of basis gives an equivalent representation; a change of the u gives associated factor systems $a_{S,T}$. What is essential, therefore, is the $\mathfrak{K}_r$ in which the representation is taken, that is, the class $\{a_{S,T}\}$ of associated factor systems.

Now let two such representations of $\mathfrak{G}$ be given:

$$\begin{array}{ll} S \mapsto u_S \mapsto A_S & \text{corresponding small factor system} \quad a_{R,T}, \\ S \mapsto v_S \mapsto B_S & \text{corresponding small factor system} \quad b_{R,T}. \end{array}$$

[1] Such a representation (independently of hypercomplex systems),

$$S \mapsto A_S; \quad T \mapsto A_T; \quad ST \mapsto A_T A_S^T = A_{ST} \cdot a_{S,T}^{-1}$$

(or its transpose), was Speiser's starting point (*Math. Zschr.* 5) for defining the factor systems $a_{S,T}$. Thus these factor systems prove to be identical with those introduced here from a different basis.

By the Kronecker product $A \times B$ of two matrices $A = (a_{ik})$, $B = (b_{\mu\nu})$, we mean the matrix $A \times B = (a_{ik} b_{\mu\nu})$.

Assertion. *The mapping $S \mapsto A_S \times B_S$ is likewise a crossed representation of $\mathfrak{G}$; specifically, it belongs to the product $\mathfrak{K}_r \times \mathfrak{S}_s$ if A_S arises from $\mathfrak{K}_r$, and B_S from $\mathfrak{S}_s$.*

Proof. The representation $S \mapsto A_S \times B_S$ is a crossed representation. Let

$$S \mapsto A_S \times B_S, \qquad T \mapsto A_T \times B_T,$$

and

$$ST \mapsto A_{ST} \times B_{ST} = (A_T A_S^T \times B_T B_S^T) a_{S,T}^{-1} b_{S,T}^{-1}.$$

Thus it must be proved that

$$(A_T \times B_T)(A_S \times B_S)^T a_{S,T}^{-1} b_{S,T}^{-1} = (A_T A_S^T \times B_T B_S^T) a_{S,T}^{-1} b_{S,T}^{-1}.$$

But this follows from the following consideration.

Represent the matrices A and B by matrix units c_{ik} and $d_{\mu\nu}$ (which have nothing to do with the matrix units of $\mathfrak{K}_r$ or $\mathfrak{S}_s$):

$$A = \sum c_{ik} \alpha_{ik}; \qquad B = \sum d_{\mu\nu} \beta_{\mu\nu}, \qquad \text{then}$$

$$A \times B = B \times A = \sum c_{ik} d_{\mu\nu} \cdot \alpha_{ik} \cdot \beta_{\mu\nu},$$

that is, a matrix in the new matrix units $c_{ik} d_{\mu\nu} = d_{\mu\nu} c_{ik}$. Multiplication of the A- and B-matrices thus corresponds bijectively to multiplication of elements in the direct product of the two matrix rings:

$$\sum c_{ik} \mathfrak{Z} \times \sum d_{\mu\nu} \mathfrak{Z}.$$

Consequently every A-matrix commutes with every B-matrix (though the A-matrices, or the B-matrices, do not commute among themselves); and this commutativity of every A-matrix with every B-matrix gives precisely—after multiplication by $a_{S,T}^{-1} b_{S,T}^{-1}$—the relation to be proved.

Chapter VI. Theory of Crossed Products

ğ 27. Representation of the $\mathfrak{K}_r$ as Crossed Products

The theory of crossed products developed in ğ 24 from factor systems will now be established anew and independently. The significance of these crossed products lies in the fact that a Galois field and its group are described *together* in $\mathfrak{K}_r$.

Theorem 1. *If $\mathfrak{Z}$ is a Galois splitting field of $\mathfrak{K}_r$, hence a maximal commutative subfield, and $\mathfrak{G}$ is its Galois group, then $\mathfrak{K}_r$ is equal to the crossed product $\mathfrak{Z} \cdot \mathfrak{G}$. Conversely, every crossed product $\mathfrak{Z} \cdot \mathfrak{G}$ generates a $\mathfrak{K}_r$ of this kind.*

Proof and definitions. Definition 1. Let $\mathfrak{G} = \{E, S, \ldots, T\}$ be the Galois group of $\mathfrak{Z}$. The assertion that $\mathfrak{K}_r$ equals the crossed product means

$$\mathfrak{K}_r = \mathfrak{Z} u_E + \cdots + \mathfrak{Z} u_T$$

with $z u_S = u_S z^S$ and $u_S u_T = a_{S,T} u_{ST}$ (the $a_{S,T}$ in $\mathfrak{Z}$ forming a small factor system).

Definition 2. The generating group $\mathfrak{G}^*$ is defined as the totality of regular elements g of $\mathfrak{K}_r$ that transform $\mathfrak{Z}$, as a whole, into itself. Thus $g^{-1} \mathfrak{Z} g = \mathfrak{Z}$, and hence $g^{-1} z g = z^S$, with S in $\mathfrak{G}$. Consequently $\mathfrak{G}$ is a group-homomorphic image of $\mathfrak{G}^*$, since every automorphism of $\mathfrak{Z}$ is generated by some g: $\mathfrak{G}^* \to \mathfrak{G}$; moreover,

$$\mathfrak{G} \cong \mathfrak{G}^* / \mathfrak{T}^* \quad \text{with} \quad \mathfrak{T}^* \supseteq \mathfrak{Z}^*,$$

(later we shall have $\mathfrak{T}^* = \mathfrak{Z}^*$; it has not yet been proved that $\mathfrak{Z}$ is also a maximal commutative subring, although this can likewise be proved independently).

1. *Proof of the representation as a crossed product.* Let $u_E, u_S, \ldots, u_T$ be elements of $\mathfrak{K}_r$ generating the automorphisms $E, \ldots, T$, so that $z u_S = u_S z^S$, and in particular $u_E = e$ by 2. It is to be shown that the sum

$$\mathfrak{M} = \{\mathfrak{Z} u_E, \ldots, \mathfrak{Z} u_T\}$$

is direct, and equal to $\mathfrak{Z}u_E + \cdots + \mathfrak{Z}u_T$; it then equals $\mathfrak{K}_r$ because the ranks agree. This follows as follows (Schwarz):

$\mathfrak{M}$ is a left and right $\mathfrak{Z}$-module, hence a representation module of $\mathfrak{Z}$ in $\mathfrak{Z}$. The n distinct representations are generated by $\mathfrak{M}$; therefore—since $\mathfrak{Z}$ is commutative of the first kind—$\mathfrak{M}$ has rank at least n. The remainder of the proof is exactly the same.

2. $\mathfrak{G} \cong \mathfrak{G}^*/\mathfrak{Z}^*$, that is, $\mathfrak{T}^* = \mathfrak{Z}^*$: only the elements of $\mathfrak{Z}$ induce the identity on $\mathfrak{Z}$ by transformation.

Indeed, suppose that $tz = zt$ for every z in $\mathfrak{Z}$, and write

$$t = z_0 + z_1 u_S + \cdots + z_{n-1} u_T.$$

Then

$$zt = zz_0 + \cdots + zz_{n-1}u_T$$

and

$$tz = z_0 z + \cdots + z_{n-1}u_T z = z_0 z + z^{S^{-1}} z_1 u_S + \cdots + z^{T^{-1}} z_{n-1} u_T.$$

Hence, because the sum is direct,

$$(z - z^{S^{-1}})z_1 u_S = 0, \ldots, (z - z^{T^{-1}})z_{n-1}u_T = 0,$$

and, since the elements $u_S, \ldots$ are regular,

$$(z - z^{S^{-1}})z_1 = 0, \ldots, (z - z^{T^{-1}})z_{n-1} = 0, \qquad \text{for every } z.$$

(The same follows from the equality of ranks.) But for each of $S, \ldots, T$ (all different from E) there is, by definition, at least one z such that $z - z^{S^{-1}} \neq 0$, and a $\bar{z}$ such that $\bar{z} - \bar{z}^{T^{-1}} \neq 0$. Thus $z_i = 0$, $i = 1, \ldots, n-1$, and hence $t = z_0$ lies in $\mathfrak{Z}^*$, as was to be proved.

3. The u's satisfy the multiplication laws $u_S u_T = a_{S,T} u_{ST}$, where the $a_{S,T}$ satisfy the crossed associativity laws

$$a_{R,S} \cdot a_{RS,T} = a_{S,T}^{R^{-1}} \cdot a_{R,ST}$$

(the $a_{S,T}$ form a small factor system).

For, by 2,

$$\mathfrak{Z}^* u_S \cdot \mathfrak{Z}^* u_T = \mathfrak{Z}^* u_{ST};$$

hence

$$u_S u_T = a_{S,T} u_{ST},$$

with $a_{S,T}$ in $\mathfrak{Z}^*$, thus in $\mathfrak{Z}$, and nonzero. From $u_R \cdot u_S u_T = u_R u_S \cdot u_T$ one further obtains

$$\begin{aligned} u_R a_{S,T} u_{ST} &= a_{S,T}^{R^{-1}} \cdot u_R u_{ST} = a_{S,T}^{R^{-1}} a_{R,ST} u_{RST} \\ &= a_{R,S} u_{RS} \cdot u_T = a_{R,S} a_{RS,T} u_{RST}, \end{aligned}$$

which gives the stated multiplication laws.

