BHARATHIDASAN UNIVERSITY
Tiruchirappalli- 620024
Tamil Nadu, India

Programme : M. Sc. Mathematics

Course Title : ALGEBRA - I

Course Code : 24S2M05CC

UNIT - IV

RING & INTEGRAL DOMAINS

Dr. C. Durairajan
Professor
Department of Mathematics

Rings

- A ring R is a set with two binary operations $*, \Delta$ such that
  1. $(R, *)$ is an abelian group.
  2. (R, Δ) is a semigroup.
  3. Two distributive laws.

  It is denoted by $(R, *, \Delta)$.
- $(\mathbb{Z}, +, \times), (\mathbb{Z}[x], +, \times), (\mathbb{Z}_n, \oplus_n, \otimes_n) and (M_2(\mathbb{Z}, +\times)$ are rings.

24/4/21

Rings

$(R, +, \times)$

1. $(R, +)$ — abelian
2. $(R, \times)$ — semigp
3. Two distributive laws

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\quad +, \times$

$\mathbb{Z}_n \quad \oplus_n, \otimes_n$

① R

Addition identity 0

multiplicative " 1

$ab = ba, \forall a, b \in R$

R – Commutative ring

$1 \in R$, R – ring with identity

Commutative $+ 1 \in R$

R – Commutative ring with identity

$S \subseteq R$, S subring of R if S itself is a ring under the operations on R

* ideal

A subset I of R is said to be an ideal of R

if ① I – subring ② $r \in R, x \in I \Rightarrow \underline{rx \in R}$

$\underline{xr \in R}$

$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$

$\underline{\mathbb{Z}, \mathbb{Q}, \mathbb{R}}$ not ideals in $\mathbb{C}$ but they are subrings

$\frac{R}{I} = \{ r+I \mid r \in R \}$ — ring quotient ring

$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$

$\phi : R \to R'$ ring homo if

① $\phi(x+y) = \phi(x) + \phi(y)$

② $\phi(xy) = \phi(x)\phi(y)$

$\forall x, y \in R$

① $\phi(0) = 0'$, $\phi(-a) = -\phi(a)$

$\ker\phi = \{ r \in R \mid \phi(r) = 0' \}$ — ideal of R (Ex.)

① $\frac{R}{\ker\phi} \cong \phi(R) = \mathrm{Im}\,\phi$

② $\frac{I+J}{I} \cong \frac{J}{I \cap J}$

If I & J are ideals of R, prove that $I+J$ & $I \cap J$ are ideals of R

$x, y \in I \cap J$

$\Rightarrow x, y \in I$ & J

$x \pm y, xy, rx \in I$ & J

$\Rightarrow x \pm y, xy, rx \in I \cap J$

ideal

— x —

I of R

when $J \subseteq I$

$$\frac{R}{I} \cong \frac{R/J}{I/J}$$

$$\phi : \frac{R}{J} \to \frac{R}{I}$$

$r+J \mapsto r+I$ i.e. $\phi(r+J) = r+I$

clearly homo (Ex.)
+ onto

$$\ker\phi = \{ r+J \mid \phi(r+J) = I \}$$

$$= \{ r+J \mid r+I = I \text{ i.e. } r \in I \}$$

$$= \frac{I}{J}$$

$$\frac{R/J}{\ker\phi} \cong \operatorname{Im}\phi \Rightarrow \frac{R/J}{I/J} \cong \frac{R}{I}$$

$10 = 2 \times 5$

2 + 5 are divisors of 10

2 & 5 are 10-divisor

$ab = 0$

~~$0a = 0$~~ $a \neq 0, b \neq 0$

if $ab = 0 \Rightarrow a$ & b are zero-divisors

A non-zero elt a of a ring R is said to be a zero-divisor or ~~divisor of~~ zero if $\exists$ a non-zero elt $b \in R$ such that $ab = 0$

A non-zero elt a of a ring R is said to be a unit if $\exists$ a non-zero elt $b \in R \ni ab = 1$

Note: ① unit elts exists in a ring with identity

② In a ring R, zero-divisors, units may or may not exist.

i.e, a ring need not contain a zero-divisor or unit elts.

Ⓘ In $(\mathbb{Z}, +, \times)$ - ring

① 1 & -1 are units because $1 \times 1 = 1$, $-1 \times -1 = 1$

② $\mathbb{Z}$ has no zero-divisors.

