27/10

RING THEORY

Integers:

$(\mathbb{Z}, +, \cdot)$

- $(\mathbb{Z}, +)$ forms an Abelian group
- $\cdot$ is associative

  $\Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$

- Distributive properties hold

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

* $\mathbb{R}[x] = \{ a_0 + a_1 x + \dots + a_n x^n \mid a_i \in \mathbb{R} \}$

Consider $(\mathbb{R}[x], +, \cdot)$

$$a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$
$$b(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m$$

WLOG, assume $m \leq n$.
and define $b_i = 0 \quad \forall i > m$

$$a(x) + b(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$a(x) \cdot b(x) = \sum_{i=0}^{m+n} c_i x^i \quad , \text{ where}$$

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$
$$\vdots$$
$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Associativity of addition in $\mathbb{R}[x]$ follows from associativity of $\mathbb{R}$.

Identity $\rightarrow$ Additive identity is zero polynomial

Inverse $\rightarrow$ Additive inverse is negative of given polynomial

DEFINITION

Let R be a non-empty set

Then R is called a ring if there are two binary operations

$$+ : R \times R \to R \qquad \cdot : R \times R \to R$$
$$(a, b) \mapsto a+b \qquad (a, b) \mapsto (a \cdot b)$$

satisfying the following axioms

1. $(\mathbb{R}, +)$ is an abelian group
2. $\cdot$ is associative, i.e, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in R$
3. Distributive properties

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c \qquad \forall a, b, c \in \mathbb{R}$$

. It need not have multiplicative identity!

$(2\mathbb{Z}, +, \cdot)$ is a ring without multiplicative identity

* Let R be a ring, then R is called

(i) Commutative if $a \cdot b = b \cdot a \quad \forall a, b \in R$

(ii) with identity if $\exists\, 1 \in R$ such that

$$a \cdot 1 = 1 \cdot a = a$$

* An element $a \in R$ is said to be a unit if there exists $b \in R$ such that $ab = ba = 1$

Units in $(\mathbb{Z}, +, \cdot)$ are ± 1

Units in $(\mathbb{R}[x], +, \cdot)$ are non-zero constants

* A ring R is called a division ring (or) skew-field if all non-zero elements are units.

* A commutative division ring is called a field.

Example :- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

→ A field R satisfies the following cancellation property, if $a \neq 0$ and $b, c \in R$

then $ab = ac \Rightarrow b = c$

→ A commutative ring R with identity is said to be an integral domain if

For $a \neq 0$, $b, c \in R$, we have $ab = ac \Rightarrow b = c$

[Doesn't follow from inverse!]

(Alternative)

A commutative ring with identity is said to be an integral domain if $ab = 0 \Rightarrow a = 0$ (or) $b = 0$

If $ab = 0$, we have

$ab = 0 = a \cdot 0$

$\Rightarrow$ If $a = 0$, we are done!

$\Rightarrow$ Else, we have $b = 0$

Lemma

If R is a ring, then $a \cdot 0 = 0$

(Proof)

$a \cdot 0 = a \cdot (0 + 0)$

$a \cdot 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow a \cdot 0 = 0$

Lemma

$a(-b) = (-a)b = ab$

(Proof)

It is enough to show that $a(-b) = -ab$

$a(-b) + ab = 0$

$\Rightarrow a(b + (-b)) = 0$

$\Rightarrow a \cdot 0 = 0$ [True!]

Lemma

Let R be a ring with identity
Suppose 1 and $1'$ are identity elements of R. Then $1 = 1'$

(Proof)

$1 = 1 \cdot 1'$
$1' = 1 \cdot 1'$

$\Rightarrow$ $1 = 1'$

Lemma

Let R be a ring with 1. If $a \in R$ is a unit, then 'a' has a unique inverse

(Proof)

$ab = ba = 1$ (b, c be inverses of a)
$ac = ca = 1$

$b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c$

$\Rightarrow$ $b = c$

Proposition

(i) A field is an integral domain.
(ii) A finite integral domain is a field.

(Proof)

(i) In a field, if $ab = 0$, and $a \neq 0$, multiply with inverse of a.

(ii) Let $R = \{a_1, a_2, \ldots, a_n\}$ be a finite integral domain

Let $a \in R$ be a non-zero element
Define $\varphi : R \longrightarrow R$
$a_i \longmapsto a a_i$

one-one :- $\varphi(a_i) = \varphi(a_j) \Rightarrow a a_i = a a_j$
From properties of integral domain,
$a a_i = a a_j$ and $a \neq 0 \Rightarrow a_i = a_j$

φ is injective (and trivially surjective!)

$\Rightarrow \exists\, a_i \in R$ such that $a\, a_i = 1$

$\Rightarrow a$ is a unit

From division ring and commutativity, we have that R is a field.