4. Converse: a crossed product is a $\mathfrak{K}_r$. Declare the direct sum

$$\mathfrak{M} = \mathfrak{Z}u_E + \cdots + \mathfrak{Z}u_T$$

to be a ring by the relations $zu_S = u_S z^S$, $u_S u_T = a_{S,T} u_{ST}$, where the $a_{S,T}$ satisfy the crossed associativity relations, so that $u_R u_S u_T$ is unambiguously defined:

1. $z_1 \cdot z_2 u_S = z_1 z_2 \cdot u_S$;
2. $z u_S \cdot u_T = z \cdot u_S u_T$.

Then $\mathfrak{M}$ is an associative ring.

Converse Theorem 2. *The crossed product $\mathfrak{Z} \cdot \mathfrak{G}$ is two-sided simple, with center P (following ideas of R. Brauer).* The proof rests on the following lemmas.

Lemma 1. *Every element commuting elementwise with $\mathfrak{Z}$ belongs to $\mathfrak{Z}$.*

Proof. Let $w = \sum_S c_{\lambda_S} u_S$, with c_{λ_S} in $\mathfrak{Z}$, and suppose that $wz = zw$ for every z in $\mathfrak{Z}$. Then

$$\sum_S z c_{\lambda_S} u_S = \sum_S c_{\lambda_S} u_S z = \sum_S c_{\lambda_S} z^{S^{-1}} u_S,$$

so $zc_{\lambda_S} = c_{\lambda_S} z^{S^{-1}}$, or $c_{\lambda_S}(z - z^{S^{-1}}) = 0$, for every z and S (by the linear independence of the u's). It follows that $c_{\lambda_S} = 0$ for $S \neq E$, since for each such S there is at least one z with $z - z^{S^{-1}} \neq 0$. Hence w lies in $\mathfrak{Z}$.

Lemma 2. *Every $\mathfrak{Z}$-bimodule $\mathfrak{A}$ that is bimodule-isomorphic to $\mathfrak{Z}u_S = u_S\mathfrak{Z}$ (with $\mathfrak{Z}$ acting on the left and right) is identical with $\mathfrak{Z}u_S$.*

Proof of 2. As a left module, $\mathfrak{A}$ is isomorphic to $\mathfrak{Z}u_S$. Thus, if $u_S \mapsto a$ in $\mathfrak{A}$, then $\mathfrak{Z}u_S \mapsto \mathfrak{Z}a$, and hence $\mathfrak{A} = \mathfrak{Z}a$. The bimodule isomorphism gives (1) $za = az^S$ (because $u_S z \mapsto az$); it follows that $\mathfrak{A} = \mathfrak{Z}u_S$. Indeed, set $a = u_S u_S^{-1} a = u_S w$. Then $za = zu_S w = u_S z^S w$, whereas (1) gives $za = u_S w z^S$. Multiplication by u_S therefore yields $z^S w = w z^S$ for every z in $\mathfrak{Z}$. Since z^S likewise runs through all of $\mathfrak{Z}$, w commutes elementwise with $\mathfrak{Z}$, and hence belongs to $\mathfrak{Z}$ by Lemma 1.

Lemma 3. *Every $\mathfrak{Z}$-bimodule in $\mathfrak{Z} \cdot \mathfrak{G}$ has the form $\mathfrak{Z}u_{S_1} + \cdots + \mathfrak{Z}u_{S_k}$, where the u_{S_1} denote any k distinct members among $u_S, \ldots, u_T$.*

Proof. As a $\mathfrak{Z}$-bimodule, the crossed product $\mathfrak{Z} \cdot \mathfrak{G}$ is completely reducible, since every summand $\mathfrak{Z}u_S$ has rank one. Moreover, as bimodules all the summands belong to distinct classes and are therefore not bimodule-isomorphic. Hence every $\mathfrak{Z}$-bimodule $\mathfrak{M}$ is, by complete reducibility, a direct summand and is itself completely reducible. Thus $\mathfrak{M} = \sum \mathfrak{A}_{S_i}$, where $\mathfrak{A}_{S_i}$ is isomorphic to $\mathfrak{Z}u_{S_i}$, and consequently, by Lemma 2, is identical with $\mathfrak{Z}u_{S_i}$. (All the $\mathfrak{A}_{S_i}$ belong to distinct classes.)

Lemma 4. *Every subring of $\mathfrak{Z} \cdot \mathfrak{G}$ containing $\mathfrak{Z}$, in particular $\mathfrak{Z} \cdot \mathfrak{G}$ itself, is two-sided simple. The subrings containing $\mathfrak{Z}$ correspond one-to-one to the subgroups of $\mathfrak{G}$.*

Proof. Every ring $\mathfrak{o}$ containing $\mathfrak{Z}$ is a $\mathfrak{Z}$-bimodule, hence by Lemma 3 has the form $\sum \mathfrak{Z} \cdot u_{S_i}$. Since $\mathfrak{o}$ is a ring, the product of two u_{S_i}'s again belongs to $\mathfrak{o}$, and so does the corresponding $\mathfrak{Z}$-module. Since there are only finitely many of them, the u_{S_i}'s therefore form a group up to factor systems. Thus $\mathfrak{o} = \mathfrak{Z} \cdot \mathfrak{H}$, where $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$. (More precisely, the $\mathfrak{Z} \cdot u_{S_i}$ form a multiplicative system.) Now let $\mathfrak{a} \neq 0$ be any two-sided ideal of $\mathfrak{o}$. It is an $\mathfrak{o}$-bimodule and hence a $\mathfrak{Z}$-bimodule and submodule of $\mathfrak{o}$. Along with any $\mathfrak{Z}u_{S_i}$, it therefore contains the whole group $\mathfrak{H}$, and thus becomes $\mathfrak{o} = \mathfrak{Z} \cdot \mathfrak{H}$.

Lemma 5. *P is the center of $\mathfrak{Z} \cdot \mathfrak{G}$.*

Proof. If w commutes elementwise with $\mathfrak{Z} \cdot \mathfrak{G}$, then in particular it commutes with $\mathfrak{Z}$, and so belongs to $\mathfrak{Z}$ by Lemma 1. Since $wu_S = u_S w^S$, commutativity then gives $w = w^S$. Thus w belongs to P.

Remark 1. The proof shows that the theorem remains valid when $\mathfrak{Z}$ is an infinite algebraic Galois field over P, since the theorems on complete reducibility remain valid (Krull, *Zahlringe*, Math. Ann. 99). Here $\mathfrak{Z} \cdot \mathfrak{G}$ is the system of all finite sums $\sum_{S_\lambda} u_{S_\lambda} \cdot c_{S_\lambda}$.

Only in Lemma 4 must one assume that $\mathfrak{o} = \mathfrak{Z} \cdot \mathfrak{H}$, as is indeed the case for the full product $\mathfrak{Z} \cdot \mathfrak{G}$; for when $\mathfrak{o}$ is infinite over $\mathfrak{Z}$, membership of $u_{S_i} u_{S_k}$ no longer implies that the system has the group property.

Remark 2. In a direct treatment, the theory of crossed matrix representations developed in ğğ 25–26 must be appended here. We shall use, at the end of ğ 28, the fact that the irreducible crossed representation has degree t, where t is the absolute number of components (the index) of $\mathfrak{K}$. Let it be emphasized once more that this representation theory establishes the identity of the factor systems introduced here as multiplication constants with the concept customarily used in the literature.

ğ 28. Product Theorem for Factor Systems

Let

$$\mathfrak{K}_r = \mathfrak{Z} \cdot \mathfrak{G} = \mathfrak{Z}u_E + \cdots + \mathfrak{Z}u_T, \qquad u_S u_T = u_{ST} a_{S,T},$$
$$\overline{\mathfrak{K}}_r = \overline{\mathfrak{Z}}\,\overline{\mathfrak{G}} = \overline{\mathfrak{Z}}\bar{u}_E + \cdots + \overline{\mathfrak{Z}}\bar{u}_T, \qquad \bar{u}_S \bar{u}_T = \bar{u}_{ST} \bar{b}_{S,T},$$

where $\mathfrak{Z}$ and $\overline{\mathfrak{Z}}$ are isomorphic Galois fields, and $\mathfrak{G}$, $\overline{\mathfrak{G}}$ their groups. Then

$$\mathfrak{K}_r \times \overline{\mathfrak{K}}_r = \widetilde{\mathfrak{Z}}\,\widetilde{\mathfrak{G}} \times P_n = \mathfrak{A}_f \times P_n = \mathfrak{A}_j,$$

with $\tilde{u}_S \tilde{u}_T = \tilde{u}_{ST} \tilde{c}_{S,T}$, where $\widetilde{\mathfrak{Z}}$ is isomorphic to $\mathfrak{Z}$ and $\overline{\mathfrak{Z}}$. This follows by counting ranks and from the fact that $\mathfrak{Z}$ is also a splitting field.

