मङ्गलायतन
विश्वविद्यालय

॥ विश्वं ज्ञाने प्रतिष्ठितम् ॥

MANGALAYATAN
UNIVERSITY

Learn Today to Lead Tomorrow

Abstract Algebra

MAL-6111

Edited By

Dr. Swati Agarwal

DIRECTORATE OF DISTANCE AND ONLINE EDUCATION
MANGALAYATAN
UNIVERSITY

CONTENTS

Units **Page No.**

UNIT

1

GROUPS AND NORMAL SUBGROUPS

NOTES

STRUCTURE

1.0. LEARNING OBJECTIVES

After going through this unit, you should be able to:

- binary operation
- order of groups and elements
- notation
- conjugate relation and conjugate class
- normalizer of an element and self conjugate element
- class equation of a finite group.

1.1. INTRODUCTION

This chapter begins with the assumption that the reader is well acquianted with the concepts of group, subgroup, Lagrange's theorem, cosets, normal subgroups etc. In this chapter, we shall be discussing conjugacy relation, normalizer, centre, class equation, in the context of a group.

1.2. BINARY OPERATION

Let S be a non-empty set. A function from S × S into S is called a **binary operation** on S. Thus, if '*' is a binary operation on S, then it means that '*' is a function from S × S into S.

If $(a, b) \in S \times S$, then the image $*(a, b)$ of (a, b) under the binary operation '*' is written $a * b$.

1.3. GROUP

A non-empty set G with a binary operation, denoted by '.', is called a **group** if :

(*i*) $x \,.\, (y \,.\, z) = (x \,.\, y) \,.\, z \quad \forall\, x, y, z \in G$

(*ii*) There exists $e \in G : x \,.\, e = x = e \,.\, x \quad \forall\, x \in G$

e is called the **identity** of G.

(*iii*) For $x \in G$, there exists $y \in G : \; x \,.\, y = e = y \,.\, x$

y is called the **inverse** of x. The inverse of x is written as x^{-1}.

If in addition, we have

(*iv*) $x \,.\, y = y \,.\, x \quad \forall\, x, y \in G$,

then G is called a **commutative group.** A commutative group is also called an **abelian group** after the famous Norwegian mathematician **N.H. Abel.** A group is called **non-commutative** or **non-abelian** if it is not commutative.

If the binary operation of a group is written as '+', then we write

(*i*) $x + (y + z) = (x + y) + z \quad \forall\, x, y, z \in G$

(*ii*) $\exists\, e \in G : x + e = x = e + x \quad \forall\, x \in G$

(*iii*) For $x \in G$, $\exists\, y \in G : x + y = e = y + x$

And for commutativity, $x + y = y + x \quad \forall\, x, y \in G$.

Remark 1. The binary operation '+' used above has got nothing to do with the ordinary addition of numbers. In fact *, +, . are just symbols representing binary operations.

Remark 2. In order to show a non-empty set G with a given binary operation to be a group, we should verify all the three conditions given above.

1.4. ORDER OF A GROUP

NOTES

If the number of elements in a group is finite, the group is said to be a **finite group,** otherwise an **infinite group.** The number of elements in a finite group is called the **order of the group.**

If a group G is finite and has n elements, then we write $o(G) = n$.

1.5. ORDER OF AN ELEMENT

Let (G, .) be a group with identity element e. For $a \in G$, if there exists a smallest natural number m such that $a^m = e$, then m is called the **order** of a and write $o(a) = m$.

If no such natural number exists then we say that a is of **infinite order.**

IMPORTANT RESULTS

1. *In a group, identity element is unique.*
2. *In a group, every element has unique inverse.*
3. *If (G, .) is a group, then* $(a^{-1})^{-1} = a \quad \forall\, a \in G$.
4. *If (G, .) is a group, then* $(a \,.\, b)^{-1} = b^{-1} \,.\, a^{-1} \quad \forall\, a, b \in G$.
5. *If (G, .) is a group and* $a \,.\, b = a \,.\, c$, *then* $b = c$.
6. *If (G, .) is a group and* $b \,.\, a = c \,.\, a$, *then* $b = c$.
7. *For a finite group, the order of every element is finite and cannot exceed the order of the group.*
8. *In a group, the order of an element and its inverse are same.*

1.6. NOTATION

Let G be a group with binary operation $*$. Let $x, y \in G$. For the sake of convenience, the element $x * y$ of G is written as xy. Under this notation the axioms of a group G takes the following form :

(*i*) $x(yz) = (xy)z \;\forall\, x, y, z \in G$

(*ii*) There exists an element e in G such that $xe = x = ex$

(*iii*) For $x \in G$, there exists an element y in G such that $xy = e = yx$.

1.7. CONJUGACY RELATION

Let G be a group and $a, b \in G$. a is said to be a **conjugate** of b if there exists an element $x \in G$ such that $a = x^{-1}\, bx$.

If a is conjugate to b then we write $a \sim b$ and this relation '$\sim$' is called the **conjugacy relation** on G.

For example in the group S_3, the element (1 2 3) is conjugate of (1 3 2), because we have :

$$(1\ 2\ 3) = (2\ 3)^{-1}\ (1\ 3\ 2)\ (2\ 3).$$

Example 1. *Show that two elements of a group are conjugate if and only if they can be put in the form ab and ba respectively, where a and b are some suitable elements of G.*

Sol. Let x and y be conjugate elements of G.

$\therefore \quad x = z^{-1}yz$ for some $z \in$ G

Let $\quad a = z^{-1}y$ and $b = z$.

$\therefore \quad ab = (z^{-1}y)z = z^{-1}yz = x$ and $ba = z(z^{-1}y) = (zz^{-1})\, y = y$

$\therefore \quad x = ab$ and $y = ba$.

Conversely, let $\quad x = ab$ and $y = ba$

Now $\quad a^{-1}xa = a^{-1}(ab)a = (a^{-1}a)(ba) = ey = y$ *i.e.*, y is conjugate to x.

Also, $\quad b^{-1}yb = b^{-1}(ba)b = (b^{-1}b)(ab) = ex = x$ *i.e.*, x is conjugate to y.

$\therefore$ x and y are conjugate. $\therefore$ The result holds.

Theorem 1. *The conjugacy relation on a group is an equivalence relation.*

Proof. Let G be a group and the conjugacy relation on G be denoted by ~. We shall show that ~ is an equivalence relation.

1. **Reflexivity.** Let $a \in$ G.

We have $\quad e^{-1}ae = eae = a$

$\therefore \quad a = e^{-1}ae$ *i.e.*, $a \sim a$

$\therefore \quad a \sim a \; \forall \; a \in$ G. $\therefore$ ~ is reflexive.

2. **Symmetry.** Let $a, b \in$ G and $a \sim b$.

$\therefore \quad \exists \; x \in \mathrm{G} : a = x^{-1}bx$

$\Rightarrow \quad xax^{-1} = x(x^{-1}bx)\, x^{-1} = (xx^{-1})\, b(xx^{-1}) = ebe = b$

$\Rightarrow \quad b = xax^{-1}$ *i.e.*, $b = (x^{-1})^{-1}\, a(x^{-1})$

$\therefore \quad b \sim a$, because $x^{-1} \in$ G

$\therefore \quad a \sim b \;\Rightarrow\; b \sim a$. $\therefore$ ~ is symmetric.

3. **Transitivity.** Let $a, b, c, \in$ G and $a \sim b$ and $b \sim c$.

$\therefore \quad \exists \; x, y \in \mathrm{G} : a = x^{-1}bx$ and $b = y^{-1}cy$,

$\therefore \quad a = x^{-1}(y^{-1}cy)x = (x^{-1}y^{-1})\, c(yx) = (yx)^{-1}\, c(yx)$

$\therefore \quad a \sim c$, because $yx \in$ G

$\therefore \quad a \sim b$ and $b \sim c \;\Rightarrow\; a \sim c$. $\therefore$ ~ is transitive.

$\therefore$ The conjugacy relation on a group is an equivalence relation.

1.8. CONJUGATE CLASS

We know that an equivalence relation on a set partitions it into mutually disjoint equivalence classes.

Let C(a) denote the equivalence class of an element a of G with respect to the conjugacy relation ~ on the group G. The set C(a) is called the **conjugate class** of a in G.

$$\begin{aligned} \therefore \quad \mathrm{C}(a) &= \{b : b \in \mathrm{G} \text{ and } b \sim a\} \\ &= \{b : b \in \mathrm{G} \text{ and } b = x^{-1}ax \text{ for some } x \in \mathrm{G}\} \\ &= \{x^{-1}ax : x \in \mathrm{G}\} \\ &= \text{set of all conjugates of } a. \end{aligned}$$

Since the relation '~' is reflexive, $a \in C(a) \quad \forall\ a \in G$.

