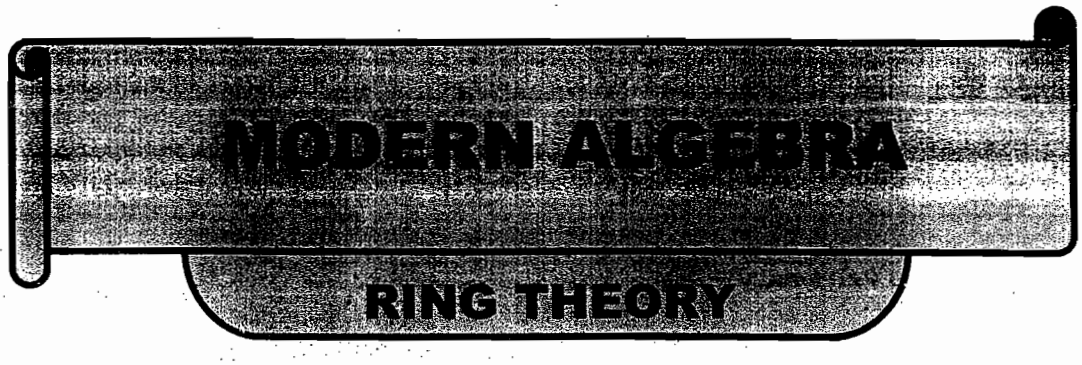
Modern Algebra
Ring Theory



CHAPTER 1

BASIC CONCEPTS AND DEFINITIONS

Ring: A ring $R \neq \phi$ is a set together with two binary operation $+$ and $\bullet$ (called addition and multiplication) satisfying the following axioms:

(a) $(R,+)$ is an abelian group.

(b) $\bullet$ is associative: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ for all $a,b,c \in R$.

(c) The distributive laws hold in R : For all $a,b,c \in R$

(i) $(a+b) \bullet c = (a \bullet c) + (b \bullet c)$

(ii) $a \bullet (b+c) = (a \bullet b) + (a \bullet c)$.

Then we denote it by $(R,+,\bullet)$

1.1. Basic Properties of Rings

Let $(R,+,\bullet)$ be a ring.

1. As $(R,+)$ is a group, the identity of this group is called the zero of the ring and denoted by 0 and $a+0=0+a=a \quad \forall a \in R$
2. Let $a,b,c \in R$, then
   (a) $a+b=a+c \Rightarrow b=c$ (cancellation law w. r. t.+)
   (b) $-(-a)=a$ (where $-a$ denotes the additive inverse of a)
   (c) The zero element of R is unique.
   (d) The additive inverse of any element in R is unique.
   (e) $a.0=0.a=0$.
   (f) $a.(-b)=(-a).b=-(a.b)$
   (g) $(-a).(-b)=a.b$

Table To Be Remembered

S. no.	Name of Ring	Addition operation	Multiplication Operation	Unity	Commutative
1	$(\mathbb{C},+,.)$	Ordinary addition	Ordinary Multiplication	1	Yes
2	$(\mathbb{R},+,.)$	Ordinary	Ordinary	1	Yes

		addition	Multiplication		
3	$(\mathbb{Q},+,.)$	Ordinary addition	Ordinary Multiplication	1	Yes
4	$(\mathbb{Z},+,.)$	Ordinary addition	Ordinary multiplication	1	Yes
5	$(m\mathbb{Z},+,.)$ where $m \neq \pm 1$	Ordinary addition	Ordinary multiplication	no	Yes
6	$R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R}\right\}$	Ordinary matrix addition	ordinary matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	No
7	$R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}\right\}$	Component wise addition	Component wise multiplication	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$	Yes
8	$R=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in \mathbb{R}\right\}$	Ordinary matrix addition	Ordinary matrix multiplication	$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$	Yes
9	$\mathbb{Z}[i]=\{a+ib : a,b \in \mathbb{Z}\}$	Ordinary addition of complex numbers	Ordinary multiplication of complex numbers	1	Yes
10	$R=\{a_0+a_1i+a_2j+a_3k : a_0,a_1,a_2,a_3 \in \mathbb{Q}\}$	Ordinary addition of complex numbers	Ordinary multiplication	1	No
11	$\mathbb{Z}_m=\{0,1,2,..,m-1\}$	Addition modulo m	Multiplication modulo m	1	Yes

12	$R=\{0,2,4,6,8\}$	Addition modulo 10	Multiplication modulo 10	6	Yes
13	$R=\left\{\begin{matrix}a+\sqrt{p}\,b; \\ p \text{ is prime} \\ a,b\in\mathbb{Q} \\ \text{number}\end{matrix}\right\}$	ordinary addition	ordinary multiplication	$1+\sqrt{p}\,0$	Yes
14	$R=\{a+ib;$ $a,b\in\mathbb{Q}\}$	ordinary addition	$a.b=0$ $\forall\ a,b$	No	Yes
15	$R=P(\mathbb{N})$, power set of $\mathbb{N}$	Symmetric Difference	Intersection	$\mathbb{N}$	Yes
16	$(\mathbb{Z},*,\bullet)$	$a*b=a+b$	$a\bullet b$ $=a+b-ab$	0	Yes
17	$R=$ Set of all real valued continuous functions defined on closed interval $[0,1]$	$(f+g)(x)=$ $f(x)+g(x)$ $\forall x\in[0,1]$	$(f.g)(x)=$ $f(x).g(x)$ $\forall\ x\in[0,1]$	$f(x)=1$ $\forall\ x\in$ $[0,1]$	Yes
18	If $(G,+)$ is an abelian group $(\text{End}\ (G),+,\circ)$ is a ring	$(f+g)(x)=$ $f(x)+g(x)$ $\forall x\in G$	Composition of functions.	I_G	No
19	$R^S=\{f:S\to R\}$; $S\neq 0$ & R be any ring. Then R^S is ring	$(f+g)(s)=$ $f(s)+g(s)$ $\forall s\in S$ Where $f(s)+$ $g(s)$ is addition of R.	$f\cdot g(s)=$ $f(s)\cdot g(s)$ Where $f(s)\cdot g(s)$ is multiplication of R.	No	No
20	$\mathbb{Q}[i]=\{a+ib$	Ordinary addition of	Ordinary multipli-	1	Yes

	$: a,b \in \mathbb{Q}$	complex numbers	cation of complex numbers		

1.2. Definitions

1. **Unity:** If $(R,\cdot)$ is monoid i.e., $\exists$ identity element in R w. r. t. multiplication then this identity element is called the **unity** of the ring. Denoted by 1.
2. **Trivial Ring:** A ring R is said to be trivial if $R=\{0\}$.
3. **Zero Ring:** Let $(G,+)$ be an abelian group. Let us define the second binary operation $(\cdot)$ on R as $a\cdot b=0\ \forall a,b\in G$, where 0 is additive identity of G. Then, $(G,+,\cdot)$ forms a ring and called zero ring.

   Note: If R is a trivial ring then R is a zero ring but converse need not be true.
4. **Commutative Ring:** Let $(R,+,\cdot)$ be a ring. Then R is said to be commutative if R is commutative under multiplication i.e., $a\cdot b=b\cdot a\ \forall a,b\in R$

   Example:

   (a) Examples 1, 2, 3, 4, 5, 8 defined in above table are commutative rings.

   Notation: Further CRU will denote a Commutative ring with Unity

   (b) Examples 19 is CRU if R is CRU.

   Note:

   (a) If R is commutative ring then $(xy)^2=x^2y^2\ \ \forall\ x,y\in R$. but not conversely.

   i.e., it is not necessary that R is commutative if $(xy)^2=x^2y^2\ \ \forall\ x,y\in R$

   Example: $R=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\middle|\ a,b\in\mathbb{Z}\right\}$

   Where $+$: ordinary matrix addition $\bullet$: ordinary matrix multiplication

   $(R,+,\bullet)$ is non-commutative ring.

   But $(xy)^2=x^2y^2\ \ \forall\ x,y\in R$

   (b) If R is ring with unity & $(xy)^2=x^2y^2\ \ \forall\ x,y\in R$

   $\Rightarrow$ R is commutative.

   Proof: We've $(xy)^2=x^2y^2\ \ \forall\ x,y\in R$ ...(1)

   Replacing y by $y+1\in R$ in (1) where 1 is unity

   We obtain

$$\left[x(y+1)\right]^2 = x^2(y+1)^2 \quad \forall\, x, y \in R$$

$$(xy+x)^2 = x^2\left(y^2+2y+1\right)$$

$$\Rightarrow (xy)^2 + (xy)x + x(xy) + x^2 = x^2y^2 + 2x^2y + x^2 \qquad ...(2)$$

Using (1) and cancellation laws of $(R,+)$ in (2)

We get

$$xyx + x^2y = 2x^2y \text{ or } xyx = x^2y \quad \forall\, x, y \in R \qquad ...(3)$$

Replacing x by $(x+1)$ in (3)

$$(x+1)y(x+1) = (x+1)^2 y$$

$$\Rightarrow (x+1)(yx+y) = (x+1)(xy+y)$$

$$\Rightarrow xyx + xy + yx + y = x^2y + xy + xy + y \qquad ...(4)$$

Using (3) & cancellation laws of $(R,+)$ in (4)

We get

$$yx = xy \quad \forall\, x, y \in R$$

Hence, R is a commutative ring.

(c) If R is commutative ring

Then for $a, b \in R$

$$(a+b)^n = a^n + {}^nC_1 a^{n-1}b + {}^nC_2 a^{n-2}b^2 + ... + b^n$$

for every positive integer n.

(d) R is commutative

if and only if $(a-b)(a+b) = a^2 - b^2 \quad \forall\, a, b \in R$

(e) Any ring of prime order is commutative

(f) A ring of order p^2 may not be commutative.

Example: $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Z}_2 \right\}$.

A forms ring with matrix addition & matrix multiplication & entries are from $\mathbb{Z}_2$.

Ring A has order $4 = 2^2$

But it is not commutative

as $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

and $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

(g) The smallest non-commutative ring is of order 4.

(h) A ring with unity & of order p^2 (p is prime) is commutative.

5. **Unit:** Let $(R,+,\cdot)$ be a ring with unity and $a \in R$. Then a is said to be unit element of R if $\exists\ b \in R$ such that $a \cdot b = b \cdot a = 1$

Examples:

(a) The units of $\mathbb{Z}$ are 1 and –1.

(b) In Ring numbers 1, 2, 3 defined in Table of rings, each non-zero element is a unit.

(c) The units in a ring $(\mathbb{Z}_6,+_6,\times_6)$ are 1 and 5.

Results:

(i) Let R be a ring with unity. Then the set of all units of R forms a group under multiplication.

(ii) Let R be a CRU, then group of units of R is an abelian group.

6. **Associate:** Let R be a ring with unity and $a,b \in R$. Then a is called associate of b if $\exists$ a unit u in R such that $a = bu$.

Example:

(a) In $(\mathbb{Z},+,\cdot)$, associate of 2 are 2 and –2.

(b) In $(\mathbb{R},+,\cdot)$, associates of 3 are all non-zero real numbers.

Observation: Let us define a relation '$\sim$' on ring with unity R as: $a \sim b \Leftrightarrow a$ and b are associates. Then '$\sim$' is an equivalence relation on ring R.

Hence, it partitions the ring R into equivalence classes.

7. **Zero–divisors:** Let R be a ring and $0 \neq a \in R$. Then a is said to be zero divisor from left if $\exists\ 0 \neq b \in R$ such that $a \cdot b = 0$ and here we call 'b' right zero divisor.

a & b are called **zero-divisor** if they are zero divisors from right as well as from left.

Examples:

(a) 4 is zero divisor in $\mathbb{Z}_{12}$ as there exist 3 in $\mathbb{Z}_{12}$ such that $4 \cdot 3 = 12 = 0$.

(b) $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is zero divisor from left in ring of 2×2 matrices over $\mathbb{R}$ as

$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. But it is not zero divisor from right as

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

(c) In ring $(P(\mathbb{N}),\Delta,\cap)$, each element is zero divisor except $\mathbb{N}$ as for each $X \in P(\mathbb{N})$ we have $Y = \mathbb{N} - X \in P(\mathbb{N})$ such that $X \cap Y = \phi$.

Observations:

(i) Let R be ring with unity. Let $U(R)$ denote the set of all units of R and $Z(R)$ denote the set of all zero divisors of R. Then $Z(R) \cap U(R) = \phi$

(ii) In $\mathbb{Z}_m$, each non-zero element is either a unit or zero divisor.

(iii) In $\mathbb{Z}_m$, $0 \neq a \in \mathbb{Z}_m$ is a unit iff a & m are co-prime.

Example: In $\mathbb{Z}_5$ units are $1, 2, 3, 4$.

(iv) There exist rings having infinite elements which are neither units nor zero divisors.

8. **Cancellation Law:** A ring R is said to satisfy the left cancellation law if for all $a, b, c \in R$

$a \neq 0, \quad ab = ac \Rightarrow b = c$

A similar definition can be given for right cancellation law.

9. **Integral Domain:** A commutative ring with unity without zero divisors is called an Integral domain.

Example: examples $1, 2, 3, 4$ defined in table of rings are Integral Domain.

We some time denote Integral domain by ID

Note: Many books do not take ring to be commutative with unity. They consider only ring without zero divisors. For exam point of view to check a ring is ID or not we should only check availability of zero divisors.

10. **Skew Field:** A ring with unity $(R, +, \cdot)$ is said to be skew-field if each non-zero element has multiplicative inverse i.e. $(R, \cdot)$ forms a group. It is also known as division ring.

Examples:

(a) Ring numbers $1, 2, 3$ defined in table of rings are skew-fields.

(b) $R = \mathbb{Z}_p^*$ is a skew-field, where p is prime.

(c) examples $9, 17$ defined in table are not skew fields.

Observations:

(i) Every skew-field is an integral domain if commutative.

(ii) If in a ring R, the equation $ax = b \ \forall \ a, b$ has a unique solution, then R is a division ring.

11. **Field:** A commutative skew-field is defined as field.

In other words, A CRU is a field if each non-zero element posses multiplicative inverse.

Examples:

(a) examples $1, 2, 3$ defined in table of rings are Fields.

(b) $\mathbb{Z}_p$ is a field, where p is prime.

Put Your Own Notes

Results:

(i) Every field is an integral domain.

(ii) Every finite integral domain is a field.

(iii) $\mathbb{Z}_p$, the ring of integers modulo p, is a field iff p is prime.

(iv) Every finite skew-field is a field.

12. Nilpotent Element: Let R be a ring and $a \in R$. Then a is said to be nilpotent element if $\exists\ n \in \mathbb{N}$ such that $a^n = 0$ i.e., $\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n \text{ times}} = 0$.

The smallest such n is defined as the index of nilpotence.

Examples:

(a) 0 is only nilpotent element of index 1 in every ring.

(b) 6 is nilpotent element of index 2 in $\mathbb{Z}_{12}$.

13. Idempotent Element: Let R be a ring and $a \in R$. Then a is said to be idempotent element if $a^2 = a$.

Examples:

(a) 0 and unity are always idempotent

(b) 5 and 6 are idempotent in $\mathbb{Z}_{10}$

(c) Each element of $\left(P(\mathbb{N}), \Delta, \cap\right)$ is idempotent.

Results on Nilpotent and Idempotent elements:

(i) In an Integral Domain 0 and 1 are the only idempotent elements.

(ii) An Integral Domain does not possess any non-zero nilpotent element.

(iii) Let R be a commutative ring and a, b are nilpotent elements of R. Then

(a) $a + b$ is also nilpotent element.

(b) $a \cdot b$ is also nilpotent element.

(c) $a \cdot c$ is also nilpotent element $\forall$ non-zero c in R.

(d) If $a \cdot b$ is nilpotent in R, then $b \cdot a$ is also nilpotent in R.

(iv) If 'a' is an idempotent element in R, then $1 - a$ is also an idempotent element in R.

(v) **Orthogonal Idempotent:** Let R be a ring and e_1, e_2 are idempotent elements. Then e_1 and e_2 are called orthogonal if $e_1 \cdot e_2 = 0$.

In general, if $e_1, e_2, \ldots, e_k$ are idempotent elements in ring R. Then $e_1, e_2, \ldots, e_k$ are called orthogonal if $e_i \cdot e_j = 0 \quad \forall i \neq j$.

(vi) If 'a' is a nilpotent element of index r in a ring with unity. Then $(1-a)$ is unit.

Since, $1 = 1 - a^r = (1-a)\left(1 + a + a^2 + \ldots + a^{r-1}\right)$

$$\Rightarrow (1-a)^{-1} = \left(1 + a + a^2 + ... + a^{r-1}\right)$$

14. Unipotent Element: Let R be a ring with unity then $a \in R$ is said to be unipotent if $1-a$ is nilpotent i.e., a is unipotent $\Leftrightarrow b = (1-a)$ is nilpotent. Also $b = 1-a \Leftrightarrow a = 1-b$.

Thus, if b is a nilpotent element in R, then $(1-b)$ is unipotent element.

Example: 7 is unipotent element in $\mathbb{Z}_{12}$ as $7 = 1-6$, where 6 is nilpotent element in $\mathbb{Z}_{12}$.

15. Factors: Let R be a commutative ring with unity and $a, b \in R$. Then b is said to be factor of a if $\exists\ c \in R$ such that $b = ac$

Note: For $a \in R$ the associates of 'a' and units in that ring are always factors of 'a' and called **improper factors**, the other factors are called **proper factors**.

16. Irreducible Element: A non-zero, non-unit element 'a' in a commutative ring with unity R is said to be irreducible element if it has no proper factor in R i.e, whenever $a = bc$, then either b is unit or c is unit. An element which is not irreducible is called reducible element.

Example: $1+i$ is an irreducible element in $\mathbb{Z}_4$.

17. Prime Element: Let R be a commutative ring with unity then a non-zero, non-unit element $p \in R$ is called prime element if $p \mid ab$ implies either $p \mid a$ or $p \mid b$, where $a, b \in R$.

Example: 2 is prime element in $\mathbb{Z}_8$.

Observations:

(i) It may be observed that $p \in R$ is not irreducible, if there exists a pair of element $a, b \in R$. such that $p = ab$ where a and b are both non-unit element of R.

(ii) It may be observed that $p \in R$ is not prime, if there exists a pair of elements, $a, b \in R$ such that $p \mid ab$, but $p \nmid a$ & $p \nmid b$.

(iii) Irreducible and prime elements in a commutative ring with unity are always non-zero and non-unit elements.

(iv) There may exist elements in ring R which are prime elements of R but not irreducible elements.

Example: In $\mathbb{Z}_6$, 2 is prime element but not irreducible element.

(v) There may exist elements in ring R which are irreducible elements of R but not prime elements.

Example: In $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$, 3 is irreducible but not prime element.

(vi) There may exist elements in ring R which are both prime and irreducible.

Example: In ring of integers $\mathbb{Z}$, element 3 is both prime as well as irreducible element.

(vii) There may exist elements in ring R which are neither prime nor irreducible.

Example: In ring of integers $\mathbb{Z}$, element 4 is neither prime nor irreducible element.

(viii) In an I.D. every prime element is irreducible element.

(ix) Set of Units of $\mathbb{Z}[i]$ is $\{1,-1,i,-i\}$

(x) Set of Units of $\mathbb{Z}$ is $\{1,-1\}$

(xi) Let F be any field. Then set of units of F is $F-\{0\}$ i.e. every non-zero element of a field is a unit.

(xii) Set of Units of $M_{n\times n}(F)$ is $GL(n,F)$.

(xiii) For $d\in\mathbb{Z}$, $\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d}:a,b\in\mathbb{Z}\}$ is an integral domain.

(xiv) For $d\in\mathbb{Z}^+$, $\mathbb{Q}[\sqrt{d}]=\{a+b\sqrt{d}:a,b\in\mathbb{Q}\}$ is a field.

(xv) Let R be an Integral Domain and a,b be two non-zero elements of R. Then a and b are associate iff $a\mid b$ and $b\mid a$.

18. Characteristic of a Ring: The smallest positive integer n is said to be characteristic of a ring R if $na=0\ \forall a\in R$ i.e. if $\underbrace{a+a+\ldots+a}_{n\text{ times}}=0$. If no such positive integer exists, then characteristic of ring is 0. It is denoted by char R.

Properties:

(i) Let R be a ring with unity 1. Then characteristic of R is equal to the order of 1 under addition provided it is finite if it is not finite then char $R=0$.

(ii) The characteristic of an integral domain is either zero or prime number.

(iii) The cardinality of a finite integral domain is of the form p^r for some prime p and $r\in\mathbb{Z}^+$

(iv) The cardinality of a finite field is of the form p^r for some prime p and $r\in\mathbb{Z}^+$

(v) The characteristic of a field is either zero or a prime number.

(vi) The characteristic of a non-zero Boolean ring is always 2.

(vii) Let R be a commutative ring with characteristic p, where p is a prime number then. $(a+b)^p=a^p+b^p\ \forall a,b\in R$

(viii) Let R be a ring with characteristic n and suppose that $ma=0\ \ \forall a\in R$ and for some $m\in\mathbb{Z}^+$ then n divides m i.e. m is multiple of n.

CHAPTER 2

SOME IMPORTANT STRUCTURES

2.1. $(Z_m, \oplus_m, \odot_m)$ is a Commutative Ring with Unity w.r.t.

$\oplus_m$: addition modulo m

$\odot_m$: multiplication modulo m

Properties:

(i) Number of units $= \phi(m)$

(ii) Let $U(\mathbb{Z}_m)$ be set of units of $\mathbb{Z}_m$, then $U(\mathbb{Z}_m)$ will form the group.

(iii) $U(\mathbb{Z}_m) = \{x \in \mathbb{Z}_m \mid g.c.d.(x,m) = 1\}$

(iv) Every non-zero element is either unit of zero-divisor.

(v) Number of zero-divisors $= m - (\phi(m) + 1)$

(vi) List of zero-divisors $= Z(\mathbb{Z}_m) = \{x \in \mathbb{Z}_m \mid g.c.d.(x,m) \neq 1\}$

(vii) $\mathbb{Z}_m$ is integral domain if and only if m is prime.

(viii) $\mathbb{Z}_m$ is field if and only if m is prime.

(ix) Number of associates of 'a' $\in \mathbb{Z}_m$ are $\phi(o(a))$. Where order of a is calculated with respect to addition.

(x) List of associates $cl(a) = \left\{x \in \mathbb{Z}_m \mid \frac{m}{g.c.d.(x,m)} = o(a)\right\}$

(xi) Number of nilpotent elements in $\mathbb{Z}_{p^n} = p^{n-1}$

(xii) List of nilpotent elements in $\mathbb{Z}_{p^n} = \{k.p \in \mathbb{Z}_{p^n} \mid k = 1,2,....\}$

(xiii) If $m = p_1^{n_1} p_2^{n_2} .... p_r^{n_r}$

Then number of nilpotent elements in

$\mathbb{Z}_m = p_1^{n_1-1} p_2^{n_2-1} p_3^{n_3-1} .... p_r^{n_r-1}$

(xiv) List of nilpotent elements in

$$\mathbb{Z}_m;\ m = p_1^{n_1}\, p_2^{n_2} \ldots . p_r^{n_r} = \left\{k.\left(p_1\, p_2 \ldots . p_r\right) \in \mathbb{Z}_m \middle| k = 1,2,\ldots.\right\}$$

(xv) $a \in \mathbb{Z}_m$ is nilpotent if and only if every prime divisor of m divides a.