Claim. *One has $\tilde{c}_{S,T} = \tilde{a}_{S,T} \tilde{b}_{S,T}$, where $\tilde{a}$ and $\tilde{b}$ are the elements of $\widetilde{\mathfrak{Z}}$ corresponding isomorphically to a and $\bar{b}$.*

The proof rests on the fact that the endomorphism ring of any left ideal of $\mathfrak{A}_j$ having absolute length n is isomorphic to $\mathfrak{A}_f = \widetilde{\mathfrak{Z}}\widetilde{\mathfrak{G}}$, and that this endomorphism ring can be determined directly for a suitable left ideal of $\mathfrak{A}_j$. More generally, with s in place of n, we have the following result, stated for convenience in terms of $\mathfrak{K}_r$.

1. Theorem 1. *The endomorphism ring of a left ideal* $\mathfrak{l}$ *of absolute length* n *in* $\mathfrak{K}_{rs} = \mathfrak{K}_r \times P_s$ *is isomorphic to* $\mathfrak{K}_r$.

The proof follows from the next lemmas.

Lemma 1. *All left ideals of absolute length* n *in* $\mathfrak{K}_{rs}$ *are operator-isomorphic. Their endomorphism rings are therefore ring-isomorphic. In particular,* $\mathfrak{l} = \mathfrak{K}_r \times \mathfrak{b}$ *has absolute length* n*, where* $\mathfrak{b}$ *denotes a simple ideal of* P_s.

Proof. The fact that the left ideals have absolute length n, that is, decompose into n absolutely indecomposable simple ideals, implies that they have the same length in $\mathfrak{K}_{rs}$, or equivalently that the same number of simple ideal summands in $\mathfrak{K}_{rs}$ occur. Their operator isomorphism follows, and with it the ring isomorphism of their endomorphism rings. Moreover, $\mathfrak{K}_r = \mathfrak{Z} \cdot \mathfrak{G}$ has absolute length n, that is, rank n^2; therefore $\mathfrak{K}_r \times P_s$ has absolute length $n \cdot s$, and hence $\mathfrak{K}_r \times \mathfrak{b}$ has absolute length n.

Lemma 2. *If* $\mathfrak{o}$ *is a ring with identity and* $\mathfrak{l} = \mathfrak{o}e_1$ *is a left ideal and direct summand, so that* e_1 *is idempotent, then the endomorphism ring of* $\mathfrak{l}$ *is isomorphic to* $e_1 \mathfrak{o} e_1$.

Proof. Multiplication by an element $e_1 r e_1$ defines an operator homomorphism of $\mathfrak{l}$ into itself. Distinct elements $e_1 r e_1$ define distinct homomorphisms, since they assign distinct elements to e_1; and every homomorphism arises in this way: $e_1 \mapsto r e_1$, and $r e_1 = e_1 r e_1$ because $e_1 e_1 = e_1$. Addition and multiplication in $e_1 \mathfrak{o} e_1$ correspond to addition and composition of the associated homomorphisms.

Lemma 3. *If one writes* $P_s = \sum_1^s c_{ik} P$*, with matrix units* c_{ik}*, and* $\mathfrak{b} = c_{11}P + \cdots + c_{s1}P$*, then the endomorphism ring of* $\mathfrak{K}_r \times \mathfrak{b}$ *is* $\mathfrak{K}_r c_{11}$*, which is isomorphic to* $\mathfrak{K}_r$.

Proof. Indeed, c_{11} commutes elementwise with $\mathfrak{K}_r$, and no element of $\mathfrak{K}_r$ is annihilated, since c_{11} is a generating idempotent of $\mathfrak{K}_r \times P_s$, and

$$c_{11} \cdot \mathfrak{K}_r \times P_s \cdot c_{11} = \mathfrak{K}_r \times c_{11} P_s c_{11} = \mathfrak{K}_r c_{11}.$$

Theorem 1 follows directly from these lemmas.

2. Determination and decomposition of $\mathfrak{K}_r \times \overline{\mathfrak{K}}_r$ **into left ideals of absolute length** n**.** By definition,

$$\mathfrak{A}_f = \mathfrak{K}_r \times \overline{\mathfrak{K}}_r = \mathfrak{Z} \cdot \mathfrak{G} \times \overline{\mathfrak{Z}} \cdot \overline{\mathfrak{G}},$$

where barred and unbarred elements commute elementwise. Hence

$$\mathfrak{A}_f = (\mathfrak{G} \times \overline{\mathfrak{G}}) \cdot (\mathfrak{Z} \times \overline{\mathfrak{Z}}) = \mathfrak{G} \times \overline{\mathfrak{G}} \cdot (\mathfrak{Z}e_1 + \cdots + \mathfrak{Z}e_n),$$

with $\mathfrak{Z}e_i = \overline{\mathfrak{Z}}e_i$, by multiplication of a Galois field with itself. Since all summands have the same rank with respect to $\mathfrak{Z}$, and therefore the same absolute length, while the absolute length of $\mathfrak{A}_f$ is n^2, every summand has absolute length n. In what follows we take

$$\mathfrak{l} = (\mathfrak{G} \times \overline{\mathfrak{G}})\mathfrak{Z}e_1,$$

where $ze_1 = e_1 \bar{z}$ fixes a definite isomorphism between $\mathfrak{Z}$ and $\overline{\mathfrak{Z}}$.

3. Crossed representation of $e_1 \mathfrak{A}_f e_1$**, and hence proof of the product theorem.** By 1 and 2, the factor systems of the product $\mathfrak{K}_r \times \overline{\mathfrak{K}}_r$ are isomorphic to those of a crossed representation of $e_1 \mathfrak{A}_f e_1 = \mathfrak{A}$.

Theorem 2. *One has* $\mathfrak{A} = \widetilde{\mathfrak{Z}} \cdot \widetilde{\mathfrak{G}}$*, with* $\widetilde{\mathfrak{Z}} = \mathfrak{Z}e_1 = \overline{\mathfrak{Z}}e_1$ *and* $\widetilde{\mathfrak{G}} = \{\ldots, e_1 u_S \bar{u}_S e_1, \ldots\}$*, where*

$$e_1 u_S \bar{u}_S e_1 \cdot e_1 u_T \bar{u}_T e_1 = e_1 u_{ST} \bar{u}_{ST} e_1 \cdot a_{S,T} e_1 \bar{b}_{S,T} e_1.$$

Thus, with $\tilde{a}_{S,T} = a_{S,T} e_1$ *and* $\tilde{b}_{S,T} = \bar{b}_{S,T} e_1$*, the product theorem is proved; here* $\tilde{a}$ *and* $\tilde{b}$ *lie in the same field* $\widetilde{\mathfrak{Z}}$.

Proof. The element e_1 becomes the identity of the ring, and the conjugates of $\tilde{z} = ze_1$ are therefore given by $\tilde{z}^S e_1$. It remains to show that the elements $u_S \bar{u}_S e_1$ induce these substitutions; this proves the crossed representation.

Lemma 1. $e_1 u_S \bar{u}_S = u_S \bar{u}_S e_1$, and hence both are equal to $e_1 u_S \bar{u}_S e_1$.

Proof. Put $u_S^{-1} e_1 u_S = e^{S}$[1], or $e_1 u_S = u_S e^S$. Then the e^S run through the conjugates $e_1, e_2, \ldots, e_n$. We have (1)[2]

$$e_1 \bar{u}_R = \bar{u}_R e^{R^{-1}}.$$

[1] This convention gives $e_1 = e^E$.

[2] Because $\sum a_i \bar{A}_i \bar{u}_R = \sum a_i \bar{u}_R \bar{A}_i^R = \bar{u}_R \sum (a_i^R)^{R^{-1}} \bar{A}_i^{-R}$.

Indeed, $e_1 = \sum a_i \bar{A}_i = \sum a_i^R \bar{A}_i^R$, where a_i runs through any $\mathfrak{Z}$-basis and $\bar{A}_i$ through the complementary $\overline{\mathfrak{Z}}$-basis; the same therefore holds for a_i^R and $\bar{A}_i^R$. Thus $e_1 \bar{u}_R = \bar{u}_R e^{R^{-1}}$, proving (1). It follows from (1) that

$$e_1 u_S \bar{u}_S = u_S e^S \bar{u}_S = u_S \bar{u}_S \cdot e^{SS^{-1}} = u_S \bar{u}_S e_1,$$

which proves Lemma 1.

Lemma 2. $ze_1 \cdot e_1 u_S \bar{u}_S e_1 = e_1 u_S \bar{u}_S e_1 \cdot z^S e_1$.

Proof. Indeed,

$$ze_1 \cdot e_1 u_S \bar{u}_S e_1 = z u_S \bar{u}_S e_1 \quad \text{(Lemma 1)} = u_S z^S \bar{u}_S e_1 = u_S \bar{u}_S e_1 \cdot z^S e_1 = b = e_1 b,$$

since z commutes with $\bar{u}$ and e_1. Put $u' = u_S \bar{u}_S e_1$. Lemma 2 says that u' indexes the substitutions of $\mathfrak{Z}e_1$, and therefore the crossed representation stated in the theorem holds.

Lemma 3. *The factor system is* $a_{S,T} e_1 \cdot \bar{b}_{S,T} e_1$.

