Ring

22/12/23

① $(\mathbb{Z}, +, \cdot) \longrightarrow$ is a ring

(i) $(\mathbb{Z}, +)$ is a commutative group

(ii) $(\mathbb{Z}, \cdot)$ is a semigroup

(iii) $a(b+c) = ab + ac$

and $(a+b)c = ac + bc \quad \forall\, a, b, c \in \mathbb{Z}$

② let $R \neq \phi$.

$R \times R \longrightarrow R \qquad\qquad R \times R \longrightarrow R$

$(a, b) \longrightarrow a+b \qquad\qquad (a, b) \longrightarrow a \cdot b$

then $(R, +, \cdot) \longrightarrow$ is a ring.

(i) $(R, +)$ is a commutative group.

(ii) $(R, \cdot)$ is a semigroup

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

$(a+b) \cdot c = ac + bc \quad \forall\, a, b, c \in R$

Similarly rational no., real no, complex no.

$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings.

Commutative ring

$(R, +, \cdot)$ is a commutative ring if

$a \cdot b = b \cdot a$ for all $a, b \in R$.

A ring R may or may not have an identity element with respect to multiplication.

if $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$.

then 1_R is the identity element wrto multiplication.

(a) Prove that $(R, +)$ is a commutative group such that $(R, +, \cdot)$ ~~but~~ is a ring with identity 1_R

Now, consider
$a + b$

$= \cancel{a \times 1R}$
$(a+b)(1_R + 1_R)$ (by left distributive property)

$\cancel{= a \cdot 1R + a 1R}$

$= a(1_R + 1_R) + b(1_R + 1_R)$

$= a1_R + a1_R + b1_R + b1_R$

$= a + a + b + b$

Again
$(a+b)(1_R + 1_R)$

$\Rightarrow (a+b)1_R + (a+b)1_R$ (by right dist. property)

$= a1_R + b1_R + a1_R + b1_R$

$= a + b + a + b$

$\Rightarrow a + a + b + b = a + b + a + b$

By cancellation property, $a * b = b * c \Rightarrow a = c$

$\Rightarrow \cancel{a} + a + b + \cancel{b} = \cancel{a} + b + a + \cancel{b}$

$\Rightarrow a + b = b + a$ (proved).

$\therefore (R, +)$ is a commutative group.

Finite commutative rings.

① $(\mathbb{Z}_n, +, \cdot)$

$[a] + [b] = [a+b]$

$[a] \cdot [b] = [a \cdot b]$ for all ~~a,b~~ $[a], [b] \in \mathbb{Z}_n$

Non-commutative rings.

$(M_{n\times n}(\mathbb{R}), +, \cdot)$ square matrices only

but if $A, B \in M$

$A\cdot B \neq B\cdot A$ matrix multiplication is not commutative

$\therefore (M_{n\times n}(\mathbb{R}), +, \cdot)$ is a non-commutative ring.

finite non-commutative ring:

~~$(M_{2\times 2}(\mathbb{Z}_2)$~~

$(M_{2\times 2}(\mathbb{Z}_2), +, \cdot)$ has 16 elements.

$2^{(2^2)} = 2^4$

Integral Domain

Divisor of zero

a, b such that $a \neq 0$ $b \neq 0$ and $a, b \in R$ in $(R, +, \cdot)$ ring

and $a\cdot b = b\cdot a = 0$

then a and b are zero divisors of each other

eg $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$

$[2][2] = [4] = [0]$

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

$[2]\cdot[3] = [6] = [0]$

Defn

A commutative ring with identity is called integral domain if R has no divisor of zero.

eg, $(\mathbb{Z}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$

$(\mathbb{Z}_6, +, \cdot)$, $(\mathbb{Z}_4, +, \cdot)$ or $(\mathbb{Z}_n, +, \cdot)$ are not integral domain (it is integral domain iff n is prime)

Division ring (Skew field)

Let $(R, +, \cdot)$ be a ring with identity

$a, b \in R$ and $a \neq 0_R$

$b \neq 0_R$

and $a \cdot b = b \cdot a = 1_R$.

then b = inverse of a.

$\therefore$ $(\mathbb{Z}, +, \cdot)$ is not a division ring,

but $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are skew fields / division rings.

A ring 'R' with identity 1_R is called a division ring / skew field if every non-zero element has an multiplicative inverse.

Field

A commutative ring with identity 1_R is called a field, if every non-zero element has an multiplicative inverse.

eg. $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

as $(\mathbb{R}, +)$ is a commutative group and $(\mathbb{R} - \{0\}, \cdot)$ is a commutative group.

(*)(*) Every field is an integer domain but ~~inverse~~ converse is not true. eg- $(\mathbb{Z}, +, \cdot)$ is integer domain, but not a field.

(*) Every field is a divison ring but converse is not true. eg- $R = \left\{ \begin{pmatrix} u & u \\ -\bar{u} & \bar{u} \end{pmatrix} u \in \mathbb{C} \right\}$

$= \left\{ \begin{pmatrix} a+ib & c+id \\ -(a-ib) & a-ib \end{pmatrix} a, b, c, d \in \mathbb{R} \right\}$

is a divison ring but not a field.

A division ring ~~[illegible]~~ is not a integral domain.

Ring of continuous functions.

$f: \mathbb{R} \longrightarrow \mathbb{R}$

$(f+g)(x) = f(x) + g(x)$

$fg(x) = f(g(x))$] not a ring.

near ring

$f: R \longrightarrow R$

$(f+g)(x) = f(x) + g(x)$

$fg(x) = f(x) \cdot g(x)$] is a ring.

$C[0,1] = \{ f : [0,1] \to \mathbb{R}$ is a continuous function $\}$ $\longrightarrow$ is a ring.

or $C[a,b] = \{ f : [a,b] \to \mathbb{R}$ is a ~~commo~~ continuous function $\}$ $\to$ is a ring.

but $f: R \to R$

$\mathcal{B} = \{ f : [a,b] \to \mathbb{R}$ is a differentiable function $\}$ $\to$ is a ring.

Are these integral domains?

$C[0,1]$

$f : [0,1] \to \mathbb{R}$

$$f(x) = \begin{cases} \frac{1}{2} - x, & 0 \leq x \leq \frac{1}{2} \\ 0 & \frac{1}{2} \leq x \leq 1 \end{cases}$$

$g : [0,1] \to \mathbb{R}$

$$g(x) = \begin{cases} 0 & 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2} & \frac{1}{2} \leq x \leq 1 \end{cases}$$

$f \cdot g =$ ~~f(x)g(x)~~ $f(x) \cdot g(x)$

this product will always be zero

$\therefore$ contains divisor of zero.

$\therefore$ $C[0,1]$ is not a ~~divisor of zero~~ integral domain

$D[0,1]$

$f : [0,1] \to \mathbb{R}$

$$f(x) = \begin{cases} \left(\frac{1}{2} - x\right)^2 & 0 \leq x \leq \frac{1}{2} \\ 0 & \frac{1}{2} \leq x \leq 1 \end{cases}$$

$g(x)\ [0,1] \to \mathbb{R}$

$$g(x) = \begin{cases} 0 & 0 \leq x \leq \frac{1}{2} \\ \left(x - \frac{1}{2}\right)^2 & \frac{1}{2} \leq x \leq 1 \end{cases}$$

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

this product will always be zero

$\therefore$ $D[0,1]$ is not a ~~divisor of zero~~ integral domain