Also, $\qquad C(a) \subseteq G \quad \forall\ a \in G$

$$\therefore \qquad G = \bigcup_{a \in G} \{a\} \subseteq \bigcup_{a \in G} C(a) \subseteq G$$

$$\therefore \qquad G = \bigcup_{a \in G} \mathbf{C(a).}$$

In particular, let G be a finite group and $G = \overset{t}{\underset{i=1}{\cup}} C(a_i)$, where the equivalence classes $C(a_1)$, $C(a_2)$, ..., $C(a_t)$ are mutually disjoint.

$$\therefore \qquad \mathbf{o(G)} = \sum_{i=1}^{t} \mathbf{o(C(a_i))}.$$

Remark. $C(e) = \{x^{-1}ex : x \in G\} = \{x^{-1}x : x \in G\} = \{e\}$

Example 2. *If G is an abelian group, then show that $C(a) = \{a\}\ \forall\ a \in G$.*

Sol. For $a \in G$,

$$\begin{aligned} C(a) &= \{x^{-1}ax : x \in G\} \\ &= \{x^{-1}\ (xa) : x \in G\} \\ &= \{(x^{-1}x)a : x \in G\} = \{ea : x \in G\} = \{a\} \end{aligned}$$

$$\therefore \qquad C(a) = \{a\}\ \forall\ a \in G.$$

Example 3. *Let G be a group containing an element of finite order n (> 1) and exactly two conjugate classes. Show that G is a finite group of order 2.*

Sol. Let $a\ (\neq e)$ be an element of group G of order n.

We know that $\quad C(e) = \{e\} \quad$ and $\quad a \neq e$.

$\therefore \qquad a \notin C(e)$

Also $\qquad a \in C(a) \quad \therefore \quad C(e) \neq C(a)$

$\therefore$ $C(e)$ and $C(a)$ are disjoint conjugate classes.

Since G has exactly two conjugate classes, we have

$$G = C(e) \cup C(a)$$

$$\Rightarrow \qquad G = \{e\} \cup C(a)$$

Let $b(\neq e)$ be any element of G.

$\therefore \qquad b \in C(a)$

$\Rightarrow \qquad b = x^{-1}ax$ for some $x \in G$

$\Rightarrow \qquad o(b) = o(x^{-1}ax) = o(a)$

$\therefore \qquad o(b) = n \quad \forall \quad b(\neq e) \in G \qquad$ ...(1)

We now show that n is prime.

Let $n = lm$, where l, m are positive integer $\leq n$.

$\therefore \qquad a^n = e \quad \Rightarrow \quad a^{lm} = e \quad \Rightarrow \quad (a^l)^m = e$

$\qquad a^l \in G \quad$ and $\quad a^l \neq e \quad \Rightarrow \quad o(a^l) = n$

$\Rightarrow \qquad m = m \quad \therefore \quad m = n \quad (\because \quad m \leq n)$

$\Rightarrow \qquad m \leq lm \quad \Rightarrow m = \quad l = 1 \quad \therefore \quad n$ is prime.

Now we shall show that $a^2 = e$.

If possible, let $a^2 \neq e$.

$\therefore$ $a^2 \in C(a)$ $\qquad (\because \quad C(e) = \{e\})$

$\Rightarrow$ $a^2 = y^{-1}ay$ for some $y\ (\neq e) \in G$

Let $a^{2^k} = y^{-k}ay^k$ $\qquad$ ...(2)

$\therefore$ $a^{2^{k+1}} = a^{2^k . 2} = (a^{2^k})^2 = (y^{-k}ay^{-k})^2$ $\qquad$ (Using (2))

$\Rightarrow$ $a^{2^{k+1}} = (y^{-k}ay^k)\ (y^{-k}ay^k) = y^{-k}a(y^ky^{-k})ay^k$

$= y^{-k}aeay^k = y^{-k}a^2y^k = y^{-k}\ (y^{-1}ay)\ y^k = y^{-(k+1)}\ ay^{k+1}$

$\therefore$ By **P.M.I.,** $a^{2^m} = y^{-m}ay^m \quad \forall \quad m \in \mathbf{N}$

$\therefore$ In particular, $a^{2^n} = y^{-n}ay^n$

$\Rightarrow$ $a^{2^n} = e^{-1}ae = a$ $\qquad (\because \quad y(\neq e) \in G \quad \Rightarrow \quad o(y) = n)$

$\Rightarrow$ $a^{2^n - 1} . a = e . a \quad \Rightarrow \quad a^{2^n - 1} = e \quad \Rightarrow \quad n/(2^n - 1)$ $\qquad (\because \quad o(a) = n)$

This is impossible, because n is prime.

$\therefore$ $a^2 = e$

$\therefore$ $o(a) = 2$ *i.e.,* $n = 2$

$\therefore$ (1) $\Rightarrow$ $o(b) = 2 \quad \forall\ b(\neq e) \in G$

$\therefore$ G is abelian.*

$\therefore$ $C(a) = \{a\}$ and thus $G = \{e\} \cup \{a\}$

$\Rightarrow$ $o(G) = 1 + 1 = 2.$

Hence the result holds.

1.9. NORMALIZER OF AN ELEMENT

Let G be a group. For $a \in G$, the set $\{x \in G : ax = xa\}$ is called the **normalizer** of the element a in G and it is denoted by $N(a)$.

Thus, the normalizer of a contains all those elements of G which commute with a.

Remarks 1. We have $ex = xe \quad \forall\ x \in G$.

$\therefore$ $N(e) = G$

2. If G is an abelian group and $a \in G$, then $ax = xa \quad \forall\ x \in G$.

$\therefore$ $N(a) = G \quad \forall\ a \in G$.

Theorem 2. *Let G be a group. For any a in G, the normalizer N(a) of a in G is a subgroup of G.*

Proof. We have $N(a) = \{x \in G : ax = xa\}$

$e \in N(a)$, because $ae = ea$ $\qquad \therefore$ $N(a)$ is non-empty.

Let $x, y \in N(a)$. $\therefore\ ax = xa,\ ay = ya$.

Now $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)\ a$

$\Rightarrow$ $a(xy) = (xy)a \quad \therefore \quad xy \in N(a)$

* Let $a, b \in G$. $\therefore$ $(ab)^2 = e$ and $a^2b^2 = ee = e$.

$\Rightarrow$ $(ab)^2 = a^2b^2 \quad \Rightarrow \quad abab = aabb \quad \Rightarrow \quad ba = ab$.

Let $x \in N(a)$ $\quad \therefore \; ax = xa$

$\Rightarrow \quad x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} \quad \Rightarrow \quad (x^{-1}a)(xx^{-1}) = (x^{-1}x)(ax^{-1})$

$\Rightarrow \quad (x^{-1}a)e = e(ax^{-1}) \; \Rightarrow \quad x^{-1}a = ax^{-1}$

$\Rightarrow \quad ax^{-1} = x^{-1}a \quad \therefore \quad x^{-1} \in N(a)$

$\therefore$ N(a) is a subgroup of G.

Remark. The normalizer N(a) may not be a normal subgroup of G.

Example 4. *Give an example to show that in a group G, the normalizer of an element is not necessarily a normal subgroup of G.*

Sol. Let X = {a, b, c}. Let S_3 be the set of all one-to-one mappings of X onto X.

$\therefore \quad S_3 = \{I, (ab), (bc), (ca), (abc), (acb)\}$.

Here the mapping (ab) stands for $a \to b$, $b \to a$, $c \leftrightarrow c$.

The set S_3 is a group with composition of mappings as the binary operation. We find the normalizer of the element (ab) of S_3.

We have $\quad I(ab) = (ab)I \quad \therefore \quad I \in N((ab))$

Also $\quad (ab) \in N((ab))$

We find (ab)(bc).

Under $(ab)(bc) : a \to a \to b, b \to c \to c, c \to b \to a$

$\therefore \quad (ab)(bc) = (abc)$

Under $(bc)(ab) : a \to b \to c, b \to a \to a, c \to c \to b$

$\therefore \quad , \quad (bc)(ab) = (acb)$

$\therefore \quad (ab)(bc) \neq (bc)(ab)$

$\therefore \quad (bc) \notin N((ab))$

Similarly (ca), (abc), (acb) are not in N((ab)).

$\therefore \quad N((ab)) = \{I, (ab)\}$

Since in general, a normalizer is a subgroup, N((ab)) is also a subgroup of S_3.

Now $\quad (bc) \in S_3$ and $(ab) \in N((ab))$

and $\quad (bc)(ab)(bc)^{-1} = (bc)(ab)(bc) = (bc)(abc) = (ac) \notin N((ab))$.

$\therefore$ N((ab)) is not a normal subgroup of S_3.

Theorem 3. *If G is a finite group and $a \in G$, then $o(C(a)) = \dfrac{o(G)}{o(N(a))}$.*

Proof. We have $C(a) = \{x^{-1}ax : x \in G\}$.

Let A be the set of all cosets of the subgroup N(a) in G.

