Lecture Notes Algebra I - Commutative Algebra[1]

Ayushi Tsydendorzhiev

October 11, 2024

[1] Held by Dr. Andreas Mihatsch at University of Bonn in summer 2023.

These are my notes for the Algebra I class. Regretfully, I'm not very good at math and these notes will be at times lengthy and/or wrong. But, well, over time I found that the best way for me personally to learn was to write everything down and explain it to myself. Maybe one day someone else will find it useful.

Contents

1 Intro to Commutative Algebra

1.1 Rings and Ideals

In these lecture notes, a ring is always commutative and unitary (has element 1).

Definition 1.1. **Ideal** $\mathfrak{a}$ = abelian subgroup, such that $\forall r \in R, a \in \mathfrak{a} : ra \in \mathfrak{a}$.

Definition 1.2. Let $S \subseteq A$ be a subset of A. Then the **ideal, generated by** S is defined as

$$(S) := \bigcap_{\substack{S \subseteq \mathfrak{a} \subseteq A \\ \mathfrak{a} \text{ is an ideal}}} \mathfrak{a}$$

Could it be a closure operator on sets?

Lemma 1.3 (Equivalent to definition 1.2)**.** Let A be a ring, and let $S \subseteq A$ be a subset. Then we have

$$(S) = \sum_{s \in S} As = \{\sum a_s s \mid a_s \in A \text{ and finitely many } a_s \neq 0\}$$

Proof: Let $\mathfrak{b}$ be the right-hand side. It is an additive subgroup, since

$$(\sum_{s \in S} a_s s)^{-1} = \sum_{s \in S} a_s^{-1} s \in \mathfrak{b}$$

and

$$\sum_{s \in S} a_s s + \sum_{s \in S} b_s s = \sum_{s \in S} (a_s + b_s) s \in \mathfrak{b}.$$

It is also closed under multiplication, thus $\mathfrak{b}$ is an ideal. Since $1s \in \mathfrak{b}$ it follows $S \subseteq \mathfrak{b}$ and hence by definition $(S) \subseteq \mathfrak{b}$.

Conversely, let $\mathfrak{a} \subseteq A$ be an ideal such that $S \subseteq \mathfrak{a}$. Then from the ideal properties we get $as \in \mathfrak{a}$ for all $s \in S$ and thus $\sum_{s \in S} a_s s \in \mathfrak{a}$ for lal finite sums. Therefore $\mathfrak{b} \subseteq \mathfrak{a}$ and finally $\mathfrak{b} \subseteq S$.

Definition 1.4. Given any ring A, we can construct **polynomial rings** $A[T]$ as formal sums over A in a single variable T:

$$A[T] := \oplus_{i=0}^{\infty} AT^i = \{\sum_{i=0}^{n} a_i T^i \mid n \geq 0, a_i \in A, a_n \neq 0\}.$$

Definition 1.5. Given a ring A and an ideal $\mathfrak{a} \subseteq A$, the additive abelian quotient group $A/\mathfrak{a}$ endowed with the multiplication

$$(a + \mathfrak{a})(b + \mathfrak{a}) := ab + \mathfrak{a}$$

forms a ring which we call a **quotient ring** of A.

Definition 1.6. Let A be a ring, then

1. $x \in A$ is **nilpotent**, if $x^n = 0$ for some $n \in \mathbb{N}$. A is **reduced** if 0 is the only nilpotent element.
2. $x \in A$ is a **zero divisor**, if there exists $y \in A$ such that $xy = 0$. A is an integral domain if 0 is the only zero divisor and $A \neq 0$.
3. $x \in A$ is a **unit**, if there exists $y \in A$ such that $xy = 1$. The set of all units in A is denoted by $A^\times$ and forms a multiplicative group.

Math consists of learning vocabularies.

Integral domains are always reduced. On the other hand, $Z[X,Y]/(XY)$ is reduced but not integral.

Lemma 1.7. Consider a map $\phi : A \to A, a \mapsto xa$ for a fixed $x \in A$. It follows that ϕ bijective $\iff$ ϕ surjective $\iff$ $x \in A^\times$.

Proof: ϕ bijective implies ϕ surjective. ϕ surjective implies $\exists a \in A : xa = 1 \implies x$ is a unit $\implies x \in A^\times$. Conversely, $x \in A^\times \implies \exists a \in A : xa = 1 \implies \forall b \in A : xab = 1b = b \implies xa = 1 = xa' \iff a = a' \implies \ker \varphi$ is trivial.

