

The Rings

Definition: A ring is an ordered triple $(R, +, \cdot)$ where R is a nonempty set and $+$, \cdot are binary operation on R , such that

$(R, +)$ is an abelian group. .1

(a. c) \cdot is associative. (b. c) $\forall a, b, c \in R$, .2

a. $(b + c) \cdot a = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in R$. .3

(1) Mean: (a) $(a + b) + c = a + (b + c), \forall a, b, c \in R$,

(b) $\exists 0 \in R$ such that $a + 0 = 0 + a = a$,

(c) $\forall a \in R$ there exists $(-a)$ such that $a + (-a) = (-a) + a = 0$,

(d) $a + b = b + a, \forall a, b \in R$,

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

(1) $(\mathbb{Z}, +)$ is abelian group.

(2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

$\therefore (\mathbb{Z}, +, \cdot)$ is a ring.

Example: $(\mathbb{Q}, +, \cdot)$ is a ring.

Definition: Let $(R, +, \cdot)$ be a ring, then R is commutative if $a \cdot b = b \cdot a, \forall a, b \in R$.

Definition: Let $(R, +, \cdot)$ be a ring, then R is said to have identity if there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a, \forall a \in R$ and a is invertible (unit) if there exists $b \in R$ such that $a \cdot b = b \cdot a = 1$.

(1) $(\mathbb{Z}, +, \cdot)$ is a ring with identity, commutative, 1 and -1 are only invertible elements.

(2) $(\mathbb{Q}, +, \cdot)$ is a ring with identity comm., and every element in \mathbb{Q} has inverse except 0.

(3) $(3\mathbb{Z}, +, \cdot)$ is a comm. with no identity.

(4) $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \dots \right)$ is a ring not comm. with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Example: $(\mathcal{P}(X), \Delta, \cap)$ is a ring?

$(\mathcal{P}(A), \cap)$ is a belian group, comm. $A \cap X = A$ (identity) no inverse.

$\forall A, B, C \text{ in } X$

$$A \cap (B \cap C) = (A \cap B) \Delta (A \cap C)$$

$$\begin{aligned} &= A \cap (B - C) \cup (A \cap (C - B)) \\ &= [(A \cap B) - (A \cap C)] \cup [(A \cap C) - (A \cap B)] \\ &= (A \cap B) \Delta (A \cap C) \end{aligned}$$

Remark: Let R be a ring such that $R \neq \{0\}$ is a ring with identity $1 \Rightarrow 1 \neq 0$.

Proof: Suppose $1 = 0$, let $a \neq 0 \in R$, $a = a \cdot 1 = a \cdot 0 = 0C$!

$\therefore 1 \neq 0$.

Definition: Let R be commutative ring. An element $a \in R$ is called zero divisor if $a \neq 0$ and there exists $b \in R, b \neq 0$ with $a \cdot b = 0$.

Example: $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Solution: $\left. \begin{matrix} \bar{2} \cdot \bar{3} = \bar{0} \\ \bar{3} \cdot \bar{4} = \bar{0} \end{matrix} \right\} \bar{0} = \bar{2}, \bar{3}, \bar{4}$ are zero divisors of Z_6

Example: $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ has no zero divisor.

Example: $(\mathbb{Z}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot)$ has no zero divisor.

H. W: $(\mathcal{P}(X), \Delta, \cap)$ has zero divisor or not?

Lemma: Let R be a ring then

$$(1) a \cdot 0 = 0 \cdot a = 0$$

$$(2) (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$$

$$(3) (-a)(-b) = a \cdot b$$

$$(4) a(b - c) = ab - ac \forall a, b, c \in R.$$

$$\text{Proof(1): } a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 = 0, 0 = a \cdot 0$$

$$\text{Proof(2): } 0 = 0 \cdot b = (a + (-a))b = ab + (-a)b$$

$$\text{Proof(3): } (-a)(-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$$

$$\text{Proof(4): } a \cdot (b - c) = a \cdot [b + (-c)]$$

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

$$= a \cdot b - a \cdot c$$

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

Definition: A commutative ring with identity is called integral domain if it has no zero divisors.

Example: $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{Z}_p, +_p, \cdot_p)$ where p is prime are integral domains.

Lemma: Let R be commutative ring with identity, R is integral domain if and only if $a \cdot b = a \cdot c$ with $a \neq 0$ then $b = c, b \cdot a = c \cdot a$.

Proof: \Rightarrow) suppose $a \cdot b = a \cdot c, a \neq 0$

$$(a \cdot b) - (a \cdot c) = 0 \text{ [associative]}$$

$$a \cdot (b - c) = 0 \text{ [R is integral domain]}$$

R has no zero divisor and $a \neq 0$ •

$$\therefore b - c = 0, b = c.$$

$$\Leftrightarrow \text{let } a \in R, a \neq 0$$

$a \cdot b = 0$ and we have $0 \cdot a = a \cdot 0 = 0, a \cdot b = a \cdot 0$

$\therefore b = 0$

Definition: Let $(R, +, \cdot)$ bearing $\emptyset = S \subseteq R$, then $(S, +, \cdot)$ is called subring if $(S, +, \cdot)$ is a ring itself.

Example: $(2\mathbb{Z}, +, \cdot)$ subring of $(\mathbb{Z}, +, \cdot)$

Definition: Let $(R, +, \cdot)$ bearing $\emptyset \neq S \subset R$, then $(S, +, \cdot)$ is subring if:

(1) $a - b \in S \forall a, b \in S$.