(xvi) Number of idempotent elements in $\mathbb{Z}_m = 2^k$. Where k is number of distinct prime divisor of m.

(xvii) Number of idempotent elements in $\mathbb{Z}_{p^n}$ are two i.e. $\{0,1\}$

Examples: Consider the ring $\left(\mathbb{Z}_{20}, \oplus_{20}, \odot_{20}\right)$

(a) Number of units $= \phi(20) = 8$

List of units $= \{1,3,7,9,11,13,17,19\}$

(b) Number of zero divisors $= 20 - (8+1) = 11$

List of zero divisors $= \{2,4,5,6,8,10,12,14,15,16,18\}$

(c) Number of associates of elements '2' $\in \mathbb{Z}_m$ $o(2)$ with respect to addition is 10 $\phi\left(o(2)\right) = \phi(10) = 4$

List of associates of '2' $\in \mathbb{Z}_m = \{2,6,14,18\}$

(d) Number of idempotent elements $= 2^2 = 4$.

Note: $\phi(n)$ used above was the Euler's ϕ function.

2.2. V = **{Set of All Functions From R to R}**

Where R is a ring. Then define addition operation as follows:

$\forall\ f,g \in V; (f+g)(x) = f(x) \oplus g(x)\ \ \forall\ x \in R$ & define multiplication as follows:

$\forall\ f,g \in V; f.g(x) = f(x) \odot g(x)\ \ \forall\ x \in R$

Where $\oplus$ & $\odot$ are addition & multiplication of ring R.

Then $(V, +, \bullet)$ is a ring.

Properties:

(i) V has unity if R has unity.

(ii) V is commutative if R is commutative ring.

(iii) V is never integral domain even if R is integral domain.

(iv) V always have infinite zero-divisors even if R (infinite) is integral domain.

(v) V is finite ring if and only if R is finite ring.

(vi) There exists elements in V. Which are neither zero-divisor nor units.

(vii) Any function which is not zero anywhere is unit hence there are infinite units in V if R is infinite.

2.3. V_c = **{Set of All Continuous Functions from R to R}**

Where R is ring

Then define addition operation as

$\forall f,g \in V_c \qquad (f+g)(x) = f(x) \oplus g(x) \quad \forall x \in R$

& define multiplication as

$\forall f,g \in V_c$

$f.g(x) = f(x) \odot g(x) \quad \forall x \in R$

Where $\oplus$ & $\odot$ are addition & multiplication respectively of ring R.

Properties:

(i) V_c has unity if R has unity

(ii) V_c is commutative if R is commutative

(iii) V_c is never integral domain even if R is integral domain

(iv) V_c is finite if and only if R is finite ring.

(v) Any function which has countable zero's is neither zero-divisor nor unit if it has atleast one zero.

(vi) Any function which does not have zero is a unit.

2.4. Lets Combine Several Rings into One Large Product: Cartesian Product

Let R_1 & R_2 are two rings

Then $R = R_1 \times R_2 = \{(a,b) | a \in R,\ b \in R_2\}$ is a ring with respect to componentwise addition & componentwise multiplication.

i.e. $(a,b)+(c,d) = (a \oplus_1 c,\ b \oplus_2 d)$

$(a,b) \cdot (c,d) = (a \odot_1 c,\ b \odot_2 d)$

Where $\oplus_i$ & $\odot_i$ are addition and multiplication of R_i $i = 1,2$ respectively.

Properties:

(i) R is commutative if and only if both R_1 & R_2 are commutative.

(ii) R has unity if and only if both R_1 & R_2 have unity.

(iii) Let $U(R)$ be the group of units of R & $U(R_i)$ is group of units for $i = 1,2$

Then $U(R) \cong U(R_1) \times U(R_2)$

(iv) If R_i's are non-trival rings then R is never integral domain i.e. always has zero-divisors.

(v) $\text{Char}(R) = k$

$k = 0$ if either $\text{Char}\, R_1 = 0$ or $\text{Char}\, R_2 = 0$

& $k = l.c.m\{\text{Char}(R_1),\ \text{Char}(R_2)\}$

If both char (R_1) & Char (R_2) are non-zero.

(vi) R is never integral domain if R_1 & R_2 are non-trivial.

2.5. Boolean Ring

A ring R is said to be Boolean ring if all of its element are idempotent.

Examples:

(i) $(\mathbb{Z}_2, \oplus_2, \odot_2)$

(ii) $\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \ldots\ldots \times \mathbb{Z}_2}_{n-\text{copies}}$ with respect to componentwise addition & componentwise multiplication.

(iii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots\ldots$ i.e. infinite Cartesian product with respect to componentwise addition & componentwise multiplication.

Properties:

(i) Boolean ring is always commutative

(ii) $a + a = 0 \quad \forall\, a$

(iii) $a + b = 0 \;\Rightarrow\; a = b$

(iv) Char $(R) = 2$

(v) Cartesian product of Boolean rings is Boolean ring.

2.6. Group Rings

Fix a commutative ring R with identity $1 \neq 0$ and let $G = \{g_1, g_2, \ldots\ldots, g_n\}$ be any finite group with group operation written multiplicatively. Define the *group ring*, RG, of G with coefficients in R to be the set of all formal sums.

$a_1 g_1 + a_2 g_2 + \ldots\ldots + a_n g_n$

$a_i \in R, \quad 1 \leq i \leq n.$

If g_1 is the identity of G we shall write $a_1 g_1$ simply as a_1. Similarly, we shall write the element $1g$ for $g \in G$ simply as g.

Addition is defined "component wise"

$$(a_1 g_1 + a_2 g_2 + \ldots + a_n g_n) + (b_1 g_1 + b_2 g_2 + \ldots + b_n g_n)$$

$$= (a_1 + g_1) g_1 + (a_2 + b_2) g_2 + \ldots + (a_n + b_n) g_n .$$

Multiplication is performed by first defining $(ag_i)(bg_j) = (ab) g_k$, where the product ab is taken in R and $g_i g_j = g_k$ is the product in the group G. This product is then extended to all formal sums by the distributive laws so that coefficient of g_k in the product

$(a_1 g_1 + \ldots + a_n g_n) \times (b_1 g_1 + \ldots + b_n g_n)$ is $\sum_{g_i g_j = g_k} a_i b_j$

It is straightforward to check that these operations make RG into a ring (again, commutativity of R is

not needed). The associativity of multiplication follows from the associativity of the group operation in

G. The ring RG is commutative if and only if G is a commutative group.

Example: Let $G = D_4$, the dihedral group of order 8 with usual generators r, s

$D_4 = r^4 = s^2 = 1 \;\&\; rs = sr^{-1}$

and let $R=\mathbb{Z}$

the elements $\alpha = r + r^2 - 2s$

and $\beta = -3r^2 + rs$

are typical members of $\mathbb{Z}D_4$. Their sum and product are then

$$\alpha + \beta = r - 2r^2 - 2s + rs$$

$$\alpha\beta = \left(r + r^2 - 2s\right)\left(-3r^2 + rs\right)$$

$$= r\left(-3r^2 + rs\right) + r^2\left(-3r^2 + rs\right) - 2s\left(-3r^2 + rs\right)$$

$$= -3r^3 + r^2s - 3 + r^3s + 6r^2s - 3r^3$$

$$= -3 - 5r^3 + 7r^2s + r^3s$$

Note: Definition of addition and multiplication in RG restricted to the elements of R is just the addition and multiplication in R.

Properties:

(i) The ring R appears in RG as the "Constant" formal sums i.e. the R multiples of the identity of G.

(ii) Elements of R commute with all elements of RG.

(iii) Unity of R is the unity of RG.

(iv) The group G also appears in RG i.e. $g_i's$ will appear as $1g_i$

(v) Multiplication in the ring RG restricted to G is just the group operation.

(vi) G is subgroup of group of units of RG.

(vii) If $|G|>1$, then RG always has zero-divisors

Explanation: Let $g \in G$ & $o(g) = m > 1$

$$g^m = 1 \Rightarrow (1-g)\left(1 + g + ... + g^{m-1}\right) = 1 - g^m = 0$$

so $1-g$ is a zero divisor.

2.7. Matrix Ring

$M_n(R)$ the set of all $n \times n$ matrices with entries from ring R forms a ring with respect to ordinary matrix addition & ordinary matrix multiplication.

Properties:

(i) If R is any non-trivial ring (even a commutative one) & $n \geq 2$ then $M_n(R)$ is not commutative with unity.

(ii) $M_n(R)$ has zero-divisors for all non-trivial ring R whenever $n \geq 2$.

(iii) If R is infinite ring $M_n(R)$ has infinite zero-divisors whenever $n \geq 2$.

(iv) Center of ring $M_n(R)$ is set of all scalar matrices if R is commutative.

(v) If $n \geq 2$ then if A is strictly upper triangular matrix or strictly lower triangular matrix then $A^n = 0$

(vi) Property (v) implies that if R is infinite then $M_n(R)$ has infinite nilpotent elements.

2.8. $C[0,1]$ = {Set of All Continuous Functions from $[0,1]$ to $\mathbb{R}$}

Then $C[0,1]$ is a ring with respect to componentwise addition & componentwise multiplication.

i.e., $(f+g)(x) = f(x) + g(x) \quad \forall x \in [0,1]$

$$f.g(x) = f(x).g(x) \quad \forall x \in [0,1]$$

Properties:

(i) $C[0,1]$ is CRU.

(ii) There are infinite number of units.

(iii) Every function which are not zero at any point is unit.

(iv) There are functions which are neither zero divisor nor units.

(v) The functions which have finite or countable number of zero's in $[0,1]$ and have atleast one zero are neither zero-divisors nor units.

(vi) There are infinite zero divisors.

Example: $f(x) = \begin{cases} 0; & 0 \leq x \leq a \\ x-a; & a \leq x \leq 1 \end{cases}$

& $g(x) = \begin{cases} x-a; & 0 \leq x \leq a \\ 0; & a \leq x \leq 1 \end{cases}$

There are infinite choices for $a \in [0,1]$

CHAPTER 3

SUBRING AND IDEALS

3.1. Subring

Let $(R,+,\bullet)$ be a ring. Then non-empty subset S of R is called a subring of R, if $(S,+,\bullet)$ is a ring.

3.1.1. Subring Test

$S \neq \phi$ & $S \subseteq R$ then S is subring of R if and only if $\forall\ a,b,\in S$

(i) $ab \in S$

(ii) $a-b \in S$

Similarly we can define subfield of a field & Subdivision ring of a Division ring.

3.2. Subfield

A non-empty subset S of field F is said to be subfield of F if S forms a field under the binary operation of F.

3.2.1. Subfield Test

$S \neq \phi$, $S \subseteq F$ is said to be subfield iff $\forall\ a,b,\in S$ & $b \neq 0$

(i) $a-b \in S$

(ii) $ab^{-1} \in S$

Examples:

(a) $\mathbb{Q}$ is subring of $\mathbb{R}$

(b) $\mathbb{Z}$ is subring of $\mathbb{C}$.

(c) The set E of even integers is a subring of the ring $\mathbb{Z}$ of integers.

(d) The intersection of two subrings of a ring R is a subring of R.

Remark: The union of two subrings of R need not be a subring of R.

(e) $\{0,2,4\}$ is subring of $\left(\mathbb{Z}_6, \oplus_6, \odot_6\right)$

(f) $\mathbb{Z}[i]=\{a+bi \mid a,b \in \mathbb{Z}\}$ is subring of $(\mathbb{C},+,\bullet)$

(g) $S =$ {The set of all $n \times n$ Diagonal matrices over R } is subring of $M_n(R)$ under matrix addition & matrix multiplication.

(h) $(\mathbb{Z}_6, \oplus_6, \odot_6)$ is not subring of $(\mathbb{Z}_{12}, \oplus_{12}, \odot_6)$

(i) $S=\{a+bi+cj+dk;\ a,b,c,d\in\mathbb{Z}\}$ & $R=\{a+bi+cj+dk;\ a,b,c,d\in\mathbb{Q}\}$ where S is set of integral quaternions & R is set of rational quaternions then S is subring of R.

(j) $S=\{(r,r)|r\in R\}$ is subring of $R\times R$ where R is a ring.

(k) $S=\left\{\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix}: a,b\in\mathbb{R}\right\}$ & $R=M_2(\mathbb{R})$ then S is not a subring of R.

(l) Centre of a ring R, denoted by $Z(R)$, is a subring of R.

(m) Normalizer $N(a)$ of an element 'a' of a ring R is a subring of R where $N(a)=\{x\in R\,|\,ax=xa\}$

Observations:

(i) Center of a division ring is a field.

(ii) Subring of a commutative ring is commutative.

(iii) Subring of a ring without zero devisor is also without zero divisors.

(iv) There exist rings with unity 1 having a subring with unity not equal to 1.

Example: Consider $M_2(\mathbb{Z})=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}: a,b,c,d\in\mathbb{Z}\right\}$ which is a ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. It is easy to verify that $S=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}: a\in\mathbb{Z}\right\}$ is a subring of $M_2(\mathbb{Z})$ with unity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Since $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

thus $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\neq\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

(v) There exist rings with unity having a subring without unity.

Example: The ring $\mathbb{Z}$ of integers is a ring with unity. But the set E of even integers is a subring of $\mathbb{Z}$ without unity.

(vi) There exist non commutative rings with commutative subring.

Example: Consider the ring $M_2(\mathbb{Z})$ of 2×2 matrices over integers is non commutative

since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

and so $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\neq\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

But the set $S=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}: a\in\mathbb{Z}\right\}$ is a subring of $M_2(\mathbb{Z})$ which is commutative, since $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

(vii) There exist rings without unity having subring with unity.

Example: $R=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}$ is a ring which has no unity. The possible unity of R are $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and it can be verified that none of these is a unity of R.

However, $S=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}$ is a subring of R, which has $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ as the unity of S.

Definition: If S and T are two subring of a ring R, then their sum is defined as $S+T=\{a+b : a \in S, b \in T\}$

(viii) Sum of two subring of a ring may not be a subring.

Example: Let $S=\left\{\begin{pmatrix} a & c \\ b & 0 \end{pmatrix} : a,b,c \in \mathbb{Z}\right\}$, $T=\left\{\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} : c \in \mathbb{Z}\right\}$

It is clear that $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \in S+T$, $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}=\begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \notin S+T$

Hence $S+T$ is not a subring of $M_2(\mathbb{Z})$

(ix) In a subring $ax=b$ can have more than one solution.

(x) If $A \subseteq B \cup C \Rightarrow A \subseteq B$ or $A \subseteq C$ where A, B & C are subring of ring R.

(xi) Subring of integral domain will be integral domain.

(xii) If R be a ring with $\text{char}\, R=n$ then $M_2(R)$ has characteristic n.

(xiii) If S is a subring of a ring R then.

(a) If $\text{char}\, S$ & $\text{char}\, R$ are finite then $\text{char}\, S \leq \text{char}\, R$

(b) If S & R have same unity, then $\text{char}\, S = \text{char}\, R$.

3.3. Left Ideal

Let R be a ring and I be a subset of R then I is said to be left ideal of R if I is subring of R and for each $r \in R$ and $a \in I$, $ra \in I$

3.3.1. Right Ideal

Let R be a ring and I be subset of R then I is said to be right ideal of R if I is subring of R and for each $a \in I$, $r \in R$, $ar \in I$

3.3.2. Ideal

A subset I of a ring R is said to be ideal if I is both left ideal and right ideal.

3.3.3. Ideal Test

A Non- empty subset A of a ring R is an ideal of R if

(a) $a-b \in A$ whenever $a,b \in A$

(b) ra & $ar \in A$ whenever $a \in A$ & $r \in R$

Remarks:

(i) Let R be a ring then subring R and $\{0\}$ are ideal of R and called improper ideal of R

(ii) An ideal $I \neq R$ of a ring R is called proper ideal

(iii) Many authors consider $\{0\}$ as proper ideal and many improper ideal.

Examples:

(a) $\{0\}$ & R are always ideals of R & called Trivial ideals

(b) $n\mathbb{Z}$ is ideal of $\mathbb{Z}$.

(c) $M_n(k\mathbb{Z})$ is ideal of $M_n(\mathbb{Z})$ $\forall k \in \mathbb{Z}$

(d) Let R be ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$.

Let $A = \{f \in R | f(0) \text{ is even integer}\}$

Then A is subring but not an ideal of R.

(e) Let R be ring of all real valued functions of a real variable. Then the subset S of all differentiable functions is a subring of R but not an ideal of R.

(f) $A = \{(px, y) | x, b \in \mathbb{Z}\}$ is ideal of $\mathbb{Z} \times \mathbb{Z}$ where p is prime.

Properties:

(i) In a commutative ring R every left ideal or right ideal is ideal of R

(ii) Every ideal of a ring R is a subring of R but converse need not be true.

Example:

The set of integers $\mathbb{Z}$ is a subring of ring of rationals $\mathbb{Q}$ but it is not ideal of $\mathbb{Q}$ as

$$\frac{1}{2} \in \mathbb{Q} \text{ and } 3 \in \mathbb{Z} \text{ but } \frac{1}{2}.3 = \frac{3}{2} \notin \mathbb{Z}$$

(iii) Arbitrary intersection of ideals of R is an ideal of R.

(iv) Union of two ideals of a ring R need not be an ideal of R.

Example: We know $I = \langle 2 \rangle = \{..., -4, -2, 0, 2, 4, ...\}$ and $J = \langle 3 \rangle = \{..., -6, -3, 0, 3, 6, ...\}$ are two ideals in the ring $\mathbb{Z}$ of integers. Now $I \cup J = \{..., -6, -4, -3, -2, 0, 2, 3, 4, 6, ...\}$ and it is easy to see that $3 \in I \cup J$ and $2 \in I \cup J$, but $3 - 2 = 1 \notin I \cup J$, hence $I \cup J$ is not an ideal of $\mathbb{Z}$.

(v) The sum of two ideals of a ring R is an ideal of R i.e. if I and J are two ideals of a ring R, then $I + J = \{a + b : a \in I, b \in J\}$ is an ideals of R.

(vi) If I and J are two ideals of a ring R, then their product IJ defined as $\{IJ = a_1b_1 + a_2b_2 + ... + a_nb_n : a_i \in I, b_i \in J, 1 \leq i \leq n$ and n being a positive integer$\}$ is an ideal of R.

(vii) If I and J are two ideals of a ring R, then $IJ \subseteq I+J$.

(viii) Let R be a ring with unity 1 and I be an ideal of R. If $1 \in I$ then $I = R$

(ix) Let R be a ring with unity 1 and I be an ideal of R. If $u \in I$ then $I = R$, where u is any unit element of R.

(x) Let F be a field then $\{0\}$ and F are only ideals of F

(xi) Let R be a ring then Centre of ring $Z(R)$ is subring of R but it need not be ideal of R.

Example: Let $M_2(\mathbb{Z})$ be the ring of all 2×2 matrices over the integers.

For any $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ and $A = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \in M_2(\mathbb{Z})$ we see that

$$AX = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ap & bp \\ cp & dp \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} = XA.$$

Hence $A = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \in Z(M_2(\mathbb{Z}))$.

We proceed to show that $Z(M_2(\mathbb{Z}))$ is not an ideal of $M_2(\mathbb{Z})$.

For $S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Z}), A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in Z(M_2(\mathbb{Z}))$, we have

$$SA = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \notin Z(M_2(\mathbb{Z})).$$

Hence $Z(M_2(\mathbb{Z}))$ is not an ideal of $M_2(\mathbb{Z})$.

Observations:

(i) If R is a commutative ring then

$N(R) = \{a \mid a \in R \ \& \ a^m = 0 \ \text{ for some } m \geq 1\}$ is an ideal in R.

$N(R)$ is called nil-radical of R.

(ii) If R is a commutative ring then $\sqrt{I} = \{a \in R \mid a^n \in I \ \text{ for some } n \geq 1\}$

Note: If $I = 0$, Then $\sqrt{I}$ is the Nil-radical.

(iii) Any ideal of $\mathbb{Z}\times\mathbb{Z}$ is of the form $m\mathbb{Z}\times n\mathbb{Z}$; $m,n \in \mathbb{Z}$

(iv) If R is commutative ring , $a_1 a_2 \ldots . a_n \in R$ then $I = Ra_1 + Ra_2 + \ldots . + Ra_n$ is a_n ideal in R.

Explanation: If $x, y \in I$, Then $x = \lambda_1 a_1 + \ldots . \lambda_n a_n$

$y = \mu_1 a_1 + \ldots . + \mu_n a_n$

$x - y = (\lambda_1 - \mu_1)a_1 + \ldots . + (\lambda_n - \mu_n)a_n \in I$

$\Rightarrow \quad x - y \in I$

$\& \quad ax = a\lambda_1 a_1 + \ldots . + a\lambda_n a_n \in I; \ a \in R$

$\Rightarrow \quad ax \in I$

Hence I is ideal.

(v) R be commutative ring & $A \subset R$. $Ann(A) = \{r \in R | ra = 0 \ \forall a \in A\}$ is an ideal.

(vi) $N(\mathbb{Z}_n)$ i.e. nil-radical of $\mathbb{Z}_n$ is non-zero iff n is divisible by square of a prime.

Reason: Let n is divisible by square of prime p.

Then $n = p^{\lambda}m; \lambda \geq 2; g.c.d.(m, p) = 1$

Then $\bar{a} = \overline{pm} \in \mathbb{Z}_n; \bar{a} \neq \bar{0}$ & $(\bar{a})^{\lambda} = 0$

Thus $\mathbb{Z}_n$ has non-zero element $\bar{a}$ in the nil-radical.

Conversely, assume that

$\exists \ \bar{a} \neq 0$ in nilradical.

Then $(\bar{a})^{\lambda} = \bar{0} \ \ (\lambda \geq 2)$

If p is prime factor of a

$\Rightarrow \quad p^{\lambda}$ divides n; $\lambda \geq 2$

Remark: In $\mathbb{Z}_n$, $\exists$ (non-zero) nilpotent element if and only if n is divisible by square of a prime.

3.3.4. Ideal Generated by a Set

Let S be any subset of a ring R. An ideal I of R is said to be generated by S if

(i) $S \subseteq I$

(ii) If J is any ideal of R such that $S \subseteq J$, then $I \subseteq J$.

We write ideal I as $I = \langle S \rangle$. Indeed $\langle S \rangle$ is the smallest ideal containing S

3.3.5. Co-maximal Ideals

Two ideals I and J of a ring R satisfying $I + J = R$ are called co-maximal ideals.

Results:

(i) Let I and J be any two ideals of a ring R. Then $I + J$ is an ideal of R generated by $I \cup J$.

(ii) If I and J are two ideals of a ring R, then $I \cup J$ is an ideal of R iff either $I \subseteq J$ or $J \subseteq I$.

(iii) Let I and J be two ideals of a commutative ring R with unity such that $I + J = R$. Then $IJ = I \cap J$.

Observations:

(i) Let I be left ideal and J is right ideal of a ring then IJ is always an ideal of R but JI may not be even one sided ideal.