Proof.

$$\begin{aligned} e_1 u_S \bar{u}_S e_1 \cdot e_1 u_T \bar{u}_T e_1 &= u_S \bar{u}_S \cdot u_T \bar{u}_T e_1 = u_{ST} a_{S,T} \cdot \bar{u}_{ST} \bar{b}_{S,T} e_1 \\ &= u_{ST} \bar{u}_{ST} \cdot a_{S,T} \bar{b}_{S,T} e_1 = e_1 u_{ST} \bar{u}_{ST} e_1 \cdot a_{S,T} e_1 \cdot \bar{b}_{S,T} e_1. \end{aligned}$$

Together with 2, this proves the theorem, and hence the product theorem for factor systems.

4. Product theorem for classes of associated factor systems:

$$\{a_{S,T}\} \cdot \{b_{S,T}\} = \{a_{S,T} \cdot b_{S,T}\}.$$

This follows directly from 3, since passage to new generators v and $\bar{v}$ also entails passage to $v\bar{v}e_1$. Indeed, $u = vc$ and $\bar{u} = \bar{v}\bar{d}$ give

$$u\bar{u}e_1 = vc \cdot \bar{v}\bar{d}e_1 = v\bar{v} \cdot c\bar{d}e_1 = v\bar{v}e_1 \cdot c\bar{d}e_1.$$

5. If $\{a\}$ is a factor system of $\{\mathfrak{K}\}$, and t is the index of $\{\mathfrak{K}\}$, then $\{a\}^t$ is the identity class. This follows because the irreducible crossed representation of $\mathfrak{G}$ has degree t, exactly as in Schur's proof following the representation of the p_{ik} (ğ 24, p. 37).

6. There is an isomorphism between the group $\mathscr{K}_\mathfrak{Z}$ of the $\{\mathfrak{K}\}$ belonging to $\mathfrak{Z}$, that is, having $\mathfrak{Z}$ as splitting field, and the group of classes $\{a_{S,T}\}$ of associated factor systems. By the construction in ğ 27 there is a one-to-one correspondence between $\{\mathfrak{K}\}$ and $\{a_{S,T}\}$; by 4 this correspondence is homomorphic, and hence is an isomorphism. In particular, the identity classes correspond:

The crossed product is equal to P, that is, is a matrix ring over the center, if and only if its factor system is associated with the identity system.

ğ 29. Principal Genus Theorem in the Minimal Case

Let $\mathfrak{K}_r = \mathfrak{Z} \cdot \mathfrak{G}$ be a crossed product, and let $\mathfrak{G}^*$ be the group of all elements that carry $\mathfrak{Z}$, as a whole, into itself by inner automorphisms (written as the cosets $\mathfrak{Z}^* u_E, \mathfrak{Z}^* u_S, \ldots$).

Definition. The "*principal genus in the minimal case*" $\mathscr{H}$ consists of all group automorphisms of $\mathfrak{G}^*$ that extend the identity on $\mathfrak{Z}^*$. The reason for this terminology appears upon specialization to cyclic fields; see ğ 30.

Theorem. *Every automorphism of the principal genus has the form* $u_S \mapsto u_S \cdot b^S b^{-1} = u_S b^{S-1}$, *where b lies in $\mathfrak{Z}$; conversely, every such assignment generates an automorphism of the principal genus.*

Proof. Suppose that the group automorphism sends $u_S \mapsto v_S$ and $z \mapsto z$ for every z in $\mathfrak{Z}$, while preserving products. It extends to a ring automorphism of $\mathfrak{K}_r$ by the assignment

$$\sum u_S c_{\lambda_S} \mapsto \sum v_S c_{\lambda_S},$$

where the c_{λ_S} lie in $\mathfrak{Z}$. Every such automorphism is known to be inner.

Let b be a generating element, so that $v_S = b u_S b^{-1}$ and $z = bzb^{-1}$. Since b commutes with every z, it lies in $\mathfrak{Z}$, and therefore

$$v_S = b u_S b^{-1} = u_S b^S b^{-1}.$$

Conversely, if $v_S = u_S b^S b^{-1}$, with b in $\mathfrak{Z}$, then $v_S = b u_S b^{-1}$. Thus we have an automorphism of $\mathfrak{K}_r$ that fixes $\mathfrak{Z}$ elementwise, and therefore carries $\mathfrak{G}^*$, by definition, into itself as a whole. It is consequently an automorphism of the principal genus.

ğ 30. Specialization to Cyclic Splitting Fields

Forming the crossed product specifically with a cyclic field $\mathfrak{Z}$ leads to interpretations of familiar norm theorems. First we have the following.

Theorem 1. *The group $\mathscr{K}_{\mathfrak{Z}}$ of the $\{\mathfrak{K}\}$ with fixed cyclic splitting field $\mathfrak{Z}$ over P is isomorphic to the group $P^*/N\mathfrak{Z}^*$, where $N\mathfrak{Z}^*$ is the group of all norms Nz of nonzero elements z of $\mathfrak{Z}$.*

Proof. The proof rests on normalizing the crossed representation and on several lemmas concerning it.

Definition. The cyclic crossed representation is called *normalized* if it has the form

$$\mathfrak{K}_r = \mathfrak{Z} + \mathfrak{Z}u + \cdots + \mathfrak{Z}u^{n-1},$$

with $zu = uz^S$ and $u^n = a$, where S is a generator of $\mathfrak{G}$. Thus one sets $u_{S^r} = u^r$, $r = 0, \ldots, n-1$, rather than, more generally, $u_{S^r} = b_r u^r$ with b_r in $\mathfrak{Z}$.

Lemma 1. *The cyclic crossed representation may always be assumed normalized. Here a lies in P, and every a in P gives such a representation.*

Proof. The first assertion is clear, since $u^{-1}zu = z^S$ implies $u^{-r}zu^r = z^{S^r}$, so that u^r generates the substitution $z \mapsto z^{S^r}$. Further, since u^n induces the identity $z \mapsto z^{S^n}$, we have $u^n = a$ with a in $\mathfrak{Z}$. But u^n commutes with all u^r; hence the same is true of a, and therefore $a^{S^r} = a$. Thus a lies in P.

Accordingly, a is the only essential multiplication constant. The associativity conditions therefore become vacuous: every a in P gives an associative system, and hence a $\mathfrak{K}_r$.

Lemma 2. *Instead of the full class $\{a_{S,T}\}$ of associated factor systems, it suffices to consider the normalized factor systems in that class, that is, those arising from normalized representations. This subset of the class will be called a normalized class. The group of full classes $\{a_{S,T}\}$ is isomorphic to the group of normalized classes.*

Proof. By Lemma 1, no normalized class is empty, so the correspondence is one-to-one. The operation is the old one, since it is defined using any representative.

Lemma 3. *The group of normalized factor systems is isomorphic to the multiplicative group P^*; the group of normalized classes is isomorphic to $P^*/N\mathfrak{Z}^*$.*

Proof. It follows from Lemma 1 that every normalized factor system has the form $[1, 1, \ldots, a, a, \ldots]$, since

$$u^\nu \cdot u^\mu = u^{\nu+\mu} \quad (\nu + \mu < n), \qquad u^\nu \cdot u^\mu = au^\varrho \quad (\nu + \mu = n + \varrho,\ 0 \le \varrho \le n-2).$$

The assignment

$$[1, \ldots, a, a, \ldots] \mapsto a, \qquad [1, 1, \ldots, b, b, \ldots] \mapsto b,$$
$$[1, \ldots, ab, \ldots] \mapsto ab$$

is a group isomorphism onto P^*, since, again by Lemma 1, a runs through all elements of P^*. Two associated normalized factor systems are obtained from one another by a transformation $v = uc$, with c in $\mathfrak{Z}$. This gives

$$v = uc, \qquad v^2 = u^2 \cdot c^S \cdot c;$$
$$v^r = u^r c^{S^{r-1}} c^{S^{r-2}} \cdots c; \qquad v^n = u^n N(c).$$

Thus $u^n = a$ implies $v^n = aN(c)$. A normalized class therefore consists of the factor systems $[1, \ldots, aN(c), aN(c), \ldots]$, where c runs through all nonzero elements of $\mathfrak{Z}$. This proves the second assertion of the lemma.

Theorem 1 now follows from Lemmas 2 and 3, together with the isomorphism between the $\{\mathfrak{K}\}$ occurring there and the classes $\{a_{S,T}\}$.

Theorem 2. *The group of the principal genus in the minimal case is isomorphic to the group of those elements c of $\mathfrak{Z}$ for which $N(c) = 1$. Thus $N(c) = 1$ implies the existence of a nonzero b in $\mathfrak{Z}$ such that $c = b^S \cdot b^{-1} = b^{S-1}$, the symbolic $(S-1)$-st power.*

Proof. The proof of Lemma 3 showed that $N(c) = 1$ is precisely the condition that the transformation $v = uc$ define an automorphism of the principal genus. Distinct c's correspond to distinct automorphisms and conversely, and products correspond to products.