Define $\phi : A \to C(a)$ by $\phi(N(a)\, x) = x^{-1}ax \quad \forall\, x \in G$

ϕ is well defined. Let $x, y \in G$ and $N(a)\, x = N(a)\, y$

$\Rightarrow \quad xy^{-1} \in N(a) \qquad (\because \; Ha = Hb \Leftrightarrow ab^{-1} \in H)$

$\Rightarrow \quad a(xy^{-1}) = (xy^{-1})a \quad \Rightarrow \quad x^{-1}(axy^{-1})\, y = x^{-1}(xy^{-1}a)\, y$

$\Rightarrow \quad (x^{-1}ax)(y^{-1}y) = (x^{-1}x)(y^{-1}ay) \quad \Rightarrow \quad x^{-1}ax = y^{-1}ay$

$\Rightarrow \quad \phi(N(a)x) = \phi(N(a)y)$.

$\therefore$ ϕ is well defined.

ϕ in one-one. Let $x, y \in G$ and $\phi(N(a)x) = \phi(N(a)y)$

$\Rightarrow$ $x^{-1}ax = y^{-1}ay$ $\Rightarrow$ $(x^{-1}ax)(y^{-1}y) = (x^{-1}x)(y^{-1}ay)$

$\Rightarrow$ $x^{-1}(axy^{-1})\, y = x^{-1}(xy^{-1}a)y$ $\Rightarrow$ $x(x^{-1}(axy^{-1})\, y)\, y^{-1} = x(x^{-1}(xy^{-1}a)\, y)\, y^{-1}$

$\Rightarrow$ $(xx^{-1})(axy^{-1})(yy^{-1}) = (xx^{-1})(xy^{-1}a)(yy^{-1})$ $\Rightarrow$ $a(xy^{-1}) = (xy^{-1})\, a$

$\Rightarrow$ $xy^{-1} \in N(a)$ $\Rightarrow$ $N(a)x = N(a)\, y$.

$\therefore$ ϕ is one-one.

ϕ is onto. Let $y \in C(a)$

$\therefore$ $\exists\, x \in G : y = x^{-1}ax$

Now $N(a)\, x \in A$ and $\phi(N(a)x) = x^{-1}ax = y$.

$\therefore$ ϕ is onto.

$\therefore$ There is one-to-one correspondence between the right cosets of $N(a)$ in G and the conjugates of a.

Since the group G is finite, we have

$$\begin{aligned} o(C(a)) &= \text{number of elements of } C(a) \\ &= \text{number of conjugates of } a \\ &= \text{number of right cosets of } N(a) \text{ in } G \quad (\because\ Q \text{ is 1–1 and onto}) \\ &= \frac{o(G)^{*}}{o(N(a))} \end{aligned}$$

$$\therefore \qquad \mathbf{o(C(a)) = \frac{o(G)}{o(N(a))}}.$$

In other words, the number of conjugates of a in G is equal to the index of $N(a)$ in G *i.e.*, $o(C(a)) = [G : N(a)]$.

Theorem 4. *If G is a finite group, then* $o(G) = \sum_{a} \frac{o(G)}{o(N(a))}$, *where the sum runs over elements a, taken one from each conjugate class.*

Proof. The relation of conjugacy is an equivalence relation on G.

$\therefore$ This relation partitions G into mutually disjoint conjugate classes.

Since G is finite, the number of distinct conjugate classes will be finite, say k. Let $C(a)$ denote the conjugate class of a. Let the k distinct conjugate classes of G be $C(a_1)$, $C(a_2)$, ..., $C(a_k)$.

$$\therefore \qquad G = C(a_1) \cup C(a_2) \cup \ldots\ldots \cup C(a_k)$$

$$\begin{aligned} \therefore \qquad o(G) &= o(C(a_1)) + o(C(a_2)) + \ldots\ldots + o(C(a_k)) \\ &= \frac{o(G)}{o(N(a_1))} + \frac{o(G)}{o(N(a_2))} + \ldots\ldots + \frac{o(G)}{o(N(a_k))} = \sum_{i=1}^{k} \frac{o(G)}{o(N(a_i))} \end{aligned}$$

$$\therefore \qquad \mathbf{o(G) = \sum_{a} \frac{o(G)}{o(N(a))}},$$

where the sum runs over elements a, taken one from each conjugate class.

[*] This is because the distinct right cosets of $N(a)$ in G forms a partition of G and the order of each right coset of $N(a)$ is same as the order of $N(a)$.

NOTES

Example 5. *If in a finite group G an element 'a' has exactly two conjugates, show that G is not simple.*

Sol. We have $o(C(a)) = 2$.

Since G is finite, we have

$$o(C(a)) = \frac{o(G)}{o(N(a))}$$

$$\therefore \qquad \frac{o(G)}{o(N(a))} = 2$$

$\therefore$ No. of right cosets of $N(a)$ in $G = 2$

$\therefore$ Index of $N(a)$ in $G = 2$

$\therefore$ $N(a)$ is a normal subgroup of G. (This is a standard result)

If possible, let $N(a) = \{e\}$.

$\therefore$ $a \in N(a) \Rightarrow a = e \Rightarrow C(a) = C(e) = \{e\} \Rightarrow o(C(a)) = 1$, which is impossible.

$$\therefore \qquad N(a) \neq \{e\}$$

If possible, let $N(a) = G$.

$$\Rightarrow \qquad \frac{o(G)}{o(N(a))} = \frac{o(G)}{o(G)} = 1 \quad \Rightarrow \quad o(C(a)) = 1, \text{ which is impossible.}$$

$$\therefore \qquad N(a) \neq G$$

$\therefore$ Neither $N(a) = \{e\}$ nor $N(a) = G$.

$\therefore$ The group G is not simple.

1.10. SELF CONJUGATE ELEMENT

Let G be a group. An element a of G is said to be **self conjugate** if no element of G, other than a, is conjugate to a.

$$\therefore \qquad x^{-1}ax = a \quad \forall\, x \in G$$

Equivalently $\qquad ax = xa, \forall\, x \in G$.

Thus, a self conjugate element of a group commutes with each element of the group.

A self conjugate element is also known as an **invariant** element.

Remark. If a is a self conjugate element of a group G, then $N(a) = G$.

1.11. CENTRE OF A GROUP

Let G be a group. The set $\{z \in G : zx = xz \;\forall\; x \in G\}$ is called the **centre** of the group G and it is denoted by Z.

$$z \in Z \quad \Rightarrow \quad zx = xz \quad \forall\, x \in G$$

$$\Rightarrow \qquad x^{-1}(zx) = x^{-1}(xz) \;\Rightarrow\; x^{-1}zx = z \quad \forall\, x \in G.$$

$\therefore$ z is a self conjugate element of G.

$\therefore$ The centre of a group consists of all its self conjugate elements.

Remark: $Z \subseteq N(a)\ \forall\, a \in G$ because

$$x \in Z \;\Rightarrow\; xy = yx\ \forall\, y \in G \;\Rightarrow\; xa = ax \;\Rightarrow\; x \in N(a).$$

Theorem 5. *Let G be a group. The centre Z of G is a normal subgroup of G.*

Proof. We have $Z = \{z \in G : zx = xz \ \forall \ x \in G\}$

$e \in Z$ because $ex = xe \quad \forall \ x \in G \quad \therefore \quad Z$ is non-empty.

Let $z_1, z_2 \in Z \quad \therefore \quad z_1x = xz_1,\ z_2x = xz_2 \quad \forall \ x \in G$

Now $(z_1z_2)\, x = z_1(z_2x) = z_1(xz_2) = (z_1x)z_2 = (xz_1)\, z_2 = x(z_1z_2), \quad \forall \ x \in G.$

$\therefore \qquad z_1z_2 \in Z$

Let $\qquad z \in Z \quad \therefore \quad zx = xz \quad \forall \ x \in G$

$\Rightarrow \qquad z^{-1}(zx)\, z^{-1} = z^{-1}(xz)\, z^{-1} \quad \Rightarrow \quad (z^{-1}z)(xz^{-1}) = (z^{-1}x)(zz^{-1})$

$\Rightarrow \qquad xz^{-1} = z^{-1}x \quad \Rightarrow \quad z^{-1}x = xz^{-1} \quad \forall \ x \in G$

$\therefore \qquad z^{-1} \in Z$

$\therefore$ Z is a subgroup of G.

Let $\qquad z \in Z, x \in G.$

$$xzx^{-1} = (xz)x^{-1} = (zx)x^{-1} = z(xx^{-1}) = ze = z \in Z$$

$\therefore \qquad xzx^{-1} \in Z \quad \forall \ z \in Z$ and $x \in G.$

$\therefore$ Z is a normal subgroup of G.

Theorem 6. *Let G be a group. $a \in Z$ if and only if $N(a) = G$.*

Proof. Let $\qquad a \in Z$

$\therefore \qquad ax = xa \quad \forall \ x \in G$

$\Rightarrow \qquad x \in N(a) \quad \forall \ x \in G$

$\Rightarrow \qquad N(a) = G$

Conversely, let $\quad N(a) = G$

$\therefore \qquad ax = xa \quad \forall \ x \in G \quad \therefore \quad x \in Z$

$\therefore$ The result follows.