Example: The set $I=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}: a,b\in\mathbb{Z}\right\}$ is a left ideal and

$J=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}: a,b\in\mathbb{Z}\right\}$ is a right ideal in the ring $M_2(\mathbb{Z})$ of 2×2 matrices over integers.

We see that $\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}=\begin{pmatrix} ac+bd & 0 \\ 0 & 0 \end{pmatrix}$

Thus $JI=\left\{\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}: x\in\mathbb{Z}\right\}$. We take $S=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\in JI$ and $T=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\in M_2(\mathbb{Z})$.

$ST=\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\notin JI$ and $TS=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\notin JI$

Hence JI is neither a left ideal nor a right ideal of $M_2(\mathbb{Z})$

(ii) The intersection of two left (right) ideals of a ring R is a left (right) ideals of R.

(iii) The intersection of a left ideal and right ideal of a ring R may not be even a one sided ideal of R.

Example: The set $I=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}: a,b\in\mathbb{Z}\right\}$ is a left ideal and

$J=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}: a,b\in\mathbb{Z}\right\}$ is a right ideal in the ring $M_2(\mathbb{Z})$ of 2×2 matrices over integers.

$I\cap J=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}: a\in\mathbb{Z}\right\}$ clearly, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\in I\cap J$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\in M_2(\mathbb{Z})$

But $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\notin I\cap J,$

$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\notin I\cap J,$

(iv) The sum of two left (right) ideals of a ring R is left (right) ideal of R.

(v) The sum of a left ideal and a right ideal of a ring R may not ideal of R.

Example: The set $I=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}: a,b\in\mathbb{Z}\right\}$ is a left ideal and

$J=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}: a,b\in\mathbb{Z}\right\}$ is a right ideal in the ring $M_2(\mathbb{Z})$ of 2×2 matrices over integers.

We have $I+J=\left\{\begin{pmatrix} x & z \\ y & 0 \end{pmatrix}: x,y,z\in\mathbb{Z}\right\}$.

Clearly, $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\in I+J$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\in M_2(\mathbb{Z})$ but

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}\notin I+J$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}\notin I+J$

Thus $I+J$ is not even a one-sided ideal of $M_2(\mathbb{Z})$.

(vi) There exist ideals I and J of a ring R such that $I\subseteq J\subseteq R$ where I is ideal of J and J is ideal of R but I is not ideal of R.

Example: Let $R=\left\{\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ 0 & 0 & z \end{pmatrix}: x_i,y_i,z\in\mathbb{Z}\right\}$,

$I=\left\{\begin{pmatrix} 0 & 0 & x \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}: x\in\mathbb{Z}\right\}$, $J=\left\{\begin{pmatrix} 0 & 0 & x \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix}: x,y\in\mathbb{Z}\right\}$.

Then I is an ideal of J, J is an ideal of R. But I is not an ideal of R, since

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\notin I.$$

(vii) Let R be a ring with unity and I be proper ideal of R then no element of I can have multiplicative inverse.

(viii) Let I be an ideal of ring R such that $I\neq R$ and R has unity 1 then $1\notin I$

(ix) Let I be an ideal of ring R and S be subring of R. Then $I\cap S$ is ideal of S

(x) Let $\mathbb{Z}$ be ring of integers and $\langle m\rangle, \langle n\rangle$ be ideals of $\mathbb{Z}$. Then

(a) $\langle m\rangle+\langle n\rangle=\langle a\rangle$, where a is *GCD* of m,n

(b) $\langle m\rangle\cap\langle n\rangle=\langle b\rangle$, where b is *LCM* of m,n

(xi) Every ideal of $M_n(R)$ ring of all $(n \times n)$ matrix over ring R, is of the form $M_n(J)$ where J is an ideal of R.

3.4. Simple Ring

A ring R is called a simple ring, if

(a) There exist two element a, b in R such that $ab \neq 0$.

(b) R has no proper ideals i.e., the only ideals of R are $\{0\}$ and R.

Results:

(i) Every division ring is simple ring

(ii) Let R be a commutative simple ring with unity. Then R is a field.

(iii) A commutative ring R with unity is a field iff it has no proper ideals.

(iv) The set of 2×2 matrices over rational numbers i.e., $M_2(\mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Q} \right\}$ is a simple ring.

(v) Characteristic of simple ring is either zero or prime.

(vi) If D is division ring $M_n(D)$ is simple.

3.4.1. Maximal Ideal

An ideal M in a ring R is called maximal ideal of R if $M \neq R$ and the only ideals containing M are M and R i.e. if $\exists$ ideal U of R such that $M \subseteq U \subseteq R$. Then either $M = U$ or $U = R$.

Examples:

(a) $A = \{(px, y) | x, y \in \mathbb{Z}\}$ is maximal ideal of $\mathbb{Z} \times \mathbb{Z}$ where p is prime.

(b) $A = \{(3x, y) | x, b \in \mathbb{Z}\}$ is maximal ideal of $\mathbb{Z} \times \mathbb{Z}$

(c) $p\mathbb{Z}$ is maximal ideal of $\mathbb{Z}$, where p is prime.

(d) $\{(0,0),(0,1)\}$ & $\{(0,0),(1,0)\}$ are the maximal ideal of $\mathbb{Z}_2 \times \mathbb{Z}_2$

(e) $2\mathbb{Z} \times \mathbb{Z}$ is maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.

(f) $A = \left\{ f \in C[0,1] : f\left(\frac{1}{2}\right) = 0 = f\left(\frac{1}{3}\right) \right\}$ is not maximal ideal.

(g) $A = \left\{ f \in C[0,1] : f\left(\frac{1}{2}\right) = 0 \right\}$ is maximal ideal.

3.4.2. Prime Ideal

Let R be a commutative ring. An ideal P is called a prime ideal if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of them is an element of P i.e. whenever $ab \in P$ then either $a \in P$ or $b \in P$.

Examples:

(a) $I=\{(a,0): a\in\mathbb{Z}\}$ then I is prime ideal of $\mathbb{Z}\times\mathbb{Z}$ but not a maximal ideal.

(b) $p\mathbb{Z}$ is prime ideal of $\mathbb{Z}$. Where p is prime number.

(c) $\{(0,0),(0,1)\}$ & $\{(0,0),(1,0)\}$ are the prime ideal of $\mathbb{Z}_2\times\mathbb{Z}_2$.

(d) $A=\left\{f\in C[0,1]: f\left(\frac{1}{2}\right)=0=f\left(\frac{1}{3}\right)\right\}$ is not prime ideal.

(e) $A=\left\{f\in C[0,1]: f\left(\frac{1}{2}\right)=0\right\}$ is prime ideal.

Results:

(i) Let R be commutative ring. Then R is field if and only if $\{0\}$ is maximal ideal of R.

(ii) An ideal $M=n\mathbb{Z}=\{nx: x\in\mathbb{Z}\}$ is maximal ideal of $\mathbb{Z}$ if and only if n is prime number.

(iii) Let R be a ring of all real-valued continuous function on the closed interval $[a,b]$. Then for $c\in(a,b)$, $M=\{f\in R: f(c)=0\}$ is maximal ideal of R.

(iv) Let R be a commutative ring with unity. Then an ideal M of R is maximal if and only if $\frac{R}{M}$ is a field.

(v) Let R be a commutative ring. Then an ideal M of R is maximal if and only if $\frac{R}{M}$ is a simple ring.

(vi) For each prime number $p, \frac{\mathbb{Z}}{\langle p\rangle}$ is a field.

(vii) Let R be a ring with unity. Then an ideal M of R is maximal if and only if $M+\langle a\rangle=R\ \forall a\notin M$.

(viii) Let R be a commutative ring. Then the ideal P of R is prime ideal in R if and only if $\frac{R}{P}$ is an integral domain.

(ix) Let R be a commutative ring with unity then every maximal ideal of R is prime ideal of R. But the converse need not be true.

Example: $\{0\}$ is prime ideal of $\mathbb{Z}$ but not maximal ideal of $\mathbb{Z}$.

(x) The prime ideals of $\mathbb{Z}$ are just the ideals generated by prime numbers p together with the ideal $\{0\}$.

(xi) Let R be a commutative ring and I, J be ideals of R and P is prime ideal of R such that $IJ \subseteq P$. Then either $I \subseteq P$ or $J \subseteq P$.

(xii) Let R be finite commutative ring with unity. An ideal I of R is maximal if and only if I is prime ideal of R.

Observation:

(i) There exists a finite commutative ring which has maximal ideal which is not prime ideal.

Example: Consider the ring $R = \{0,2,4,6\}$ under addition and multiplication modulo 8. Then R is a finite commutative ring without unity has ideal $\{0,4\}$ which is maximal but not prime.

(ii) The intersection of two prime ideals of a ring R may not be prime ideal of R.

(iii) The intersection of two maximal ideals of a ring R may not be maximal ideal of R

Example: Let $I = \langle 2 \rangle = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$ and

$J = \langle 3 \rangle = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$,

Then I and J are two prime (maximal ideals) of $\mathbb{Z}$ we have

$I \cap J = \{..., -12, -6, 0, 6, 12, ...\} = \langle 6 \rangle$

Then $I \cap J$ is neither a prime ideal nor maximal ideal of $\mathbb{Z}$

(iv) The sum of two prime (maximal) ideals of a ring R may not be prime (maximal) ideal of R.

Example: Let $R = \mathbb{Z}$ and $I = \langle 2 \rangle, J = \langle 3 \rangle$ be prime ideals of $\mathbb{Z}$. Then

$I + J = \langle 2 \rangle + \langle 3 \rangle = \mathbb{Z}$, which is not a prime ideal.

Note: Similar example can be used in the case of maximal ideals.

(v) The product of two prime (maximal) ideal of a ring R may not be prime (maximal) ideal.

Example: In ring of integers $\mathbb{Z}$ and $I = \langle 2 \rangle, J = \langle 3 \rangle$ are prime ideals of $\mathbb{Z}$.

But $IJ = \langle 2 \rangle \langle 3 \rangle = \langle 6 \rangle$ which is not a prime ideal.

Note: Similar argument can be used for the case of maximal ideals.

(vi) Let R be commutative ring with ideal I then if P is prime ideal of I then P is prime ideal of R.

(vii) Let R be Boolean ring. Then each proper prime ideal P of R is maximal ideal.

CHAPTER 4

RING OF POLYNOMIALS

One of the mathematical concepts that students are most familiar with and most comfortable with is that of a polynomial. In high school students study polynomials with integer coefficients, rational coefficients, real coefficients, and perhaps even complex coefficients. Notice that all of these sets of polynomials with addition of polynomials and multiplication of polynomials are rings and in each case the set of coefficients is also a ring in this chapter we abstract all of these examples into one.

4.1. Polynomial Ring

Let R be a ring, then the set $R[x]=\left\{a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0 : a_i \in R,\ n \in \mathbb{N}\cup\{0\}\right\}$ forms a ring with respect to addition and multiplication of polynomials as defined below

if $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$

& $g(x)=b_mx^m+b_{m-1}x^{m-1}+...+b_1x+b_0$

be two elements in $R[x]$

then

$$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+.....$$

$$f(x).g(x)=C_{m+n}x^{m+n}+....+C_2x^2+C_1x+C_0$$

Where $C_k=a_0b_k+a_1b_{k-1}+...+a_kb_0$ the ring $R[x]$ is considered as ring of polynomials.

Note:

(a) In the first place, we'll call 'x' an indeterminate rather than a variable. The symbols $x,x^2,...$ here are not unknown elements or variables from the ring R. These are there only for convenience, say as place indicators for the elements $a_1,a_2,...$ of the ring.

(b) One of the polynomials in the ring $\mathbb{Z}[x]$ is $1x$, which we shall write simply as x. Now x is not 1 or 2 or any other element of $\mathbb{Z}[x]$, thus from now we'll never write such things as "$x=1$" or "$x=2$". We call x an indeterminate rather than a variable to emphasize this change. Also we'll never write an expression such as "$x^2-4=0$", simply because x^2-4 is not the zero polynomial in our ring $\mathbb{Z}[x]$.

Examples:

(a) $\mathbb{Z}[x]$

(b) $\mathbb{R}[x]$

(c) $\mathbb{C}[x]$

(d) $\mathbb{Z}_n[x]$

(e) $\mathbb{Q}[x]$

4.2. Degree of a Polynomial

Let $f(x)=a_0+a_1x+...+a_nx^n \in R[x]$, we say that $f(x)$ is a non-zero polynomial if atleast one of the co-efficients $a_0,a_1,...,a_n$ is non-zero.

We say that $f(x)$ has degree n if $a_n \neq 0$ .We write it as $\deg f(x)=n$ or $\deg f=n$.

In other words, the degree of $f(x)$ is the largest integer i for which the i^{th} co-efficient of $f(x)$ is not zero. Consequently, if $\deg f(x)=n$, then $a_n \neq 0$ and $a_i=0 \quad \forall i>n$

We say degree of $f(x)$ is zero if $a_0 \neq 0$ and $a_i=0 \ \forall i>0$

In this case $f(x)$ is called a constant polynomial.

Remarks:

(i) We do not define degree of the zero polynomial.

(ii) If $f(x)\neq 0 \in R[x]$, then the degree of $f(x)$ is a non-negative integer

Note: Let R be a ring and $f(x)$ and $g(x)$ be two non-zero polynomials in $R[x]$ then

(iii) If $f(x)+g(x)\neq 0$, then $\deg\big(f(x)+g(x)\big)\leq \max\{\deg f(x),\deg g(x)\}$

(iv) If $f(x).g(x)\neq 0$, then $\deg\big(f(x).g(x)\big)\leq \deg f(x)+\deg g(x)$

(v) If R is an integral domain, then $\deg\big(f(x).g(x)\big)=\deg f(x)+\deg g(x)$
Provided $f(x).g(x)\neq 0$

(vi) $\exists$ rings $R[x]$, which has polynomials $f(x), g(x)$ such that

(a) $\deg\big(f(x)+g(x)\big)<\max\{\deg f(x),\deg g(x)\}$

(b) $\deg\big(f(x).g(x)\big)<\deg f(x)+\deg g(x)$ Provided that $f(x)+g(x)\neq 0$ & $f(x).g(x)\neq 0$

Example:

(a) Let $f(x)=2+3x+4x^2 \in \mathbb{Z}[x]$ & $g(x)=2+3x-4x^2 \in \mathbb{Z}[x]$
$f(x)+g(x)=4+6x$ $\deg\big(f(x)+g(x)\big)=1<\max\{\deg f(x),\deg g(x)\}$

(b) Let $f(x)=1+2x^2, g(x)=3+x+2x^3$ $f(x),g(x)\in \mathbb{Z}_4[x]$
$f(x)\cdot g(x)=3+x+6x^2+4x^3+4x^5$

$= 3 + x + 2x^2 + 0x^3 + 0x^5$

$= 3 + x + 2x^2 \Rightarrow \deg\big(f(x), g(x)\big) = 2$

Hence $2 = \deg\big(f(x) \cdot g(x)\big) < \deg f(x) + \deg g(x) = 5$

Observations:

(i) If ring R is CRU then $R[x]$ is CRU. Moreover, unity of $R[x]$ is same as that of R.

Proof: If R is commutative

$f(x) = a_0 + a_1 x + \ldots + a_m x^m$

$g(x) = b_0 + b_1 x + \ldots + b_n x^n$

be two numbers of $R[x]$, then by definition of product.

$f(x)g(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \ldots.$

$= b_0 a_0 + (b_0 a_1 + b_1 a_0)x + \ldots.$

$= g(x) f(x)$

if R has unity 1 then the polynomial $e(x) = 1 + 0x + 0x^2 + \ldots.$ is unity of $R[x]$.

Converse of the above result is also true.

(ii) If R be a commutative ring with unity then units of R are also units of $R[x]$

Proof: Let a_0 be unit in R

$\Rightarrow$ $\exists$ some $b_0 \in R$ such that $a_0 b_0 = 1$

Let $f(x) = a_0 + 0x + 0x^2 + \ldots$

& $g(x) = b_0 + 0x + 0x^2 + \ldots$

then $f(x).g(x) = a_0 b_0 = 1$

$\Rightarrow$ $f(x)$ is unit in $R[x]$.

(iii) If R is an integral domain then units of R and $R[x]$ are same.

(iv) If R is CRU and have zero-divisors then $R[x]$ may have more units than R.

(v) If R is an integral domain, then $R[x]$ is also an integral domain.

Proof: Let R be an integral domain

Let $f(x), g(x)$ be two non-zero elements of $R[x]$ such that $f(x)g(x) = 0$

where $f(x)=a_0+a_1x+....+a_mx^m$

$g(x)=b_0+b_1x+....+b_nx^n$

Since both $f(x)$ & $g(x)$ can not be constant polynomials

If constants then $a_0\neq 0,\ b_0\neq 0$

So $a_0b_0\neq 0$

$\therefore\ f(x)g(x)\neq 0$

Since atleast one of them is non-constant polynomial its degree is ≥ 1.

R being an integral domain

$\deg\big(f(x)g(x)\big)=\deg f(x)+\deg g(x)\geq 1$

Which is a contradiction as $f(x)g(x)=0$

$\Rightarrow$ either $f(x)=0$ or $g(x)=0$

$\Rightarrow$ $R[x]$ is an integral domain.

(vi) If R is a field then $R[x]$ is an integral domain. Infact, $R[x]$ can never be field.

Proof: Consider a non-zero polynomial

$f(x)=0+1x+0x^2+...$

Let $g(x)=b_0+b_1x+b_2x^2+....$ be the multiplicative inverse of $f(x)$

then $f(x)g(x)=c_0+c_1x+c_2x^2$

should be unity $e(x)=1+0x+0x^2+....$ of $R[x]$

$\Rightarrow\quad c_0=1,\quad c_i=0\ \ \forall\, i>0$

where $c_0=a_0b_0=0.b_0=0\neq 1$

hence no $g(x)$ can be inverse of $f(x)=x$

$\Rightarrow$ $R[x]$ is not a field.

(vii) If R is a field. Then an element of $R[x]$ is unit if and only if it is a non-zero constant polynomial over R. i.e., $\alpha\in R[x]-\{0\}$ is unit $\Leftrightarrow\ \alpha\in R-\{0\}$

(viii) If R is a non-trivial ring. Then $R[x]$ is always infinite ring.

(ix) If characteristic of a commutative ring R is m. Then characteristic of ring $R[x]$ is also m.

(x) If I is ideal of ring R, then $I[x]$ is ideal of ring $R[x]$.

(xi) If R be CRU & A be an ideal of R. Then $\frac{R[x]}{A[x]} \cong \frac{R}{A}[x]$.

(xii) If R be a ring. Then $\frac{R[x]}{\langle x \rangle} \cong R$ where $\langle x \rangle$ is ideal generated by x.

(xiii) If R is CRU & P be any prime ideal of R. Then $P[x]$ is prime ideal of $R[x]$.

(xiv) If R is CRU & M is maximal ideal of R. Then $M[x]$ may not be maximal ideal of $R[x]$.

Example: Let $R = \mathbb{Z}$, the ring of integers & $2\mathbb{Z}$ be maximal ideal of $\mathbb{Z}$.

But $2\mathbb{Z}[x]$ is not maximal ideal of $\mathbb{Z}[x]$

(xv) If F be an infinite field and $f(x) \in F[x]$, if $f(a) = 0$ for infinitely many elements a of F. Then $f(x)$ is a zero polynomial. Consequently, if $f(x), g(x) \in F[x]$ and if $f(a) = g(a)$ for infinitely many elements 'a' of F then $f(x) = g(x)$.

(xvi) If R is a ring. Then R can be embedded in $R[x]$ i.e., every ring R is isomorphic to a subring of $R[x]$

Proof: Define a mapping $\phi : R \to R[x]$

as $\phi(a) = a + 0x + 0x^2 + \ldots \quad \forall\, a \in R$

this one-to-one since for any $a, b \in R$

$\phi(a) = \phi(b)$

$\Rightarrow \quad a + 0x + 0x^2 + \ldots = b + 0x + 0x^2 + \ldots$

$\Rightarrow \quad a = b$

Now, we show that ϕ is a homomorphism.

We have, $\phi(a+b) = (a+b) + 0x + 0x^2 + \ldots$

$= \left(a + 0x + 0x^2 + \ldots\right) + \left(b + 0x + 0x^2 + \ldots\right)$

$= \phi(a) + \phi(b)$

and $\phi(ab) = ab + 0x + 0x^2 + \ldots$

$= \left(a + 0x + 0x^2 + \ldots\right)\left(b + 0x + 0x^2 + \ldots\right)$

$= \phi(a) \cdot \phi(b)$

Hence ϕ is an isomorphism from R into $R[x]$

i.e., R can be embedded in $R[x]$

(xvii) If R & R' are two isomorphic rings then $R[x]$ and $R'[x]$ are also isomorphic rings.

(xviii) If $\phi: R \to R'$ be a ring homomorphism then define $\psi: R[x] \to R'[x]$ as $\psi\left(a_0 + a_1x + ... + a_nx^n\right) = \phi(a_0) + \phi(a_1) + ... + \phi(a_n)x^n$ ψ is also a ring homomorphism.

(xix) For each prime p, $x^{p-1} - 1 = (x-1)(x-2)...(x-(p-1))$ in $\mathbb{Z}_p[x]$.

(xx) Let R be a commutative ring if $f(x) = a_0 + a_1x + ... + a_mx^m \in R[x]$ is a zero-divisor, then $\exists$ an element $b \neq 0$ in R such that $ba_0 = ba_1 = ... = ba_m = 0$

(xxi) Let $f(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$ then

(a) $f(x)$ is unit in $R[x] \Leftrightarrow a_0$ is unit and $a_1, a_2, ..., a_n$ are nilpotent in R.

(b) $f(x) \in R[x]$ is nilpotent $\Leftrightarrow a_0, a_1, ..., a_n$ are nilpotent in R.

(xxii) A polynomial $f(x) \in F[x]$ (where F is a field) of degree n can have atmost n zeros counting multiplicity.

(xxiii) The quotient ring $\dfrac{\mathbb{R}[x]}{\langle x^2+1 \rangle}$ is isomorphic to field of complex numbers $\mathbb{C}$.

4.3. Division Algorithm

Let R be a field and $f(x), g(x) \in R[x]$ with $g(x) \neq 0$. Then $\exists$ unique polynomials $q(x)$ and $r(x)$ in $R[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

4.3.1. The Remainder Theorem

Let F be a field and $a \in F$ and $f(x) \in F[x]$, then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

4.3.2. The Factor Theorem

Let F be a field and $a \in F$ and $f(x) \in F[x]$. Then a is a zero of $f(x)$ iff $x - a$ is a factor of $f(x)$

4.3.3. Greatest Common Divisor (GCD)

Let R be a commutative ring and $f(x)$, $g(x)$ be two non-zero elements of $R[x]$. A non-zero element $h(x) \in R[x]$ is called GCD of $f(x)$ and $g(x)$ if

(i) $h(x)$ divides $f(x)$ and $h(x)$ divides $g(x)$ and

(ii) Whenever we have $0 \neq k(x) \in R[x]$ such that $k(x) / f(x), k(x) / g(x)$ then $k(x) / h(x)$. It is denoted by $(f(x), g(x)) = h(x)$

4.3.4. Least Common Multiple (LCM)

Let R be a commutative ring and $f(x), g(x)$ be two non-zero elements of $R[x]$. A non-zero element $l(x) \in R[x]$ is called LCM of $f(x)$ and $g(x)$ if

(a) $f(x)/l(x),\ g(x)/l(x)$

(b) Whenever we have $0 \neq h(x) \in R[x]$ such that $f(x)/h(x)$ and $g(x)/h(x)$. Then $l(x)/h(x)$, LCM of $f(x), g(x)$ is denoted by $[f(x), g(x)] = l(x)$.

