3. Rings and Fields

3.1. Ring.

A non-empty set R is said to form a *ring* with respect to two binary compositions, addition $(+)$ and multiplication $(.)$ defined on it, if the following conditions are satisfied.

(1) $(R,+)$ is a commutative group,

(2) $(R,.)$ is a semigroup and

(3) for any three elements $a,b,c \in R$

the left distributive law $a.(b+c) = a.b + a.c$ and

the right distributive law $(b+c).a = b.a + c.a$ both hold.

Therefore a non-empty set R is a ring with respect to two binary compositions $+$ and $.$, if

(i) $a+b \in R$ for all a,b in R,

(ii) $a+(b+c) = (a+b)+c$ for all a,b,c in R,

(iii) there exists an element, denoted by 0, in R such that $a+0 = a$ for all a in R,

(iv) for each element a in R there exists an element, denoted by $-a$, in R such that $a+(-a) = 0$,

(v) $a+b = b+a$ for all a,b in R,

(vi) $a.b \in R$ for all a,b in R,

(vii) $a.(b.c) = (a.b).c$ for all a,b,c in R,

(viii) $a.(b+c) = a.b + a.c$ and

$(b+c).a = b.a + c.a$ for all a,b,c in R.

The ring is denoted by $(R,+,.)$, or by R when no confusion regarding the underlying binary compositions arises.

R is said to be a *commutative ring* if the multiplication is commutative. In this case, the two distributive laws state the same thing and it is said to be *the* distributive law.

The additive identity element in R is called the *zero element* in R. An element e in R is said to be a *multiplicative identity* in R if $e.a = a.e = a$ for all a in R. R may or may not contain a multiplicative identity. If, however, such an element exists in R, it is unique and it is said to be *the unity* in R and R is called a ring *with unity*. The unity is denoted by I.

Theorem 3.1.1. If I be a multiplicative identity in a ring R then I is unique.

Proof. If possible, let there be two multiplicative identities I, I'.

Then $I.a = a.I = a$ and $I'.a = a.I' = a$ for all a in R.

Now $I.I' = I'$, by the property of I

$= I$, by the property of I'.

Therefore $I = I'$ and this proves that I is unique.

Examples.

1. $(\mathbb{Z}, +)$ is a commutative group and $(\mathbb{Z}, .)$ is a commutative monoid, 1 being the identity element. The distributive law holds. Therefore $(\mathbb{Z}, +, .)$ is a commutative ring with unity.

$(\mathbb{Q}, +, .)$ is a commutative ring with unity.

$(\mathbb{R}, +, .)$ is a commutative ring with unity.

$(\mathbb{C}, +, .)$ is a commutative ring with unity.

2. $(2\mathbb{Z}, +)$ is a commutative group and $(2\mathbb{Z}, .)$ is a commutative semigroup. The distributive law holds.

Therefore $(2\mathbb{Z}, +, .)$ is a commutative ring. It is a ring without unity.

Note. Let $n \in \mathbb{N}$. Then $(n\mathbb{Z}, +, .)$ is a commutative ring. This is a ring without unity.

3. Ring of real matrices. Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices whose elements are real numbers.

$(M_2(\mathbb{R}), +)$ is a commutative group, where $+$ denotes matrix addition and $(M_2(\mathbb{R}), .)$ is a monoid, where $.$ denotes matrix multiplication. The distributive laws hold.

Therefore $(M_2(\mathbb{R}), +, .)$ is a ring with unity. The identity matrix I_2 is the unity in the ring. This is a non-commutative ring.

Let $n \in \mathbb{N}$. Then $(M_n(\mathbb{R}), +, .)$ is the ring of all $n \times n$ real matrices. It is a non-commutative ring with unity, I_n being the unity in the ring.

Note. $(M_n(\mathbb{C}), +, .)$ is the ring of all $n \times n$ complex matrices. It is a non-commutative ring with unity, I_n being the unity in the ring.

4. Ring of integers modulo n. For a fixed $n \in \mathbb{N}$, let $\mathbb{Z}_n$ be the classes of residues of integers modulo n. $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$.

$(\mathbb{Z}_n, +)$ is a commutative group, where $+$ denotes addition (mod n).

$(\mathbb{Z}_n, .)$ is a commutative monoid where $.$ denotes multiplication (mod n). The distributive law holds.

Therefore $(\mathbb{Z}_n, +, .)$ is a commutative ring with unity. $\bar{1}$ is the unity in the ring.

5. **Ring of Gaussian integers.** Let us consider the subset of $\mathbb{C}$ given by $\mathbb{Z}[i] = \{a + ib : a,\ b \in \mathbb{Z}\}$.

$\mathbb{Z}[i]$ is the set of all complex numbers of the form $a + ib$, where a and b are integers.

$\mathbb{Z}[i]$ forms a ring under addition and multiplication of complex numbers. This is a commutative ring with unity.

This ring is called the *ring of Gaussian integers.*

6. **Ring of Gaussian numbers.** Let us consider the subset of $\mathbb{C}$ given by $\mathbb{Q}[i] = \{a + ib : a,\ b \in \mathbb{Q}\}$.

$\mathbb{Q}[i]$ is the set of all complex numbers of the form $a + ib$, where a and b are rational numbers.

$\mathbb{Q}[i]$ forms a ring under addition and multiplication of complex numbers. This is a commutative ring with unity.