Corollary. If G is a finite group and $a \in Z$, then $o(N(a)) = o(G)$.

Proof. $a \in Z \ \Rightarrow \ N(a) = G.$

$\therefore \qquad o(N(a)) = o(G). \qquad (\because \quad$ G is finite)

Theorem 7. *If G be a finite group, then $o(G) = o(Z) + \sum\limits_{a \notin Z} \dfrac{o(G)}{o(N(a))}$, where the sum runs over elements a, taken one from each conjugate class which contain more than one element.*

Proof. We know that

$$o(G) = \sum_{a} \frac{o(G)}{o(N(a))},$$

where the sum runs over elements a, taken one from each conjugate class.

Let $a \in G \quad \therefore \quad a$ may or may not be in Z.

Case I. a ∈ Z

$\Rightarrow \qquad ax = xa \quad \forall \ x \in G$

$\Rightarrow \qquad N(a) = G$

$$\therefore \qquad \frac{o(G)}{o(N(a))} = \frac{o(G)}{o(G)} = 1.$$

$\therefore$ For each $a \in Z$, we have $\dfrac{o(G)}{o(N(a))} = 1$

$$\therefore \qquad \sum_{a \in Z} \frac{o(G)}{o(N(a))} = 1 + 1 + \ldots\ldots\ o(Z) \text{ times} = o(Z)$$

Case II. a $\notin$ Z

$\therefore$ $ax \neq xa$ for at least one $x \in$ G $\therefore$ N$(a) \subset$ G

$$\therefore \quad (1) \quad \Rightarrow \qquad o(G) = \sum_{a \in Z} \frac{o(G)}{o(N(a))} + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

$$\therefore \qquad \mathbf{o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}},$$

where the sum runs over elements a taken one from each conjugate class which contain more than one element.

1.12. CLASS EQUATION OF A FINITE GROUP

Let G be a finite group. For $a \in$ G, let N(a) denote the normalizer of a.

We have the equation :

$$\mathbf{o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}},$$

where the sum runs over elements a, taken one from each conjugate class which contain more than one element.

This equation is called the **class equation** of the finite group G.

Theorem 8. *If $o(G) = p^n$, where p is a prime number and n is a natural number, then centre $Z \neq \{e\}$.*

Proof. If $n = 1$, then o(G) $= p$, a prime number.

$\therefore$ G is a cyclic group and hence abelian.

$\therefore$ Centre Z of G = G

$\therefore$ $\qquad o(Z) > 1 \quad \therefore \quad Z \neq \{e\}$.

Now, let us suppose that $n > 1$. Since G is a finite group, its class equation is

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \qquad \text{...(1)}$$

$$a \notin Z \;\Rightarrow\; N(a) \neq G \;\Rightarrow\; N(a) \subset G$$

By Lagrange's theorem, let

$$o(N(a)) = p^{n_a} \text{ for some } 0 < n_a < n.$$

The number n_a cannot be 0, because N(a) contains at least e and a.

$$\therefore \qquad \frac{o(G)}{o(N(a))} = \frac{p^n}{p^{n_a}} = p^{n-n_a} = p.p^{n-n_a-1}$$

$$(n_a < n \;\Rightarrow\; n - n_a > 0 \;\Rightarrow\; n - n_a - 1 \geq 0)$$

$$\therefore \qquad p \Big/ \frac{o(G)}{o(N(a))} \quad \forall\, a \notin Z$$

$$\Rightarrow \qquad p \Big/ \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

NOTES

Also $\qquad o(\text{G}) = p^n$ implies $p / o(\text{G})$.

$$\therefore \qquad p \Bigg/ \left(o(\text{G}) - \sum_{a \notin Z} \frac{o(\text{G})}{o(\text{N}(a))} \right)$$

$\therefore \qquad (1) \Rightarrow p/o(\text{Z}) \qquad (\because e \in \text{Z} \;\Rightarrow\; o(\text{Z}) \neq 0)$

$\Rightarrow \qquad o(\text{Z}) > 1$

$\therefore$ Z must contain more than one element *i.e.*, $z \neq \{e\}$.

Example 6. *If $o(G) = p^2$, where p is a prime number, then show that G is abelian.*

Sol. Let Z be the centre of the group G.

$\therefore$ Z is a subgroup of G.

By *Lagrange's theorem*, $o(\text{Z})/o(\text{G})$ *i.e.*, $o(\text{Z})/p^2$

$\therefore \qquad o(\text{Z}) = 1 \quad \text{or} \quad p \quad \text{or} \quad p^2$

Since $o(\text{G}) = p^n$, where $n = 2$, we have $\text{Z} \neq \{e\}$.

$\therefore \qquad o(\text{Z}) \neq 1.$

If possible, let $\quad o(\text{Z}) = p.$

$\therefore \qquad \text{G} - \text{Z} \neq \phi.\quad$ Let $a \in \text{G} - \text{Z}$

$\therefore \qquad a \in \text{G} \quad \text{and} \quad a \notin \text{Z}.$

For $b \in \text{Z}$, we have $ba = ab$. $\;\therefore\; b \in \text{N}(a)$. Thus $\text{Z} \subsetneq \text{N}(a)$

Also $a \in \text{N}(a)$ and $a \notin \text{Z} \;\therefore\; \text{Z} \neq \text{N}(a)$

$\therefore \qquad o(\text{N}(a)) > o(\text{Z})$ *i.e.*, $o(\text{N}(a)) > p$

By *Lagrange's theorem*, $o(\text{N}(a))/p^2$.

$\therefore$ We have $\quad o(\text{N}(a)) = p^2 \quad \therefore \quad \text{N}(a) = \text{G}.$

$\Rightarrow \; a \in \text{Z}$. This is against the choice of a.

$\therefore$ Our supposition is wrong.

$\therefore \quad o(\text{Z}) \neq p. \quad \therefore$ The only choice is $o(\text{Z}) = p^2$.

$\therefore$ Z = G. Thus, $ab = ba \; \forall \; a, b \in \text{G}$.

$\therefore$ G is abelian.

Remark : The above example gives an interesting result as :

'Groups of orders 4, 9, 25, 49, 121, ... are all abelian.

SUMMARY

- The conjugacy relation on a group is an equivalence relation on the group G and the corresponding equivalence classes partitions the group G into mutually disjoint equivalence classes, called **conjugate classes.**
- The normalizer N(a) of a in G is a subgroup of G.
- If G is a finite group, then $o(\text{G}) = \sum_{a} \frac{o(G)}{o(N(a))}$, where the sum runs over elements a, taken one from each conjugate class.

- The centre of a group G is a normal subgroup of G.
- The number of conjugate clásses of a non-abelian group of order p^3, where p is prime, is $p^2 + p - 1$.
- If G is a finite group, then $o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{(N(a))}$, where the sum runs over elements a, taken one from each conjugate class which contain more than one element.

  This equation is called the class equation of the finite group G.

REVIEW QUESTIONS

1. Show that in a group G the cyclic subgroup generated by an element a of G is contained in the normalizer of a.
2. Let a be any element of a group G. If $x, y \in$ G give rise to the same conjugate of a then they belong to the same right coset of N(a) in G.
3. Let a be any element of a group G. If $x, y \in$ G belong to the same right coset of N(a) in G, then they give rise to the same conjugate of a.
4. Show that the normalizer of a self conjugate element is the whole group.
5. Let Z be the centre of a group G. If $a \in$ Z then show that the cyclic subgroup of G which is generated by a is a normal subgroup of G.
6. If G is a non-abelian group and $o(G) = p^3$, where p is prime then show that the centre of G has exactly p elements.
7. Show that a group of order 9 is abelian.
8. Show that the centre of a non-abelian group of order 125 always have 5 elements in its centre.
9. Let H be a subgroup of the centre Z of a group G. If G/H is cyclic, show that G is abelian.
10. If $o(G) = p^n$, where p is a prime number and n is a natural number, then prove that $N \cap Z \neq \{e\}$, where N ($\neq \{e\}$) is any normal subgroup of G.
11. Find the number of conjugate classes of a non-abelian group G if:

    (*i*) $o(G) = 27$ (*ii*) $o(G) = 125$.

NOTES

UNIT 2

GROUP AUTOMORPHISMS

STRUCTURE

2.0 LEARNING OBJECTIVES

After going through this unit, you should be able to:

- automorphism, homomorphism
- kernel of a homomorphism isomorphism
- isomorphic groups.

2.1. INTRODUCTION

We know that a one-one homomorphism from one group into another group is called an isomorphism. In case both groups are same and the homomorphism is one-one and onto then we can derive some very interesting results. An isomorphism in such a particular case is called an *automorphism*. In this chapter, we shall also discuss inner automorphisms and group of automorphisms.