4.4. Irreducible Polynomial and Reducible Polynomial

Let R be an integral domain. A polynomial $f(x) \in R[x]$ of positive degree $(\text{i.e. } \deg \geq 1)$ is said to be an irreducible polynomial over R if it can not be expressed as product of two polynomials of positive degree. In other words, if whenever $f(x) = g(x)h(x)$ then $\deg g = 0$ or $\deg h = 0$.

A polynomial of positive degree which is not irreducible is called reducible over R.

Remarks:

(i) Polynomials of degree 1 are irreducible over field F.

(ii) We should be careful while talking about irreducible elements and irreducible polynomials as the following example shows us the difference between the two.

Example: Consider the polynomial $f(x) = 2x^2 + 2$. Since it can not be expressed as product of two positive degree polynomials in $\mathbb{Z}[x]$.

We notice it is irreducible polynomial over $\mathbb{Z}$.

Again,

$2x^2 + 2 = 2(x^2 + 1)$

= product of two polynomials

$= g(x)h(x)$ (say)

Since g & h are the non-units in $\mathbb{Z}$ and therefore of $\mathbb{Z}[x]$.

We find $2x^2 + 2$ can be expressed as product of two non-units and thus $f(x) = 2x^2 + 2$ is not an irreducible element in $\mathbb{Z}[x]$.

Hence an irreducible polynomial need not be an irreducible element.

(iii) But every irreducible element in $R[x]$ is an irreducible polynomial where R is an integral domain with unity.

Proof: Let $f(x) \in R[x]$ be any irreducible element.

Suppose $f(x)$ is reducible polynomial

Then $f(x) = g(x)h(x); g(x), h(x) \in R[x]$ where degree $g(x) > 0$, degree $h(x) > 0$

Since degree of g & h is positive.

$\Rightarrow g$ & h are not constant polynomials

$\therefore g, h \notin R$

$\Rightarrow g, h$ cannot be units in R

$\Rightarrow g, h$ cannot be units in $R[x]$

$\Rightarrow f(x)$ is not irreducible element.

This contradiction proves our result.

(iv) If F is a field, then every irreducible polynomial of $F[x]$ is irreducible element of $F[x]$ and conversely.

4.5. Irreducibility Tests

1. If a polynomial $f(x)$ is of degree >1 and $f(a)=0$ for some $a \in F$. Then $f(x)$ is reducible over F, where F is a field.

2. **Reducibility Test for degree 2 and 3 :** Let F be a field if $f(x) \in F[x]$ and $\deg f(x)=2$ or 3 then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

   Example:

   (a) $f(x)=2x^2+4 \in \mathbb{R}[x]$

   Since $f(x)$ has no zero in $\mathbb{R}$

   $\Rightarrow$ $f(x)$ is irreducible over $\mathbb{R}$

   But, it is reducible over $\mathbb{C}$.

   (b) $f(x)=x^2-2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$, since $f(x)$ has no zero in $\mathbb{Q}$. But it is reducible over $\mathbb{R}$.

   (c) $f(x)=x^2+1$ is irreducible over $\mathbb{Z}_3$, but reducible over $\mathbb{Z}_5$.

3. Let $f(x) \in \mathbb{Z}[x]$ if $f(x)$ is reducible over $\mathbb{Z}$, then it is reducible over $\mathbb{Q}$.

4. **Mod p irreducibility Test:** Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f \geq 1$. Let $f_p(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the co-efficients of $f(x)$ modulo p if $f(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg f(x)=\deg f_p(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

   Remark: Be careful, do not use the converse of above statement if $f(x) \in \mathbb{Z}[x]$ and $f_p(x)$ is reducible over $\mathbb{Z}_p$ for some p, $f(x)$ may still be irreducible over $\mathbb{Q}$.

   For example, consider $f(x)=21x^3-3x^2+2x+8$

Then $f_2(x)=x^3+x^2\in\mathbb{Z}_2[x]$

$f_2(x)=x^2(x+1)$ is reducible

But $f(x)$ is irreducible over $\mathbb{Q}$.

Note that, this example shows that mod p irreducibility test may fail for some p and work for others.

To conclude that a particular $f(x)\in\mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$. All we need to do is to find a single p for which the corresponding polynomial $f_p(x)$ is $\mathbb{Z}_p[x]$ is irreducible.

However, this is not always possible since $f(x)=x^4+1$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}_p$ for every prime p. The mod p irreducibility test can be helpful in checking for irreducibility of polynomials of degree greater than 3 and polynomials with rational coefficients.

Examples:

(a) $f(x)=21x^3-3x^2+2x+9$

then over $\mathbb{Z}_2$, we have $f_2(x)=x^3+x^2+1$

$f_2(0)=1$ and $f_2(1)=1$

$\Rightarrow$ $f_2(x)$ is irreducible over $\mathbb{Z}_2$

$\Rightarrow$ $f(x)$ is irreducible over $\mathbb{Q}$.

(b) $f(x)=6x^3+8x^2+6x-4$

then over $\mathbb{Z}_5$, $f_5(x)=x^3+3x^2+x-4$

$f_5(0)=1$, $f_5(1)=1$, $f_5(2)=3$

$f_5(3)=3$, $f_5(4)=2$

$\Rightarrow$ $f_5(x)$ irreducible over $\mathbb{Z}_5$

$\Rightarrow$ $f(x)$ is irreducible over $\mathbb{Q}$.

5. Let F be a field and $a\in F$ and $a\neq 0$

(a) If $af(x)$ is irreducible over F, then $f(x)$ is irreducible over F.

(b) If $f(ax)$ is irreducible over F, then $f(x)$ is irreducible over F.

(c) If $f(x+a)$ is irreducible over F, then $f(x)$ is irreducible over F.

6. Eisenstein's Criterion: Let $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0\in\mathbb{Z}[x]$ if $\exists$ a prime p such that $p\nmid a_n$, $p\mid a_{n-1}$, $p\mid a_{n-1}\ldots p\mid a_0$ and $p^2\nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Examples:

(a) Let $f(x)=x^2-4x+2$

Let $p=2$ then $p/-4,\ p/2,\ p\nmid 1,\ p^2\nmid 2$

$\Rightarrow f(x)$ is irreducible over $\mathbb{Q}$.

(b) Consider the polynomial $f(x)=x^2+1$

Since, there is no prime which divides 1.

We can not apply the Eisenstein's Criterion to $f(x)$.

Consider $f(x+1)=(x+1)^2+1$

$=x^2+2x+2$

$a_0=2, a_1=2, a_2=1$

Take $p=2$, then $p/2,\ p\nmid 1,\ p^2\nmid 2$

$\Rightarrow f(x+1)$ is irreducible over $\mathbb{Q}$

$\Rightarrow f(x)$ is irreducible.

(c) Let $f(x)=x^3+x^2-2x-1$

Since there is no prime that divides 1, we can not apply the criterion here.

Consider $f(x+1)=(x+1)^3+(x+1)^2-2(x+1)-1$

$=x^3+4x^2+3x-1$

We have the same situation

Let us consider

$f(x-1)=(x-1)^3+(x-1)^2-2(x-1)-1$

$=x^3-2x^2-x-1$

Again it is not possible to apply the criterion.

Consider $f(x+2)=x^3+7x^2+14x+7$

Then $p=7$ will work here

as $7/7,\ 7/14,\ 7/7,\ 7\nmid 1,\ 7^2\nmid 7$

thus by Eisenstein's Criterion, $f(x+2)$ is irreducible & hence $f(x)$ is irreducible.

Remark: One may note that Eisenstein's Criterion is not necessary for irreducibility of a polynomial. As we have seen there does not exists prime p such that $p/1$ (although the polynomial could be irreducible). x^3-x+1 is irreducible over $\mathbb{Q}$ but Eisenstein's Criterion is not applicable.

Example: The polynomial $f(x)=x^3-x+1$ is irreducible over $\mathbb{Q}$.

Suppose it is reducible, then it has a root in $\mathbb{Q}$.

Let $\frac{m}{n}\{m,n\in\mathbb{Z}\ \&\ n\neq 0,(m,n)=1\}$ be a root.

Then $\frac{m^3}{n^3}-\frac{m}{n}+1=0$

$\Rightarrow m^3-mn^2+n^3=0$

$\Rightarrow m^3=n^2(m-n)$

$\Rightarrow n^2/m^3 \Rightarrow n/m^3.1 \Rightarrow n/1\ [\text{as } (m,n)=1]$

$\Rightarrow n=\pm 1$

$\Rightarrow \frac{m}{n}=\pm m$

or that $m^3-m+1=0$

$\Rightarrow m(m^2-1)=-1$

$\Rightarrow \frac{m}{-1}$ or that $m=\pm 1$

which gives $1-1+1=0$

which is not possible. Hence x^3-x+1 is not reducible over $\mathbb{Q}$.

7. If p is a prime number, then the polynomial x^n-p is irreducible over the rational numbers $\mathbb{Q}$.

8. **Irreducibility of pth Cyclotomic Polynomial:** For any prime p, the pth cyclotomic polynomial $\phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\ldots+x+1$ is irreducible over $\mathbb{Q}$.

Proof: $\phi_p(x)=x^{p-1}+x^{p-2}+\ldots+x+1=\frac{x^p-1}{x-1}$

Now

$$\phi_p(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=\frac{x^p+{}^pC_1x^{p-1}+\ldots{}^pC_rx^{p-r}+\ldots+{}^pC_p-1}{x}$$

$$=\frac{x^p+{}^pC_1x^{p-1}+\ldots+{}^pC_{p-1}x}{x}$$

$$=x^{p-1}+{}^pC_1x^{p-2}+\ldots+{}^pC_{p-1}$$

Since, p is prime number

$p/{}^pC_r\ \forall 1\le r\le p-1$

Also ${}^{p}C_{p-1} = p$ or $p^2 \nmid {}^{p}C_{p-1}$ & $p \nmid 1$

Hence, by Eisenstein's Criterion $f(x+1)$ is irreducible

Therefore $f(x)$ is irreducible.

Examples:

(a) $1+x+x^2$ is irreducible over $\mathbb{Q}$.

(b) $1+x+x^2+...+x^{16}$ is irreducible over $\mathbb{Q}$.

Observations:

(i) Maximal ideals of $\mathbb{Z}[x]$ is of the form $\langle p,x\rangle = \{pf(x)+xg(x) | f(x),g(x)\in\mathbb{Z}[x]\}$ where p is prime integer.

(ii) If p is prime number, then the number of reducible polynomials of the form x^2+ax+b over $\mathbb{Z}_p$ are $\frac{p(p+1)}{2}$.

(iii) If p is prime number. Then number of irreducible polynomials over $\mathbb{Z}_p$ of the form x^2+ax+b are $\frac{p(p-1)}{2}$.

(iv) $\langle x\rangle$ is prime ideal of $\mathbb{Z}[x]$.

(v) $\langle x\rangle$ is NOT maximal ideal of $\mathbb{Z}[x]$.

(vi) $\langle x+1\rangle$ is maximal ideal of $\mathbb{Q}[x]$.

(vii) $\langle x^2+1\rangle$ is maximal ideal of $\mathbb{R}[x]$.

(viii) Let F be a field with p^n elements then $(F,+) \cong \underbrace{\mathbb{Z}_p+\mathbb{Z}_p+...+\mathbb{Z}_p}_{n\text{-copies}}$ & $(F-\{0\},\bullet) \cong \mathbb{Z}_{p^n-1}$.

4.6. Some Important Theorem

1. Let F be a field and $p(x)\in F[x]$. Then $\langle p(x)\rangle$ is maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F.
2. Let F be a field and $p(x)$ is irreducible polynomials over F. Then $\frac{f[x]}{\langle p(x)\rangle}$ is a field.
3. Let F be a field and $p(x),a(x),b(x)\in F[x]$ if $p(x)$ is irreducible over F and $p(x)/a(x)b(x)$ then $p(x)/a(x)$ or $p(x)/b(x)$.
4. Let $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0\in\mathbb{Z}[x]$ and $a_n\neq 0$ let $q=\frac{r}{p}\in\mathbb{Q}$ be such that $f(q)=0$, where r and p are relative prime. Then r divides a_0 and p divides a_n.
5. For each prime p, $\exists$ field of cardinality p^n $\forall n\in\mathbb{N}$.

4.7. Construction of Such Fields

Algorithm:

(i) Take a irreducible polynomial $p(x)$ in $\mathbb{Z}_p[x]$ of degree n.

(ii) Make ideal $\langle p(x)\rangle$

(iii) Make a quotient ring $\dfrac{\mathbb{Z}_p[x]}{\langle p(x)\rangle}$

Which is our required field

Notice that any member $k(x)+\langle p(x)\rangle$ of $\dfrac{\mathbb{Z}_p[x]}{\langle p(x)\rangle}$ is of the form

$a_0+a_1x+\ldots+a_{n-1}x^{n-1}+\langle p(x)\rangle$

Thus $\dfrac{\mathbb{Z}_p[x]}{\langle p(x)\rangle}=\left\{a_0+a_1x+\ldots+a_{n-1}x^{n-1}+\langle p(x)\rangle \,\middle|\, a_i\in\mathbb{Z}_p\right\}$

Since $a_i\in\{0,1,2,\ldots,p-1\}$

There $a_i's$ can be chosen in p ways each choice of a_i can be selected in n ways. We find number of elements in $\dfrac{\mathbb{Z}_p[x]}{\langle p(x)\rangle}$ will be

$\underbrace{p\times p\times\ldots\times p}_{n\text{-copies}}$

Hence $\dfrac{\mathbb{Z}_p[x]}{\langle p(x)\rangle}$ is a field of p^n elements

Example: To construct a field of 9 elements.

Consider $f(x)=2+x+x^2$

Clearly, $f(x)$ is irreducible polynomial in $\mathbb{Z}_3[x]$

$\Rightarrow \langle f(x)\rangle$ is maximal ideal of $\mathbb{Z}_3[x]$

$\Rightarrow \dfrac{\mathbb{Z}_3[x]}{\langle f(x)\rangle}$ is a field

Now, for $f(x),p(x)\in\mathbb{Z}_3[x]$

$\exists\ t(x),r(x)\in\mathbb{Z}[x]$ such that

$p(x)=f(x).t(x)+r(x)$

Where either $r(x)=0$ or $\deg r(x)<\deg f(x)=2$

In either case $r(x)$ is of the type $ax+b$; where $a,b\in\mathbb{Z}_3$

So $p(x)-r(x)=f(x)t(x)\in\langle f(x)\rangle$

i.e., $p(x)-r(x)\in I$ where $I=\langle f(x)\rangle$

$\Rightarrow\ p(x)-r(x)+I=I$

i.e., $p(x)+I=r(x)+I=ax+b+\langle f(x)\rangle$

Hence any member $p(x)+\langle f(x)\rangle$ of $\dfrac{\mathbb{Z}_3[x]}{\langle f(x)\rangle}$ is of the form

$ax+b+\langle f(x)\rangle$

Thus $\dfrac{\mathbb{Z}_3[x]}{\langle f(x)\rangle}=\{ax+b+\langle f(x)\rangle \mid a,b\in\mathbb{Z}_3\}$

Since $a,b\in\{0,1,2,3\}$ can be chosen in three ways and for each choice a,b can be selected in three ways.

We find the numbers of elements of $\dfrac{\mathbb{Z}_3[x]}{\langle f(x)\rangle}$ will be $3\times3=9$

CHAPTER 5

ED, PID, UFD

5.1 Square Free Number

Let d be a non-zero rational number, then it is said to be square free if it is not divisible by square of any prime number.

5.1.1 Quadratic Field

Let d be a square free number. Let us define $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ as a subset of $\mathbb{C}$, the set of complex number. Clearly, $\mathbb{Q}(\sqrt{d})$ is subfield of $\mathbb{C}$.

Examples:

(a) $\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$ is a quadratic field.

(b) $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ is a quadratic field.

5.2 Principal Ideal

An ideal generated by a single element is said to be principal ideal.

Examples:

(a) Every ideal of $\mathbb{Z}_m$ is principal ideal.

(b) Every ideal of $(\mathbb{Z}, +, \bullet)$ is principal.

Observation: If $(R, +, \bullet)$ is a ring and $(R, +)$ is cyclic group then every ideal is generated by single element hence principal ideal.

5.2.1 Principal Ideal Ring

A CRU is defined as PIR if every ideal is principal.

Examples:

(a) $\mathbb{Z}_m$ is principal ideal ring.

(b) $\mathbb{Z}$ is principal ideal ring.

5.2.2 Principal Ideal Domain

An integral domain R is said to be principal ideal domain if each ideal I of R is a principal ideal.

i.e., $I = \langle a \rangle = \{ar : r \in R\}$ for some $a \in I$

Examples:

(a) Every field is PID.

(b) $\mathbb{Z}_p[x]$ is PID.

(c) $\mathbb{Z}[x]$ is not PID.

5.2.3 Norm on an Integral Domain

Let R be an integral domain then function $N: R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0)=0$ is called norm on domain if $N(a)>0 \quad \forall\, 0 \neq a \in R$, N is called positive norm also.

Examples:

(a) In $\mathbb{Z}[i]$, the ring of Gaussian integers, the function $N: \mathbb{Z}[i] \to \mathbb{Z}^+ \cup \{0\}$ defined as $N(a+ib)=a^2+b^2 \quad \forall\, a+ib \in \mathbb{Z}[i]$ is a norm.

(b) In any integral domain R, the function $N: R \to \mathbb{Z}^+ \cup \{0\}$ defined as $N(a)=0 \quad \forall\, a \in R$ is a norm on R.

5.2.4 Euclidean Domain

Let R be an integral domain if $\exists$ a norm N on R such that

(i) $N(a \cdot b) \geq N(a) \quad \forall\, a,b \neq 0 \in R$

(ii) For any $a \in R, b \in R-\{0\} \quad \exists\, q,r \in R$ such that $a=bq+r$, $r=0$ or $N(r)<N(b)$ then R is said to be Euclidean domain.

Examples:

(a) $\mathbb{Z}$ is ED with norm $N(a)=|a|$, the usual absolute value of a.

(b) Every field F is ED with norm N as $N(a)=1 \quad \forall\, 0 \neq a \in F$

Proof: Let $0 \neq a, \quad b \neq 0 \quad \in F$, then $ab \neq 0$ consequently.

$N(a)=1$ and $N(ab)=1$

$\Rightarrow \; N(a) \leq N(ab)$

Also $b \neq 0 \in F \quad \Rightarrow b^{-1} \in F$

So $a=\left(ab^{-1}\right)b+0=tb+r$

where $t=ab^{-1} \in F \quad \& \quad r=0 \in F$

hence F is ED

(c) $\mathbb{Z}[i]$ is ED with norm $N(a+ib)=a^2+b^2 \quad \forall\, a,b \in \mathbb{Z}$

(d) The ring $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}: a,b \in \mathbb{Z}\}$ is an ED under the norm N defined as $N\left(a+b\sqrt{2}\right)=\left|a^2-2b^2\right| \quad \forall\, a,b \in \mathbb{Z}$

(e) The field of rational numbers $\mathbb{Q}$ is not an Euclidean domain under the norm N defined as $N(a)=|a|$, the usual absolute value.

(f) The ring $\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}: a,b \in \mathbb{Z}\}$ is not an ED as there does not exists any norm on $\mathbb{Z}[\sqrt{-5}]$.

5.2.5 Unique Factorization Domain (U.F.D.)

An integral domain R with unity is called a unique factorization domain (U.F.D.), if it satisfies the following conditions:

(i) Each non-zero element of R is either a unit or can be expressed as a product of finite number of irreducible elements of R.

(ii) The above Decomposition is unique upto the order and associates of the irreducible elements it means if a non-zero, non-unit element $a \in R$ is expressible as $a = p_1 p_2 \ldots . p_r$ and $a = q_1 q_2 \ldots . q_s$ where $p_i's$ and $q_i's$ are irreducible elements of R, then $\exists$ a one-to-one correspondence between $p_i's$ and $q_i's$ such that the corresponding elements are associates. In particular $r = s$.

Examples:

(a) $\mathbb{R}[x]$, ring of polynomials over field of real numbers $\mathbb{R}$.

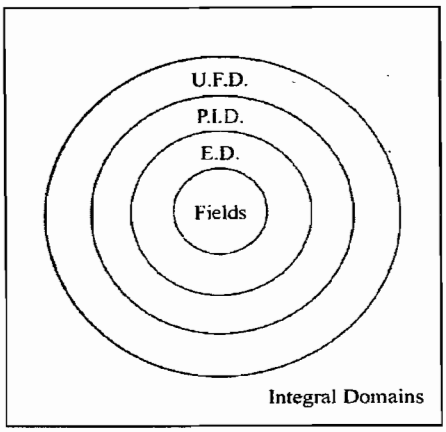
(b) $\mathbb{C}[x]$, ring of polynomials over field of complex number $\mathbb{C}$.

(c) The ring $\mathbb{Z}[i]$ of Gaussian integers.

(d) $\mathbb{Z}[x]$ is U.F.D.

(e) For $D<0$, $\mathbb{Z}\left[\sqrt{D}\right]=\left\{a+\left(\frac{1+\sqrt{D}}{2}\right)b;\ a,b\in\mathbb{Z}\right\}$ is U.F.D. if and only if $D=-1,-2,-3,-7,-11,-19,-43,-67,-163$

(f) For $n>3$, $\mathbb{Z}\left[\sqrt{-n}\right]=\left\{a+b\sqrt{-n}:a,b\in\mathbb{Z}\right\}$ is never U.F.D.



Note: All the containments are proper recall that $\mathbb{Z}$ is a E.D. but not a field. The quadratic ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a P.I.D. but not E.D., $\mathbb{Z}[x]$ is a U.F.D. But not PID and $\mathbb{Z}\left[\sqrt{-5}\right]$ is an integral domain but not U.F.D.

5.3 Observations Over ED, PID, UFD

(i) If R is a field, then $R[x]$ is ED.

Proof: Since R is field $\Rightarrow$ $R[x]$ is I.D.

Further for any two non-zero polynomials $f(x), g(x) \in R[x]$, we have

$$\deg\{f(x)g(x)\} = \deg f(x) + \deg g(x) \geq \deg f(x)$$

$(\text{Since } \deg g(x) \geq 0)$

$$\because \quad \deg f(x) \leq \deg(f(x)g(x)) \qquad \ldots(1)$$

We define the norm N on $R[x]$ as follows.

$$N(f) = \deg f(x) \quad \forall\, f(x) \neq 0 \in R[x] \qquad \ldots(2)$$

then $N(f) \geq 0$

from (1) & (2), we see that

$$N(f) \leq N(fg) \quad \forall\, f \neq 0,\ g \neq 0 \in R[x]$$

and by division algorithm for $f(x) \neq 0,\ g(x) \neq 0 \in R[x]$

there exists $f(x), r(x) \in R[x]$

such that $f(x) = t(x)g(x) + r(x)$,

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$$\therefore \quad f = tg + r \text{ where } r = 0 \text{ or } N(r) < N(g)$$

$\Rightarrow$ $R[x]$ is E.D. & hence P.I.D. and U.F.D.