Lemma 1.8. If A is reduced then $A[T_i, i \in I]$ is reduced as well for any index set I.

Definition 1.9. Let A be a ring. Define **nilradical** of A

$$\operatorname{nil}(A) = \{a \in A \mid a \text{ nilpotent}\}.$$

Proposition 1.10 (Properties of nilradical)**.**

1. $\operatorname{nil}(A)$ is an ideal,
2. $A/\operatorname{nil}(A)$ is reduced,
3. **Universal property of nilradicals:** For any reduced ring B, any ring map $\phi : A \to B$ factors through $A/\operatorname{nil}(A)$.

Kernels are ideals; nilradicals are ideals too. If the codomain ring is reduced then $\operatorname{nil}(A) \subseteq \ker(\varphi)$. So dimension has to do with certain properties of "flatness".

Proof:

1. Let $a, b \in \operatorname{nil}(A) \implies a^n = 0$. Then $\forall x \in A : (xa)^n = x^n a^n = 0$. Furthermore, $(a+b)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^{n+m-1} y^i = 0$, since either $(n+m-1-i) \geq n$ or $i \geq m$.
2. Let $\overline{x} = x + \operatorname{nil}(A)$. Then $\overline{x}$ is nilpotent iff $x \in \operatorname{nil}(A) \implies \overline{x} = 0$.
3. Let B be reduced and let $\varphi : A \to B$ be a ring map. If $x^n = 0$ for $x \in \operatorname{nil}(A)$, then $\varphi(x)^n = 0$, so $\varphi(x) = 0$ since B is reduced. In other words, $\operatorname{nil}(A) \subseteq \ker(\varphi)$, hence $\ker(\varphi)$ factors through $A/\operatorname{nil}(A)$ according to the universal property of the quotients.

1.2 *Fields*

This chapter was very light on content.

Definition 1.11. A ring A is a field if $A \neq 0$ and $A^\times = A \setminus \{0\}$.

Non-zero and all elements are invertible.

Lemma 1.12. A is a field $\iff$ the only ideals are $\{0\}$ and A.

Definition 1.13. An ideal $\mathfrak{m}$ is **maximal** if $\mathfrak{m} \neq A$ and there is no ideal $\mathfrak{a}$ such that $\{0\} \subset \mathfrak{a} \subset \mathfrak{m}$.

Corollary 1.14. Let A be a ring. An ideal $\mathfrak{m}$ is maximal $\iff$ $A/\mathfrak{m}$ is a field.

1.3 *Principal ideal domains*

Definition 1.15. An integral domain A is a **principal ideal domain** (PID) if every ideal $\mathfrak{a} \subset A$ is **principal**, i. e. of the form $\mathfrak{a} = (f)$ for some $f \in A$.

$\mathbb{C}[\varepsilon]/(\varepsilon^2)$ is not an integral domain, but every ideal is principal (there are only three).

Definition 1.16. A ring is a **principal ideal ring** if every ideal is principal.

Definition 1.17. Let A be an integral domain. Then $p \in A$ is **prime** if p is not the zero element or not a unit and $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Theorem 1.18. In PIDs, prime factorization theorem holds.

In unique factorization domains factorization in **irreducible** elements holds. The condition of being a prime element is stronger then being irreducible. For example, 3 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

1.4 *Power series*

Definition 1.19. Let A be a ring. Then

$$A[\![T]\!] := \{\text{infinite series } \sum_{i=0}^{\infty} a_i T^i \mid a_i \in A\} \cong A^{\mathbb{Z}_{\geq 0}}.$$

Proposition 1.20. Let A be a ring. Then $f \in A[\![T]\!]^\times$ if and only if $a_0 \in A^\times$.

Exercise 1.21. Show that a prime $p \neq 3$ is of the form $p = x^2 - xy + y^2$ iff $p \equiv 1 \pmod 3$.

Proof: Observe that $p \equiv x^2 - xy + y^2 \equiv x^2 + 2xy + y^2 \mod 3$. This implies $p \equiv (x+y)^2 \mod 3$. The quadratic residue classes $\mod 3$ are $0^2 = 0, 1^2 = 1, 2^2 = 1$, which implies either $p = 3$ or $p \equiv 1 \mod 3$.