Remark. Theorem 2 justifies the term principal genus. Correspondingly, one may call the quotient group

$$\mathfrak{Z}^*/\mathscr{H} \quad (\mathscr{H} = \text{principal genus}) \cong \mathfrak{Z}^*/\mathfrak{Z}^{*S-1}$$

the group of genera in the minimal case. This group is isomorphic to $N(\mathfrak{Z}^*)$; in conjunction with Theorem 1,

$$\begin{aligned}\text{group of genera in the minimal case} &= \mathfrak{Z}^*/\mathscr{H} \cong \mathfrak{Z}^*/\mathfrak{Z}^{*S-1} \cong N(\mathfrak{Z}^*)\\ &= \text{group of the } \{\mathfrak{K}\} \text{ belonging to } \mathfrak{Z} = \mathscr{K}_{\mathfrak{Z}} \cong P^*/N(\mathfrak{Z}^*).\end{aligned}$$

ğ 31. Applications of the Cyclic Special Case

The cyclic crossed representation gives new proofs of the theorems proved in ğ 20: every finite field is commutative, and apart from the quaternions there is no proper noncommutative field extension of the field of real numbers. These proofs might be described as class field theory in the minimal case.

1. Every field with finitely many elements is commutative (Theorem 10, ğ 20).

The proof rests on two familiar facts about finite commutative fields (Galois fields).

1. *Galois fields are cyclic over each of their subfields.*

2. *If $\mathfrak{Z}$ is a Galois field, hence cyclic over P, then every element of P is the norm of an element of $\mathfrak{Z}$: $P^* = N\mathfrak{Z}^*$.*

Now let $\mathfrak{K}$ be finite, P its center, and $\mathfrak{Z}$ a cyclic splitting field. By the conclusion of ğ 30 and by 1, the group $\mathscr{K}_\mathfrak{Z}$ of the $\{\mathfrak{K}\}$ belonging to $\mathfrak{Z}$ is isomorphic to $P^*/N\mathfrak{Z}^*$, and hence by 2 is equal to the identity $\{P\}$. This means that there is no field distinct from P with center P: $\mathfrak{K} = P$.

2. The only proper noncommutative field extension of the field P of real numbers is the quaternion field (Theorem 9, ğ 20).

Proof. The field P must be the center, since its only commutative extension is the field $\mathfrak{Z}$ of complex numbers, and, because $\mathfrak{Z}$ is algebraically closed, there is no noncommutative field extension having $\mathfrak{Z}$ as center. At the same time, only $\mathfrak{Z}$ can occur as a splitting field, and $\mathfrak{Z}$ is cyclic over P. Every positive number is a norm, so the group $P^*/N\mathfrak{Z}^*$ has order two. Apart from $\{P\}$, there is therefore just one class $\{\mathfrak{K}\}$, namely the quaternions. The normal form follows at once if one takes -1 as a normalized factor system in the associated class. Then $\mathfrak{K} = \mathfrak{Z} + \mathfrak{Z}u$, with $u^2 = -1$. Thus $\mathfrak{K} = P + Pi + (P + Pi)u$, with $i^2 = -1$, $u^2 = -1$.

Remark on 1. The familiar fact 2 can itself be proved from the conclusion of ğ 30 as follows. We have $\mathscr{H} = \mathfrak{Z}^{*S-1} \cong \mathfrak{Z}^*/P^*$, since all and only the elements of P^* induce the identity automorphism of the principal genus, or equivalently go to the identity under application of $S - 1$. Thus, when $\mathfrak{Z}$ is finite, the number of elements of $\mathscr{H}$ is the index of P^* in $\mathfrak{Z}^*$. Consequently the number of elements of $\mathfrak{Z}^*/\mathscr{H}$ equals that of P^*; the same therefore holds for $N(\mathfrak{Z}^*) = \mathfrak{Z}^*/\mathscr{H}$, and hence $P^* = N(\mathfrak{Z}^*)$. Compare: number of genera = number of ambiguous classes. In this number-theoretic terminology, however, "in the minimal case" must always be added.

3. *If P is a p-adic ground field and $\mathfrak{Z}$ is cyclic of degree n over P, then the group $\mathscr{K}_\mathfrak{Z}$ of the $\{\mathfrak{K}\}$ belonging to $\mathfrak{Z}$ is isomorphic to the Galois group of $\mathfrak{Z}$.*

By the conclusion of ğ 30, this is a direct consequence of "class field theory in the small," which says

$$P^*/N\mathfrak{Z}^* \simeq \mathfrak{G}.$$

Remark on 3. It follows that the group order of the elements of $\mathscr{K}_\mathfrak{Z}$, that is, the exponent of $\{\mathfrak{K}\}$, equals its index. For the exponent of a generator of $\mathscr{K}_\mathfrak{Z}$ is n, and so is its index, as a divisor of n and a multiple of the exponent. Thus $\mathscr{K}_\mathfrak{Z}$ contains only classes whose indices divide n and for which $\mathfrak{Z}$ is a splitting field. Going further, H. Hasse showed in Math. Ann. 104 that $\mathscr{K}_\mathfrak{Z}$ consists of all classes $\{\mathfrak{K}\}$ whose index divides n. Every cyclic splitting field $\mathfrak{Z}$ of degree n over a p-adic P therefore yields the same group $\mathscr{K}_\mathfrak{Z}$ of field classes $\{\mathfrak{K}\}$.

The two facts

1. the group of all $\{\mathfrak{K}\}$ over P whose index divides n is cyclic of degree n;

2. every cyclic splitting field of degree n over P generates the full group of the $\{\mathfrak{K}\}$,

may be regarded as the essential content of the converse theorem of local class field theory.

Necessary and Sufficient Multiplicity Conditions for Noether's Fundamental Theorem of Algebraic Functions

By Heinrich Kapferer in Freiburg im Breisgau
(With a supplement jointly with E. Noether in Göttingen.)
Math. Ann. 97 (1927), pp. 559–567

The following is a sharpening of Noether's fundamental theorem, in the form of necessary and sufficient multiplicity conditions.[1] Following the ideal-theoretic interpretation of the theorem,[2] but without using ideal-theoretic concepts or theorems here or below, I combine the complex of facts constituting Noether's fundamental theorem into the following two separate assertions.[3]

Theorem Ia. For every common zero $x = \alpha,\ y = \beta$ of two relatively prime polynomials φ, ψ in x, y, with arbitrary complex coefficients, there exists a least positive rational integer ϱ such that the module $(\varphi, \psi, p^\varrho)$ denotes exactly the same totality of polynomials as the module $(\varphi, \psi, p^\sigma)$, where $p = (x - \alpha, y - \beta)$ and σ is any rational integer greater than ϱ.[4]

Theorem Ib. Denote this conceptually uniquely determined totality of polynomials by q, or by q_i when the i-th of the s distinct zeros, $x = \alpha_i,\ y = \beta_i$, is in question. Then:

A necessary and sufficient condition for a given polynomial K in x, y to have the divisibility property $K \equiv 0(\varphi, \psi)$ is the simultaneous satisfaction of the following s congruences:

$$K \equiv 0(q_1), \quad K \equiv 0(q_2), \quad \ldots, \quad K \equiv 0(q_s).$$

Historically—compare the introduction to Max Noether's fundamental paper on this subject[5]—the fundamental theorem arose from attempts to solve the following basic problem: *given any polynomial K in x, y, one should be able to determine whether or not it is divisible by (φ, ψ)*; equivalently, whether there exist two further polynomials λ and μ in x, y such that

$$K = \lambda \cdot \varphi + \mu \cdot \psi$$

is an identity in x, y.

Noether's theorem does not solve this problem; rather, it must be regarded only as a *reduction*, albeit a fundamental one,[6] to the simpler question of necessary and sufficient conditions for each individual congruence $K \equiv 0(q)$. When does $K \equiv 0(q)$ hold? Only once this question has been answered is Max Noether's original problem settled. That is the aim of the present paper, and it is in fact attained by giving finitely many *multiplicity conditions, readily checkable in practice, that are necessary and sufficient for $K \equiv 0(q)$*. A sufficient, but not necessary, condition for $K \equiv 0(q)$ is familiar and frequently used and cited in the literature, roughly in the following form:

For the congruence $K \equiv 0(\varphi, \psi)$ to hold, it is *sufficient* that every intersection point of $\varphi = 0$ and $\psi = 0$ occur in the polynomial K with "sufficiently" high multiplicity.

This result is contained as a special case in Theorem I, since a point of multiplicity ϱ on K is equivalent to $K \equiv 0(p^\varrho)$; a fortiori, $K \equiv 0(\varphi, \psi, p^\varrho)$, that is, $K \equiv 0(q)$. The converse, however, is false.

The announced solution can be characterized briefly as follows. To each q one can associate a system of t *positive* rational integers $(g_1), (g_2), \ldots, (g_t)$, and to the module (K, q) an equally large number of *positive or negative* rational integers $(K_1), (K_2), \ldots, (K_t)$, such that the following *main theorem* holds.

Theorem II. *A necessary and sufficient condition for $K \equiv 0(q)$ is the simultaneous satisfaction of the t conditions*

$$(K_1) \geq (g_1), \quad (K_2) \geq (g_2), \quad \ldots, \quad (K_t) \geq (g_t).$$

Here

$$(g_1) + (g_2) + \cdots + (g_t) = \mu,$$

[1] For a detailed exposition I refer to my paper of the same title in the special issue of the *Heidelberger Akademie-Berichte*, 1927, "Beiträge zur Algebra," arranged by A. Loewy, Freiburg im Breisgau, and containing papers by various authors.