(ii) Let A, B be non-zero ideals of a PID R, generated by a and b respectively then $A.B$ is ideal of R generated by ab i.e. if $A = \langle a \rangle$ & $B = \langle b \rangle$, then $AB = \langle ab \rangle$

(iii) If R is a PID, then each non-zero element $a, b \in R$ have GCD in R. Also, if $d \in R$ is GCD of a and b then $d = \lambda a + \mu b$; for some $\lambda, \mu \in R$

(iv) Let R be a integral domain and a, b be non-zero elements of R then

(a) a / b and $b / a \Rightarrow \langle a \rangle = \langle b \rangle$

(b) a and b are associate $\Rightarrow \langle a \rangle = \langle b \rangle$

(v) Let R be a PID. Let $d_1 \in R$ be GCD of a and b, then $d_2 \in R$ is a GCD of a and b if and only if d_1 and d_2 are associates.

Proof: Let d_1 be g.c.d. of $a, b \in R$

Let $d_2 \in R$ be an associate of d_1 then $d_1 = ud_2$ for some unit $u \in R$.

If follows that d_2 / d_1, where d_1 / a and d_1 / b

Consequently, d_2 / a and d_2 / b $\qquad \ldots(1)$

let $x \in R$ be such that x/a and x/b. ...(2)

Then x/d_1, since d_1 is g.c.d. of a and b.

We have $d_1 = ud_2$

$\Rightarrow d_2 = u^{-1}d_1$

$\Rightarrow d_1/d_2$

Hence x/d_1 and $d_1/d_2 \Rightarrow x/d_2$ ...(3)

from (1),(2) and (3); d_2 is also a g.c.d. of a and b.

Conversely,

Let d_1 and $d_2 \in R$ be any two greatest common divisors of a and b then d_1/a and d_1/b

also, d_2/a and d_2/b

since d_1 is g.c.d. of a & $b \Rightarrow d_2/d_1$

since d_2 is g.c.d. of a & $b \Rightarrow d_1/d_2$

as d_2/d_1 & d_1/d_2

$\Rightarrow d_1$ & d_2 are associates

(vi) Two non-zero elements of a PID R are relatively prime if and only if g.c.d. of a & b is unit.

(vii) If R is a PID and a,b are non-zero elements of R, then a,b have L.C.M. in R.

(viii) If R is a PID and $l_1 \in R$ be L.C.M. of $a,b \in R$, then $l_2 \in R$ is L.C.M. of a and b iff l_1 & l_2 are associates.

(ix) Let R be a PID and a,b are two non-zero elements of R, then $\text{LCM}(a,b).\text{GCD}(a,b) = a.b.u$ for some unit u of R.

Proof: Since R is a PID, a & b possess g.c.d. and l. c.m. we suppose that

$d = (a,b)$ = g.c.d. of a & b

$l = [a,b] = l$.c.m. of a & b

By definition of l.c.m. a/l and b/l ...(1)

$\Rightarrow \quad l = ax, \quad l = by$ for some $x, y \in R$

Since d is gcd of a & b

$\exists\ \lambda$ & $\mu \in R$ such that

$d = \lambda a + \mu b \Rightarrow l(\lambda a + \mu b) = ld$

$\Rightarrow ld = l\lambda a + l\mu b$

$\Rightarrow ld = by\lambda a + ax\mu b$

$\Rightarrow ld = ab(\mu x + \lambda y) \Rightarrow ab / ld$ ...(2)

By definition of g.c.d.

d / a and d / b

$\Rightarrow a = dr$ and $b = ds$ for some $r, s \in R$

$\Rightarrow ab = dr\, ds = (drs)d$ ...(3)

Now

$a = dr$ and dr / drs

$\Rightarrow a / drs,\ b = ds$

and $ds / drs \Rightarrow b / drs$

$\therefore a / drs$ and b / drs ...(4)

From (1) and (4)

l / drs and so $drs = lt$

For some $t \in R$

Putting in (3) gives

$ab = ltd = (ld)t$

$\Rightarrow ld / ab$ ...(5)

From (2) and (5) ab and ld are associates.

Consequently,

$ld = u\,ab$, for some unit $u \in R$

Hence $[a,b](a,b) = abu$, for some unit $u \in R$.

(x) Let R be PID & $a \in R$ then a is prime element $\Leftrightarrow$ a is irreducible element.

(xi) Let R be a PID, which is not a field, then an ideal $I = \langle a \rangle$ is maximal ideal if and only if a is an irreducible element of R.

(xii) Let R be a PID and I be non-zero ideal such that $I \neq R$, then I is prime ideal if and only if I is maximal ideal.

Proof: Let $I \neq R$ be non-zero prime ideal

Since R is PID, $I = \langle a \rangle$ for some $0 \neq a \in I$ we shall prove P is maximal ideal of R.

Let M be any ideal of R such that $I \subseteq M \subseteq R$. We can write $M = \langle b \rangle$ for some $b \in M$

Since $a \in I$ and $I \subseteq M \Rightarrow a \in M$

$\Rightarrow a = bx$, for some $x \in R$

Since I is prime ideal of R and $a \in I$

either $b \in I$ or $x \in I$ if $b \in I$

Put Your Own Notes

then $\langle b\rangle \subseteq I \Rightarrow M \subseteq I \Rightarrow M = I$

if $x \in I = \langle a\rangle$, then $x = ay$ for some $y \in R$

consequently,

$a = bx \Rightarrow a = bay \Rightarrow a.1 = a.by$

$\Rightarrow by = 1 \Rightarrow b$ is a unit

Since M is an ideal of R. Containing a unit b, $M = R$

Hence I is a maximal ideal of R.

Conversely, every maximal ideal of R is a prime ideal of R. Because R is commutative ring with unity.

(xiii) If R is a P.I.D. then every ascending chain of ideals $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq .... \subseteq \langle a_n\rangle \subseteq ...$ is finite

(xiv) The quotient ring of a PID by a prime ideal is again a PID.

(xv) If R is an ED with norm N and $a \in R$ be arbitrary then a is unit if and only if $N(a) = N(1)$

Proof: Since R is a ED, $1 \in R$

Then by definition of ED

$$N(1) \leq N(1.x) \quad \forall\, x \neq 0 \in R \qquad ...(1)$$

$\therefore \quad N(1) \leq N(x) \quad \forall\, x \neq 0 \in R$

Condition is necessary

Let $a \in R$ be a unit in R

then $a/1$ i.e. $\exists$ some $b \in R$ such that

$ab = 1$, then by definition of ED

$N(a) \leq N(ab)$ or $N(a) \leq N(1)$

From (1) $N(1) \leq N(a)$

Hence $N(1) = N(a)$

Condition is sufficient

Let $N(1) = N(1)$ we shall prove that a is unit.

By definition of E.D. for $1, a \in R \ \exists\ r, t \in R$ such that $1 = at + r$
where either $r = 0$ or $N(r) < N(a)$

if $r \neq 0$ then $N(r) < N(a) \Rightarrow N(r) < N(1)$

which contradicts (1).

$\therefore \quad r = 0$ and so $1 = at \Rightarrow a/1$

$\Rightarrow a$ is unit.

(xvi) As a consequence of above result it follows that the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

(xvii) In ring of Gaussian integers, $\mathbb{Z}[i]$ $a+ib$ is not a unit then $a^2+b^2>1$

(xviii) Let R be an ED with norm N and a,b be two non-zero elements of R. Then b is not a unit of R if and only if $N(a)<N(ab)$

(xix) Let R be an ED with norm N. Then

(a) $N(a)=N(-a)$ $\forall\, 0\neq a\in R$

(b) If $N(a)=0$ & $0\neq a\in R$, then a is unit in R.

(c) $N(a)=N(ab)$ if and only if b is unit in R where $0\neq a, 0\neq b, a,b\in R$

(xx) R is a U.F.D. $\Leftrightarrow$ $R[x]$ is a U.F.D.

(xxi) In U.F.D. every pair of non-zero elements have a g.c.d. and l.c.m.

5.4 Content of a Polynomial

Let R be a PID and $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ such that $a_n\neq 0$ be a non-zero polynomial over R. The content of $f(x)$ is greatest common divisor of co-efficients $a_0,a_1,...,a_n$ is denoted by $c(f)$.

5.4.1 Primitive Polynomial

Let R be a principal ideal domain then a non-zero polynomial $f(x)$ over R is said to be primitive if the content of $f(x)$ is unity of R.

Results:

(i) Let R be a U.F.D. and $f(x)$ be a non-zero polynomial $f(x)$ over R then $f(x)=af_1(x)$, where $a=c(f)$ & $f_1(x)\in R[x]$ is primitive polynomial.

(ii) If R is U.F.D. and $f(x),g(x)\in R[x]$ then $C(fg)=C(f).C(g)$

(iii) **Gauss Lemma:** Let R bet a U.F.D., then the product of two primitive polynomials in $R[x]$ is a primitive polynomials in $R[x]$

(iv) If R is U.F.D. and $f(x),g(x)\in R[x]$ such that their product $f(x).g(x)$ is primitive polynomial then $f(x)$ and $g(x)$ are also primitive polynomials.

(v) There exists polynomials which are primitive and irreducible both.

Example: $f(x)=x^3-6x+3\in Q[x]$

(vi) There exists polynomials which are primitive and reducible.

Example: $f(x)=x^2-5x+6=(x-2)(x-3)\in Q[x]$

(vii) There exists polynomials which are not primitive but irreducible.

Example: $f(x)=2x^2-4\in\mathbb{Z}[x]$

(viii) There exists polynomials which are neither primitive nor irreducible.

Example: $f(x)=2x^2-8=(2x-4)(x+2)\in Q[x]$

(ix) If R is U.F.D. then any $f(x)\in R[x]$ is an irreducible element if and only if either $f(x)$ is an irreducible element of R or $f(x)$ is an irreducible primitive polynomial of $R[x]$.

CHAPTER-6

RING HOMOMORPHISM

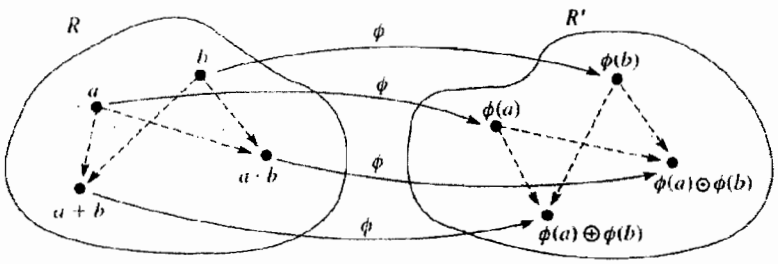
6.1. Let $R \& R'$ are two rings and then a map $\phi: R \to R'$ is defined as ring homomorphism if

(i) $f(a+b) = f(a) \oplus f(b) \quad \forall a,b \in R$

(ii) $f(a \cdot b) = f(a) \odot f(b) \quad \forall a,b \in R$

Where $+ \& \cdot$ are addition & multiplication of ring R and $\oplus \& \odot$ are addition & multiplication of R' respectively.

Let us try to understand the schematic representation of a ring homomorphism by given figure:-



The dashed arrows indicate the results of performing the ring operations.

Example:

(a) Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| \, a,b \in \mathbb{Z} \right\}$ be ring & $\mathbb{Z}$ is ring of integers.

Then, $\phi: R \to \mathbb{Z}$

Such that $\phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a - b$

ϕ is a ring homomorphism.

(b) F be the ring of all mappings $\mathbb{R}$ into $\mathbb{R}$ with point wise addition and point wise multiplication.

Then $\forall\, a \in \mathbb{R}$, we have the evaluation homomorphism $\phi_a(f) = f(a) \quad \forall\, f \in F$

(c) The map $\phi: \mathbb{Z} \to \mathbb{Z}_n$

Where $\phi(a)$ is the remainder of a modulo n then ϕ is a ring homomorphism for each positive integer n.

$\phi(a+b) = \phi(a) + \phi(b)$ (From group Theory)

$a = q_1 n + r_1 \quad \& \quad b = q_2 n + r_2$ (By division algorithm)

Put Your Thoughts

$a \cdot b = (q_1 n + r_1) \cdot (q_2 n + r_2)$

$= n(q_1 q_2 n + r_1 q_2 + q_1 r_2) + r_1 r_2$

$\phi(a \cdot b) = r_1 r_2 = \phi(a) \odot_n \phi(b)$

$\Rightarrow \phi : \mathbb{Z} \to \mathbb{Z}_n$ is ring homomorphism and this homomorphism is called **natural homomorphism** from $\mathbb{Z}$ to $\mathbb{Z}_n$

(d) **Projection Homomorphism:** let $R_1, R_2, ...R_n$ be rings, $\forall i$ The map $\pi_i : R_1 \times R_2 \times ... \times R_n \to R_i$, defined by $\pi_i(r_1, r_2, r_3, ..., r_n) = r_i$

(e) $\phi : \mathbb{C} \to \mathbb{C}$ such that

$\phi(a+ib) = a - ib$

Then ϕ is a ring homomorphism.

As $\phi[(a+ib)+(c+id)] = \phi((a+c)+i(b+d))$

$= (a+c) - i(b+d)$

$= (a-ib)+(c-id)$

$= \phi(a+ib)+\phi(c+id)$

And

$\phi[(a+ib)(c+id)] = \phi((ac-bd)+i(ad+bc))$

$= (ac-bd) - i(ad+bc)$

$= (a-ib)c - id(a+ib)$

$= (a-ib)(c-id)$

$= \phi(a+ib)\phi(c+id)$

Results & Properties: Let ϕ be a homomorphism from a ring R to a ring R'.

Let A be a subring of R and B an ideal of R' then

(i) $\phi(0) = 0'$

(ii) $\phi(-a) = -\phi(a) \ \forall a \in R$

Because ϕ is a group homomorphism from $(R,+)$ to $(R', \oplus)$ as well.

(iii) For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$

(iv) $\phi(A) = \{\phi(a) | a \in A\}$ is a sub ring of R'

(v) $\phi^{-1}(B) = \{r \in R | \phi(r) \in B\}$ is an ideal of R

(vi) If A is an ideal and ϕ is onto R'. Then $\phi(A)$ is an ideal in R'.

(vii) If R is commutative then $\phi(R)$ is commutative.Z

(viii)If R has a unity 1, $R' \neq \{0\}$ and ϕ is onto, then $\phi(1)$ is the unity of R'.

(ix) If $a \in R$ is nilpotent element then $\phi(a) \in R'$ is nilpotent.

(x) If $e \in R$ is idempotent element then $\phi(e) \in R'$ is idempotent.

(xi) Let R, S, T be three rings such that $f: R \to S$ and $g: S \to T$ are ring homomorphism then their composition $gof: R \to T$ is also a ring homomorphism.

6.2. Kernel of Homomorphism

Let ϕ be a homomorphism from a ring R to a ring R'

Then $\ker\phi$ is defined as:

$$\ker\phi = \{r \in R \mid \phi(r) = 0\}$$

Example: Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| \, a, b \in \mathbb{R} \right\}$ be a ring & $\phi: R \to \mathbb{R}$ such that $\phi\left(\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\right) = a$ be ring homomorphism.

Then $\ker\phi = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in \mathbb{R} \right\}$.

Properties: If ϕ is a homomorphism from a ring R to a ring R', then

(i) $\ker\phi = \{0\}$ if and only if f is one- one

(ii) $\ker\phi$ is an ideal in R

(iii) Every ideal in ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping.

$$\phi: R \to \frac{R}{A}$$

Such that $\phi(r) = r + A$

Where $\frac{R}{A}$ is quotient ring.

(iv) If $\ker\phi$ has m elements then ϕ is m to 1 map.

6.3. Isomorphism

A one- one homomorphism is defined as isomorphism.

6.3.1. Isomorphism Rings

Two rings R & R' are said to be isomorphic if $\exists$ one-one onto homomorphism between them.

And then Rings R & R' are said to be abstractly identical i.e. they represent same structure (Object) in two different notations (language).

Properties: If ϕ is a homomorphism from R to R' then:

(i) ϕ is an isomorphism if and only if ϕ is onto and $\ker\phi = \{r \in R \mid \phi(r) = 0'\} = \{0\}$

(ii) If ϕ is an isomorphism from R onto R' Then ϕ^{-1} is an isomorphism from R' onto R.

(iii) Every isomorphic image of an integral domain is an integral domain.

(iv) Every isomorphic image of a field is a field

(v) Every isomorphic image of a division ring is a division ring.

Example:

(a) As abelian groups, $\langle \mathbb{Z}, + \rangle$ and $\langle 2\mathbb{Z}, + \rangle$ are isomorphic under the map $\phi : \mathbb{Z} \to 2\mathbb{Z}$

Where $\phi(x) = 2x \ \forall x \in \mathbb{Z}$

But ϕ is not ring Isomorphism.

Because; $\phi(xy) = 2xy$

& $\phi(x) = 2n, \phi(y) = 2y$

$\phi(x)\phi(y) = 2x \cdot 2y = 4xy \neq \phi(xy)$

(b) Let $r, s \in \mathbb{Z}$ & $g.c.d.(r,s) = 1$

Then the rings $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are Isomorphic rings.

Additively, they both are cyclic abelian group of order rs with generators

1 & $(1, 1)$ in an additive group Isomorphism

Now, for multiplicative condition:

$\phi(m \cdot n) = mn(1,1) = [m \cdot (1,1)][n \cdot (1,1)]$

$= \phi(m) \cdot \phi(n)$

(c) $\phi : \mathbb{C} \to \mathbb{C}$; Where $\mathbb{C}$ is ring of complex numbers.

Such that $\phi(a + ib) = a - ib$ is a ring Isomorphism

Observations:

(i) Let R be a commutative ring of characteristic 2. Then the mapping $\phi : R \to R$ Such that

$\phi(a) = a^2$ is a ring homomorphism.

(ii) Any Homomorphism from a field F to a ring R is either one- one or zero map.

(iii) If m & n are distinct positive integer then $m\mathbb{Z}$ and $n\mathbb{Z}$ are NOT Isomorphic rings.

(iv) There exists a homomorphism from a non- commutative ring whose image is a commutative ring.

Example: Let $R=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a,b \in \mathbb{Z}\right\}$.

Then R is a non-commutative ring under matrix addition and matrix multiplication. Now consider a mapping.

$\phi : R \to \mathbb{Z}$ defined as $\phi\left(\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\right) = a$ is an onto homomorphism.

Hence, $\mathbb{Z}$ is a homomorphic image of R.

Where $\mathbb{Z}$ is commutative ring and R is non- commutative ring.

(v) There exists homomorphism from a ring without unity whose image is ring with unity.

Example: Consider the same example discussed in observation (iv)

(vi) The ring homomorphism from ring of integers to itself is either zero mapping or identity mapping.

(vii) There exists a ring homomorphism $\phi : R \to R'$ such that ring R has unity but R' does not have unity.

Example: Let $\phi : \mathbb{Z} \to E$ (E is ring of ever integers)

& $\phi(x) = 0 \quad \forall \ x \in \mathbb{Z}$

Here, we find E does not have unity But $\mathbb{Z}$ has unity 1.

(viii) There exists a ring homomorphism $\phi : R \to R'$ such that ring R has unity 1 but $f(1)$ is not unity of ring R'.

(ix) Let R & R' be rings & $\phi : R \to R'$ be a homomorphism then

(a) If U is left ideal of R, then $\phi(U)$ is left ideal of R'

(b) If U is right ideal of R, then $\phi(U)$ is right ideal of R'

(x) Let R & R' be rings

(a) The mapping $\phi : R \times R' \to R$ given by $\phi((a,b)) = a$ is an onto ring homomorphism.

(b) The mapping $\phi : R \to R \times R'$ given by $\phi(a) = (a,0)$ is one to one ring homomorphism.

(c) $R \times R'$ & $R' \times R$ are Isomorphic rings.

(xi) There exists a ring homomorphism from $\mathbb{Z}_2$ to a sub ring of $\mathbb{Z}_{2n}$ if and only if n is odd positive integer.

(xii) The homomorphic image of commutative ring is commutative.

(xiii) Let R be commutative ring and suppose $px = 0 \ \forall x \in R$, where p is a prime number. Then the mapping $\phi(x) = x^p \ \forall x \in R$ is a homomorphism & this map is known as Frobenius map.

(xiv) The relation of being Isomorphic is an equivalence relation.

(xv) Let R & R' be commutative rings with unity if $\phi: R \to R'$ be ring homomorphism from R onto R'. Then if char R is nonzero $\Rightarrow$ char R' divides char R.

6.4. Quotient Rings

Let R be a ring and let I be an ideal of R. Since $a,b \in I \Rightarrow a-b \in I$ we find I is a subgroup of $\langle R,+\rangle$ is abelian, I will be normal subgroup of R.

And thus we can talk of $\frac{R}{I}$, the quotient group.

$\frac{R}{I} = \{r+I \mid r \in R\}$ = set of all cosets of I in R (clearly left and right cosets are equal)

We know $\frac{R}{I}$ forms a group under 'addition' defined by:

$$(r+I)+(s+I)=(r+s)+I$$

We now define a binary composition (product) on $\frac{R}{I}$ by

$$(r+I)\cdot(s+I)=rs+I$$

It is a easy exercise to check that this product is well defined on $\frac{R}{I}$

Since $(a+I)[(b+I)(c+I)] = (a+I)(bc+I)$

$$= a(bc)+I$$
$$= (ab)\,c+I$$
$$= (ab+I)(c+I)$$
$$= [(a+I)(b+I)](c+I)$$

Associativity holds with respect to this product.

Again, as $(a+I)[(b+I)+(c+I)] = (a+I)(b+c+I)$

$$= a\,(b+c)+I$$
$$= ab+ac+I$$
$$= (ab+I)+(ac+I)$$
$$= (a+I)(b+I)+(a+I)(c+I)$$

We find left distributive holds. Similarly, one can check that right distributivity also holds in $\frac{R}{I}$.

And hence $\frac{R}{I}$ forms a ring, called the **Quotient Ring** or Residue Class ring of R by I.

Now, Look at it from another angle. Let R be a ring and I an ideal of R.

Define $a,b \in R$, $a \equiv b(\text{mod } I)$ if $a-b \in I$

Note that this relation is an equivalence relation on R. Hence, it will partition R into equivalence classes.

Let for any $a \in R$, $cl(a)$ be the corresponding equivalence class of a.

Then, $\text{cl(a)} = \{r+R | r = a(\text{mod } I)\}$

$$= \{r \in R | r-a \in I\}$$

$$= \{r \in R | r-a = x; \text{ for some } x \in I\}$$

$$= \{r \in R | r = a+x; \text{ for some } x \in I\}$$

$$= \{a+x | x \in I\}$$

$$= a+I.$$

Thus, the quotient ring $\frac{R}{I}$ is nothing but the ring of all equivalence classes as defined above.