Goal: Now the hard part. We want to look at fibers of map

$$\begin{aligned} \mathrm{Spec}(\varphi) : \mathrm{Spec}(\mathbb{Z}[\zeta]) &\longrightarrow \mathrm{Spec}(\mathbb{Z}) \\ \mathfrak{a} &\longmapsto \varphi^{-1}(\mathfrak{a}) \end{aligned}$$

I'm not sure what exactly this map is. I think it's the inclusion map, e. g. it maps $\mathfrak{m}$ to (p) such that $(p) \subseteq \mathfrak{m}$. In a sense $\mathbb{Z}[\zeta]$ has a certain "torsion" which allows for bigger, stronger maximal ideals than in $\mathbb{Z}$.

We know that for any $\mathfrak{m} \in \mathrm{Spec}(\mathbb{Z}[\zeta])$, the intersection $\mathfrak{m} \cap \mathbb{Z} = (p)$. Specifically for $\mathbb{Z}[\zeta]$, we know $\mathbb{Z}[\zeta_3] \cong \mathbb{Z}[T]/(T^2+T+1)$ because minimal polynomial of ζ is $m_\zeta = T^2 + T + 1$.

Prime Ideals: Given $\mathbb{Z}[T]/(T^2+T+1)$, what prime ideals can exist there? The answer is partially known. It's either (p) for p prime, or (p, h_i) for h_i lift of an irreducible factor of T^2+T+1. So we should think hard about the question of irreducibility of m_ζ.

Irreducibility of m_ζ: If $p = 3$, then

$$\begin{aligned} \{\mathfrak{m} \subset \mathbb{Z}[T]/(m_\zeta) \mid \mathfrak{m} \cap \mathbb{Z} = (3)\} &= \{\mathfrak{m} \subset A \mid (3) \subseteq \mathfrak{m}\} \\ &= \mathrm{Spec}(\mathbb{Z}[T]/(m_\zeta)) \big/ (3)) \\ &= \mathrm{Spec}(\mathbb{Z}[T]/(m_\zeta, 3) \\ &= \mathrm{Spec}(\mathbb{F}_3[T] \Big/ (m_\zeta \mod (3))) \\ &= \{(h_i) \mid \text{ irreducible factors } h_i \in \mathbb{F}_3[T] \text{ of } m_\zeta\} \\ &= \{(p, \widetilde{h}_i) \mid \widetilde{h}_i = \text{ lift of } h_i \text{ to } \mathbb{Z}[T]\}. \end{aligned}$$

What kind of lift? Basically we remember something along the lines of the 3rd isomorphism theorem, stating

$$\frac{A/\mathfrak{m}}{\mathfrak{m}/(p)} = \frac{A}{(p)},$$

but in this case it's more of

$$\frac{A/\mathfrak{m}}{(p)} = \frac{A/(p)}{\mathfrak{m}/(p)}.$$

This schema works for any p, so essentially we are interested in factorizations of m_ζ over any $\mathbb{F}_p[T]$. By a straight-forward calculation, have $\mathfrak{m}_\zeta = (T+2)^2$.

If m_ζ is irreducible, then the fiber is given by (p) only, since $\mathbb{F}_p[T]/(m_\zeta)$ is a field.

If $p \equiv 1 \mod (3)$ then $\mathbb{F}_p^\times$ has order $p - 1$ and as such has a non-trivial third root of unity if and only if $3 \mid (p-1)$. This obviously holds, which means $\mathfrak{m}_\zeta = (T-\alpha)(T-\alpha^2)$.
This property doesn't hold if $p \equiv 2 \mod 3$, implying $\mathfrak{m}_\zeta$ irreducible, otherwise it wouldn't be minimal.
Summarizing the above, have

$$\mathrm{Spec}(\mathbb{Z}[\zeta]) = \coprod_{0 \text{ or } p \text{ prime}} \begin{cases} (0) & \\ (3, \zeta+2) & \text{p=3} \\ (p, \zeta-\alpha), (p, \zeta-\alpha^2) & p \equiv 1 \mod (3) \\ (p) & p \equiv 2 \mod (3) \end{cases}$$

Is 0 even prime?

Now observe that $\mathbb{Z}[\zeta]$ is a PID. Let $(\pi) \in \mathrm{Spec}(Z[\zeta])$ with π prime. Now skipping some computations we claim $\pi = p$ by norm function and unique decomposition theorem, which implies $\pi = x + iy \in \mathbb{Z}[\zeta]$ such that $N(\pi) = x^2 - xy + y^2 = p$.