II In $(n\mathbb{Z}, +, \times)$, $n > 1$,

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots \}$$

Since $n > 1 \Rightarrow 1 \notin n\mathbb{Z}$

$\Rightarrow n\mathbb{Z}$ has no unit & no zero-divisors

III In $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ - ring

$\mathbb{Z}_n$ has both zero-divisor & unit elts

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$1 \times 1 = 1$

$5 \times 5 = 1$ in $\mathbb{Z}_6$

$\underset{\neq 0}{2} \times \underset{\neq 0}{3} = 0$

$\underset{\neq 0}{4} \times \underset{\neq 0}{3} = 0$

$\therefore$ 1 & 5 are units & 2, 3, 4 are zero-divisors

Lemma Let R be a finite ring with identity. Then every non-zero elt in R is either zero-divisor or unit.

Proof. Let $R = \{a_1 = 0, a_2 = 1, a_3, \dots, a_n\}$

Let $a \neq 0$ in R. Define

$$\phi : R \to aR = \{ar \mid r \in R\}$$

by $\phi(r) = ar \quad \forall r \in R$

$a \in R$
$aR \subseteq R$
$\neq$

$2 \in \mathbb{Z}_6$
$2\mathbb{Z}_6 = \{2r \mid r \in \mathbb{Z}_6\}$
$= \{2\cdot 0, 2\cdot 1, 2\cdot 2, 2\cdot 3, 2\cdot 4, 2\cdot 5\}$
$= \{0, 2, 4, 0, 2, 4\}$
$\subseteq \mathbb{Z}_6$

ϕ may 1-1

① If ϕ is 1-1,

$x \neq y \Rightarrow \phi(x) \neq \phi(y)$

$\Rightarrow R = aR$

Since $1 \in R \Rightarrow 1 \in aR$

$\Rightarrow 1 = ar$ for some $r \neq 0$

$\Rightarrow a$ is a unit

② If ϕ is not 1-1

$\Rightarrow x \neq y \Rightarrow \phi(x) = \phi(y)$

$x - y \neq 0$

$\Rightarrow ax = ay$

$\Rightarrow ax - ay = 0$

$\Rightarrow \underline{a}(\underline{x-y}) = 0$

$\Rightarrow a$ is a zero-divisor

Corollary Every non-zero elt in $\mathbb{Z}_n$ is either a unit or a zero-divisor

Proof: $\mathbb{Z}_n$ is a ring with identity 1

By the previous Lemma

$\Rightarrow$ Every non-zero elt in $\mathbb{Z}_n$ is a unit or a zero-divisor

Note: In $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

Let $i \in \mathbb{Z}_n$ $\ni$ $(i, n) = 1$

$\Rightarrow \exists\, r, s \in \mathbb{Z}$ $\ni$ $ir + ns = 1$

$x, y \in \mathbb{Z}$, $(x, y) = d$
$\exists\, m \,\&\, n \in \mathbb{Z}$ $\ni$
$xm + yn = d$

In $\mathbb{Z}_n$

$\Rightarrow ir = 1$

$\Rightarrow iq = 1$ where $r \equiv q \pmod{n}$

$\Rightarrow q$ is the inverse of i

Every elt which is relatively prime to n is a unit

By the above Lemma, all other non-zero elts are zero-divisors

$m \in \mathbb{Z}_n$, $(m, n) = d \neq 1$

$\Rightarrow d \mid m$ & $d \mid n$

$\Rightarrow m = qd$ & $n = q_1 d$

$\frac{n}{d} < n$ since $d > 1$

$m\,\frac{n}{d} = \frac{m}{d}\,n = 0$ in $\mathbb{Z}_n$

$\Rightarrow m$ is a zero-divisor

Integral domain

A Commutative ring with identity is said to be an integral domain if it has no zero-divisor

Eg: ① $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, p is a prime are integral domains

② If n is not a prime, $\mathbb{Z}_n$ is not an integral domain

③ The set $M_{n\times n}(\mathbb{F})$ of all $n\times n$ square matrix over a field $\mathbb{F}$ is not an integral domain

- A commutative ring with unity is said to be an **integral domain** if it has no zero-divisors.
- $\mathbb{Z}, 2\mathbb{Z}, \mathbb{Z}_7$ are integral domains but $\mathbb{Z}_4$ is not because $2 \otimes_4 2 = 0$.
- Let D be an integral domain. Then there exists a field F(the field of quotients of D) that contains a subring isomorphic to D.
- A finite integral domain is a field.
- The **characteristic of a ring R** is the least positive integer n such that $na = 0$ for all $a \in R$. If such n does not exist, then the characteristic of the ring is 0.