In fact, the binary operations defined earlier would translate to

$\text{cl(a)} + \text{cl}(b) = \text{cl}(a+b)$; $a,b, \in R$

$\text{cl(a)} \cdot \text{cl}(b) = \text{cl}(ab)$

It would be interesting exercise for the reader to verify that $\frac{R}{I}$ thus defined forms a ring.

In fact, if R has unity 1 then $\text{cl}(1)$ will be unity of $\frac{R}{I}$.

$\frac{R}{I}$ is therefore also called **Quotient ring** of R modulo I.

Observations: Let R be a ring and U be ideal of R.

(i) If R is a commutative ring, then $\frac{R}{U}$ is also commutative ring.

(ii) If R has unity 1, Then $\frac{R}{U}$ has unity $1+U$

(iii) If R is Boolean ring then $\frac{R}{U}$ is also Boolean ring.

(iv) If $S = \{ab-ba | a,b \in R\}$

Then $\frac{R}{U}$ is commutative ring if and any if $S \subseteq U$

(v) Converse of observation (i) & (ii) may not be true.

Example: Let $R=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} ; a,b\in\mathbb{Q}\right\}$ & $U=\left\{\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix};b\in\mathbb{Q}\right\}$

Clearly U is an ideal of R

Now, $\frac{R}{U}=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}+U \;\; ; a,b\in\mathbb{Q}\right\}$

$=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}+U \;\; ; a,b\in\mathbb{Q}\right\}$

Is quotient ring of R. Here $\frac{R}{U}$ is CRU but R is not commutative & does not have unity.

6.5. Some Important Theorems

Retracing the steps backwards, we prove ψ is one-

Fundamental Theorem of Ring Homomorphism

Let ϕ be a onto ring homomorphism from R to R' then the mapping from $\frac{R}{\ker\phi}$ to R'.

Given by $\psi(r+\ker\phi)=\phi(r)$ an isomorphism. In symbols,

$$\frac{R}{\ker\phi}\cong R'$$

Proof: Let $\phi: R\to R'$ be onto ring homomorphism define $\psi:\frac{R}{\ker\phi}\to R'$

Such that $\psi(r+I)=\phi(r) \;\; \forall\, r\in R$ where $I=\ker\phi$

Then ψ is well defined

As $x+I = y+I$

$\Rightarrow \;\; x-y\in I=\ker\phi$

$\Rightarrow \;\; \phi(x-y)=0$

$\Rightarrow \;\; \phi(x)-\phi(y)=0$

$\Rightarrow \;\; \phi(x)=\phi(y)$

$\Rightarrow \;\; \psi(x+I)=\psi(y+I)$

one.

Again, as

$\psi[(x+I)+(y+I)]=\psi[(x+y)+I]$

$=\phi(x+y)$

$=\phi(x)+\phi(y)$

$= \psi(x+I)+\psi(y+I)$

$\psi\left[(x+I)(y+I)\right] = \psi(xy+I) = \phi(xy)$

$= \phi(x)\phi(y)$

$= \psi(x+I)\ \psi(y+I)$

$\therefore\ \psi$ is a homomorphism

Now if $r' \in R'$ be any element then as $\phi : R \to R'$ is onto, $\exists\, r \in R$ such that $\phi(r) = r'$ for this r,

As $\psi(r+I) = \phi(r) = r'$

We find $r+I$ is required pre-image of r' under ψ showing there by that ψ is onto and hence an isomorphism.

Thus $\frac{R}{\ker\phi} \cong R'$ and

by symmetry $R' \cong \frac{R}{\ker\phi}$

1. **First Theorem of Isomorphism:** Let $B \subseteq A$ be two ideals of a ring R. Then

   $\frac{R}{A} \cong \frac{R/B}{A/B}$

2. **Second Theorem of Isomorphism:** Let A, B be two ideals of a ring R,

   then $\frac{A+B}{A} \cong \frac{B}{A \cap B}$

   and hence $\frac{A+B}{B} \cong \frac{A}{A \cap B}$

3. **Lattice Isomorphism Theorem for Rings:** Let I be an ideals of R. The correspondence $A \leftrightarrow \frac{A}{I}$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of sub rings of $\frac{R}{I}$.

   Furthermore, A (a subring containing I) is an ideal of R if and only if $\frac{A}{I}$ is an ideal of $\frac{R}{I}$.

4. ***Theorem:*** If P is an ideal of ring R.

   Then $\frac{R}{P}$ is an integral domain if and any if P is prime ideal.

5. ***Theorem:*** The ideals of $\frac{R}{I}$ are of the form $\frac{K}{I}$, where K is an ideal of R and $I \subset K$.

6. ***Theorem:*** Let R be a CRU & $M \neq R$ be an ideal in R. Then $\frac{R}{M}$ is a field if and any if M is maximal ideal.

7. ***Theorem:*** The Set N of all nilpotent elements in a commutative ring R forms an ideal of R and then $\frac{R}{N}$ has no non- zero nilpotent elements. (N is called nil radical of R)

8. **Chinese Remainder Theorem:** Let $A_1, A_2 \ldots\ldots A_k$ be ideals in R.

The map $\phi : R \to \frac{R}{A_1} \times \frac{R}{A_2} \times \ldots\ldots \times \frac{R}{A_k}$

Defined by

$\phi(r) = (r + A_1, r + A_2, \ldots\ldots r + A_k)$

is a ring homomorphism with $\ker \phi = A_1 \cap A_2 \cap \ldots\ldots \cap A_k$

if for each $i, j \in \{1, 2, \ldots\ldots k\}$ with $i \neq j$ the ideal A_i and A_j are co-maximal, then this map is surjective and $A_1 \cap A_2 \cap \ldots\ldots \cap A_k = A_1 A_2 \ldots\ldots A_k$

So $\frac{R}{(A_1 A_2 \ldots\ldots A_k)} = \frac{R}{(A_1 \cap A_2 \cap \ldots\ldots \cap A_k)}$

$\cong \frac{R}{A_1} \times \frac{R}{A_2} \times \ldots\ldots \times \frac{R}{A_k}$

Where R is commutative ring with unity.

Corollary: Let n be a positive integer and let $p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k}$ be its factorization into powers of distinct primes.

Then $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{\lambda_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p_2^{\lambda_2}\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{p_k^{\lambda_k}\mathbb{Z}}$ as rings.

6.6. Applications of Ring Homomorphism

(i) **Test for divisibility by 9:**

An integer n with decimal representation $a_k a_{k-1} \ldots\ldots a_0$ is divisible by 9 if and any if $a_k + a_{k-1} + \ldots + a_0$ is divisible by 9. To verify this, observe that $n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots\ldots + a_0$ then, letting ϕ denote the natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_9$ $\left[\text{in particular } \phi(10) = 1\right]$. We note that n is divisible by 9 if and only if

$0 = \phi(x) = \phi(a_k)(\phi(10))^k + \phi(a_{k-1})(\phi(10))^{k-1} + \ldots + \phi(a_0)$

$= \phi(a_k) + \phi(a_{k-1}) + \ldots + \phi(a_0)$

$= \phi(a_k + a_{k-1} + \ldots + a_0)$

But $\phi(a_k + a_{k-1} + \ldots + a_0) = 0$ is equivalent to $a_k + a_{k-1} + \ldots + a_0$ being divisible by 9.

Similarly we can use homomorphism to test divisibility by $3,4,11$ etc.

(ii) Consider the sequence $3,7,11,15....$

Is it possible that one of these integers is sum of two squares?

If so, the equation $3+4k=a^2+b^2$ is satisfied for some integer k,a & b. Then applying natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_4$ to both sides of this equation, we see the equation $3=x^2+y^2$ has a solution in $\mathbb{Z}_4$. But, by direct substitution, one may verify that this equation has no solution. Thus, no integer in the sequence is sum of two squares.

6.7. Embedding of Ring

A ring R is said to be embedded in a ring R'.If there is an isomorphism from R into R'.

i.e., R is isomorphic to a sub ring. We also say that R' is an extension ring or over ring of R.

Remark: Since f is an isomorphism of R into R', $f(R)$ is sub ring of R' and further R and $f(R)$ are isomorphic rings. Thus upto isomorphism R is a subring of R' and it is in this sense that we say R is embedded in R' or R' is an extension ring or over ring of R.

6.8. Prime Field

A field that does not have proper subfield is known as prime field.

Example:

(a) $\mathbb{Z}_p$ is prime field if p is prime.

(b) $\mathbb{Q}$ is prime field.

Observations: Every Ring can be embedded in a ring with unity.

Explanation: Let R be a ring

We take $R\times\mathbb{Z}=\{(r,m)|r\in R,m\in\mathbb{Z}\}$

We define addition and multiplication in $R\times\mathbb{Z}$ as follow:-

$(r,m)+(s,n)=(r+s\ ,\ m+n)$

$(r,m)\cdot(s,n)=(rs+ms+nr,mn)$

It is easy to verify that $R\times\mathbb{Z}$ forms a ring with unity $(0,1)$

Then Define a mapping

$f:R\to R\times\mathbb{Z}$

As $f(r)=(r,0)\ \forall r\in R$.

Then f is well-defined for $r=s$

$\Rightarrow\quad (r,0)=(s,0)$

$\Rightarrow\qquad r=s$

Next is to show that f is homomorphism.

Let $r,s \in R$

$f(r+s)=(r+s,0)=(r,0)+(s,0)=f(r)+f(s)$

$f(rs)=(rs,0)=(rs+0s+0r,00)$

$=(r,0)(s,0)$

$=f(r)f(s)$

Hence f is an isomorphism of R into $R\times\mathbb{Z}$, So R is embedded in ring $R\times\mathbb{Z}$ with unity $(0,1)$

Remark: If R is any ring not necessarily containing unity, Then its extension ring with unity is $R\times\mathbb{Z}$.

(i) Every ring with or without unity can be embedded in a ring of endomorphism of some additive abelian group.

(ii) Every ring with unity has a subring either Isomorphic to $\mathbb{Z}_m$ or $\mathbb{Z}$.

(iii) Every field has a subfield Isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Q}$.

(iv) Every integral domain can be embedded in a field.

(v) $\mathbb{Z}_p$ Can be embedded into a field F if $\text{char}\, F = p$

(vi) $\mathbb{Q}$ can be embedded into a field F if $\text{char}\, F = 0$

6.9. Field of Quotients

Let D be an integral domain, then there exists a field F that field F is called field of quotients of D.

Example: Field of quotients of integral domain $\mathbb{Z}$ of integers is $\mathbb{Q}$ (all rational numbers)

Observation:

(i) The field of quotients of integral domain D is the smallest field containing D. i.e., If F be the field of quotients of D. Then if K is any field which contains D, Then K contains a subfield Isomorphic to F.

(ii) Field of quotients of a finite integral domain D is D itself.

(iii) If D_1 & D_2 are two Isomorphic integral domain with F_1 and F_2 are Isomorphic. But NOT conversely.

Example: Let $D_1=\mathbb{Z}$, $D_2=E$ (all even integers)

Then D_1 & D_2 are not isomorphic integral domains. However their field of quotients are $\mathbb{Q}$ & $\mathbb{Q}$ and $\mathbb{Q}\cong\mathbb{Q}$.

Some Examples

S.No.	Integral Domain	Field of Quotient
(i)	Ring of integers $(\mathbb{Z})$	Field of rational numbers $(\mathbb{Q})$
(ii)	Ring of even integers $(2\mathbb{Z})$	Field of rational numbers $(\mathbb{Q})$
(iii)	$3\mathbb{Z}$	Field of rational numbers $(\mathbb{Q})$
(iv)	$\mathbb{Z}[i]=\{x+iy \;;\; x,y\in\mathbb{Z}\}$	$\mathbb{Q}[i]=\{x+iy \mid x,y\in\mathbb{Q}\}$
(v)	$\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d};a,b\in\mathbb{Z}\}$	$\mathbb{Q}[\sqrt{d}]=\{a+b\sqrt{d};a,b\in\mathbb{Q}\}$
(vi)	$\mathbb{Z}_p$	$\mathbb{Z}_p$

ASSIGNMENT SHEET - 1

1. Let $C([0,1])$ be the ring of all real valued continuous functions on $[0,1]$. Which of the following statements are true?

(a.) $C([0,1])$ is an integral domain.

(b.) The set of all functions vanishing at 0 is a maximal ideal.

(c.) The set of all functions vanishing at both 0 and 1 is a prime ideal.

(d.) If $f \in C([0,1])$ is such that $(f(x))^n = 0$ for all $x \in [0,1]$ for some $n > 1$, then $f(x) = 0$ for all $x \in [0,1]$.

2. We denote the characteristic of R by char (R). In the following, let R and S be nonzero commutative rings with unity. Then

(a.) Char(R) is always a prime number.

(b.) if S is a quotient ring of R, then either char(S) divides char(R), or char(S) = 0.

(c.) if S is a subring of R containing 1_R then char(S) = char(R).

(d.) if char(R) is a prime number, then R is a field.

3. Let R be the ring obtained by taking the quotient of $(\mathbb{Z}/6\mathbb{Z})[X]$ by the principal ideal $I = <2X + 4>$. Then

(a.) R has infinitely many elements.

(b.) R is a field.

(c.) 5 is a unit in R.

(d.) 4 is a unit in R.

4. For which of the following values of n, does the finite field $\mathbb{F}_{5^n}$ with 5^n elements contain a non-trivial 93^{rd} root of unity?

(a.) 92

(b.) 30

(c.) 15

(d.) 6

5. Let **F** be a finite field such that for every a $a \in \mathbf{F}$ the equation $x^2 = a$ has a solution in **F**. Then

(a.) The characteristic of **F** must be 2

(b.) **F** must have a square number of elements

(c.) The order of **F** is a power of 3

(d.) **F** must be a field with prime number of elements

6. Let R be a commutative ring. Let I and J be ideals of R.

Let $I - J = \{x - y \mid x \in I, y \in J\}$

and

$IJ = \{xy \mid x \in I, y \in J\}$. Then

(a.) $I - J$ is an ideal and IJ is an ideal in R

(b.) $I - J$ is an ideal and IJ need not be an ideal in R

(c.) $I - J$ need not be an ideal but IJ is an ideal in R

(d.) Neither $I - J$ nor IJ need to be an ideal in R.

7. In ring of Gaussian integers $\mathbb{Z}[i]$,

(a.) 5 and 7 are irreducible

(b.) 5 is irreducible but 7 is reducible

(c.) 5 is reducible but 7 is irreducible

(d.) Neither 5 nor 6 is irreducible

8. Let I_1, I_2 be two ideals of a comparative ring R with identity. Which one of the following is true?

(a.) $I_1 + I_2$ and $I_1 \cap I_2$ are ideals of R

(b.) $I_1 + I_2$ is an ideal of R, but $I_1 \cap I_2$ is not an ideal of R

(c.) $I_1 + I_2$ is not an ideal of R, but $I_1 \cap I_2$ is an ideal of R

(d.) Neither $I_1 + I_2$ nor $I_1 \cap I_2$ is an ideal of R

9. Let R be the ring of all 2×2 matrices

E the ring of all even integers.

T the ring of integers (mod 10) and

S the ring of all multiples of 6.

Then

(a.) Only E has no zero divisors

(b.) Only R and S have no zero divisors

(c.) Only E and S have no divisors

(d.) Only E and T have no zero divisors

10. Let I be any ideal in the ring $\mathbb{Z}$ of integers. Then

(a.) I can be generated by one element

(b.) $I=\langle 0\rangle$ or $I=\mathbb{Z}$

(c.) There is an ideal I' such that $I\oplus I'=\mathbb{Z}$

(d.) I is generated by a prime number

11. Let A be a finite integral domain with unity $1\in A$. Then the order of 1 in the additive group $(A, +)$ is

(a.) A prime

(b.) Zero

(c.) An arbitrary integer

(d.) A power of a prime number

12. A non-zero element 'a' of a ring R is said to be nilpotent if $a^n=0$ for some integer n. In the ring of integers (mod 8) all the nilpotent elements are

(a.) 2,4 and 6

(b.) 2 and 4

(c.) 4

(d.) 0, 2, 4 and 6

13. R be a commutative ring with unity and I is a prime ideal which is true.

(a.) I must be maximal ideal of R.

(b.) If $\frac{R}{I}$ is finite ring then I is maximal ideal.

(c.) I is never maximal ideal.

(d.) If I is maximal ideal then $\frac{R}{I}$ must finite ring.

14. Let $R=\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ and $I=\mathbb{Z}\times\mathbb{Z}\times\{0\}$. Then which of the following statement is correct?

(a.) I is a maximal ideal but not a prime ideal of R.

(b.) I is a prime ideal but not a maximal ideal of R.

(c.) I is both maximal ideal as well as a prime ideal of R.

(d.) I is neither a maximal ideal nor a prime ideal of R.

15. Which one of the following ideals of the ring $\mathbb{Z}[i]$ of Gaussian integers is NOT maximal?

(a.) $\langle 1+i\rangle$

(b.) $\langle 1-i\rangle$

(c.) $\langle 2+i\rangle$

(d.) $\langle 3+i\rangle$

16. The number of maximal ideals in $\mathbb{Z}_{27}$ is

(a.) 0

(b.) 1

(c.) 2

(d.) 3

17. Let R be the ring of all real valued continuous functions on $[0,1]$. $I=\{f\in R: f(0)=0\}$. Then

(a.) I is not an ideal of R

(b.) I is an ideal, but not prime ideal of R

(c.) I is a prime ideal, but not a maximal ideal of R

(d.) I is a maximal ideal R

18. Let $M_3(R)$ be the ring of all 3×3 real matrices. If $I, J \subseteq M_3(\mathbb{R})$ are defined as

$$I=\left\{\begin{pmatrix} a & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} | a,b,c \in \mathbb{R}\right\},$$

$$J=\left\{\begin{pmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{pmatrix} | a,b,c \in \mathbb{R}\right\} \text{ Then}$$

(a.) I is a right ideal and J is a left ideal

(b.) I *and* J are both left ideals

(c.) I *and* J are both right ideals

(d.) I is a left ideal and J a right ideal

19. Let the set $\frac{\mathbb{Z}}{n\mathbb{Z}}$ denote the ring of integers modulo n under addition and multiplication modulo n. Then $\frac{\mathbb{Z}}{9\mathbb{Z}}$ is not a sub ring of $\frac{\mathbb{Z}}{12\mathbb{Z}}$ because

(a.) $\mathbb{Z}/9\mathbb{Z}$ is not a subset of $\mathbb{Z}/12\mathbb{Z}$

(b.) G.C.D. (9, 12) = $3 \neq 1$

(c.) 12 is not a power of 3

(d.) 9 does not divide 12

20. Let $S=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c, \in R\right\}$ be the ring under matrix addition and multiplication.

Then the subset $\left\{\begin{pmatrix} 0 & p \\ 0 & 0 \end{pmatrix} : p \in R\right\}$ is

(a.) Not an ideal of S

(b.) An ideal but not a prime ideal of S

(c.) Is a prime ideal but not a maximal ideal of S

(d.) Is a maximal ideal of S

21. Set of multiples of 4 forms an ideal in $\mathbb{Z}$, the ring of integers under usual addition and multiplication. This ideal is

(a.) A prime ideal but not a maximal ideal

(b.) A maximal ideal but not a prime ideal

(c.) Both prime and maximal ideal

(d.) Neither a prime ideal nor a maximal ideal

22. Which one of the following is TRUE?

(a.) The characteristic of the ring $6\mathbb{Z}$ is 6

(b.) The ring $6\mathbb{Z}$ has a zero divisor

(c.) The characteristic of the ring $(\mathbb{Z}/6\mathbb{Z})\times6\mathbb{Z}$ is zero

(d.) The ring $6\mathbb{Z}\times6\mathbb{Z}$ is an integral domain.

23. For $n \in \mathbb{N}$, let $n\mathbb{Z}=\{nk : k \in \mathbb{Z}\}$. Then the number of units of $\mathbb{Z}/11\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$, respectively, are

(a.) 11, 12

(b.) 10, 11

(c.) 10, 4

(d.) 10, 8

24. Let R be the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$ under point-wise addition and multiplication. Let $I=\{f:\mathbb{R}\to\mathbb{R} \mid f$ is a bounded function $\}$, $J=\{f:\mathbb{R}\to\mathbb{R} \mid f(3)=0\}$. Then

(a.) J is an ideal of R but I is not an ideal of R

(b.) I is an ideal of R but J is not an ideal of R

(c.) Both I and J are ideal of R

(d.) Neither I nor J is an ideal of R

25. Let R be the ring of all 2×2 matrices with integer entries. Which of the following subsets of R is an integral domain?

(a.) $\left\{\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} : x, y \in \mathbb{Z}\right\}$

(b.) $\left\{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x, y \in \mathbb{Z}\right\}$

(c.) $\left\{\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} : x \in \mathbb{Z}\right\}$

(d.) $\left\{\begin{pmatrix} x & y \\ y & z \end{pmatrix} : x, y, z \in \mathbb{Z}\right\}$

26. A ring R has maximal ideals

(a.) if R is infinite

(b.) if R is finite

(c.) if R is finite with at least 2 elements

(d.) only if R is finite

27. The power set $P(X)$ of a set X with the binary operations symmetric difference Δ and intersection $\cap$ form a ring (the symmetric difference is the addition and the intersection is the multiplication) called the power set ring of the set X. If the set X has at least 3 elements, then in the power set ring $(P(X), \Delta, \cap)$ of X, every elements is

(For $A, B \in P(X)$, the subset $A \Delta B := (A \setminus B) \cup (B \setminus A)$ is called the symmetric difference of A and B)

(a.) a unit

(b.) idempotent.

(c.) nilpotent.

(d.) a non-zero divisor.

28. The set $\{0, 2, 4\}$ under addition and multiplication modulo 6 is

(a.) not a ring with unity (identity)

(b.) a ring with 0 as unity (identity)

(c.) a ring with 2 as unity (identity)

(d.) a ring with 4 as unity (identity)

29. Suppose a and b are elements in R, a commutative ring with unity. Then the equation $ax = b$

(a.) always has exactly one solution

(b.) has a solution only if a is a unit

(c.) has more than one solution only if $b = 0$

(d.) may have more than one solution

30. Let $C[0, 1]$ be the ring of continuous real-valued functions on [0, 1], with addition and multiplication defined pointwise. For any subset S of [0, 1] let $Z(S) = \{f \in C[0, 1] \mid f(x) = 0 \text{ for all } x \in S\}$. Then which of the following statements are true?

(a.) If Z(S) is an ideal in C[0, 1] then S is closed in [0, 1].

(b.) If Z(S) is a maximal ideal then S has only one point.

(c.) If S has only one point then Z(S) is a maximal ideal.

(d.) None of these

31. Pick out the true statements:

(a.) The set $\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a \in \mathbb{R}, a \neq 0\right\}$ is a group with respect to matrix multiplication.

(b.) The set $\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R}\right\}$ is a commutative ring with identity with respect to matrix addition and matrix multiplication.

(c.) The set $\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}\right\}$ is a field with respect to matrix addition and matrix multiplication.

(d.) None of these

32. Let $\mathbb{C}[0, 1]$ denote the ring of all continuous real-valued function on $[0, 1]$ with respect to pointwise addition and pointwise multiplication. Pick out the true statements:

(a.) $\mathbb{C}[0, 1]$ is an integral domain.