Basically the whole trick is: observe that norm $N(x)$ defined on $Z[\zeta]$ has some nice formula such as $x^2 + ny$. Since maximal ideals in $\mathbb{Z}$ correspond to prime numbers, we can try to extend $\mathbb{Z}$ such that these prime ideals are generated by some "smaller" elements, such that its norm equals precisely to p. By the virtue of our coordinates being integer we prove the claim.

Exercise 1.22. Let A be a principal ideal domain that is not a field, let $\mathfrak{m} \subset A$ be a maximal idea. Prove that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is a one-dimensional vector space over $A/\mathfrak{m}$ for any $n \geq 0$.

Proof: That's a lot to unpack. Start with definition for $\mathfrak{m}^n/\mathfrak{m}^{n+1}$.

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} = (a)^n/(a)^{n+1}$$

where a is generator of $\mathfrak{m}$. As such, any element in $(a)^n$ is of the form $ca^n, c \in A$. Now if we look at the quotient as if it were a graded ring, "going up" one degree to a^{n+1} annihilates element to 0, which happens precisely if you multiply by some element $x \in (a) \implies (a) \cdot (a)^n = 0 \in {(a)^n}/{(a)^{n+1}}$. So it's natural to describe $(a)^n$ as a one-dimensional vector space over $A/(a)$. If A is a field then $\mathfrak{m} = (0)$ and as such it is 0-dimensional over A.

This is what *associated graded ring* does. Essentially it's a direct sum $\bigoplus_{n=0}^{\infty}(a)^n/(a)^{n+1}$.

Exercise 1.23. Compute all fibres of $\mathrm{Spec}(\mathbb{Z}[T]) \to \mathrm{Spec}(\mathbb{Z})$.

Proof: Assume that $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime $p \in \mathbb{Z}$. Then $\overline{\mathfrak{p}} := \mathfrak{p}/p\mathbb{Z}[T]$ is a prime ideal in $\mathbb{F}_p[T]$. Since $\mathbb{F}_p[T]$ is a PID, $\overline{\mathfrak{p}} = (\overline{f}) \in \mathbb{F}_p[T]$. Hence we have

This part we've already seen.

- $\mathfrak{p} = (p)$ if $p = 0$,
- $\mathfrak{p} = (p, f)$ if $\overline{\mathfrak{p}} = (\overline{f})$, where f is any lift of $\overline{f} = f \mod p$.

Assume $\mathfrak{p} \cap \mathbb{Z} = (0)$. Consider $\mathfrak{q} = \mathfrak{p}\mathbb{Q}[T]$, i. e. the ideal in $\mathbb{Q}[T]$ generated by elements in $\mathfrak{p}$. We claim that $\mathfrak{q}$ is a prime ideal in $\mathbb{Q}[T]$.

This part we haven't seen. It uses localization.

If $\mathfrak{q}$ isn't prime and $1 \in \mathfrak{q}$, then we can write $1 = \sum f_i a_i$ with $f_i \in \mathbb{Q}[T], a_i \in \mathfrak{p}$. Let $0 \neq m \in \mathbb{Z}$ be the common denominator of all coefficients of all $f_i \in \mathbb{Q}[T]$. Then $mf_i \in \mathbb{Z}[T]$ for all $i = 1, \ldots, n$, hence $m1 = \sum(mf_i)a_i \in \mathfrak{p}$ which yields the contradiction with $\mathfrak{p} \cap \mathbb{Z} = (0)$. This means $1 \notin \mathfrak{q}$ and thus $\mathfrak{q} \neq \mathbb{Q}[T]$.

The $\mathfrak{q} \neq \mathbb{Q}[T]$ part.

Let $gh \in \mathfrak{q}$ for some $g, h \in \mathbb{Q}[T]$. Then we can write $gh = \sum f_i a_i$ with $f_i \in \mathbb{Q}[T]$ and $a_i \in \mathfrak{p}$. Now choose common denominator $0 \neq m \in \mathbb{Z}$ such that $mg, mh, mf_i \in \mathbb{Z}[T]$. Then we lift g and h to $\mathbb{Z}$ and observe

The $\mathfrak{q}$ is prime part.

$$mg \cdot mh = m \sum \underbrace{(mf_i)}_{\in \mathbb{Z}[T]} \underbrace{a_i}_{\in \mathfrak{p} \subseteq \mathbb{Z}[T]} \in \mathfrak{p}$$

and by the prime ideal property either $mf \in \mathfrak{p}$ or $mg \in \mathfrak{p}$. Multiplying by $m^{-1} \in \mathbb{Q}$, we get either $g \in \mathfrak{q}$ or $h \in \mathfrak{q}$, implying that $\mathfrak{q}$ is prime.

