Chapter - 7 Introduction to Rings

① Defⁿ (Ring): A ring R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

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

(ii) $\times$ (multiplication) is associative : i.e.

$$a \times (b \times c) = (a \times b) \times c \quad \forall\, a, b, c \in R$$

(iii) Left and right distributive laws holds in R : i.e. $\forall\, a, b, c \in R$

$$(a+b) \times c = (a \times c) + (b \times c) \quad \text{and}$$

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

② Defⁿ (Commutative Ring):

A ring R is said to be commutative if multiplication is commutative.

③ The ring R is commutative if multiplication is commutative.

③ The ring R is said to have an identity if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \quad \forall\, a \in R$$

Que: Write an example of a commutative ring with identity.

Sol^n (i) The ring of integers $\mathbb{Z}$ under the usual operations of addition and multiplication is a commutative ring with identity (the integer 1).

(ii) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex number $\mathbb{C}$ are commutative rings with identity.

(iii) The quotient group $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (the element $\bar{1}$) under of operations of addition and multiplication of residue classes (frequently referred to as "modular arithmetic".

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

Que: Prove that $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ is a ring.

Sol^n

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{n-1}\}$$

Addition modulo n, $\quad a \oplus_n b = r$

r is remainder when $a+b$ is divided by n.

$$a \otimes_n b = r$$

For this we can consider $\mathbb{Z}_6$ with $\oplus_6$ and $\otimes_6$.

A) To prove $\mathbb{Z}_6$ is an abelian group under addition $\oplus_6$.

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

$\oplus_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	0	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

(i) Associative: For any $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_6$

$$(\bar{a} \oplus \bar{b}) \oplus \bar{c} = \bar{a} \oplus (\bar{b} \oplus \bar{c})$$

(ii) <u>Existence of identity:</u> For any $\bar{a} \in \mathbb{Z}_6$, $\exists\ \bar{0} \in \mathbb{Z}_6$ such that

$$\bar{a} \oplus \bar{0} = \bar{a} = \bar{0} \oplus \bar{a}$$

(iii) <u>Existence of inverse:</u> For any $\bar{a} \in \mathbb{Z}_6$,

inverse of $\bar{a}$ is $\bar{6} - \bar{a}$, and the inverse of $\bar{0}$ is $\bar{0}$.

i.e. $\quad inv_+ \bar{0} = \bar{0}$

when $\bar{a} \neq \bar{0}$, $\quad inv\ \bar{a} = \bar{6} - \bar{a}$

(iv) <u>Commutative law:</u> For all $\bar{a}, \bar{b} \in \mathbb{Z}_6$

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

Hence $(\mathbb{Z}_6, \oplus_6)$ is an abelian group.

B) To prove $\otimes_6$ is associative.

For all $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_6$

$(\bar{a} \otimes \bar{b}) \otimes c$

$= \bar{a} \otimes (\bar{b} \otimes \bar{c})$

$\otimes_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

c) <u>Commutative:</u> $\forall\ \bar{a}, \bar{b} \in \mathbb{Z}_6$

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

D) <u>Distributive law:</u> $\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_6$

(i) $(\bar{a} \oplus \bar{b}) \otimes c = (\bar{a} \otimes \bar{c}) \oplus (\bar{b} \otimes \bar{c})$ and

$\bar{a} \otimes (\bar{b} \oplus \bar{c}) = (\bar{a} \otimes \bar{b}) \oplus (\bar{a} \otimes \bar{c})$

Hence $(\mathbb{Z}_6, \oplus_6, \otimes_6)$ is a ~~ring~~ commutative ring.

Similarly, we can show that $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ is a ring.

<u>Alternatively</u>: $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ is a commutative ring.

A) $\mathbb{Z}_n$ is an abelian group under addition.

(i) <u>Associative</u>: $\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$

$$(\bar{a} \oplus \bar{b}) \oplus \bar{c} = \bar{a} \oplus (\bar{b} \oplus \bar{c})$$

(ii) <u>Existence of ~~inverse~~ identity</u>: for all $\bar{a} \in \mathbb{Z}_n$ $\exists\ \bar{0} \in \mathbb{Z}_n$ such that

$$\bar{a} \oplus \bar{0} = \bar{a} = \bar{0} \oplus \bar{a}$$

(iii) <u>Existence of inverse</u>: $inv_+ \, 0 = 0$ and when $\bar{a} \neq \bar{0}$, $inv_+ \, \bar{a} = \bar{n} - \bar{a}$

(iv) <u>Commutative law</u>: $\forall\ \bar{a}, \bar{b} \in \mathbb{Z}_n$

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

Hence $(\mathbb{Z}_n, \oplus_n)$ is an abelian group.

B) Multiplication is associative.

$\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$

$$(\bar{a} \otimes \bar{b}) \otimes \bar{c} = \bar{a} \otimes (\bar{b} \otimes \bar{c})$$

c) Multiplication is commutative:

$\forall\ \bar{a}, \bar{b} \in \mathbb{Z}_n$

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

D) Distributive law: $\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$

$$(\bar{a} \oplus \bar{b}) \otimes \bar{c} = (\bar{a} \otimes \bar{c}) \oplus (\bar{b} \otimes \bar{c})$$

and

$$\bar{a} \otimes (\bar{b} \oplus \bar{c}) = (\bar{a} \otimes \bar{b}) \oplus (\bar{a} \otimes \bar{c})$$

Hence $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ is a commutative ring.