  For example, the characteristic of $\mathbb{Z}_n$ is n but the characteristic of $\mathbb{Z}$ is 0. The characteristic of an integral domain is either 0 or a prime integer.

Continue ...

- A nonempty subset A of a ring R is an **ideal** if
  1. $a - b, ab \in A$ for all $a, b \in A$ and
  2. $ar, ra \in A$ for all $a \in A$ and $r \in R$.

Example

- The prime ideals of $\mathbb{Z}$ are $(0), (2), (3), (5), \cdots$.
  These are all maximal except (0).
- If $A = \mathbb{Z}[x]$, the polynomial ring in one variable over $\mathbb{Z}$ and p is a prime number, then $(0), (p), (x), (p, x) = \{ap + bx \mid a, b \in A\}$ are all prime ideals of A. Only maximal ideal in these is (p, x).
- Let a be an element of a ring R, then $aR = \{ar \mid r \in R\}$ is an ideal. This ideal is generated by a.

Continue . . .

1. An ideal generated by a single element of the ring is called a **Principal ideal** lf the ring. In a ring, every ideal is a principal ideal, then the ring is called the **Principal Ideal ring.** If it is an integral domain, then it is calleda **Principal Ideal domain(PID).**

Example

$\mathbb{Z}$ and $\mathbb{F}[x]$ are PID where $\mathbb{F}$ is a field.

2. Let A be a subring of R. Then the set $\{r + A \mid r \in R\}$ of cosets forms a ring under $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ iff A is an ideal of R
3. $\frac{2\mathbb{Z}}{6\mathbb{Z}} = \{0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$.

Continue . . .

- A proper ideal A of a commutative ring R is said to be a prime ideal if for $a, b \in R$, $ab \in A$ implies $a \in A$ or $b \in A$.
- A proper ideal A of a commutative ring R is said to be a maximal ideal if there is no ideal in between A and R.
- $2\mathbb{Z}, 3\mathbb{Z}$ are prime ideal but $4\mathbb{Z}, 6\mathbb{Z}$ are not because $2.2 = 4 \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$ and $3.3 = 6 \in 6\mathbb{Z}$ but $3 \notin 6\mathbb{Z}$
- Let R be a commutative ring with unity and let A be an ideal of R. Then
  1. Every maximal ideal is a prime ideal.
  2. $\frac{R}{A}$ is an integral domain iff A is a prime ideal.
  3. $\frac{R}{A}$ is an field iff A is a maximal ideal.

28/11/2021

M – maximal ideal of R

$$M \subseteq U \subseteq R$$
$$\downarrow$$
$$M \text{ or } R$$

R – Commutative ring with 1

M – maximal iff $\frac{R}{M}$ – field

A proper ideal P of R is said to be a <u>prime ideal</u> if $a, b \in R$, $ab \in P \Rightarrow a \in P$ or $b \in P$

<u>$5\mathbb{Z}$</u> is a prime ideal of $\mathbb{Z}$

$\underline{ab} \in 5\mathbb{Z} \Rightarrow ab = \underline{5n}$ for some $n \in \mathbb{Z}$

$\Rightarrow 5 \mid ab$

$\Rightarrow 5 \mid a$ or $5 \mid b$

If p is a prime, $p \mid mn \Rightarrow p \mid m$ or $p \mid n$

$\Rightarrow a = 5r$ or $b = 5s$ for some $r, s \in \mathbb{Z}$

$\Rightarrow a \in 5\mathbb{Z}$ or $b \in 5\mathbb{Z}$

$\therefore$ $5\mathbb{Z}$ is a <u>prime ideal</u> of $\mathbb{Z}$

<u>Ex.</u> Let p be a prime integer. Prove that $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$

<u>Lemma</u> Let R be a commutative ring with identity. Then P is a prime ideal of a ring R iff $\frac{R}{P}$ is an integral domain