(2) $a \cdot b \in S \forall a, b \in S$.

Example:

\mathbb{Z} subring of $(\mathbb{Q}, +, \cdot)$.

\mathbb{Q} subring of $(\mathbb{R}, +, \cdot)$.

\mathbb{R} subring of $(\mathbb{C}, +, \cdot)$.

$(\{\bar{0}, \bar{2}, \bar{4}\}, +, \cdot)$ is subring of \mathbb{Z}_6

$(\{\bar{0}, \bar{3}\}, +, \cdot)$ is subring of \mathbb{Z}_6 .

Example: Let $(R, +, \cdot)$ bearing $R \times R = \{(a, b), a, b \in R\}$

$$(a, b) + (c, d) = (a + c, b + d), (a, b) \cdot (c, d) = (ac, bd)$$

Proof: (1) $(R \times R, +)$ is abelian group

$$(2) (a, b) \cdot [(c, d) + (e, f)] = (a, b) \cdot (c + e, d + f)$$

$$= (a(c + e), b(d + f))$$

$$= (ac + ae, bd + bf) = (ac, bd) + (ae, bf)$$

$$= (a, b) \cdot (c, d) + (a, b) \cdot (e, f)$$

identity = (1,1)

$$(a, b) \cdot (1,1) = (a \cdot 1, b \cdot 1) = (a, b)$$

(3) $S = R \times \{e\} = \{(a, 0), a \in R\}$ S is subring of $R \times R$.

Proof: $S \neq \emptyset$ since $(0,0) \in S$

$$(a, 0) - (b, 0) = (a - b, 0) \in S$$

$$(a, 0), (b, 0) = (ab, 0) \in S$$

Identity = $(1,0)$

Definition: Let R be a ring the center of a ring R is denoted by $\text{Cent } R$ is the set $\text{Cent } R = \{x \in R \text{ such that } x \cdot r = r \cdot x\}$.

Lemma: $\text{Cent } R$ is a subring of R .

Proof: $\text{Cent } R \neq \emptyset$ [$0 \in \text{Cent } R, 0 \cdot a = a \cdot 0 = 0$] let $a, b \in \text{Cent } R$

$\Rightarrow ax = xa, bx = xb$

$$x(a - b) = xa - xb = ax - bx = (a - b)x \text{ [since } a, b \in \text{Cent } R \text{]}$$

$$x(a \cdot b) = xa \cdot b = ax \cdot b = a \cdot bx$$

$\therefore \text{Cent } R$ is subring.

Remark:

(1) Let R be a ring, n positive integer,

$$na = \underbrace{a + a + \dots + a}_{n \text{ times}}, a^n = \underbrace{a \cdot a \cdot a \cdot a}_{n \text{ times}}$$

(2) if R is a ring with 1 and a is invertible

$$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \dots a^{-1}}_{n \text{ times}} a^0 = 1.$$

Remark: Let R be a ring and $n, m \in \mathbb{Z}$

(1) $(n + m)a = na + ma$.

$$(2) n(a - b) = na - nb.$$

$$(3) (nm)a = n(ma) = m(na).$$

$$\begin{aligned} \text{Proof(1): } (n + m)a &= \underbrace{a + a + \cdots + a}_{(n+m) \text{ times}} = \underbrace{a + a + \cdots + a}_{n \text{ times}} + \underbrace{a + a + \cdots + a}_{m \text{ times}} \\ &= na + ma \end{aligned}$$

$$\begin{aligned} \text{Proof(2): } n(a - b) &= \underbrace{(a - b) + (a - b) + \cdots + (a - b)}_{n \text{ times}} \\ &= \underbrace{a + a + \cdots + a}_{n \text{ times}} - \underbrace{b - b - \cdots - b}_{n \text{ times}} \\ &= na - nb \end{aligned}$$

Definition: Let $(R, +, \cdot)$ be a ring, if there exists a positive integer n such that $na = 0, \forall a \in R$, then the smallest positive integer with this property is called characteristic of R . If no such positive integer exists we say R has characteristic zero, we denote the characteristic of R by $\text{Char } R$.

Example: $\text{Char } \mathbb{Z} = 0, \text{Char } \mathbb{Q} = 0, \text{Char } \mathbb{Z}_6 = 6, \text{Char } \mathbb{Z}_4 = 4, \text{Char } \mathbb{Z}_n = n$.

$$\begin{aligned} &(\mathbb{Z}_2, \Delta, \cap), \text{Char } \mathbb{Z}_2 = 2 \\ &2A = A \Delta A = A \cup A - A \cap A = \emptyset \end{aligned}$$

Theorem: Let R be a ring with identity then $\text{Char } R = n > 0$ if and only if n is the smallest positive integer such that $n \cdot 1 = 0$.

Proof: \Rightarrow $\text{Char } R = n > 0$, then $na = 0$, then $n \cdot 1 = 0$ suppose \exists positive integer m such that $m < n, m \cdot 1 = 0$ and let $a \in R$

$$\begin{aligned} ma &= \underbrace{a + a + \cdots + a}_{m \text{ times}} = \underbrace{a \cdot 1 + a \cdot 1 + \cdots + a \cdot 1}_{m \text{ times}} \\ &= (m \cdot 1) \cdot a = 0 \cdot a = 0 \end{aligned}$$