[2] See, for example, B. L. van der Waerden, "Zur Nullstellentheorie der Polynomideale," Math. Ann. 96 (1926), p. 203.

[3] In ğ 1 of the paper cited, I proved the two assertions separately and directly, that is, without ideal-theoretic concepts.

[4] The letters p and q were chosen to recall the substantive agreement of the objects denoted with the concepts of prime ideal p and primary ideal q customary in the more recent literature.

[5] Max Noether, "Über einen Satz aus der Theorie der algebraischen Funktionen," Math. Ann. 6 (1872).

[6] The reduction in question is comparable to the familiar one from elementary number theory: the divisibility of a natural number A by another such number B is equivalent to divisibility of A by $p_1^{a_1}$, by $p_2^{a_2}$, …, by $p_s^{a_s}$, where $p_1, p_2, \ldots, p_s$ are the distinct prime divisors of $B = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$. The concept of a "primary ideal"—denoted by q in the text—is precisely the analogue of a prime-power. See E. Noether, "Idealtheorie in Ringbereichen," Math. Ann. 83 (1921), Introduction.

where μ is the intersection multiplicity corresponding to q, as defined by the resultant.

For the proof, assume without loss of generality that the zero corresponding to q is $x = 0,\ y = 0$. In general, if $A(x, y)$ is any polynomial[7] in x, y, let the symbol (A) denote the number of times that y occurs as a factor in $A(0, y)$; if $A(0, y)$ vanishes identically, set $(A) = \infty$. The numbers $(g_1), (g_2), \ldots, (g_t)$ associated with q are defined by the following system of equations, which forms the methodological basis of the procedure:

$$\begin{aligned} f_1 \cdot g_1(0,y) : y^{(g_1)} - g_1 \cdot f_1(0,y) : y^{(g_1)} &= x \cdot h_1, \\ f_2 \cdot g_2(0,y) : y^{(g_2)} - g_2 \cdot f_2(0,y) : y^{(g_2)} &= x \cdot h_2, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots & \\ f_r \cdot g_r(0,y) : y^{(g_r)} - g_r \cdot f_r(0,y) : y^{(g_r)} &= x \cdot h_r. \end{aligned} \tag{1}$$

This system is constructed solely from the given pair of polynomials φ, ψ. The polynomials f_1, g_1 are defined to be identical with φ, ψ, apart possibly from their order, which is chosen so that $(f_1) \geq (g_1)$. Under this convention, and only then, h_1 is a polynomial.

The polynomials f_2, g_2 are defined to be identical with h_1, g_1, subject to $(f_2) \geq (g_2)$. In general, the pair f_r, g_r is defined to be identical with h_{r-1}, g_{r-1}, subject to $(f_r) \geq (g_r)$.

The system (1) can be continued indefinitely in the manner described, but the main theorem requires only its first t equations, where t is fixed by the following fact.

Lemma I. There exists a natural number t, in fact $t \leqq \mu$, where μ denotes the intersection multiplicity with which $x = 0,\ y = 0$ occurs in $\varphi = 0,\ \psi = 0$, such that the first t numbers defined by (1), namely $(g_1), (g_2), \ldots, (g_t)$, are all *greater than zero*, while (g_{t+1}) and every subsequent one are *zero*.

Indeed, taking account of the product theorem for resultants, the intersection multiplicity at $x = 0,\ y = 0$ of $f_r = 0,\ g_r = 0$ is

$$\mu - (g_1) - (g_2) - \cdots - (g_r),$$

which implies *termination after at most μ steps*. At the same time one obtains

$$\mu = (g_1) + (g_2) + \cdots + (g_t), \tag{2}$$

a noteworthy formula because, quite generally, it gives a rational and readily practicable method for determining the intersection multiplicity once the zero in question is known.

After the numbers (g_i) have thus been found, the numbers (K_i) are determined by the following system, corresponding to (1):

$$\begin{aligned} K_1 \cdot g_1(0,y) : y^{(g_1)} - g_1 \cdot K_1(0,y) : y^{(g_1)} &= x \cdot K_2, \\ K_2 \cdot g_2(0,y) : y^{(g_2)} - g_2 \cdot K_2(0,y) : y^{(g_2)} &= x \cdot K_3, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots & \\ K_r \cdot g_r(0,y) : y^{(g_r)} - g_r \cdot K_r(0,y) : y^{(g_r)} &= x \cdot K_{r+1}. \end{aligned} \tag{3}$$

The polynomial K_1 is defined to be identical with K. It is clear that K_2 is a polynomial if and only if $(K_1) \geq (g_1)$. If this is satisfied, K_3 is a polynomial if and only if $(K_2) \geq (g_2)$. In general, assuming that K_r is already a polynomial, K_{r+1} is a polynomial if and only if $(K_r) \geq (g_r)$.

The proof of the main theorem, Theorem II, now rests on the following further result.

Lemma II. Put $(f_i, g_i, p^e) = q^{(i)}$. Then for every i in the infinite sequence of integers $1, 2, \ldots$, the following holds:

For the congruence

$$K_i \equiv 0(q^{(i)}),$$

it is necessary and sufficient that the following two conditions be satisfied simultaneously:

$$(K_i) \geq (g_i) \quad \text{and} \quad K_{i+1} \equiv 0(q^{(i+1)}).$$

The proof[8] of the lemma results by combining the systems (1) and (3). By Lemma I, g_{t+1} no longer vanishes at the origin. Consequently the module $q^{(t+1)}$ consists of *all* polynomials, that is, it is the unit ideal, and $K_{t+1} \equiv 0(q^{(t+1)})$ becomes trivial. Applying Lemma II t times therefore proves the main theorem.

[7] If rational functions $C(x, y) : D(x, y)$ are also admitted for $A(x, y)$, then $(A) = (C) - (D)$; in that case (A) may therefore also take negative values.

[8] See also the proof in Remark I of the "Supplement."

Without proofs—which may be found in the paper cited above—I append two further consequences of the main theorem.

Supplement I. The number t in the main theorem is identical with the least[9] positive number ν such that

$$x^\nu \equiv 0(q).$$

Supplement II. The systems (1) and (3), together with the systems obtained by interchanging x and y, provide, when suitably combined, a rational method for the exact numerical determination of the exponent ρ "belonging" to q, that is, the minimal exponent ρ of Theorem Ia.

E. Bertini[10] gave a general formula for ρ. The cited paper shows, by the example $\varphi = x^3+y^4;\ \psi = x^2+y^3$, that this formula does not always give the minimal value of ρ. Finally, Bertini's formula itself can be established in a new way by means of our main theorem.

An interesting *specialization of the main theorem* follows from the additional assumption that the zero of $q = (\varphi, \psi, p^e)$ in question is a *simple* point of at least one of the two curves $\varphi = 0,\ \psi = 0$. If it is, for example, a simple point of ψ, then the number t of the main theorem can be shown to equal exactly μ, and the t inequalities of the main theorem may be replaced by a *single* multiplicity condition. This leads to the following general theorem.

Theorem III. If *all* intersection points of $\varphi = 0$ and $\psi = 0$ are *simple* points of ψ, then—assuming K relatively prime to ψ—a *necessary and sufficient* condition for the congruence $K \equiv 0(\varphi, \psi)$ is that K vanish at all these points, and in such a way that the intersection multiplicity for the pair $K = 0,\ \psi = 0$ is at each point *at least* as large as for the pair $\varphi = 0,\ \psi = 0$.

Theorem III is noteworthy for another special reason. The multiplicity condition it requires can be tested, independently of formula (2), which rests on (1), by finitely many *differentiations*. This is immediately clear upon recalling the following "theorem," which I stated in 1923.[11]

Let A and B be any two relatively prime polynomials in x, y, and let P be a common point *which is a simple point of* B. Then the multiplicity of this point as an intersection point equals a number μ if and only if the multiplicity of the same point for the pair of curves $A' = 0,\ B = 0$ is *exactly* $\mu - 1$, where

$$A' = \frac{\partial A}{\partial x} \cdot \frac{\partial B}{\partial y} - \frac{\partial A}{\partial y} \cdot \frac{\partial B}{\partial x}.$$

Finally, the main theorem, Theorem II, can with a slight modification also be transferred to homogeneous polynomials in three variables x, y, z. The transfer is particularly elegant in the special case above. Indeed, one can show:

Supplement to Theorem III. Theorem III remains completely unchanged, even in its wording, if φ, ψ, K are understood to be *homogeneous* polynomials in *three* variables.[12]

Supplement, Jointly with E. Noether[13]

The system (1) also gives a rational method for *determining a complete residue system modulo* q, by which is meant a complete system of representatives of the *finitely many* residue classes that are *linearly independent* modulo q, relative to the coefficient field P. This makes the individual steps in the proof of the main theorem very transparent; at the same time, as a secondary result, one obtains the fact that the *resultant multiplicity* μ *agrees with the length of the ideal* q,

---

[9] Thus the *exact* exponents are obtained here, in contrast to the estimates of Miss Grete Hermann, "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale" (using posthumous theorems of K. Hentzelt), Math. Ann. 95 (1926), where, for a much more general problem, only upper bounds are given.