Since $\mathbb{Q}[T]$ is a PID, we can write $\mathfrak{q} = (h)$ for some irreducible $h \in \mathbb{Q}[T]$. We can lift it to some $mh \in \mathbb{Z}[T]$. Further factoring out the gcd of all coefficients, we can assume that mh is primitive. From *Gauss's lemma* it follows: if $mh \in \mathbb{Z}[T]$ is primitive and $f \in \mathbb{Z}[T]$, then $mh \mid f$ in $\mathbb{Z}[T]$ iff $mh \mid f$ in $\mathbb{Q}[T]$.

In other words: if a primitive polynomial mh divides polynomial f in $\mathbb{Z}[T]$, it does so in $\mathbb{Q}[T]$.

As a consequence, we have $\mathfrak{q} \cap \mathbb{Z}[T] = (h) \in \mathbb{Z}[T]$ with irreducible and primitive h. Later we show $\mathfrak{q} \cap \mathbb{Z}[T] = \mathfrak{p}$.

Note 1.24. What do we actually do here? At first, we look at the intersection between $\mathbb{Z}[T]$ and the smaller ring $\mathbb{Z}$. We find out it's empty (zero). What do we do know? We investigate the bigger fraction field of $\mathbb{Z}[T]$, its localization at 0 and look at what kind of ideal does $\mathbb{Q}[T]\mathfrak{p}$ generate. In some sense since our first, superficial method didn't work we localize around 0 and dig deeper at what does $\mathfrak{p}$ actually generate there. From there on we find out that $\mathbb{Q}[T]\mathfrak{p}$ generates another prime ideal $\mathfrak{q}$, which is generated by a single element $h \in \mathbb{Q}[T]$. By Gauss's lemma (sheer luck) this element also is in $\mathbb{Z}[T]$, implying $\mathfrak{p} = (h)$. Insane, right? At first, we know nothing about prime ideals. But we know about their images in $\mathbb{Z}$. And this information is enough to hunt them down in two different realms.

Exercise 1.25. Assume A is Noetherian. Prove $A[[T]]$ is Noetherian (Hilbert's Basis Theorem).

Noetherian property is stable by passage to finite type extensions and localization.

Proof: As a reminder, Noetherian $\iff$ every ideal is finitely generated. Let $\mathfrak{a} \in A[[T]]$ be a ideal. We show $\mathfrak{a}$ is finitely generated. For each integer n, denote

$$I_n = \{a \in A \mid f = ax^n + \textit{higher order terms} \in \mathfrak{a}\} \in A$$

Then we see that $I_0 \subset I_1 \subset \ldots$ stabilizes, as A is Noetherian. Choose d_0 such that $I_{d_0} = I_{d_0+1} = \ldots$ For each $d \leq d_0$ choose elements

$$f_{d,j} \in I \cap (T^d) \qquad j = 1 \ldots n_d$$

such that if we write $f_{d,j} = a_{d,j}T^d + \textit{higher order terms}$ then $I_d = (a_{d,1} \ldots a_{d,n_d})$.

Example: Let $d_0 = 10$. Then we have

$$I_0 \subset I_1 \subset \ldots \subset I_{10} = I_{11} = I_{12} = \ldots$$

Now choose

$j =$	1	2	3	4	5	6	7	8	9	10
$f_{0,j}$	1	2	3	4	5	6	7	8	9	10
$f_{1,j}$	1	2	3	4	5	6	7	8	9	10
$f_{2,j}$	1	2	3	4	5	6	7	8	9	10
$f_{3,j}$	1	2	3	4	5	6	7	8	9	10
$f_{4,j}$	1	2	3	4	5	6	7	8	9	10
$f_{5,j}$	1	2	3	4	5	6	7	8	9	10
$f_{6,j}$	1	2	3	4	5	6	7	8	9	10
$f_{7,j}$	1	2	3	4	5	6	7	8	9	10
$f_{8,j}$	1	2	3	4	5	6	7	8	9	10
$f_{9,j}$	1	2	3	4	5	6	7	8	9	10
$f_{10,j}$	1	2	3	4	5	6	7	8	9	10

2 *Intro to Homological Algebra*

In this chapter, M, N, P are A-modules.