Examples

(i) $\mathbb{Z}$

(ii) $\mathbb{Z}/_{n\mathbb{Z}}$

well defined : $\begin{matrix} \bar{a} = \bar{x} \\ \bar{b} = \bar{d} \end{matrix} \Rightarrow \overline{ab} = \overline{xd}$?

$n \mid \bar{a} - \bar{x}$

$n \mid \bar{b} - \bar{d}$

$$ab - xd = ab - xb + xb - xd$$
$$= (a-x)b + x(b-d)$$

$\Rightarrow n \mid ab - xd$

- $\bar{a}(\bar{b}\,\bar{c}) = (\bar{a}\,\bar{b})\,\bar{c}$

$\Leftrightarrow \bar{a}(\overline{bc}) = (\overline{ab})\,\bar{c}$

$\Leftrightarrow \overline{a(bc)} = \overline{(ab)c}$

$\Leftrightarrow a(bc) = (ab)c \rightarrow$ True!

- It is commutative because

$\bar{a}\,\bar{b} = \bar{b}\,\bar{a}$

$\Leftrightarrow \overline{ab} = \overline{ba}$

$\Leftrightarrow ab = ba \rightarrow$ True!

- Distributive

$\bar{a}(\bar{b} + \bar{c}) = \bar{a}\,\bar{b} + \bar{a}\,\bar{c}$

$\Leftrightarrow \bar{a}(\overline{b+c}) = \overline{ab} + \overline{ac}$

$\Leftrightarrow \overline{a(b+c)} = \overline{ab+ac}$

$\Leftrightarrow a(b+c) = ab + ac \rightarrow$ True!

$\Rightarrow (\mathbb{Z}/_{n\mathbb{Z}})$ is a commutative ring with $\bar{1}$

Proposition

$\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\Leftrightarrow$ n is prime

(Proof)

($\Rightarrow$) Suppose n is not a prime

$\Rightarrow$ $n = d_1 d_2$ for some $1 < d_1, d_2 < n$

$\Rightarrow$ $\bar{d_1}\,\bar{d_2} = \bar{n} = \bar{0}$

$\bar{d_1} \neq \bar{0}$ because $\bar{d_1} = \bar{0} \Rightarrow n \mid d_1$ ($\Rightarrow\Leftarrow$) $(1 < d_1 < n)$

($\Leftarrow$) Let n be a prime and suppose

$\bar{a} \cdot \bar{b} = \bar{0}$

$\Rightarrow$ $n \mid ab$ $\Rightarrow$ $n \mid a$ (or) $n \mid b$

$\Rightarrow$ $\bar{a} = \bar{0}$ (or) $\bar{b} = \bar{0}$

$\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ is integral domain

Definition

Let R be a commutative ring with 1

Define $U(R) = \{ a \in R \mid a \text{ is a unit} \}$

Then $(U(R), \cdot)$ is a group

(Proof)

If $a, b \in U(R)$, $\exists\ c, d$ such that $ac = 1 = bd$

$\Rightarrow$ $(ab)(cd) = (ac)(bd) = 1 \cdot 1 = 1$

commutative !

$\Rightarrow$ $ab \in U(R)$

$\Rightarrow$ $U(\mathbb{Z}/n\mathbb{Z}) = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1 \}$

If $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{b}\,\bar{d} = \bar{1}$

$(\Rightarrow)$ $n \mid bd - 1$ $(\Leftrightarrow)$ $bd = 1 + kn$ for some k

$\Leftrightarrow$ $bd - kn = 1$

$\Leftrightarrow$ $\gcd(b, n) = 1$

$M_n(R)$

Let R be a ring with 1

$$M_n(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & \vdots \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \;\middle|\; a_{ij} \in R \right\}$$

$A = (a_{ij})_{i,j=1}^{n}$ $\qquad$ $A+B = (a_{ij} + b_{ij})_{i,j=1}^{n}$

$B = (b_{ij})_{i,j=1}^{n}$ $\qquad$ $AB = (c_{ij})_{i,j=1}^{n}$ where

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

$M_n(R)$ is a ring

It is not commutative !

Ex :-

$$\left.\begin{aligned} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}\right\} \text{ Not equal !}$$

Let R be a ring

$$R[x] = \{ a_0 + a_1 x + \cdots + a_n x^n : a_i \in R \}$$

Exercises

(i) $R[x]$ is a ring with identity

(ii) R is an integral domain $\Rightarrow$ $R[x]$ is an integral domain

* Given $f(x) \in R[x]$, we define

$$\deg f(x) = \begin{cases} n, & \text{where } n = \max\{k \mid a_k \neq 0\} \text{ and } f(x) \neq 0 \\ -\infty, & \text{if } f(x) = 0 \end{cases}$$

(iii) If R is an integral domain, then

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$$