2.2. AUTOMORPHISM

NOTES

A mapping ϕ from a group G to itself is called an **automorphism** of group G if

(*i*) $\phi(ab) = \phi(a)\,\phi(b)\ \forall\ a, b \in G$ (*ii*) ϕ is one-one

(*iii*) ϕ is onto.

Illustration. Let G be a group. The identity mapping $i : G \to G$ defined by $i(x) = x$, $x \in G$ is an automorphism. This automorphism is called the **trivial automorphism** of G.

2.3. HOMOMORPHISM

A mapping ϕ from a group G into a group G′ is called a **homomorphism** of G into G′ if $\phi(ab) = \phi(a)\,\phi(b)\quad \forall\ a, b \in G$.

If binary operation in G is $*$ then ab stands for $a * b$ and if the binary operation in G′ is $*'$, then $\phi(a) *' \phi(b)$ is written briefly $\phi(a)\,\phi(b)$.

2.4. KERNEL OF A HOMOMORPHISM

If ϕ is a homomorphism of group G into group G′, then the set

$$\{a \in G : \phi(a) = \text{identity element of } G'\}$$

is called the **kernel of the homomorphism** ϕ and write **ker** ϕ.

Since $\phi(e) = e'$, so $e \in \ker \phi$.

$\therefore$ ker ϕ is always a non-empty set.

2.5. ISOMORPHISM

A mapping ϕ from a group G into a group G′ is called an **isomorphism** of G into G′ if

(*i*) ϕ is a homomorphism *i.e.*, $\phi(ab) = \phi(a)\,\phi(b)\quad \forall\ a, b \in G$

(*ii*) ϕ is one-one.

Remark. If $\phi : G \to G'$ is a mapping and we write $\phi(ab) = \phi(a)\,\phi(b)$, then it should be clearly understood that

(*i*) ab is that element of the group G which is obtained by applying the binary operation of G on the ordered pair $(a, b) \in G \times G$.

(*ii*) $\phi(a)\,\phi(b)$ is that element of the group G′ which is obtained by applying the binary operation of G′ on the ordered pair $(\phi(a), \phi(b)) \in G' \times G'$.

2.6. ISOMORPHIC GROUPS

Two groups G and G′ are called **isomorphic groups** if there exists an isomorphism of G onto G′. If groups G and G′ are isomorphic groups then we write $G \cong G'$.

Remark. If groups G and G′ are isomorphic then there may exist one or more than one isomorphism from G onto G′.

IMPORTANT RESULTS

1. *If ϕ is a homomorphism of group G into group G′, then $\phi(e) = e'$.*
2. *If ϕ is a homomorphism of group G into group G′, then*

$$\phi(a^{-1}) = [\phi(a)]^{-1} \quad \forall\, a \in G.$$

3. *If ϕ is an isomorphism of a group G into group G′, then*

$$o(a) = o(\phi(a)) \quad \forall\, a \in G.$$

4. *Let $\phi : G \to G'$ be a homomorphism. The homomorphism ϕ is an isomorphism of G into G′ if and only if ker $\phi = \{e\}$.*

Example 1. *Let G be a non-abelian group and $f : G \to G$ be defined by $f(x) = x^{-1}$. Show that f is not an automorphism.*

Sol. Let $x, y \in$ G.

$\therefore \qquad f(xy) = (xy)^{-1}x^{-1}$ and $f(x)\, f(y) = x^{-1}y^{-1}$

Since $y^{-1}x^{-1}$ and $x^{-1}y^{-1}$ may not be equal, we have

$$f(xy) \neq f(x)\, f(y), \text{ in general.}$$

$\therefore$ f is not an automorphism.

Example 2. *let $G = (a)$ be a cyclic group of order 12. Let $f : G \to G$ be defined by $f(x) = x^3$, $x \in G$. Show that f is not an automorphism.*

Sol. $a, a^5 \in$ G and $a \neq a^5$.

Also, $\qquad f(a) = a^3$ and

$$f(a^5) = (a^5)^3 = a^{15} = a^{12}\, a^3 = ea^3 = a^3$$

$\therefore \qquad f(a) = f(a^5) \quad \therefore$ f is not one-one.

$\therefore$ f is not an automorphism.

Example 3. *Let G be the group of positive real numbers under multiplication. Let $\phi : G \to G$ be defined by $\phi(x) = x^2$, $x \in G$. Show that ϕ is an automorphism.*

Sol. We have $\phi(x) = x^2$, $x \in$ G.

ϕ is a homomorphism. Let $x, y \in$ G.

$$\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\, \phi(y).$$

$\therefore$ ϕ is a homomorphism from G to G.

ϕ is one-one. Let $x, y \in$ G and $\phi(x) = \phi(y)$.

$\Rightarrow \qquad x^2 = y^2 \quad \Rightarrow \quad x = \pm\, y \quad \Rightarrow \quad x = y \quad (\because\ x, y$ are both +ve)

$\therefore \qquad \phi(x) = \phi(y) \quad \Rightarrow \quad x = y \quad \therefore$ ϕ is one-one.

ϕ is onto. Let $x \in$ G.

$\therefore$ x is a +ve real number.

$\therefore$ $\sqrt{x}$ is also a +ve real number.

We have $\qquad \phi(\sqrt{x}) = (\sqrt{x})^2 = x \quad \therefore$ ϕ is onto.

$\therefore$ ϕ is an automorphism of G.

Example 4. *Let G be a group. Show that the mapping $x \to x^{-1}$ from G to G is an automorphism if and only if G is abelian.*

Sol. Let $f : G \to G$ be the mapping defined by $f(x) = x^{-1}$, $x \in G$. Let the group G be abelian.

f is well defined. Since inverse of an element is unequally defined, the mapping f is well defined.

f is a homomorphism. Let $x, y, \in G$.

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y) \qquad (\because \quad y^{-1}x^{-1} = x^{-1}y^{-1})$$

$\therefore$ f is a homomorphism.

f is one-one. Let $x, y \in G$ and $f(x) = f(y)$.

$$\Rightarrow \qquad x^{-1} = y^{-1} \;\Rightarrow\; (x^{-1})^{-1} = (y^{-1})^{-1} \;\Rightarrow\; x = y.$$

$\therefore$ f is one-one.

f is onto. Let $x \in G$.

$$\therefore \qquad x^{-1} \in G \text{ and } f(x^{-1}) = (x^{-1})^{-1} = x$$

$\therefore$ f is onto.

$\therefore$ f is an automorphism of the group G.

Conversely, let f be an automorphism of group G. Let $x, y \in G$.

$$\therefore \qquad f(xy) = f(x)f(y) = x^{-1}y^{-1} = (yx)^{-1} = f(yx)$$

Since f is one-one, we have $xy = yx$.

$\therefore$ The group G is abelian.

Example 5. *Let G be any abelian group in which $a^2 \neq e$ for some $a \in e$ for some $a \in G$. Show that G has non-trivial automorphisms.*

Sol. Define $f : G \to G$ by $f(x) = x^{-1}$, $x \in G$.

Since G is abelian, f is an automorphism.

If possible, let be the trivial automorphism.

$$\therefore \qquad f(x) = i(x) \;\forall\; x \in G$$

$\therefore$ In particular, $f(a) = i(a)$

$\Rightarrow$ $a^{-1} = a \;\Rightarrow\; aa^{-1} = aa \;\Rightarrow\; a^2 = e$, which is impossible.

$\therefore$ f is a non-trivial automorphism of G.

$\therefore$ G has nontrivial automorphisms.

Theorem 1. *Let f be an automorphism of a group G. If H is a subgroup of group G, then f(H) is also a subgroup of G.*

Proof. We have $f(H) = \{f(h) : h \in H\}$.

$$e \in H \Rightarrow f(e) \in f(H) \quad \therefore \quad f(H) \neq \phi$$

Let $\qquad f(h_1), f(h_2) \in f(H)$

Now $\qquad f(h_1)(f(h_2))^{-1} = f(h_1)\, f(h_2^{-1}) = f(h_1h_2^{-1}) \in f(H)$

$$(\because \quad h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H)$$

$\therefore$ $f(H)$ is a subgroup of G.

Theorem 2. *Let f be an automorphism of a group G. If N is a normal subgroup of group G, then f(N) is also a normal subgroup of G.*

Proof. We have $f(N) = \{f(n) : n \in N\}$.

$$e \in N \Rightarrow f(e) \in f(N) \quad \therefore \quad f(N) \neq \phi$$

Let $\qquad f(n_1), f(n_2) \in f(N)$

Now $\quad f(n_1)\,(f(n_2))^{-1} = f(n_1)f(n_2^{-1}) = f(n_1n_2^{-1}) \in f(\text{N})$

$$(\because\ n_1, n_2 \in \text{N} \;\Rightarrow\; n_1n_2^{-1} \in \text{N})$$

$\therefore\;$ $f(\text{N})$ is a subgroup of G.

Let $f(n) \in f(\text{N})$ and $g \in \text{G}$. Since f is onto, there exists $x \in \text{G}$ such that $g = f(x)$.