2.1 *Preliminaries & Motivation*

Definition 2.1. A map $f : M \times N \to P$ is **bilinear**, if it is linear in each variable separately. $\forall a \in A, m, m' \in M, n, n' \in N :$

- $f(m, n + n') = f(m, n) + f(m, n')$
- $f(m, an) = af(m, n)$
- $f(m + m', n) = f(m, n) + f(m', n)$
- $f(am, n) = af(m, n)$

Linear maps are completely determined by their action on bases. How can we determine bilinear maps? For free modules it is enough to know their action on all pairs (v_i, w_j), where v_i and w_j are basis vectors for M and N. We would gladly extend this case to the bilinear case.

If we were to take the basis of $V \times W$, for example $\mathbb{R} \times \mathbb{R}$, then knowing the action of f on $(1, 0)$ and $(0, 1)$ is not enough, since $f(1, 0) = f(1, 0 + 0) = f(1, 0) + f(1, 0) \implies f(1, 0) = 0$. Turns out the most general way to map linear maps to bilinear maps is by mapping (v, w) to $v \otimes w$.

2.2 Tensor Product

Definition 2.2. For any two M, N define a pair

$$(A\text{-module } T, \text{bilinear map } g : M \times N \to T)$$

as **the tensor product** of M and N over A, if it has the following property:

Given any P and any A-bilinear mapping $f : M \times N \to P$, there exists a unique A-linear mapping $f' : T \to P$ such that $f = f' \circ g$. It always exists and is unique.

In other words, we have a bijection $\{\text{bilinear maps } M \times N \to P\} \longleftrightarrow \{\text{linear maps } M \otimes N \to P\}$.

Exercise 2.3. Show $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$

Proof:

Step 1: Fix $p \in P$, define $\phi_p : M \times N \longrightarrow M \otimes (N \otimes P), (m, n) \longrightarrow m \otimes (n \otimes p)$. This map is bilinear. It induces a linear map $\overline{\phi_p} : M \otimes N \to M \otimes (N \otimes P)$.

Step 2: Consider the induced map $\overline{\phi_p}$. It is linear in p, meaning $\overline{\phi_{p+p'}} = \overline{\phi_p} + \overline{\phi_{p'}}$, $\overline{\phi_{ap}} = a\overline{\phi_p}$.

Step 3: Since the above is true for all $p \in P$, consider bilinear maps

$$(M \otimes N) \times P \to M \otimes (N \otimes P)$$

which sends

$$\left[\left(\sum_i m_i \otimes n_i\right), p\right] \longrightarrow \overline{\varphi_p}(\sum_i m_i \otimes n_i)p$$

It induces a linear map

$$(M \otimes N) \otimes P \to M \otimes (N \otimes P)$$

And we're done?

Theorem 2.4. Important equivalences for modules over A

- $A \otimes_A M \cong M$,
- $M \otimes N \cong N \otimes M$,
- $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$,
- $(\bigoplus_{i \in I} M_i) \otimes N \cong \bigoplus_{i \in I}(M_i \otimes N)$,
- $A/\mathfrak{a} \otimes M \cong M/\mathfrak{a}M$

2.3 Modules

In this section we discuss module properties.

Definition 2.5. Classification of finiteness properties I.
0. M is free iff M has basis.
1. M is finitely generated iff $A^{\oplus m} \longrightarrow M \longrightarrow 0$ is exact.
2. M is finitely presented iff $A^{\oplus n} \longrightarrow A^{\oplus m} \longrightarrow M \longrightarrow\!\!\!\!\rightarrow 0$ is exact.

0. implies that $f : A^{\oplus m} \longrightarrow M$ is an isomorphism. 1. implies that $f : A^{\oplus m} \longrightarrow M$ is surjective., which implies that M is generated by some finite $(m_1 \dots m_m)$ but the kernel of f has some non-trivial part. The caveat is that the basis may not exist, e.g. $\mathbb{Z} = (2, 3)$ but minimal generating set is $\emptyset$.

Important disclaimer: This classification doesn't apply to rings. Apparently, it's because the category of rings is not *abelian*.

Some examples:

- Finitely generated free module — $\mathbb{Z} = 1_{\mathbb{Z}}, \mathbb{R}^2 = \{(1, 0), (0, 1)\}_{\mathbb{R}}$.
- Finitely generated non-free module — $\mathbb{Z}/n\mathbb{Z} = (1)_{\mathbb{Z}}$, but $1 \cdot n = 0$.
- Non-finitely generated free module — $\bigoplus_{i=1}^{\infty} \mathbb{Z}$.
- Non-finitely generated non-free module — $\mathbb{Q}$ over $\mathbb{Z}$.