<u>Proof:</u> Assume that P is a prime ideal of R

Since R is a commutative ring with 1

$\Rightarrow \underline{\frac{R}{P}}$ is a commutative ring with identity $1+P$

Let $a+P,\ b+P \in \frac{R}{P}$ with

$$(a+P)(b+P) = \text{zero elt in } \frac{R}{P} = P$$

$$\Rightarrow ab+P = P$$

$$\Rightarrow ab \in P$$

$a+H = b+H$

$a-b \in H$

$b-a \in H$

Since P is a prime ideal

$$\Rightarrow a \in P \text{ or } b \in P$$

$$\Rightarrow a+P = P \text{ or } b+P = P$$

i.e, $a+P = \text{zero of } \frac{R}{P}$ or $b+P = \text{zero of } \frac{R}{P}$

$\therefore \frac{R}{P}$ is an integral domain

Conversely, we assume that $\frac{R}{P}$ is an integral domain

Suppose $ab \in P$

$$\Rightarrow ab+P = P$$

$$\Rightarrow (a+P)(b+P) = P$$

Since $\frac{R}{P}$ is ID $\Rightarrow a+P = P$ or $b+P = P$

$$\Rightarrow a \in P \text{ or } b \in P$$

$\therefore P$ is a prime ideal

—— x ——

Theorem Let R be a commutative ring with identity. If M is a maximal ideal, then M is a prime ideal of R

Proof. Given M is a maximal ideal of a commutative ring R with identity

$$\Rightarrow \frac{R}{M} \text{ is a field}$$

$$\Rightarrow \frac{R}{M} \text{ is an integral domain}$$

$$\Leftrightarrow M \text{ is a prime ideal}$$

$\therefore$ In a commutative ring with identity, every maximal ideal is a prime ideal.

—— x ——

Example $\langle x \rangle$ is an ideal generated by x

Let us define

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}$$

by $\phi(a_0 + a_1 x + \cdots + a_n x^n) = a_0$ for all $a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$

① Prove that ϕ is a ring homo

(i) $\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x))$

(ii) $\phi(f(x) g(x)) = \phi(f(x)) \phi(g(x))$

② Show that ϕ is onto

Let $n \in \mathbb{Z}$. Choose $f(x) = \underline{n} + a_1 x + \cdots + a_n x^n$

By defn $\phi(f(x)) = n$

$\therefore \phi$ is onto

$\therefore \phi : \mathbb{Z}[x] \to \mathbb{Z}$ is onto homo

Consider

$$\ker \phi = \{ f(x) \in \mathbb{Z}[x] \mid \phi(f(x)) = 0 \}$$

$$= \{ \quad " \quad \mid \text{constant term of } f(x) = 0 \}$$

$$\ker \phi = \{ a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_i \in \mathbb{Z},\ n \geq 0 \}$$

$$= \{ x(a_1 + a_2 x + \cdots + a_n x^{n-1}) \mid a_i \in \mathbb{Z},\ n \geq 0 \}$$

$$= \{ x g(x) \mid g(x) \in \mathbb{Z}[x] \}$$

Since $\langle x\rangle = \{x g(x) \mid g(x) \in \mathbb{Z}[x]\}$

$\Rightarrow \ker\varphi = \langle x\rangle$

By the Fundamental Theorem of homo (1st isomorphism th)

$$\Rightarrow \frac{\mathbb{Z}[x]}{\langle x\rangle} \cong \mathbb{Z}$$

If $\langle x\rangle$ is maximal

$$\Rightarrow \frac{\mathbb{Z}[x]}{\langle x\rangle} \text{ a field, a} \Rightarrow\Leftarrow\ \mathbb{Z} \cong \frac{\mathbb{Z}[x]}{\langle x\rangle}$$

is not a field

$\therefore \langle x\rangle$ is not a maximal ideal in $\mathbb{Z}[x]$

(2) Since $\mathbb{Z}$ is an ID

$$\Rightarrow \mathbb{Z} \cong \frac{\mathbb{Z}[x]}{\langle x\rangle} \text{ is an ID}$$

$\frac{\mathbb{Z}[x]}{\langle x\rangle}$ is ID iff $\langle x\rangle$ is a prime ideal

Note that $\mathbb{Z}[x]$ is a Commutative ring with identity.
$\langle x\rangle$ is a prime ideal but not a maximal ideal