(b.) Let $a \in [0, 1]$. Set $I = \{f \in \mathbb{C}[0, 1] \mid f(a) = 0\}$. Then I is an ideal in $\mathbb{C}[0, 1]$.

(c.) If I is any proper ideal in $\mathbb{C}[0, 1]$, then there exists at least one point $a \in [0, 1]$ such that $f(a) = 0$ for all $f \in I$.

(d.) None of these

33. Let R be a (commutative) ring (with unity). Let I and J be ideal in R. Pick out the true statements:

(a.) $I \cup J$ is an ideal in R

(b.) $I \cap J$ in an ideal in R

(c.) $I + J = \{x + y : x \in I, y \in J\}$ is an ideal in R.

(d.) None of these

34. Pick out the rings which are integral domains:

(a.) $\mathbb{R}[x]$, the ring of all polynomials in one variable with real coefficients

(b.) $C^1[0, 1]$, the ring of continuously differentiable real-valued function on the interval $[0, 1]$ (with respect to point wise addition and point wise multiplication)

(c.) $\mathbb{M}_n(\mathbb{R})$ the ring of all $n \times n$ matrices with real entries.

(d.) None of these

35. Pick out the units in $\mathbb{Z}[\sqrt{3}]$

(a.) $-7+4\sqrt{3}$

(b.) $5+3\sqrt{3}$

(c.) $2-\sqrt{3}$

(d.) $-3-2\sqrt{3}$

36. Pick out the integral domains from the following list of rings:

(a.) $\{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\}$

(b.) The ring of continuous functions from $[0, 1]$ into $\mathbb{R}$

(c.) The ring of complex analytic functions on the disc $\{z \in \mathbb{C} \mid |z|<1\}$

(d.) The polynomial ring $\mathbb{Z}[x]$.

37. Let P be a prime ideal in a commutative ring R and let $S = R \setminus P$, i.e., the complement of P in R Pick out the true statements:

(a.) S is closed under addition

(b.) S is closed under multiplication

(c.) S is closed under addition and multiplication

(d.) None of these

38. Pick out the true statement (s):

(a.) The set of all 2×2 matrices with rational entries (with the usual operations of matrix addition and matrix multiplication) is a ring which has no non-trivial ideals.

(b.) Let $R = C[0, 1]$ be considered as a ring with the usual operations of $I = \{f : [0, 1] \to \mathbb{R} \mid f(1/2) = 0\}$. Then I is a maximal ideal.

(c.) Let R be a commutative ring and let P be a prime ideal of R. Then R/P is an integral domain.

(d.) None of these

39. Pick out the true statements:

(a.) Let R be a commutative ring with identity. Let M be an ideal such that every element of R not in M is a unit. Then R/M is a field.

(b.) Let R be as above and let M be an ideal such that R/M is an integral domain. Then M is a prime ideal.

(c.) Let $R = C[0, 1]$ be the ring of real-valued continuous functions on $[0, 1]$ with respect to pointwise addition and pointwise multiplication. Let $M = \{f \in R \mid f(0) = f(1) = 0\}$. Then M is a maximal ideal.

(d.) None of these

40. The number of element of a principal ideal domain can be

(a.) 15

(b.) 25

(c.) 35

(d.) 36

41. Let m be an odd integer >6. Then the multiplicative inverse of 2 in the ring $(\mathbb{Z}_m, +_m, \cdot_m)$ (where $+_m$ and $\cdot_m$ denote the addition and multiplication modulo m respectively.)

(a.) does not exist.

(b.) is $\frac{m-1}{2}$.

(c.) is $\frac{m+1}{2}$.

(d.) is $m-2$.

42. Consider $S = \mathbb{C}[x^5]$, complex polynomials is x^5, as a subset of $T = \mathbb{C}[x]$, the ring of all complex polynomials. Then

(a.) S is neither an ideal nor a sub ring of T

(b.) S is an ideal, but not a sub ring of T

(c.) S is a sub ring but not an ideal of T

(d.) S is both a sub ring and an ideal of T

43. Let F be a field of 8 elements and $F = \{x \in F \mid x^7 = 1 \text{ and } x^k \neq 1 \text{ for all natural numbers } k < 7\}$. Then the number of elements in A is

(a.) 1

(b.) 2

(c.) 3

(d.) 6

44. Which of the following can not be cardinality of a field?

(a.) 6

(b.) 4

(c.) 27

(d.) 7

45. Which of the following statements are true?

(a.) There exists a finite field in which the additive group is not cyclic.

(b.) If F is a finite field, there exists a polynomial p over F such that $p(x) \neq 0$ for all $x \in F$, where 0 denotes the zero in F.

(c.) Every finite field is isomorphic to a subfield of the field of complex numbers.

(d.) None of these

46. The number of subfields of a field of cardinality 2^{100} is

(a.) 2

(b.) 4

(c.) 9.

(d.) 100.

47. Let **F** be a field with 5^{12} elements. What is the total number of proper subfields of **F** ?

(a.) 3

(b.) 6

(c.) 8

(d.) 5

48. Which of following statement is true.

(a.) $\exists$ a field of order 36 but not order 49.

(b.) $\exists$ a field of order 36.

(c.) $\nexists$ field of order 36 and 49

(d.) $\nexists$ field of order 36.

49. Let $\mathbb{Z}_{10}$ denote the ring of integers modulo 10. Then the number of ideals in $\mathbb{Z}_{10}$ is

(a.) 2

(b.) 3

(c.) 4

(d.) 5

50. The number of subfields of a finite field of order 3^{10} is equal to

(a.) 4

(b.) 5

(c.) 3

(d.) 10

51. Let p, q be distinct primes. Then

(a.) $\mathbb{Z}/_{p^2q\mathbb{Z}}$ has exactly 3 distinct ideals

(b.) $\mathbb{Z}/_{p^2q\mathbb{Z}}$ has exactly 3 distinct maximal

(c.) $\mathbb{Z}/_{p^2q\mathbb{Z}}$ has exactly 2 distinct maximal

(d.) $\mathbb{Z}/_{p^2q\mathbb{Z}}$ has a unique maximal ideal

52. If S is a finite commutative ring with 1 then

(a.) Each prime ideal is a maximal ideal

(b.) S may have a prime ideal which is not maximal

(c.) S has no nontrivial maximal ideals

(d.) S is a field

53. Suppose $(F, +, \cdot)$ is the finite field with 9 elements. Let $G = (F, +)$ *and* $H = (F \setminus \{0\}, \cdot)$ denote the underlying additive and multiplicative groups respectively. Then

(a.) $G \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

(b.) $G \cong (\mathbb{Z}/9\mathbb{Z})$

(c.) $H \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

(d.) $G \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ *and* $H \cong (\mathbb{Z}/8\mathbb{Z})$

54. The number of non-zero ideals of $\frac{\mathbb{Z}}{100\mathbb{Z}}$ is

(a.) 4

(b.) 8

(c.) 10

(d.) 6

55. If p is prime, and $\mathbb{Z}_{p^4}$ denote the ring of integers modulo p^4, then the number of maximal ideals in $\mathbb{Z}_{p^4}$ is

(a.) 4

(b.) 2

(c.) 3

(d.) 1

56. For $n \geq 1$, let $(\mathbb{Z}/n\mathbb{Z})^*$ be the group of units of $(\mathbb{Z}/n\mathbb{Z})$. Which of the following groups are cyclic?

(a.) $(\mathbb{Z}/10\mathbb{Z})^*$

(b.) $(\mathbb{Z}/2^3\mathbb{Z})^*$

(c.) $(\mathbb{Z}/100\mathbb{Z})^*$

(d.) $(\mathbb{Z}/163\mathbb{Z})^*$

57. Let a,b,c,d be real numbers with $a < c < d < b$. Consider the ring $C[a,b]$ with pointwise addition and multiplication. If $S = \{f \in C[a,b] : f(x) = 0 \text{ for all } x \in [c,d]\}$, then

(a.) S is NOTan ideal of C [a,b]

(b.) S is an ideal of C [a,b] but NOT a prime ideal of C [a,b]

(c.) S is a prime ideal of C [a,b] but NOT a maximum ideal of C [a,b]

(d.) S is a maximum ideal of C [a,b]

58. Let F_{125} be the field of 125 elements. The number of non-zero elements $\alpha \in F_{125}$ such that $\alpha^5 = \alpha$ is _____

59. The possible valued for the degree of an irreducible polynomial in $\mathbb{R}[x]$.

(a.) 2

(b.) 3

(c.) 4

(d.) 5

60. The number of non-zero elements in the field $\mathbb{Z}_p$, where p is an odd prime number, which are squares, i.e., of the form $m^2, m \in \mathbb{Z}_p, m \neq 0$._____

61. Let M denote the set of all 2 × 2 matrices over the reals. Addition and multiplication on M are as follows:

$A=(a_{ij})$ and $B = (b_{ij})$, then $A + B = (c_{ij})$, where $c_{ij} = a_{ij} + b_{ij}$, and $A \cdot B = (d_{ij})$, where $d_{ij} = a_{ij}b_{ij}$

Then which one of the following is valid for $(M, +, \cdot)$?

(a.) M is a field

(b.) M is an integral domain which is not a field

(c.) M is a commutative ring which is not an integral domain

(d.) M is a non-commutative ring

62. Consider $\mathbb{Z}[x]$, the set of all polynomials with integer coefficients and $\mathbb{Q}[\sqrt{2}]$, the set of all real numbers of the form $a + b\sqrt{2}$ with a, b rational numbers. Which of the following is correct about $\mathbb{Z}[x]$ and $\mathbb{Q}[\sqrt{2}]$?

(a.) Both are rings, but only one has unity

(b.) Both are commutative rings, but only one is an integral domain

(c.) Both are integral domains, but only one is a field

(d.) Both are fields

63. Let (R, +) be an abelian group. If multiplication $(\cdot)$ is defined on R by setting $a.b = 0$ for all a, b, $\in R$, then which one of the following statements is correct?

(a.) $(R,+,\cdot)$ is not a ring.

(b.) $(R,+,\cdot)$ is a ring, but not commutative.

(c.) $(R,+,\cdot)$ is a commutative ring, but has no unity.

(d.) $(R,+,\cdot)$ is not a field.

64. Consider the following assertions

i. The characteristic of the ring $(\mathbb{Z},+,\cdot)$ is zero.

ii. For every composite number, n, $\mathbb{Z}_n$, the ring of residue classes modulo n, is a field.

iii. $\mathbb{Z}_5$, the ring of residue classes modulo 5, is an integral domain.

iv. The ring of all complex numbers is a field.

Which of the above assertions are correct?

(a.) i, iii and iv

(b.) i, ii and iii

(c.) i, ii and iv

(d.) i, iii and iv

65. Let F be a finite field with n elements. What is the possible value of n?

(a.) 1

(b.) 36

(c.) 37

(d.) 125

66. If R is a finite integral domain with n element, then what is the number of invertible elements under multiplication in R?

(a.) 1

(b.) n

(c.) n – 1

(d.) [n/2] where [·] is the bracket function

67. Consider the ring $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n}\}$ of congruent modulo n classes. Under addition and multiplication modulo n, consider the following statements is/are are correct:

(a.) In $\mathbb{Z}_6$, $\overline{4}$ divides $\overline{2}$

(b.) In $\mathbb{Z}_8$, $\overline{3}$ divides $\overline{7}$

(c.) In $\mathbb{Z}_{15}$, $\overline{9}$ divides $\overline{12}$

(d.) None of these

68. The zero divisors in Z_8 are

(a.) $\overline{3}$, $\overline{4}$, $\overline{5}$

(b.) $\overline{1}$, $\overline{2}$, $\overline{4}$

(c.) $\overline{2}$, $\overline{4}$, $\overline{7}$

(d.) $\overline{2}$, $\overline{4}$, $\overline{6}$

69. The characteristic of the ring $Z_4 \times Z_6$ is

(a.) 0

(b.) 6

(c.) 12

(d.) 24

70. Let F be a field containing 11 elements. Which one of the following is correct?

(a.) If α is a non-zero element of F, then $5\alpha \neq 0$

(b.) $\alpha 5 = 1$ for every non-zero $\alpha \in$ F where 1 is the multiplicative identity of F

(c.) $\alpha 10 = 1$ for all $\alpha \in F$

(d.) Let α be a non-zero element of F. It is possible to find a proper subset S of F such that $\alpha \in S$ and $\beta s \in S$ for any $\beta \in F$, $s \in S$

ASSIGNMENT SHEET - 2

1. Consider the following statements:

1. Every PID is ED
2. The group of units in the ring $\frac{\mathbb{Z}}{37\mathbb{Z}}$ is cyclic
3. There is a field with 6^5 elements.

(a.) (1) is true but (2) and (3) are false.

(b.) (2) is true but (1) and (3) are false.

(c.) (3) is true but (1) and (2) are false.

(d.) All these statement is false.

2. Let R be the ring $\mathbb{Z}[x]/\langle\langle(x^2+x+1)(x^3+x+1)\rangle\rangle$ What is the cardinality of the ring R ?

(a.) 27

(b.) 32

(c.) 64

(d.) Infinite

3. Let $p(x)=9x^5+10x^3+5x+15$ and $q(x)=x^3-x^2-x-2$ be two polynomials in $\mathbb{Q}[x]$. Then, over $\mathbb{Q}$,

(a.) $p(x)$ and $q(x)$ are both irreducible

(b.) $p(x)$ is reducible but $q(x)$ is irreducible

(c.) $p(x)$ is irreducible but $q(x)$ is reducible

(d.) $p(x)$ and $q(x)$ are both reducible

4. Pick out the cases where the given ideal is a maximal ideal.

(a.) The ideal $15\mathbb{Z}$ in $\mathbb{Z}$.

(b.) The ideal $I=\{f: f(0)=0\}$ in the ring $C[0, 1]$ of all continuous real valued functions on the interval $[0, 1]$.

(c.) The ideal generated by x^3+x+1 in the ring of polynomials $\mathbb{F}_3[x]$, where $\mathbb{F}_3$ is field of three elements.

(d.) None of these

5. Which of the following statements is false?

(a.) The polynomial x^2+x+1 is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$

(b.) The polynomial x^2-2 is irreducible in $\mathbb{Q}[x]$

(c.) The polynomial x^2+1 is reducible in $\mathbb{Z}/5\mathbb{Z}[x]$

(d.) The polynomial x^2+1 is reducible in $\mathbb{Z}/7\mathbb{Z}[x]$.

6. Consider the polynomial ring $\mathbb{Q}[x]$. The ideal of $\mathbb{Q}[x]$ generated by x^2-3 is

(a.) maximal but not prime

(b.) prime but not maximal

(c.) both maximal and prime

(d.) neither maximal nor prime

7. $\mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle$ is

(a.) a field having 8 elements

(b.) a field having 9 elements

(c.) an infinite field

(d.) NOT a field

8. Let $\mathbb{R}[X]$ be the ring of real polynomials in the variable X. The number of ideals in the quotient ring $\mathbb{R}[X]/\langle(X^2-3X+2)\rangle$ is

(a.) 2

(b.) 3

(c.) 4

(d.) 6

9. Let $R=\mathbb{Q}[x]$. Let I be the principal ideal $\langle x^2+1\rangle$ and J be the principal ideal $\langle x^2\rangle$. Then

(a.) $\frac{R}{I}$ is a field and $\frac{R}{J}$ is a field

(b.) $\frac{R}{I}$ is an integral domain and $\frac{R}{J}$ is a field

(c.) $\frac{R}{I}$ is a field and $\frac{R}{J}$ is a PID

(d.) $\frac{R}{I}$ is a field and $\frac{R}{J}$ is not an integral domain.

10. Let $\mathbb{Z}_n$ be the ring of integers modulo n, where n is an integer ≥ 2 .Then Choose the correct in the following:

(a.) $\mathbb{Z}_n$ is a field then n is prime

(b.) If $\mathbb{Z}_n$ is an integral domain then n is prime

(c.) If there is an injective ring homomorphism of $\mathbb{Z}_5$ to $\mathbb{Z}_n$ then n is multiple of 5

(d.) None of these

11. Let F be a finite field. If $f : F \to F$, given by $f(x) = x^3$ is a ring homomorphism, then

(a.) $F = \mathbb{Z}/3\mathbb{Z}$

(b.) $F = \mathbb{Z}/2\mathbb{Z}$ or characteristic of $F = 3$

(c.) $F = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$

(d.) Characteristic F is 3

12. 'Consider $\mathbb{Z}_5$ as field modulo 5 and let $f(x) = x^5 + 4x^4 + 4x^3 + 4x^2 + x + 1$ Then the zero of $f(x)$ and over $\mathbb{Z}_5$ are 1 and 3, with respective multiplicity

(a.) 1 and 4

(b.) 2 and 3

(c.) 2 and 2

(d.) 1 and 2

13. Let R be the polynomial ring $\mathbb{Z}_2[x]$ and write the elements of $\mathbb{Z}_2$ as {0, 1}. Let $\langle f(x) \rangle$ denote the ideal generated by the element $f(x) \in R$. If $f(x) = x^2 + x + 1$, then the quotient ring $R/\langle f(x) \rangle$ is

(a.) a ring but not an integral domain.

(b.) an integral domain but not a field.

(c.) a finite field of order 4.

(d.) an infinite field.

14. Let $\mathbb{R}[x]$ be the polynomial ring in x with real coefficients and let $I = \langle x^2 + 1 \rangle$ be the ideal generated by the polynomial $x^2 + 1$ in $R[x]$. Then

(a.) I is a maximal ideal

(b.) I is a prime ideal but NOT a maximal ideal

(c.) I is NOT a prime ideal

(d.) R[x] /I has zero divisors

15. Let F_4, F_8 and F_{16} be finite fields of 4,8 and 16 elements respectively. Then,

(a.) F_4 is isomorphic to a subfield of F_8

(b.) F_8 is isomorphic to a subfield of F_{16}

(c.) F_4 is isomorphic to a subfield of F_{16}

(d.) None of the above

16. Let PID, ED, UFD denote the set of all principal ideal domains, Eucliden domains, unique factorization domains, respectively. Then

(a.) $UFD \subset ED \subset PID$

(b.) $PID \subset ED \subset UFD$

(c.) $ED \subset PID \subset UFD$

(d.) $PID \subset UFD \subset ED$

17. Let I_1 be the ideal generated by $x^4 + 3x^2 + 2$ and I_2 be the ideal generated by $x^3 + 1$ in $\mathbb{Q}[x]$. If $F_1 = \frac{\mathbb{Q}[x]}{I_1}$ and $F_2 = \frac{\mathbb{Q}[x]}{I_2}$, then

(a.) F_1 and F_2 are fields

(b.) F_1 is a field, but F_2 is not a field

(c.) F_1 is not a field while F_2 is a field

(d.) Neither F_1 nor F_2 is a field.

18. For which of the following primes p, does not polynomial $x^4 + x + 6$ have a root of multiplicity > 1 over a field of characteristic p ?

(a.) $p = 2$

(b.) $p = 3$

(c.) $p = 5$

(d.) $p = 7$

19. Which of the following statements is true about $S = \mathbb{Z}[x]$?

(a.) S is an Euclidean domain since all its ideals are principal

(b.) S is an Euclidean domain since $\mathbb{Z}$ is an Euclidean domain

(c.) S is not an Euclidean domain since S is not even an integral domain

(d.) S is not an Euclidean domain since it has non-principal ideals

20. For positive integers n and m, where $n, m > 1$, suppose that $n\mathbb{Z}$ and $m\mathbb{Z}$ are isomorphic as rings. Then,

(a.) there is no restriction on n and m

(b.) $n = m$

(c.) $g.c.d(n, m) = 1$

(d.) necessarily $n \mid m$ or $m \mid n$, but not both

21. The number of roots of the polynomial $x^3 - x$ in $\frac{\mathbb{Z}}{6\mathbb{Z}}$ is

(a.) 1

(b.) 2

(c.) 3

(d.) 6

22. Let $\mathbb{Z}$ be the ring of integers under the usual addition and multiplication. Then every nontrivial ring homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ is

(a.) Both injective and surjective

(b.) Injective but not surjective

(c.) Surjective but not injective

(d.) Neither injective nor surjective

23. Let $\mathbb{Q}$ be the field of rational number and consider $\mathbb{Z}_2$ as a field modulo 2. Let $f(x) = x^3 - 9x^2 + 9x + 3$ Then $f(x)$ is

(a.) irreducible over but reducible over $\mathbb{Z}_2$

(b.) irreducible over both $\mathbb{Q}$ and $\mathbb{Z}_2$

(c.) reducible over $\mathbb{Q}$ but irreducible over $\mathbb{Z}_2$

(d.) reducible over both $\mathbb{Q}$ and $\mathbb{Z}_2$

24. The number of element of a principal ideal domain can be

(a.) 15

(b.) 25

(c.) 35

(d.) 36

25. Let R be a ring. If R[x] is a principal ideal domain, then R is necessarily a

(a.) Unique Factorization Domain

(b.) Principal Ideal Domain

(c.) Euclidean Domain

(d.) Field

26. Let R be the ring of polynomials over $\mathbb{Z}_2$ and let I be the ideal of R generated by the polynomial $x^3 + x + 1$. Then the number of elements in the quotient ring $\frac{R}{I}$ is

(a.) 2

(b.) 4

(c.) 8

(d.) 16

27. Let m and n be coprime natural numbers. Then the kernel of the ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, defined by $\phi(x) = (\bar{x}, \bar{x})$ is

(a.) $m\mathbb{Z}$

(b.) $mn\mathbb{Z}$

(c.) $n\mathbb{Z}$

(d.) $\mathbb{Z}$

28. The ring $\mathbb{Z}[x]$ is a

(a.) unique factorization domain, but not a principal ideal domain

(b.) a principal ideal domain, but not a Euclidean domain

(c.) A Euclidean domain but not a field.

(d.) A field

29. Let R be a Principal Ideal Domain and a, b any two non-unit elements of R. Then the ideal generated by a and b is also generated by

(a.) $a + b$

(b.) ab

(c.) $gcd(a, b)$

(d.) $lcm(a, b)$

30. The polynomial $x^3 + 5x^2 + 5$ is

(a.) Irreducible over $\mathbb{Z}$ but reducible over $\mathbb{Z}_5$

(b.) Irreducible over both $\mathbb{Z}$ and $\mathbb{Z}_5$

(c.) Reducible over $\mathbb{Z}$ but irreducible over $\mathbb{Z}_5$

(d.) Reducible over both $\mathbb{Z}$ and $\mathbb{Z}_5$

31. Which of the following rings is a PID?

(a.) $\mathbb{Q}[X,Y]/\langle X\rangle$

(b.) $\mathbb{Z}\oplus\mathbb{Z}$

(c.) $\mathbb{Z}[X]$

(d.) $M_2(\mathbb{Z})$, the ring of 2×2 matrices with entries in $\mathbb{Z}$

32. Let $f(x)\in\mathbb{Z}_5[x]$ be a polynomial such that $\frac{\mathbb{Z}_5[x]}{\langle f(x)\rangle}$ is a field, where $\langle f(x)\rangle$ denotes the ideal generated by $f(x)$. Then one of the choices for $f(x)$ is

(a.) $x+1$

(b.) x^2+3

(c.) x^2+1

(d.) x^3+3

33. Consider $\mathbb{Z}_5$ and $\mathbb{Z}_{20}$ as ring modulo 5 and 20, respectively. Then the number of homomorphism $\phi\colon \mathbb{Z}_5\to\mathbb{Z}_{20}$ is

(a.) 1

(b.) 2

(c.) 4

(d.) 5

34. The polynomial ring $\mathbb{Z}[x]$ is

(a.) A Euclidean domain but not a PID

(b.) A PID but not Euclidean

(c.) Neither PID nor Euclidean

(d.) Both PID and Euclidean

35. The polynomial $f(x)=x^5+5$ is

(a.) Irreducible over $\mathbb{C}$

(b.) Irreducible over $\mathbb{R}$

(c.) Irreducible over $\mathbb{Q}$

(d.) Not irreducible $\mathbb{Q}$

Where $\mathbb{Q}$ denotes the field of rational number.