Now $\quad gf(n)\,g^{-1} = f(x)\,f(n)\,(f(x))^{-1} = f(x)\,f(n)\,f(x^{-1}) = f(xnx^{-1}) \in f(\text{N})$

$$(\because\ n \in \text{N}, x \in \text{G} \;\Rightarrow\; xnx^{-1} \in \text{N})$$

$\therefore\;$ $f(\text{N})$ is a normal subgroup of G.

Example 6. *Let G be a group and Z, the centre of G. If f is any automorphism of G, show that $f(Z) \subseteq Z$.*

Sol. We have $\quad \text{Z} = \{z \in \text{G} : zx = xz \ \forall\ x \in \text{G}\}$.

Let $f(z) \in f(\text{Z})$. Let x be any element of G. Since f is onto, there exists $y \in \text{G}$ such that $f(y) = x$.

Now $\quad f(z) \in f(\text{Z}) \;\Rightarrow\; z \in \text{Z}$

$\Rightarrow \quad zy = yz \;\Rightarrow\; f(zy) = f(yz)$

$\Rightarrow \quad f(z)\,f(y) = f(y)\,f(z) \Rightarrow f(z)x = x\,f(z)$

$\therefore \quad f(z) \in \text{Z} \qquad \therefore\; f(\text{Z}) \subseteq \text{Z}.$

Example 7. *Let G be a group and f, an automorphism of G. If for $a \in G$,*

$N(a) = \{x \in G : ax = xa\}$, show that $N(f(a)) = f(N(a))$.

Sol. We have $\text{N}(a) = \{x \in \text{G} : ax = xa\}$.

$\therefore \quad \text{N}(f(a)) = \{x \in \text{G} : f(a)\,x = xf(a)\}$

Let $\quad x \in \text{N}(f(a))$.

$\Rightarrow \quad f(a)x = xf(a) \;\Rightarrow\; f(a)\,f(y) = f(y)f(a) \qquad$ (Taking $x = f(y)$, $y \in \text{G}$)

$\Rightarrow \quad f(ay) = f(ya) \;\Rightarrow\; ay = ya \qquad (\because\ f$ is one-one)

$\Rightarrow \quad y \in \text{N}(a) \;\Rightarrow f(y) \in f(\text{N}(a))$ *i.e.*, $x \in f(\text{N}(a))$

$\therefore \quad \text{N}(f(a)) \subseteq f(\text{N}(a))$.

Now, let $\quad b \in f(\text{N}(a)) \quad \therefore\; \exists\, c \in \text{N}(a) : f(c) = b$

$c \in \text{N}(a) \;\Rightarrow\; ac = ca$

$\Rightarrow \quad f(ac) = f(ca) \;\Rightarrow\; f(a)\,f(c) = f(c)\,f(a)$

$\Rightarrow \quad f(a)b = bf(a) \;\Rightarrow\; b \in \text{N}(f(a))$

$\therefore \quad f(\text{N}(a)) \subseteq \text{N}(f(a))$.

Combining, we get $\text{N}(f(a)) = f(\text{N}(a))$.

2.7. INNER AUTOMORPHISM

Let G be a group and let a be any arbitrary but fixed element of G.

Let f_a be a mapping from G into G defined by $\;f_a(x) = a^{-1}xa,\;\; x \in \text{G}$.

f_a is well defined. Let $x, y \in \text{G}$.

$$x = y \;\Rightarrow\; a^{-1}xa = a^{-1}ya \;\Rightarrow\; f_a(x) = f_a(y)$$

$\therefore\;$ f_a is well defined.

$\mathbf{f_a}$ **is a homomorphism.** Let $x, y \in G$.

$$f_a(xy) = a^{-1}(xy)a = a^{-1}(x(aa^{-1})y)a = (a^{-1}xa)(a^{-1}ya) = f_a(x)\, f_a(y)$$

$\therefore$ f_a is a homomorphism.

$\mathbf{f_a}$ **is one-one.** Let $x, y \in G$ and $f_a(x) = f_a(y)$

$\Rightarrow$ $a^{-1}xa = a^{-1}ya \quad \Rightarrow \quad a(a^{-1}xa)\, a^{-1} = a(a^{-1}ya)\, a^{-1}$

$\Rightarrow$ $(aa^{-1})\, x(aa^{-1}) = (aa^{-1})\, y(aa^{-1}) \quad \Rightarrow \quad exe = eye \quad \Rightarrow \quad x = y.$

$\therefore$ f_a is one-one.

$\mathbf{f_a}$ **is onto.** Let $x \in G$.

$\therefore$ $axa^{-1} \in G$ and

$$f_a(axa^{-1}) = a^{-1}(axa^{-1})a = (a^{-1}a)x(a^{-1}a) = exe = x$$

$\therefore$ Given $x \in G$, $\exists\, axa^{-1} \in G : f_a(axa^{-1}) = x$.

$\therefore$ f_a is onto.

$\therefore$ f_a is an automorphism of G.

For $a \in G$, the automorphism $f_a(x) = a^{-1}xa$, $x \in G$ is called an **inner automorphism** of the group G corresponding to the element a.

An automorphism which is not an inner automorphism is called an **outer automorphism**.

Example 8. *Let G be the additive group of the integers. Find the inner automorphism of G corresponding to the element 5 of G.*

Sol. The inner automorphism f_a of group G corresponding to the element a of G is defined as $f_a(x) = a^{-1}xa\ \forall\ x \in G$.

In this particular case, the binary operation is '+'.

$\therefore$ $f_5(x) = (-5) + x + 5 \quad \forall\ x \in G$

i.e., $\mathbf{f_5(x) = x \quad \forall\ x \in G.}$

Example 9. *Given an example of a group in which the inner automorphism corresponding to two distinct elements of the group may be same.*

Sol. Let $G = \{1, -1, i, -i\}$. G is a group with usual multiplication as the binary operation.

$1 \in G$ and $f_1(x) = (1)^{-1}\, x\, (1) \quad \forall\ x \in G$

$\therefore$ $f_1(x) = (1)\, x\, (1) = x \quad \forall\ x \in G$

Also, $-1 \in G$ and $f_{-1}(x) = (-1)^{-1}\, (x)\, (-1) \quad \forall\ x \in G$

$\therefore$ $f_{-1}(x) = (-1)\, x\, (-1) = x \quad \forall\ x \in G.$

$\therefore$ $f_1 = f_{-1}$.

2.8. GROUP OF AUTOMORPHISMS

Let G be a group and let A(G) be the set of all automorphisms of G. We shall show that the set A(G) is a group with respect to composition of functions as the binary operation.

Let $f, g \in A(G)$.

For $x \in G$, $(fg)^*(x) = f(g(x)) \in G$

$\therefore$ fg is a mapping from G to G. Let $x, y \in$ G.

$\therefore$ $(fg)(xy) = f(g(xy)) = f(g(x)\, g(y)) = f(g(x))\, f(g(y)) = (fg)(x)(fg)(y).$

$\therefore$ fg is a homomorphism.

Let $x, y \in$ G and $(fg)(x) = (fg)(y)$.

$\Rightarrow$ $f(g(x)) = f(g(y)) \Rightarrow g(x) = g(y)$ ($\because$ f is one-one)

$\Rightarrow$ $x = y$. ($\because$ g is one-one)

$\therefore$ fg is one-one.

Let $x \in$ G. Since f is onto, $\exists\, y \in \text{G} : f(y) = x$.

Also, $y \in$ G and g is onto, so $\exists\, z \in \text{G} : g(z) = y$.

$\therefore$ $x = f(y) = f(g(z)) = (fg)(z)$

$\therefore$ Given $x \in \text{G}, \exists\, z \in \text{G} : (fg)(z) = x$.

$\therefore$ fg is onto.

$\therefore$ fg is an automorphism of the group G *i.e.*, $fg \in$ A(G).

$\therefore$ Composition of functions is a binary operation on A(G).

Associativity. Let $f, g, h \in$ A(G).

For $x \in$ G, $(f(gh))(x) = f(gh(x)) = f(g(h(x)))$

Also $((fg)h)(x) = (fg)(h(x)) = f(g(h(x))$

$\therefore$ $(f(gh))(x) = ((fg)h)(x). \quad \forall\, x \in \text{G}$

$\therefore$ $f(gh) = (fg)h \quad \forall\, f, g, h \in \text{A(G)}.$

Existence of identity. Let the identity function on G be denoted by i.

$\therefore$ i is one-one onto.

Also, for $x, y \in$ G, we have $i(xy) = xy = i(x)\, i(y)$.

$\therefore$ i is an automorphism of G *i.e.*, $i \in$ A(G).

Also, for $f \in$ A(G),

$$(fi)(x) = f(i(x)) = f(x) \quad \text{and} \quad (if)(x) = i(f(x)) = f(x).$$

$\therefore$ $(fi)(x) = f(x) = (if)(x) \quad \forall\, x \in \text{G}$

$\therefore$ $fi = f = if \quad \forall\, f \in \text{A(G)}.$

$\therefore$ 'i' is the identity of A(G).