$R = 2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is a Commutative ring with no identity

$M = 4\mathbb{Z}$ is an ideal of R
$= \{0, \pm 4, \pm 8, \pm 12, \dots\}$

Clearly no ideals between M & R

$M = 4\mathbb{Z} \subseteq 2\mathbb{Z} = R$

$m\mathbb{Z} \subseteq n\mathbb{Z}$ iff $n \mid m$

$4\mathbb{Z} \subseteq r\mathbb{Z} \subseteq 2\mathbb{Z}$

$\Rightarrow r \mid 4$ & $2 \mid r$

$\Rightarrow$ $r = 1, 3, 4$ & $r = 2, 4, 6 \ldots$

$\Rightarrow$ $r = 2, 4$

$\Rightarrow r\mathbb{Z} = 2\mathbb{Z}$ or $4\mathbb{Z}$

i.e., $r\mathbb{Z} = R$ or M

$\therefore$ $4\mathbb{Z}$ is a maximal ideal of $2\mathbb{Z}$

$2 \cdot 2 = 4 \in 4\mathbb{Z} = M$

If M is a prime $(ab \in M \Rightarrow a \in M$ or $b \in M)$

$\Rightarrow 2 \in M$ or $2 \in M$

But, $2 \in M$, $\Rightarrow \Leftarrow$ $2 \notin M$

$\therefore$ M is not a prime ideal

——— x ———

D is an ID

$a, b \in D$, a divides b if $\exists\, c \in D \ni b = ac$

$2|6$ in $\mathbb{Z}$ $\Rightarrow$ $6 = 3 \times 2$

$2|3$ in $\mathbb{Z}$ $\Rightarrow$ $\exists\, c \in \mathbb{Z} \ni 3 = 2c$ not possible in $\mathbb{Z}$

$\frac{1}{c}\frac{3}{4}$

$2|3$ in $\mathbb{Q}$ $\Rightarrow$ $3 = 2 \times \frac{3}{2}$ ✓

$c = \frac{3}{2} \in \mathbb{Q}$

Let D be an integral domain. Let $a, b \in D$

If there exists $c \in D$ such that $a = bc$, then

b divides a or b is a factor of a

Every unit is a divisor of 1 or divides 1.

Let u be an unit in D

$\Rightarrow u^{-1}$ exists

$\Rightarrow u \cdot u^{-1} = 1$

$\Rightarrow u$ is a factor of 1 or u divides 1.

—— x ——

Two elts a and b are said to be an associate in D if there exists a unit $u \in D$ such that $a = ub$ or $b = au$.

For example, $D = \mathbb{Z}$

$-2, 2$ are associate because ± 1 are units of $\mathbb{Z}$

$2 = -1(-2)$ or $-2 = (-1) \times 2$

$n, -n$ are associate

—— x ——

$6 = 2 \times 3$

$= \cancel{(-2) \times (-3)}$

$= \cancel{3 \times 2}$

$= \cancel{(-3) \times (-2)}$

Fundamental theorem of Arithmetic

Every integer can be written as a product of prime powers in a unique way except its associates and order

A non-zero, non-unit elt a in an integral domain D is said to be an irreducible elt. if it can be written as a product of two non-unit elts. i.e, $a = \underline{b}\,\underline{c} \Rightarrow$ either b is unit or c is unit.

7 is irr. elt in $\mathbb{Z}$

$$7 = \underline{(-1)}(-7)$$

$\therefore$ All prime integers in $\mathbb{Z}$ are irreducible elts

—— x ——

REFERENCES

- M. Artin, **Algebra**, Prentice Hall of India, New Delhi, 1994.
- David S. Dummit and Richard M. Foote,**Abstract Algebra**, 2nd Edition, Wiley Student Edition, 2008.
- I. N. Herstein, **Topics in Algebra**, John Wiley, 2nd Edition, 1975.
- Joseph Gallian, **Contemporary Abstract Algebra** , 9th Edition
- C. Lanski, **Concepts in Abstract Algebra**, AMS Indian edition, 2010.
- Serge Lang, **Algebra** - Revised third edition, Springer, Verlag - 2002.
- R. Solomon, **Abstract Algebra**, AMS Indian edition, 2010.
- John B. Fraleigh, **A First course in Abstract Algebra**, Narosa Publishing House, 2003.