[10] E. Bertini, Math. Ann. 34 (1889).

[11] H. Kapferer, "Über die Multiplizität der Schnittpunkte von zwei algebraischen Kurven," Jahresber. DMV 32 (1923).

[12] The question of the conditions for a homogeneous congruence in three variables $K(x, y, z) \equiv 0(\varphi(x, y, z), \psi(x, y, z))$ has also been the central question of an investigation by A. Ostrowski, "Über die Maxwellsche Erzeugung der Kugelfunktionen," Jahresber. DMV 33 (1925), although under highly specialized hypotheses. That note assumes that φ splits entirely into linear factors, that φ and K have the same degree, and that $\psi = x^2 + y^2 + z^2$. Since ψ is entirely free of singularities, the main theorem of Ostrowski's note may be regarded as a special case of our Theorem III.

[13] The ideal-theoretic interpretation is due to E. Noether; the underlying proof of (5) and (6) is due to H. Kapferer.

that is, with the rank of the residue-class ring, or the number of residue classes linearly independent over P.[14)]

Using the notation of (1) and Lemma II, the complete residue system is characterized by the following result.

Theorem IV. *A complete residue system modulo q is given by the polynomials*

$$h_t,\ h_t y, \ldots, h_t y^{(g_t)-1};\ \ldots;\ h_i,\ h_i y, \ldots, h_i y^{(g_i)-1};\ \ldots;\ h_1,\ h_1 y, \ldots, h_1 y^{(g_1)-1}.$$

For each i, the polynomials $h_i, h_i y, \ldots, h_i y^{(g_i)-1}$ form a complete residue system of $q^{(i+1)}$ modulo $q^{(i)}$.

It follows immediately from the definition that $q^{(i+1)} = (q^{(i)}, h_i)$, and hence $q^{(i)} \equiv 0(q^{(i+1)})$. Theorem IV will therefore be proved once it is shown that

$$h_i x \equiv 0(q^{(i)}); \qquad h_i y^{(g_i)} \equiv 0(q^{(i)}) \tag{4}$$

and

$$\text{from } h_i F(y) \equiv 0(q^{(i)}) \text{ it follows that } F(y) \equiv 0(y^{(g_i)}). \tag{5}$$

Relations (4) say that the linear combinations of $h_i, h_i y, \ldots, h_i y^{(g_i)-1}$ exhaust the residue classes of $q^{(i+1)}$ modulo $q^{(i)}$, while (5) expresses linear independence. Since $q^{(t+1)}$ is the unit ideal—which now follows from the finite length of q—this proves Theorem IV. It also shows that the length of q is $(g_1) + \cdots + (g_t)$, and hence by (2) agrees with the resultant multiplicity.

The first relation in (4) is read directly from (1); the second follows as follows.

We have $h_i g_i \equiv 0(q^{(i)})$, and hence, by the first relation in (4), also $h_i g_i(0, y) \equiv 0(q^{(i)})$, or $h_i y^{(g_i)} \cdot (g_i(0, y) : y^{(g_i)}) \equiv 0(q^{(i)})$. Since $g_i(0, y) : y^{(g_i)} \not\equiv 0(y)$, it follows that $h_i y^{(g_i)} \equiv 0(q^{(i)})$.

Before proving (5), we record a *remark* read directly from (1). The polynomials f_i and g_i can have as common divisor only a polynomial $d(y)$ in y that is not divisible by y: $f_i = d_i(y)\bar{f}_i$, $g_i = d_i(y)\bar{g}_i$, where $\bar{f}_i$ and $\bar{g}_i$ are relatively prime. Since $d_i(y) \not\equiv 0(p)$, we also have $q^{(i)} = (\bar{f}_i, \bar{g}_i, p^e)$. Moreover, for every $\sigma \geq \varrho$, this is equal to $(\bar{f}_i, \bar{g}_i, p^\sigma)$, as a divisor of q for every such σ. Thus $q^{(i)}$ is the primary component of $(\bar{f}_i, \bar{g}_i)$ belonging to the origin.

Let $\gamma_1, \delta_1; \ldots; \gamma_r, \delta_r$ be the zeros of $(\bar{f}_i, \bar{g}_i)$ distinct from $x = 0,\ y = 0$, and let $\tau_1, \ldots, \tau_r$ be the exponents of the corresponding primary components of $(\bar{f}_i, \bar{g}_i)$. In the product

$$P = ((x - \gamma_1) + u(y - \delta_1))^{\tau_1} \cdots ((x - \gamma_r) + u(y - \delta_r))^{\tau_r},$$

specialize the indeterminate u to an element of P in such a way that $P \not\equiv 0(p)$ remains true. Set $G(x, y)$ equal to the product of the specialized P with $d(y)$. Then $G(x, y) \not\equiv 0(p)$ and $q^{(i)} \cdot G(x, y) \equiv 0(f_i, g_i)$.

The assumption $h_i F(y) \equiv 0(q^{(i)})$ therefore gives $h_i F(y) G(x, y) \equiv 0(f_i, g_i)$, or, together with (1), the identities

$$h_i F(y) G = A f_i + B g_i; \qquad h_i x = (g_i(0, y) : y^{(g_i)}) \cdot f_i - (f(0, y) : y^{(g_i)}) g_i.$$

It follows that

$$\bar{f}_i(xA - F(y)H) \equiv 0(\bar{g}_i); \qquad H = G(x, y) \cdot g_i(0, y) : y^{(g_i)} \not\equiv 0(p).$$

Since $\bar{f}_i$ and $\bar{g}_i$ are relatively prime, we further obtain

$$xA - F(y)H \equiv 0(\bar{g}_i).$$

Thus $F(y)H \equiv 0(\bar{g}_i, x) \equiv 0(\bar{g}_i, x, p^\sigma) = (y^{(g_i)}, x)$, and hence $F(y) \equiv 0(y^{(g_i)})$. This proves (5), and therefore Theorem IV.

Remark I. Relations (4) and (5), together with Lemma II, may be written as reciprocal relations between ideal quotients,[15)] while the proof of the second relation also proves Lemma II:

$$q^{(i)} : q^{(i+1)} = (q^{(i)}, x) = (y^{(g_i)}, x); \qquad q^{(i)} : (q^{(i)}, x) = q^{(i+1)}.^{16)} \tag{6}$$

[14)] Without loss of generality the field P is assumed algebraically closed. To this extent all the preceding theorems, with the exception of the differentiation condition, remain valid. The length of q is also defined as the length of a composition series of ideals running from p to q. See E. Noether, Jahresber. DMV 34 (1925), p. 101 (oblique pagination); more fully, H. Grell, Math. Ann. 97 (1927), p. 529. The proofs in the literature for the agreement of the two multiplicities, for n variables, are very complicated; the simplest is the as yet unpublished posthumous proof of Hentzelt.

[15)] As usual, the quotient $\mathfrak{a} : \mathfrak{b}$ means the totality of polynomials $c(x, y)$ such that $\mathfrak{b}c \equiv 0(\mathfrak{a})$.

[16)] According to the general theory of irreducible ideals, either of these two reciprocal relations implies the other; see Macaulay, *Modular Systems*, nos. 72 and 73, Cambridge Tracts 19 (1916).

The first relation summarizes (4) and (5). As for the second, note that $x \cdot q^{(i+1)} \equiv 0(q^{(i)})$ was proved in (4); the converse is obtained analogously to (5). From $xM \equiv 0(q^{(i)})$ one obtains as above

$$xMG \equiv 0(f_i, g_i); \quad \text{hence} \quad xMG \cdot g_i(0,y) : y^{(g_i)} \equiv 0(xh_i, g_i).$$

Since $g_i \not\equiv 0(x)$ by definition—$(f_i) \geq (g_i)$—it follows that

$$M \cdot (G \cdot g_i(0,y) : y^{(g_i)}) \equiv 0(h_i, g_i) \equiv 0(q^{(i+1)}), \quad \text{and hence} \quad M \equiv 0(q^{(i+1)}).$$

The necessity of the condition in Lemma II now follows as follows. From $K_i \equiv 0(q_i)$ one gets $K_i(0,y) \equiv 0(y^{(g_i)}, x)$, hence $(K_i) \geq (g_i)$, and therefore, by (3),

$$xK_{i+1} \equiv 0(q^{(i)}); \quad \text{hence, by the second relation in (6)}, \quad K_{i+1} \equiv 0(q^{(i+1)}).$$

The sufficiency of the condition is read off immediately, and finitely many applications of Lemma II yield the main theorem. Likewise, iteration of the second relation in (6) gives Supplement I: namely $q : x^t = q^{(t+1)}$, the unit ideal, and t is the least such power because $q : x^{t-1} = q^{(t)}$.

Remark II. For a polynomial K not divisible by q, one can say further: if $K \equiv 0(q^{(i+1)})$ but $K \not\equiv 0(q^{(i)})$, then $(K, q^{(i)}) = (h_i y^{(K)}, q^{(i)})$. Indeed, by Theorem IV, $K \equiv h_i y^{\lambda} c(y)$ modulo $q^{(i)}$, with $c(y) \not\equiv 0(y)$; hence

$$(K, q^{(i)}) = (h_i y^{\lambda}, q^{(i)}).$$

Here $y^{(g_i)-\lambda} K \equiv 0(q^{(i)})$, and by (5) this is the least such power. By Lemma II, however, $(g_i) - (K)$ is this least power; hence $\lambda = (K)$.