This ring is called the *ring of Gaussian numbers.*

7. **Ring of Quaternions.** Let us consider the set H of 2×2 complex matrices given by

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

$\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}$ can be expressed as $aI + bJ + cK + dL$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

$(H, +, .)$ is a ring with respect to matrix addition and matrix multiplication. This is a non-commutative ring with unity, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity.

This ring is called the *ring of real quaternions.*

The subset $\left\{ \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} : a, b, c, d \in \mathbb{Q} \right\}$ forms a ring with unity. This ring is called the *ring of rational quaternions.* This is also a non-commutative ring with unity.

The subset $\left\{ \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ forms a ring with unity. This ring is called the *ring of integral quaternions.* This is also a non-commutative ring with unity.

8. Polynomial rings.

Let R be a ring and x an indeterminate. By a polynomial in x over R we mean an expression $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ where n is a non-negative integer and $a_0, a_1, a_2, \ldots, a_n$ (called coefficients of the polynomial) all belong to R.

A polynomial in x is generally denoted by $p(x)$, $q(x)$, $g(x)$ etc. The set of all polynomials over R is denoted by $R[x]$.

We define equality of two polynomials, addition and multiplication of two polynomials in $R[x]$.

(i) Two polynomials $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n \in R[x]$ are said to be equal if $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2, \ldots, a_n = b_n$.

(ii) Addition of two polynomials $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in R[x]$ is defined by

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m \\ &\quad + a_{m+1}x^{m+1} + \cdots + a_nx^n, \text{ if } m < n \\ &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \\ &\quad + b_{n+1}x^{n+1} + \cdots + b_mx^m, \text{ if } m > n. \\ &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n, \text{ if } m = n. \end{aligned}$$

(iii) Multiplication of two polynomials $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in R[x]$ is defined by

$f(x).g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n}$, where

$c_j = a_0b_j + a_1b_{j-1} + \cdots + a_jb_0$ taking

$a_{n+1} = a_{n+2} = \cdots = a_{m+n} = 0$, $b_{m+1} = b_{m+2} = \cdots = b_{m+n} = 0$.

Then $(R[x], +, .)$ is a ring. It is called the *polynomial ring* over R. If R be a ring with unity then the ring $(R[x], +, .)$ is also a ring with unity.

The identity element of the ring $(R[x], +, .)$ is the constant polynomial 1, 1 being the unity in the ring R. Here $a_0 = 1$, $a_i = 0$ for $i \geq 1$.

The zero element of the ring is the zero polynomial 0 ($a_i = 0$ for all i).

In particular, if we consider the set S given by

$$S = \{a_0 + a_1x + \cdots + a_rx^r : a_i \in \mathbb{Z},\ r \geq 0\},$$

then S forms a commutative ring with unity under addition and multiplication of polynomials. This ring is denoted by $\mathbb{Z}[x]$.

Similarly, $\mathbb{Q}[x]$ is the ring of all polynomials over $\mathbb{Q}$; $\mathbb{R}[x]$ is the ring of all polynomials over $\mathbb{R}$.

9. Ring of continuous functions.

Let S be the set of all real valued continuous functions on the closed and bounded interval $[a, b]$. Let $f : [a, b] \to \mathbb{R}$, $g : [a, b] \to \mathbb{R}$ be the elements of S.

We define addition and multiplication of f and g by

$(f+g)(x) = f(x) + g(x),\ x \in [a, b]$

$(f.g)(x) = f(x).g(x),\ x \in [a, b]$.

Then $(S, +, .)$ is a commutative ring with unity. The function i defined by $i(x) = 1$ for all $x \in [a, b]$ is the unity in the ring. The function o defined by $o(x) = 0$ for all $x \in [a, b]$ is the zero element in the ring. This ring is denoted by $C[a, b]$.

10. Zero ring. Trivial ring.

Let $(A, +)$ be an abelian group with the identity element 0. Let multiplication $(.)$ be defined on A by $a.b = 0$ for every pair of elements $a, b \in A$. Then A is closed under multiplication.

Let $a, b, c \in A$. Then $a.(b.c) = a.0 = 0$, by definition.

Also $(a.b).c = 0.c = 0$, by definition.

Hence multiplication is associative on A.

Let $a, b, c \in A$. Then $a.(b + c) = 0$ and $a.b + a.c = 0 + 0 = 0$.

Thus $a.(b + c) = a.b + a.c$. Similarly, $(b + c).a = b.a + c.a$.

Hence distributive laws hold in A.

Therefore $(A, +, .)$ is a ring . This ring is called a **zero-ring**.

Thus every abelian group is the additive group of a certain zero- ring.

In particular, the element 0 in the abelian group A forms a ring by itself. This ring is called the **trivial ring**. In this ring 0 is the additive as well as the multiplicative identity.

A **non-trivial** ring R means R has *at least* two elements.

We shall see later that if R be a non-trivial ring with unity, then the unity is different from the zero element in R.

Theorem 3.1.2. In a ring $(R, +, .)$,

(i) $a.0 = 0.a = 0$ for all $a \in R$, 0 being the zero element in R;

(ii) $a.(-b) = (-a).b = -(a.b)$ for all $a, b \in R$;

(iii) $(-a).(-b) = a.b$ for all $a, b \in R$.

Proof. (i) We have $a.0 = a.(0 + 0)$

$= a.0 + a.0$ [left distributive law]