Existence of inverse. Let $f \in$ A(G)

$\therefore$ f is one-one mapping of G onto G.

$\therefore$ f^{-1} exists and is also one-one onto.

Let $x, y \in$ G.

Let $f^{-1}(x) = x'$ and $f^{-1}(y) = y'$.

$\therefore$ $f(x') = x$ and $f(y') = y$

$\therefore$ $f^{-1}(xy) = f^{-1}(f(x')\, f(y')) = f^{-1}(f(x'y')) = (f^{-1}f)(x'y') = i(x'y') = x'y' = f^{-1}(x)\, f^{-1}(y).$

$\therefore$ f^{-1} is a homomorphism.

$\therefore$ f^{-1} is an automorphism of G *i.e.*, $f^{-1} \in$ A(G).

Also $ff^{-1} = i = f^{-1}f$

$\therefore$ f^{-1} is the inverse of f.

*For the sake of simplicity, we have written fog as fg.

$\therefore$ A(G) is a group with composition of mappings as the binary operation. The group A(G) is called the **group of automorphisms** of the group G.

Example 10. *Let G be a cyclic group of order 4. Show that the group of automorphisms of G is of order 2.*

Sol. Let $\quad G = \{e, a, a^2, a^3\}$, where $a^4 = e$.

$\therefore \quad o(e) = 1, o(a) = 4, o(a^2) = 2, o(a^3) = 4$

$(\because \quad (a^2)^2 = a^4 = e \,;\, a^3 \neq e, (a^3)^2 = a^6 = a^2 \neq e, (a^3)^3 = a^9 = a \neq e, (a^3)^4 = a^{12} = e)$

Let f be an automorphism of G.

$\therefore \quad o(f(b)) = o(b) \ \forall \ b \in G$

$\Rightarrow \quad f(e) = e$

$f(a) = a$ or $a^3 \qquad (\because \quad o(a) = o(a^3) = 4)$

$f(a^2) = a^2 \qquad (\because$ There is only one element of order 2)

$f(a^3) = a$ or a^3

Since an automorphism is also 1 – 1 and onto, we have only two possible automorphisms, say ϕ and ψ defined as :

$$\phi(e) = e, \phi(a) = a, \phi(a^2) = a^2, \phi(a^3) = a^3$$

and
$$\psi(e) = e, \psi(a) = a^3, \psi(a^2) = a^2, \psi(a^3) = a.$$

$\therefore \quad o(A(G)) = 2.$

2.9 CHARACTERISTIC SUBGROUP

A subgroup H of a group G is called a **characteristic subgroup** of the group G if $f(H) \subseteq H \quad \forall \ f \in A(G)$.

Example 11. *Let $G = \{e, a, a^2, a^3\}$ be a cyclic group of order 4. Show that $H = \{e, a^2\}$ is a characteristic subgroup of G.*

Sol. Since G is a cyclic group of order 4, we have $A(G) = \{\phi, \psi\}$, where

$$\phi(e) = e, \phi(a) = a, \quad \phi(a^2) = a^2, \phi(a^3) = a^3$$

and
$$\psi(e) = e, \psi(a) = a^3, \psi(a^2) = a^2, \psi(a^3) = a.$$

$\therefore \quad \phi(H) = \{\phi(e), \phi(a^2)\} = \{e, a^2\} = H$

and $\quad \psi(H) = \{\psi(e), \psi(a^2)\} = \{e, a^2\} = H.$

$\therefore$ H is a characteristic subgroup of G.

Example 12. *Show that every subgroup of a finite cyclic group is a characteristic subgroup.*

Sol. Let $\quad G = (a)$ be a finite cyclic group of order n.

$\therefore \quad G = \{a^0 \,(= e), a, a^2, \ldots\ldots, a^{n-1}\}$

Let H be any subgroup of G.

$\therefore$ $H = (a^m)$ for some integer m, where $0 \le m < n$. Let f be any automorphism of G.

$\therefore \quad f(a) \in G$. Let $f(a) = a^k$ for some k such that $0 \le k < n$.

Let $\quad h \in H. \quad \therefore \quad h = (a^m)^l$ for some integer l

Now $\quad f(h) = f((a^m)^l) = f(a^{ml})$

$= (f(a))^{ml} = (a^k)^{ml} = a^{kml}$

$= (a^m)^{kl} \in \text{H}$

NOTES

$\therefore\;$ $f(h) \in \text{H} \;\forall f \in \text{A(G)}, h \in \text{H}$

$\therefore\;$ H is a characteristic subgroup of G.

Example 13. *Show that a characteristic subgroup of a group G is a normal subgroup of G.*

Sol. Let H be a characteristic subgroup of group G.

$\therefore\;$ H is a subgroup of G and $f(\text{H}) \subseteq \text{H} \;\forall f \in \text{A(G)}$.

$\Rightarrow \quad f(h) \in \text{H} \quad \forall f \in \text{A(G)}$ and $h \in \text{H}$ ...(1)

Let $\quad h \in \text{H}$ and $g \in \text{G}$.

$\therefore \quad ghg^{-1} = (g^{-1})^{-1}\, hg^{-1} = f_{g^{-1}}\,(h)$,

where $f_{g^{-1}}$ is the inner automorphism of G corresponding to g^{-1}.

$\therefore\;$ Using (1), $f_{g^{-1}}\,(h) \in \text{H}$

$\Rightarrow \quad ghg^{-1} \in \text{H} \;\forall\; h \in \text{H}$ and $g \in \text{G}$

$\therefore\;$ H is a normal subgroup of G.

Example 14. *Let S be the conjugate class of a non-identity element of a group G. Let $\phi \in A(G)$. Show that $\phi(S)$ is a slwo the conjugate class of some non-identity element of G.*

Sol. Let S be the conjugate class of $a(\neq e) \in \text{G}$.

$\therefore \quad \text{S} = \{x^{-1}ax : x \in \text{G}\}$

$\therefore \quad \phi(\text{S}) = \{\phi(x^{-1}ax) : x \in \text{G}\}$

Now $\quad \phi(x^{-1})\, \phi(a)\, \phi(x) = (\phi(x))^{-1}\, \phi(a)\, \phi(x)$

$\therefore\;$ $\phi(x^{-1}ax)$ is a conjugate of $\phi(a)$, because $\phi(x) \in \text{G}$.

$\therefore\;$ $\phi(\text{S}) \subseteq \text{C}[\phi(a)]$ Similarly, $\text{C}[\phi(a)] \subseteq \phi(s)$.

$\therefore\;$ $\phi(\text{S}) = \text{C}[\phi(a)]$ *i.e.*, $\phi(\text{S})$ is the conjugate class of non-trivial element $\phi(a)$ of G.

$\phi(a) = e \;\Rightarrow\; \phi(a) = \phi(e) \;\Rightarrow\; a = e$, which is not true.)

Example 15. *Let G be a finite cyclic group of order n. Show that $o(A(G)) = \phi(n)$, where ϕ is the Euler's function.*

Sol. Let $\quad \text{G} = (a)$.

$\therefore \quad o(a) = n \quad \text{G} = \{a^0(= e), a^1, a^2, \ldots\ldots\, a^{n-1}\}$

Let $\quad f \in \text{A(G)}$

$\therefore\;$ $f(a^k) = (f(a))^k$ for $k \in \mathbf{Z}$

$\therefore\;$ f is completely known, if we know $f(a)$.

Let $\;f(a) = a^m \in \text{G}$, where m is some integer such that $0 \in m < n$.

Since f is an automorphism,

$$(f(a))^n = f(a^n) = f(e) = e.$$

$\therefore \quad o(f(a)) \leq n$

If possible, let $\;o(f(a)) = \lambda, \quad 0 \leq \lambda < n$

$\therefore \quad (f(a))^\lambda = e \quad \text{or} \quad f(a^\lambda) = f(e) \quad \text{or} \quad a^\lambda = e$

$\therefore\quad o(a) < n,$ which is impossible.

$\therefore\qquad o(f(a)) = n$

Let $\qquad (m, n) = d$, where $d \geq 1$. Let $d > 1$.

$\therefore\qquad (f(a))^{n/d} = (a^m)^{n/d} = (a^n)m/d = (e)^{m/d} = e$

$\therefore\quad o(f(a)) < n$, which is impossible. $\qquad (\because\quad n/d < n)$

$\therefore\quad d$ cannot be greater than 1 and we have $d = 1\quad$ *i.e.*, $\quad (m, n) = 1$

$\therefore\quad$ If $f \in A(G)$, then $f(a) = a^m$, where $(m, n) = 1$.

$\therefore\qquad o(A(G)) = \phi(n)$.

Theorem 3. *The set I(G) of all inner automorphisms of a group G is a normal subgroup of the group A(G) of automorphisms of G.*

Proof. The elements of I(G) are also automorphisms of the group G.