(Received October 24, 1926.)

Bibliography

1. Über die Bildung des Formensystems der ternären biquadratischen Form.
   Sitz. Ber. d. Physikal.-mediz. Sozietät in Erlangen 39 (1907), pp. 176–179

2. Über die Bildung des Formensystems der ternären biquadratischen Form.
   J. Reine Angew. Math. 134 (1908), pp. 23–90 and one table

3. Zur Invariantentheorie der Formen von n Variabeln.
   J. Ber. d. DMV 19 (1910), pp. 101–104

4. Zur Invariantentheorie der Formen von n Variabeln.
   J. Reine Angew. Math. 139 (1911), pp. 118–154

5. Rationale Funktionenkörper.
   J. Ber. d. DMV 22 (1913), pp. 316–319

6. Körper und Systeme rationaler Funktionen.
   Math. Ann. 76 (1915), pp. 161–196

7. Der Endlichkeitssatz der Invarianten endlicher Gruppen.
   Math. Ann. 77 (1916), pp. 89–92

8. Über ganze rationale Darstellung der Invarianten eines Systems von beliebig vielen Grundformen.
   Math. Ann. 77 (1916), pp. 93–102. (See also no. 16)

9. Die allgemeinsten Bereiche aus ganzen transzendenten Zahlen.
   Math. Ann. 77 (1916), pp. 103–128. (See also no. 16)

10. Die Funktionalgleichungen der isomorphen Abbildung.
    Math. Ann. 77 (1916), pp. 536–545

11. Gleichungen mit vorgeschriebener Gruppe.
    Math. Ann. 78 (1918), pp. 221–229. (See also no. 16)

12. Invarianten beliebiger Differentialausdrücke.
    Nachr. v. d. Ges. d. Wiss. zu Göttingen 1918, pp. 37–44

13. Invariante Variationsprobleme.
    Nachr. v. d. Ges. d. Wiss. zu Göttingen 1918, pp. 235–257

14. Die arithmetische Theorie der algebraischen Funktionen einer Veränderlichen in ihrer Beziehung zu den übrigen Theorien und zu der Zahlkörpertheorie.
    J. Ber. d. DMV 28 (1919), pp. 182–203

15. Die Endlichkeit des Systems der ganzzahligen Invarianten binärer Formen.
    Nachr. v. d. Ges. d. Wiss. zu Göttingen 1919, pp. 138–156

16. Zur Reihenentwicklung in der Formentheorie.
    Math. Ann. 81 (1920), pp. 25–30

17. Jointly with W. Schmeidler: Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzenausdrücken.
    Math. Z. 8 (1920), pp. 1–35

18. Über eine Arbeit des im Kriege gefallenen K. Hentzelt zur Eliminationstheorie.
    J. Ber. d. DMV 30 (1921), p. 48

19. Idealtheorie in Ringbereichen.
    Math. Ann. 83 (1921), pp. 24–66

20. Ein algebraisches Kriterium für absolute Irreduzibilität.
    Math. Ann. 85 (1922), pp. 26–33

21. Formale Variationsrechnung und Differentialinvarianten.
Encyklopädie d. math. Wiss. III, 3 (1922), pp. 68–71 (in R. Weitzenböck, *Differentialinvarianten*)

22. Edition of K. Hentzelt †: Zur Theorie der Polynomideale und Resultanten.
Math. Ann. 88 (1923), pp. 53–79

23. Algebraische und Differentialvarianten.
J. Ber. d. DMV 32 (1923), pp. 177–184

24. Eliminationstheorie und allgemeine Idealtheorie.
Math. Ann. 90 (1923), pp. 229–261

25. Eliminationstheorie und Idealtheorie.
J. Ber. d. DMV 33 (1924), pp. 116–120

26. Abstrakter Aufbau der Idealtheorie im algebraischen Zahlkörper.
J. Ber. d. DMV 33 (1924), p. 102

27. Hilbertsche Anzahlen in der Idealtheorie.
J. Ber. d. DMV 34 (1925), p. 101

28. Gruppencharaktere und Idealtheorie.
J. Ber. d. DMV 34 (1925), p. 144

29. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p.
Nachr. v. d. Ges. d. Wiss. zu Göttingen 1926, pp. 28–35

30. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern.
Math. Ann. 96 (1927), pp. 26–61

31. Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl- oder Funktionenkörpers.
J. Reine Angew. Math. 157 (1927), pp. 82–104

32. Jointly with R. Brauer: Über minimale Zerfällungskörper irreduzibler Darstellungen.
Sitz. Ber. d. PreuSS. Akad. d. Wiss. 1927, pp. 221–228

33. Hyperkomplexe GröSSen und Darstellungstheorie in arithmetischer Auffassung.
Atti Congresso Bologna 2 (1928), pp. 71–73

34: Hyperkomplexe GröSSen und Darstellungstheorie.
Math. Z. 30 (1929), pp. 641–692

35. Über Maximalbereiche aus ganzzahligen Funktionen.
Rec. Soc. Math. Moscou 36 (1929), pp. 65–72

36. Idealdifferentiation und Differente.
J. Ber. d. DMV 39 (1930), p. 17

37. Normalbasis bei Körpern ohne höhere Verzweigung.
J. Reine Angew. Math. 167 (1932), pp. 147–152

38. Jointly with R. Brauer and H. Hasse: Beweis eines Hauptsatzes in der Theorie der Algebren.
J. Reine Angew. Math. 167 (1932), pp. 399–404

39. Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und zur Zahlentheorie.
Verhandl. Intern. Math.-KongreSS Zürich 1 (1932), pp. 189–194

40. Nichtkommutative Algebren.
Math. Z. 37 (1933), pp. 514–541

41. Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper.
Math. Ann. 108 (1933), pp. 411–419

42. Zerfallende verschränkte Produkte und ihre Maximalordnungen.
Actualités scientifiques et industrielles 148 (1934), 15 pp.

43. Idealdifferentiation und Differente.
J. Reine Angew. Math. 188 (1950), pp. 1–21

Notwendige und hinreichende Multiplizitätsbedingungen zum Noetherschen Fundamentalsatz der algebraischen Funktionen, by H. Kapferer
(With a supplement jointly with E. Noether.)
Math. Ann. 97 (1927), pp. 559–567

List of Short Communications and Book Reviews by Emmy Noether

Short communications published in the Jahresberichte der Deutschen Mathematiker-Vereinigung

Über Invarianten beliebiger Differentialausdrücke, 27, Part II (1918), p. 28
Invariante Variationsprobleme, 27, Part II (1918), p. 47
Endlichkeit ganzzahliger binärer Invarianten, 28, Part II (1919), p. 29
Über ganzzahlige Polynome und Potenzreihen, 28, Part II (1919), pp. 29–30
Zerlegungssätze der Modultheorie, 29, Part II (1920), p. 54
Elementarteile und allgemeine Idealtheorie, 30, Part II (1921), p. 32
Hinweis auf eine Formel von Lipschitz, 30, Part II (1921), p. 48
Das Analogon eines Hilbertschen Satzes in der allgemeinen Idealtheorie, 32, Part II (1923), pp. 20–21
Gruppentheoretische Bemerkungen zum Problem der Axiomatik, 33, Part II (1925), p. 21
Galoissche Theorie in beliebigen Körpern, 33, Part II (1925), p. 120
Hilbertsche Anzahlen in der Idealtheorie, 34, Part II (1926), p. 101
Differentialquotienten von Idealen und Verzweigungstheorie, 38, Part II (1929), p. 81

Book reviews published in the Jahresberichte der Deutschen Mathematiker-Vereinigung

E. Study, *Einleitung in die Theorie der Invarianten linearer Transformationen auf Grund der Vektorenrechnung*. Part I. (Die Wissenschaft, vol. 71.) Braunschweig, 1923, Vieweg.
36, Part II (1927), p. 71

Leopold Kroneckers Werke, vol. 4. Edited by K. Hensel. VI + 509 pp. Leipzig and Berlin, 1929, B. G. Teubner.
40, Part II (1931), pp. 11–12

Leopold Kroneckers Werke, vol. 5. Edited by K. Hensel. 527 pp. Leipzig and Berlin, 1930, B. G. Teubner.
41, Part II (1932), p. 17

Leopold Kroneckers Werke, vol. III.2. Edited by K. Hensel. 215 pp. Leipzig and Berlin, 1931, B. G. Teubner.
42, Part II (1933), pp. 38–39

D. E. Rutherford, *Modular Invariants*. Cambridge Tracts no. 27. Cambridge, 1932, VII + 84 pp.
43, Part II (1934), pp. 94–95

R. Dedekind, *Gesammelte mathematische Werke*, vols. I–III. Edited by R. Fricke, Emmy Noether, and Øystein Ore. Vieweg, Braunschweig, 1930–1932
(vol. I: 1930; II: 1931; III: 1932)

G. Cantor, *Briefwechsel mit R. Dedekind*. Edited by Emmy Noether and J. Cavaillès, 60 pp. Actualités scient. et ind. 581, Paris, 1937