Definition 2.6. Classification of finiteness properties II.
Every module has a presentation $M = N/K$.
0. M is free iff N is finitely generated and $K = 0$.
1. M is finitely generated iff N is finitely generated.
2. M is finitely presented iff N, K are finitely generated.

The N/K quotient is a hidden way to express $\mathrm{coker}(A^{\oplus n} \to A^{\oplus m})$, so modules can be also thought of in terms of the $A^{\oplus n} \to A^{\oplus m}$ map.

There is no simple way to describe rings as cokernels in exact sequences, see margin note above.

2.4 *Exactness properties*

- Tensoring is right-exact
- Localization of rings is exact
- Localization of modules is exact

2.5 *Universal properties*

- Universal property of quotients
- Universal property of direct products
- Universal property of direct sums
- Universal property of polynomial rings
- Universal property of tensor products

2.6 Flat modules

Definition 2.7. An A-module M is *flat*, if $T_N : M \mapsto M \otimes_A N$ is *exact*.

Theorem 2.8. The following are equivalent:

- N is flat
- T_N is exact
- If $f : M \to M'$ is injective, then $T_N(f)$ is injective
- If $f : M \to M'$ is injective and M, M' finitely generated, then $T_N(f)$ is injective

Proof: $(i) \iff (ii)$ by definition, $(ii) \iff (iii)$ by right-exactness, $(iii) \implies (iv)$ clear, $(iv) \implies (iii)$: Let $f : M' \to M$ be injective and let $u = \sum x_i \otimes y_i \in \ker(f \otimes 1)$, so that $0 = \sum f(x_i') \otimes y_i \in M \otimes N$. Let M_0' be the submodule generated by the x_i' and let u_0 denote $\sum x_i' \otimes y_i$ as an element of $M_0' \otimes N$. By *some lemma* there exists a finitely generated submodule M_0 of M containing $f(M_0')$ and such that $\sum f(x_i') \otimes y_i = 0$ as an element of $M_0 \otimes N$.

2.7 Finitely generated modules

Theorem 2.9 (Nakayama's Lemma)**.** Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A contained in the Jacobson radical $\mathfrak{R}$ of A. Then $\mathfrak{a}M = M$ implies $M = 0$.

Jacobson radical — intersection of all the maximal ideals of A.

Lemma 2.10. Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal of A such that $\mathfrak{a}M = M$. Then there exists $x \equiv 1 \bmod \mathfrak{a}$ such that $xM = 0$.

Lemma 2.11. Let M be a finitely generated A-module, let $\mathfrak{a}$ be an ideal of A, and let ϕ be an A-module endomorphism of M such that $\phi(M) \subseteq \mathfrak{a}M$. Then ϕ satisfies and equation of the form

$$\phi^n + a_1\phi^{n-1} + \ldots + a_n = 0$$

where the a_i are in $\mathfrak{a}$.

Proof: Let $M = (x_1 \ldots x_n)$. Then $\phi(x_i) \in \mathfrak{a}M$, so that we have say $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ for $1 \leq i \leq n, a_{ij} \in \mathfrak{a}$ because $\phi(x_i)$ is still a linear combination of generators of M. By Cayley-Hamilton, ϕ satisfies its own characteristic equation, hence the statement.

3 Commutative Algebra I

3.1 Integral Dependence and Going-Up Theorem

The general setting is that we have commutative unital ring A and its extension ring B. We want to understand the map

$$\mathrm{Spec}(B) \to \mathrm{Spec}(A), \quad \mathfrak{q} \mapsto \mathfrak{q} \cap A$$

In field theory, the main objects were finite and algebraic field extensions. Integral ring extensions are their ring theory counterpart.

Theorem 3.1 (Going-Up Theorem)**.** Let $A \subseteq B$ be an integral extension. Suppose

$$\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_n$$

is a prime ideal chain in B. Suppose

$$\mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_m$$

is a (longer) prime ideal chain in A such that $\forall i \leq n : \mathfrak{p}_i = \mathfrak{q}_i \cap A$. Then there exists a continuation $\mathfrak{q}_{n+1} \subseteq \ldots \subseteq \mathfrak{q}_m$ of prime ideals in B.