36. The number of non-trivial ring homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{28}$ is

(a.) 1

(b.) 3

(c.) 4

(d.) 7

37. Let I denote the ideal generated by $x^4+x^3+x^2+x+1$ in $\mathbb{Z}_2[x]$ and $F=\mathbb{Z}_3[x]/I$. Then,

(a.) F is an infinite field

(b.) F is a finite field of 4 elements

(c.) F is a finite field of 8 elements

(d.) F is a finite field of 16 elements

38. The polynomial $x^3-7x^2+15x-9$ is

(a.) Irreducible over both $\mathbb{Z}$ and $\mathbb{Z}_3$

(b.) Irreducible over $\mathbb{Z}$ but reducible over $\mathbb{Z}_3$

(c.) Reducible over $\mathbb{Z}$ but irreducible over $\mathbb{Z}_3$

(d.) Reducible over both $\mathbb{Z}$ and $\mathbb{Z}_3$

39. The polynomial $f(X):=X^2+aX+1$ in $\mathbb{Z}_3[X]$ is

(a.) irreducible in $\mathbb{Z}_3[X]$

(b.) irreducible in $\mathbb{Z}_3[X]$ if and only if $a=0$

(c.) irreducible in $\mathbb{Z}_3[X]$ if and only if $a=1$

(d.) always reducible in $\mathbb{Z}_3[X]$.

40. Let $f(x)=x^3+2x^2+1$ and $g(x)=2x^2+x+2$. Then over $\mathbb{Z}_3$,

(a.) $f(x)$ and $g(x)$ are irreducible

(b.) $f(x)$ is irreducible, but $g(x)$ is not

(c.) $g(x)$ is irreducible, but $f(x)$ is not

(d.) Neither $f(x)$ nor $g(x)$ is irreducible.

41. Let $\mathbb{F}_p$ denote the field $\frac{\mathbb{Z}}{p\mathbb{Z}}$, where p is a prime. Let $\mathbb{F}_p[x]$ be the associated polynomial ring. Which of the following quotient rings are fields?

(a.) $\frac{\mathbb{F}_5[x]}{\langle x^2+x+1\rangle}$

(b.) $\frac{\mathbb{F}_2[x]}{\langle x^3+x+1\rangle}$

(c.) $\frac{\mathbb{F}_3[x]}{\langle x^3+x+1\rangle}$

(d.) None of these

42. Let R be a commutative ring and $R[x]$ be the polynomial ring in one variable over R.

(a.) If R is a U.F.D., then $R[x]$ is a U.F.D.

(b.) If R is a P.I.D, then $R[x]$ is a P.I.D.

(c.) If R is an Euclidian domain, then $R[x]$ is an Euclidean domain

(d.) If R is a field, then $R[x]$ is an Euclidean domain.

43. Let $\langle p(x)\rangle$ denote the ideal generated by the polynomial $p(x)$ in $\mathbb{Q}[x]$. If $f(x)=x^3+x^2+x+1$ and $g(x)=x^3-x^2+x-1$, then

(a.) $\langle f(x)\rangle+\langle g(x)\rangle=\langle x^3+x\rangle$

(b.) $\langle f(x)\rangle+\langle g(x)\rangle=\langle f(x)\cdot g(x)\rangle$

(c.) $\langle f(x)\rangle+\langle g(x)\rangle=\langle x^2+1\rangle$

(d.) $\langle f(x)\rangle+\langle g(x)\rangle=\langle x^2-1\rangle$

44. Determine which of the following polynomials are irreducible over the indicated rings.

(a.) $x^5-3x^4+2x^3-5x+8$ over $\mathbb{R}$.

(b.) x^3+2x^2+x+1 over $\mathbb{Q}$.

(c.) x^3+3x^2-6x+3 over $\mathbb{Z}$.

(d.) x^4+x^2+1 over $\mathbb{Z}/2\mathbb{Z}$.

45. Which of the following polynomials are irreducible in the ring $\mathbb{Z}[x]$ of polynomials in one variable with integer coefficients?

(a.) x^2-5.

(b.) $1+(x+1)-(x+1)^2+(x+1)^3+(x+1)^4$.

(c.) $1+x+x^2+x^3+x^4$.

(d.) $1+x+x^2+x^3$.

46. Let F and F' be two finite fields of order q and q' respectively. Then:

(a.) F' contains a subfield isomorphic to F if and only if $q \le q'$.

(b.) F' contains a subfield isomorphic to F if and only if q divides q'.

(c.) If the g.c.d of q and q' is not 1, then both are isomorphic to subfields of some finite field L.

(d.) Both F and F' are quotient rings of the ring $\mathbb{Z}[X]$.

47. Which of the polynomials are irreducible over the given rings?

(a.) $X^5+3X^4+9X+15$ over $\mathbb{Q}$, the field of rationals

(b.) X^3+2X^2+X+1 over $\mathbb{Z}/7\mathbb{Z}$, the ring of integers modulo 7

(c.) X^3+X^2+X+1 over $\mathbb{Z}$, the ring of integers

(d.) $X^4+X^3+X^2+X+1$ over $\mathbb{Z}$, the ring of intgers.

48. Consider the ring $R=\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}:a,b\in\mathbb{Z}\}$ and the element $\alpha=3+\sqrt{-5}$ of R. Then

(a.) α is prime

(b.) α is irreducible

(c.) R is not a unique factorization domain

(d.) R is not an integral domain.

49. Let $f(x)=x^3+x^2+x+1$ and $g(x)=x^5+1$. Then in $\mathbb{Q}[x]$

(a.) g.c.d $(f(x),g(x))=x+1$

(b.) g.c.d $(f(x),g(x))=x^2-1$

(c.) l.c.m. $(f(x),g(x))=x^5+x^3+x^2+1$

(d.) l.c.m. $(f(x),g(x))=x^5+x^4+x^3+x^2+1$

50. Let $\mathbb{R}[x]$ be the polynomial ring over $\mathbb{R}$ in one variable. Let $I \subseteq \mathbb{R}[x]$ be an ideal. Then

(a.) I is a maximal ideal if and only if I is a non-zero prime ideal

(b.) I is a maximal ideal if and only if the quotient ring $\mathbb{R}[x]/I$ is isomorphic to $\mathbb{R}$

(c.) I is a maximal ideal if and only if $I = \langle f(x) \rangle$, where $f(x)$ is non-constant irreducible polynomial over $\mathbb{R}$

(d.) I is a maximal ideal if and only if there exists a non-constant polynomial $f(x) \in I$ of degree $\exists$

51. Let $f(x) = x^4 + 3x^3 - 9x^2 + 7x + 27$ and let p be a prime. Let $f_p(x)$ denote the corresponding polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Then

(a.) $f_2(x)$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$

(b.) $f(x)$ is irreducible over $\mathbb{Q}$

(c.) $f_3(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$

(d.) $f(x)$ is irreducible over $\mathbb{Z}$

52. Which of the following is an irreducible factor of $x^{12} - 1$ over $\mathbb{Q}$?

(a.) $x^8 + x^4 + 1$.

(b.) $x^4 + 1$.

(c.) $x^4 - x^2 + 1$.

(d.) $x^5 - x^4 + x^3 - x^2 + x - 1$.

53. Let R be a Euclidean domain such that R is not a field. Then the polynomial ring $R[X]$ is always

(a.) a Euclidean domain.

(b.) a principal ideal domain, but not a Euclidean domain.

(c.) a unique factorization domain, but not a principal ideal domain.

(d.) not a unique factorization domain.

54. Which of the following quotient rings are fields?

(a.) $\mathbf{F}_3[X]/\langle (X^2 + X + 1) \rangle$, where $\mathbf{F}_3$ is the finite field with 3 elements.

(b.) $\mathbb{Z}[X]/\langle (X - 3) \rangle$

(c.) $\mathbb{Q}[X]/\langle (X^2 + X + 1) \rangle$

(d.) $\mathbf{F}_2[X]/\langle (X^2 + X + 1) \rangle$ where $\mathbf{F}_2$ is the finite field with 2 elements.

55. Let A denote the quotient ring $\frac{\quad}{\mathbf{s}}$. Then

(a.) There are exactly three distinct proper ideals in A.

(b.) There is only one prime ideal in A

(c.) A is an integral domain.

(d.) Let f, g be in $\mathbb{Q}[X]$ such that $\bar{f} \cdot \bar{g} = 0$ in A. Here $\bar{f}$ and $\bar{g}$ denote the image of f and g respectively in A. Then $f(0) \cdot g(0) = 0$.

56. Let $c \in \mathbb{Z}_3$ be such that $\dfrac{\mathbb{Z}_3[X]}{\langle X^3 + cX + 1 \rangle}$ is a field. Then c is equal to _____

57. The number of ring homeomorphisms form $\mathbb{Z}_2 \times \mathbb{Z}_2$ to $\mathbb{Z}_4$ is equal to _____

58. Pick out the true statements:

(a.) Let R be a commutative ring with identity. Let M be an ideal such that every element of R not in M is a unit. Then R/M is a field.

(b.) Let R be as above and let M be an ideal such that R/M is an integral domain. Then M is a prime ideal.

(c.) Let $R = C[0, 1]$ be the ring of real-valued continuous functions on $[0, 1]$ with respect to pointwise addition and pointwise multiplication. Let $M = \{f \in R \mid f(0) = f(1) = 0\}$. Then M is a maximal ideal.

(d.) None of these

59. Pick out the true statement(s):

(a.) The set of all 2×2 matrices with rational entries (with the usual operations of matrix addition and matrix multiplication) is a ring which has no non-trivial ideals.

(b.) Let $R = C[0, 1]$ be considered as a ring with the usual operations of $I = \{f : [0, 1] \to \mathbb{R} \mid f(1/2) = 0\}$. Then I is a maximal ideal.

(c.) Let R be a commutative ring and let P be a prime ideal of R. Then R/P is an integral domain.

(d.) None of these

60. Let $C(\mathbb{R})$ denote the ring of all continuous real-valued functions on $\mathbb{R}$, with the operations of pointwise addition and pontwise multiplication. Which of the following form an ideal in this ring?

(a.) The set of all C^∞ functions with compact support.

(b.) The set of all continuous functions with compact support.

(c.) The set of all continuous functions which vanish at infinity, i.e., functions f such that $\lim_{|x|\to\infty} f(x) = 0$.

(d.) None of these

61. The number of roots of the equation $x^6+x^5+x^4+x^3+x^2+x^1+1 = 0$ in Z_7 is

(a.) 1

(b.) 2

(c.) 3

(d.) 4

62. Which one of the following statements is correct where R[x] denotes the polynomial ring in the one variable x over a ring R:

(a.) If R is a field then R[x] is a field

(b.) If R is an integral domain, then R[x] is a field

(c.) If R is a field then R[x] is an integral domain

(d.) Every integral domain is a field.

ASSIGNMENT SHEET - 3

1. For the rings $L = \dfrac{\mathbb{R}[x]}{\langle x^2 - x + 1\rangle}$;

$M = \dfrac{\mathbb{R}[x]}{\langle x^2 + x + 1\rangle}$; $N = \dfrac{\mathbb{R}[x]}{\langle x^2 + 2x + 1\rangle}$

Which one of the following is TRUE?

(a.) L is isomorphic to M; L is not isomorphic to N; M is not isomorphic to N

(b.) M is isomorphic to N; M is not isomorphic to L; N is not isomorphic to L

(c.) L is isomorphic to M; M is isomorphic to N

(d.) L is not isomorphic to M; L is not isomorphic to N; M is not isomorphic to N

2. In which of the following fields, the polynomial $x^3 - 312312x + 123123$ is irreducible in $\mathbb{F}[x]$?

(a.) The field $\mathbb{F}_3$ with 3 elements

(b.) The field $\mathbb{F}_7$ with 7 elements

(c.) The field $\mathbb{F}_{13}$ with 13 elements

(d.) The field $\mathbb{Q}$ of rational numbers

3. Pick out the rings which are integral domains:

(a.) $\mathbb{R}[x]$, the ring of all polynomials in one variable with real coefficients

(b.) $C^1[0, 1]$, the ring of continuously differentiable real-valued function on the interval $[0,1]$ (with respect to point wise addition and point wise multiplication)

(c.) $\mathbb{M}_n(\mathbb{R})$ the ring of all $n \times n$ matrices with real entries.

(d.) None of these

4. The degree of the extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ Over the field $\mathbb{Q}(\sqrt{2})$ is

(a.) 1

(b.) 2

(c.) 3

(d.) 6

5. Let Q denote the field of rational numbers, the ring $\mathbb{Q}[x]/\langle x^2 + 1\rangle$ is isomorphic to

(a.) The field of complex numbers.

(b.) $\mathbb{Q}[x]/\langle x^2\rangle$

(c.) $\mathbb{Q}[x]/\langle\langle x^2 + 2x + 2\rangle\rangle$

(d.) None of above.

6. Pick out the correct statements from the following list:

(a.) A homomorphic image of a UFD (unique factorization domain) is again a (UFD).

(b.) The element $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

(c.) Units of the ring $\mathbb{Z}[\sqrt{-5}]$ are the units of $\mathbb{Z}$

(d.) The element 2 is a prime element in $\mathbb{Z}[\sqrt{-5}]$

7. Let K be a field, L a finite extension of K and M a finite extension of L. Then

(a.) $[M:K] = [M:L] + [L:K]$

(b.) $[M:K] = [M:L]\,[L:K]$

(c.) $[M:L]$ divides $[M:K]$

(d.) $[L:K]$ divides $[M:K]$.

8. Let K be an extension of the field $\mathbb{Q}$ of rational numbers

(a.) If K is a finite extension then it is an algebraic extension

(b.) If K is an algebraic extension then it must be a finite extension

(c.) If K is an algebraic extension then it must be an infinite extension

(d.) If K is a finite extension then it need not be an algebraic extension

9. An algebraic number is one which occurs as the root of a monic polynomial with rational coefficients. Which of the following numbers are algebraic?

(a.) $5 + \sqrt{3}$

(b.) $7 + 2^{1/3}$

(c.) $\cos\dfrac{2\pi}{n}$, when $n \in \mathbb{N}$.

(d.) None of these

10. Suppose that R is unique factorization domain and that $a, b \in R$ are distinct irreducible elements. Which of the following statements is **TRUE**?

(a.) The ideal $\langle 1+a \rangle$ is a prime ideal

(b.) The ideal $\langle a+b \rangle$ is a prime ideal

(c.) The ideal $\langle 1+ab \rangle$ is a prime ideal

(d.) The ideal $\langle a \rangle$ is not necessarily a maximal ideal

11. Which of the following is a field?

(a.) $\dfrac{\mathbb{C}[x]}{\langle x^2+2 \rangle}$

(b.) $\dfrac{\mathbb{Z}[x]}{\langle x^2+2 \rangle}$

(c.) $\dfrac{\mathbb{Q}[x]}{\langle x^2-2 \rangle}$

(d.) $\dfrac{\mathbb{R}[x]}{\langle x^2-2 \rangle}$

12. Let G denote the group of all the automorphisms of the field $F_{3^{100}}$ that consists of 3^{100} elements. Then the number of distinct subgroups of G is equal to

(a.) 4

(b.) 3

(c.) 100

(d.) 9

13. If $\mathbb{Z}[i]$ is the ring of Gaussian integers, the quotient $\mathbb{Z}[i]/\langle (3-i) \rangle$ is isomorphic to

(a.) $\mathbb{Z}$

(b.) $\dfrac{\mathbb{Z}}{3\mathbb{Z}}$

(c.) $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$

(d.) $\dfrac{\mathbb{Z}}{10\mathbb{Z}}$

14. Consider the algebraic extension $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ of the field $\mathbb{Q}$ of rational numbers. Then $[E:\mathbb{Q}]$ the degree of E over $\mathbb{Q}$, is

(a.) 3

(b.) 4

(c.) 7

(d.) 8

15. Let ω be a complex number such that $\omega^3 = 1$ and $\omega \neq 1$. Suppose L is the field $\mathbb{Q}(\sqrt[3]{2}, \omega)$ generated by $\sqrt[3]{2}$ and ω over the field $\mathbb{Q}$ of rational numbers. Then the number of subfields K of L such that $\mathbb{Q} \subsetneq \mathbb{K} \subsetneq L$ is

(a.) 2

(b.) 3

(c.) 4

(d.) 5

16. Find the degree of the field extension $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2})$ over $\mathbb{Q}$

(a.) 4

(b.) 8

(c.) 14

(d.) 32

17. For a positive integer n, let $f_n(x) = x^{n-1} + x^{n-2} + \ldots + x + 1$. Then

(a.) $f_n(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every positive integer n.

(b.) $f_p(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every prime number p.

(c.) $f_{p^e}(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every prime number p and every positive integer e.

(d.) $f_p\left(x^{p^{e-1}}\right)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every prime number p and every positive integer e.

18. Which of the following is true

(a.) $\sin 7^\circ$ is algebraic over $\mathbb{Q}$.

(b.) $\cos \pi/17$ is algebraic over $\mathbb{Q}$.

(c.) $\sin^{-1} 1$ is algebraic over $\mathbb{Q}$.

(d.) $\sqrt{2} + \sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$.

19. For a positive integer m, let a_m denote the number of distinct prime ideals of the ring $\frac{\mathbb{Q}[x]}{\langle x^m - 1\rangle}$. Then

(a.) $a_4 = 2$

(b.) $a_4 = 3$

(c.) $a_5 = 2$

(d.) $a_5 = 3$.

20. Let $\mathbb{Z}[i]$ denote the ring of Gaussian integers. For which of the following values of n is the quotient ring $\mathbb{Z}[i]/n\mathbb{Z}[i]$ as integer domain?

(a.) 2

(b.) 13

(c.) 19

(d.) 7

21. Let $F = F_3[X]/\langle (x^3 + 2x - 1)\rangle$, where F_3 is the field with 3 elements. Which of the following statements are true?

(a.) F is a field with 27 elements

(b.) F is a separable but not a normal extension of F_3

(c.) The automorphism group of F is cyclic

(d.) The automorphism group of F is abelian but not cyclic

22. Let G be the Galois group of the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Then, which of the following statements are true?

(a.) G is cyclic

(b.) G is non-abelian

(c.) The order of G is 20

(d.) G has an element of order 4

23. Let R be the ring of all entire functions, i.e. R is the ring of functions $f:\mathbb{C}\to\mathbb{C}$ that are analytic at every point of $\mathbb{C}$, with respect to pointwise addition and multiplication. Then

(a.) The units in R are precisely the nowhere vanishing entire functions, i.e., $f:\mathbb{C}\to\mathbb{C}$ such that f is entire and $f(\alpha)\neq 0$ for all $\alpha\in\mathbb{C}$

(b.) The irreducible elements of R are, up to multiplication by a unit, linear polynomials of the form $z-\alpha$, where $\alpha\in\mathbb{C}$, i.e. if $f\in R$ is irreducible, then $f(z)=(z-\alpha)g(z)$ for all $z\in\mathbb{C}$ where g is a unit in R and $\alpha\in\mathbb{C}$

(c.) R is an integral domain.

(d.) R is a unique factorization domain.

24. Consider the polynomial $f(x) = x^4 - x^3 + 14x^2 + 5x + 16$. Also for a prime number p, let $\mathbb{F}_p$ denote the field with p elements. Which of the following are always true?

(a.) Considering f as a polynomial with coefficients in $\mathbb{F}_3$, it has no roots in $\mathbb{F}_3$.

(b.) Considering f as a polynomial with coefficients in $\mathbb{F}_3$, it is a product of two irreducible factors of degree 2 over $\mathbb{F}_3$.

(c.) Considering f as a polynomial with coefficients in $\mathbb{F}_7$, it has an irreducible factor of degree 3 over $\mathbb{F}_7$.

(d.) f is a product of two polynomials of degree 2 over $\mathbb{Z}$.

25. Which of the following is/are true?

(a.) Given any positive integer n, there exists a field extension of $\mathbb{Q}$ of degree n

(b.) Given a positive integer n, there exist fields F and K such that $F\subseteq K$ and K is Galois over F with $[K:F]=n$

(c.) Let K be a Galois extension of $\mathbb{Q}$ with $[K:\mathbb{Q}]=4$ then there is a field L such that $K\supseteq L\supseteq\mathbb{Q}, [L:\mathbb{Q}]=2$ and L is a Galois extension of $\mathbb{Q}$.

(d.) There is an algebraic extension K of $\mathbb{Q}$ such that $[K:\mathbb{Q}]$ is not finite

26. Which of the following integral domains are Euclidean domains?

(a.) $\mathbb{Z}\left[\sqrt{-3}\right]=\left\{a+b\sqrt{-3}:a,b\in\mathbb{Z}\right\}$

(b.) $\mathbb{Z}[x]$

(c.) $\mathbb{R}[x^2,x^3]=\left\{f=\sum_{i=0}^{n}a_i x^i\in\mathbb{R}[x]:a_1=0\right\}$

(d.) $\left(\frac{\mathbb{Z}[x]}{\langle(2,x)\rangle}\right)[y]$ Where x, y are independent variables and $\langle(2,x)\rangle$ is the ideal generated by 2 and x.

27. Let p and q be two distinct primes. Pick the correct statements from the following:

(a.) $\mathbb{Q}(\sqrt{p})$ Is isomorphic to $\mathbb{Q}(\sqrt{q})$ as fields.

(b.) $\mathbb{Q}(\sqrt{p})$ is isomorphic to $\mathbb{Q}(\sqrt{q})$ as vector spaces over $\mathbb{Q}$

(c.) $\left[\mathbb{Q}(\sqrt{p}),(\sqrt{q}):\mathbb{Q}\right]=4$

(d.) $\mathbb{Q}(\sqrt{p},\sqrt{q})=\mathbb{Q}(\sqrt{p}+\sqrt{q})$

28. Let $\omega=\cos\frac{2\pi}{10}+i\sin\frac{2\pi}{10}$.

Let $K=\mathbb{Q}(\omega^2)$ and let $L=\mathbb{Q}(\omega)$. Then

(a.) $[L:\mathbb{Q}]=10$

(b.) $[L:K]=2$

(c.) $[K:\mathbb{Q}]=4$

(d.) $L=K$

29. Let R be a ring. If R [x] is a principal ideal domain, then R is necessarily a

(a.) Unique Factorization Domain

(b.) Principal Ideal Domain

(c.) Euclidean Domain

(d.) Field

30. What is the degree of the following numbers over $\mathbb{Q}$?

(a.) $\sqrt{2}+\sqrt{3}$

(b.) $\sqrt{2}\sqrt{3}$