As I understand it, this means $\{\text{prime ideal chains in } A\} \longleftrightarrow \{\text{prime ideal chains in } B\}$. Equivalently, A and B have the same Krull dimension.

3.2 The Spectrum, Again

4 Intro to Algebraic Geometry

4.1 Noether Normalization and Hilbert's Nullstellensatz

Theorem 4.1 (Noether normalization theorem)**.** Let k be a field. Let A be a finitely generated k-algebra. Then there exist algebraically independent $\{x_1 \ldots x_n\} \in A$ such that A is finite over $k[x_1 \ldots x_n]$.

Theorem 4.2 (Hilbert's Nullstellensatz)**.** Let k be a field. Let A be a finitely generated k-algebra, and let $\mathfrak{m} \subseteq A$ be a maximal ideal. Then $A/\mathfrak{m}$ is a finite field extension of k.

Theorem 4.3 (Weak Nullstellensatz)**.** Let

- k be an algebraically closed field,
- $f_1 \ldots f_m \in k[X_1 \ldots X_n]$ arbitrary,
- $A := k[X_1 \ldots X_n]/(f_1 \ldots f_m)$.

Then there exists a solution $x \in k^n \iff (f_1 \ldots f_m) \neq k[X_1 \ldots X_n]$. Moreover, there exist infinitely many solutions iff $\dim_k(A) = \infty$.

Theorem 4.4 (Bezout's theorem)**.** Let

- k be an algebraically closed field,
- $f, g \in k[X, Y]$ be of degrees n, m,
- $S := \{(x, y) \in k^2 \mid f(x, y) = g(x, y) = 0\}$ be their solution set,
- $A := k[X, Y]/(f, g)$.

Then the following holds:
S is infinite $\iff$ f, g have a common non-trivial factor
S finite $\implies$ $|S| \leq \dim_k(A) \leq nm$.

4.2 *Algebraic Sets and Ideals*

Definition 4.5. • Algebraic set $Z \subseteq k^n$

$\iff$ exists some subset S of $k[X_1 \dots X_n]$, such that $\forall z \in Z : \forall f \in S f(z) = 0$

$\iff$ definable by some polynomial formula.

Der Unterschied zu semi-algebraischen Mengen ist, dass semi-algebraische Mengen durch Ungleichungen definierbar sind.

- Vanishing set $Z(S)$

  $\iff$ Menge der Nullstellen von S.

- Zariski topology

  $\iff$ Algebraic sets form closed sets on k^n.

- Vanishing ideal

  $\iff$ Given (any) set $Y \subset k^n$, we define the vanishing ideal $I(Y)$ as the set of functions equal to zero for all $y \in Y$.

- Radical

  $\iff$ Any power $x^n \in \mathfrak{a} \implies x \in \mathfrak{a}$ for all $x \in A$.

Theorem 4.6 (Hilbert's Nullstellensatz, Algebraic Geometry)**.** Let k be an algebraically closed field. Then Z and I define mutually inverse bijections between algebraic subsets of k^n and radical ideals in $k[X_1 \dots X_n]$ via $Z \mapsto I(Z)$ and $Z(\mathfrak{a}) \leftarrow\!\shortmid \mathfrak{a}$.

More generally, we have $Z(I(Z)) = Z$ for all algebraic subsets $Z \subseteq k^n$ and $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ for all ideals $\mathfrak{a} \subseteq k[X_1 \dots X_n]$.

Definition 4.7. Jacobson ring

4.3 *Krull dimension*

Theorem 4.8 (Krull's principal ideal theorem)**.** f

Theorem 4.9. Let k be a field. Then $\dim(k[X_1 \ldots X_n]) = n$.

4.4 *Transcendence Degree*

Definition 4.10. Transcendence basis, transcendence degree

4.5 *Irreducible components, Minimal Prime Ideals*

Definition 4.11. Irreducible algebraic set, irreducible component

4.6 *Krull's Principal Ideal Theorem*

5 *Intro to Algebraic Number Theory*

5.1 *Integral closure*

Definition 5.1. Algebraic number field, ring of algebraic integers
Norm, trace, characteristic polynomial

5.2 *Localization and Discrete Valuation Rings*

5.3 *Dedekind Rings*

5.4 *Fractional Ideals*

5.5 *Ideal Class Group*

5.6 *The Splitting of Primes*

5.7 *Quadratic Norm Equations*

5.8 *Hilbert Class Fields and a Theorem of Gauss*

Not important.