$\therefore\qquad I(G) \subseteq A(G)$

The identity mapping (i) of G is an inner automorphism of G because for $x \in G$

$$i(x) = x = e^{-1}xe = f_e(x).\quad \therefore\quad I(G) \neq \phi.$$

Let $\qquad f_a, f_b \in I(G)$.

For $\quad x \in G, (f_b f_{b^{-1}})(x) = f_b(f_{b^{-1}}(x)) = f_b((b^{-1})^{-1}\ xb^{-1}) = f_b(bxb^{-1})$

$$= b^{-1}(bxb^{-1})\ b = (b^{-1}b)\ x\ (b^{-1}b) = exe = x = i(x)$$

Also $\qquad (f_{b^{-1}}f_b)(x) = f_{b^{-1}}(f_b(x)) = f_{b^{-1}}(b^{-1}xb) = (b^{-1})^{-1}(b^{-1}xb)(b^{-1})$

$$= (bb^{-1})\ x\ (bb^{-1}) = exe = x = i(x)$$

$\therefore\qquad (f_b f_{b^{-1}})(x) = i(x) = (f_{b^{-1}}f_b)(x)\ \ \forall\ \ x \in G$

$\Rightarrow\qquad f_b f_{b^{-1}} = i = f_{b^{-1}}f_b\ \ \Rightarrow\ \ (f_b)^{-1} = f_{b^{-1}}.$

Now for $x \in G$,

$$(f_a(f_b)^{-1})(x) = (f_a f_{b^{-1}})(x) = f_a(f_{b^{-1}}(x)) = f_a((b^{-1})^{-1}\ x\ b^{-1}) = f_a(bxb^{-1})$$

$$= a^{-1}(bxb^{-1})\ a = (a^{-1}b)\ x\ (b^{-1}\ a) = (b^{-1}\ a)^{-1}\ x\ (b^{-1}\ a) = f_{b^{-1}a}(x)$$

$\therefore\qquad (f_a(f_b)^{-1})(x) = f_{b^{-1}a}(x)\ \forall\ x \in G$

$\therefore\qquad f_a(f_b)^{-1} = f_{b^{-1}a}$

$\therefore\qquad f_a(f_b)^{-1} \in I(G) \qquad (\because\ \ a, b \in G \Rightarrow b^{-1}a \in G \Rightarrow f_{b^{-1}a} \in I(G))$

$\therefore\quad$ I(G) is a subgroup of A(G).

Let $\qquad f_a \in I(G)\quad$ and $\quad f \in A(G)$.

For $x \in G$, $\quad (ff_a f^{-1})(x) = (ff_a)(f^{-1}(x)) = f(f_a(f^{-1}(x)))$

$$= f(a^{-1}f^{-1}(x)\ a) = f(a^{-1})\ f(f^{-1}(x))\ f(a) = f(a^{-1})\ (ff^{-1})(x)\ f(a)$$

$$= f(a^{-1})x\ f(a) = (f(a))^{-1}\ x\ f(a) = f_{f(a)}(x). \qquad (\because\quad ff^{-1} = i)$$

$\therefore \qquad ff_a f^{-1} = f_{f(a)}$

$\therefore \qquad ff_a f^{-1} \in I(G) \qquad (\because \; f(a) \in G \Rightarrow f_{f(a)} \in I(G))$

$\therefore$ I(G) is a normal subgroup of A(G).

Example 16. *If $G = S_3$, show that $I(G) \cong G$.*

Sol. We have $G = S_3$ and S_3 is the set of all one-to-one mappings of the set $\{a, b, c\}$ onto itself.

$$\therefore \qquad S_3 = \{I, (a\ b), (b\ c), (a\ c), (a\ b\ c), (a\ c\ b)\}$$

We have already seen that the centre Z of S_3 is $\{I\}$.

Also, $\qquad I(G) \cong G/Z$

$\therefore \qquad I(G) \cong G/\{I\}$

$\therefore \qquad I(G) \cong G$ because $G/\{I\} \cong G$.

Remark: For the above group, we have

$$I(G) = \{f_1, f_{(a\ b)}, f_{(b\ c)}, f_{(a\ c)}, f_{(a\ b\ c)}\}.$$

SUMMARY

- Let f be an automorphism of a group G. If H is a subgroup of group G, then f(H) is also a subgroup of G.
- Let f be an automorphism of a group G. If N is a normal subgroup of group G, then f(N) is also a normal subgroup of G.
- For an abelian group, the only inner automorphism is the identity mapping whereas for non-abelian groups there exists non-trivial inner automorphisms.
- The set I(G) of all inner automorphism of a group G is a normal subgroup of the group A(G) of automorphisms of G.
- If I(G) is the set of all inner automorphisms of a group G and Z its centre, then $I(G) \cong G/Z$.

REVIEW QUESTIONS

1. Show that the identity mapping on a group G is an automorphism.
2. Let G be the group of integers under addition. Show that the mapping $\phi : G \to G$ defined by $\phi(x) = -x, x \in G$ is an automorphism.
3. Let G be the group of complex numbers under addition. Show that the mapping $\phi : G \to G$ defined by $\phi(z) = \bar{z}$, $z \in G$ is an automorphism.
4. If G is a cyclic group of order 12. find the set of all automorphisms of the group G.
5. Let G be a finite group. Let f be an automorphism of G with the property : $f(x) = x$ for $x \in G$ if and only if $x = e$. Show that every $g \in G$ can be expressed as $(f(x))x^{-1}$ for some $x \in G$.
6. Let G be a finite group. Let f be an automorphism of G with the property : $f(x) = x$ for $x \in G$ if and only if $x = e$. If $f^2 = I$, then show that G is abelian.
7. In the group $\{1, -1, i, -i\}$ with respect to usual multiplication, show that inner automorphisms of the group corresponding to i and $-i$ are identical.

8. Let G be a group and ϕ an automorphism of G. If $a \in G$ is of finite order, then $o(\phi(a)) = o(a)$.

9. Let G be a finite cyclic group of order n. If the mapping $f : x \to x^m$, $x \in G$ is an automorphism, show that $(m, n) = 1$.

10. Show that the group of automorphism of a cyclic group is abelian.

11. Let G be an abelian group. Show that $H = \{x \in G : x^n = e, n \text{ being a fixed integer}\}$ is a characteristic group of G.

12. If G is a group, N a normal subgroup of G, H a characteristic subgroup of N, show that H is a normal subgroup of G.

NOTES

UNIT

3

STRUCTURE THEOREM FOR FINITE ABELIAN GROUPS

STRUCTURE

3.0 LEARNING OBJECTIVES

After going through this unit, you should be able to:

- direct product
- exponent of a group
- structure theorem for finite Abelian group.

3.1. INTRODUCTION

In this chapter, we shall prove a very important famous classical theorem called **'structure theorem for finite abelian groups'.** This theorem is also known as the **'Fundamental theorem on finite abelian groups'**. For this purpose, we require the concepts of external direct product and internal direct product.

3.2. EXTERNAL DIRECT PRODUCT

Let $G_1, G_2, ..., G_n$ be any n groups. Let G be the cartesian product $G_1 \times G_2 \times ...... \times G_n$ of the groups $G_1, G_2, ..., G_n$.

$\therefore \quad G = G_1 \times G_2 \times ...... \times G_n = \{(a_1, a_2, ..., a_n) : a_i \in G_i, 1 \le i \le n\}$.

For $(a_1, a_2, ..., a_n), (b_1, b_2, ..., b_n) \in G$, we define the product

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) \text{ as } (a_1b_1, a_2b_2, ..., a_nb_n).$$

where the product a_ib_i in the ith component is the product of the elements a_i and b_i as calculated in the group G_i.

$\therefore$ This product is well defined binary operation on $G_1 \times G_2 \times ...... \times G_n$ *i.e.*, on G.

Now we shall show that G is a group relative to this product.

Let $\quad a = (a_1, a_2, ..., a_n), b = (b_1, b_2, ..., b_n),$

$\quad c = (c_1, c_2, ..., c_n) \in G.$

Associativity.

$$\begin{aligned} a(bc) &= (a_1, a_2, ..., a_n)((b_1, b_2, ..., b_n)(c_1, c_2, ..., c_n)) \\ &= (a_1, a_2, ..., a_n)(b_1c_1, b_2c_2, ..., b_nc_n) \\ &= (a_1(b_1c_1), a_2(b_2c_2), ..., a_n(b_nc_n)) \\ &= ((a_1b_1)c_1, (a_2b_2)c_2, ..., (a_nb_n)c_n) \\ &= (a_1b_1, a_2b_2, ..., a_nb_n)(c_1, c_2, ..., c_n) \\ &= ((a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n))(c_1, c_2, ..., c_n) = (ab)c. \end{aligned}$$

$\therefore \quad a(bc) = (ab)c.$

Existence of identity. Let $e = (e_1, e_2, ..., e_n)$, where e_i is the identity of the group G_i, $1 \le i \le n$.

Now $\quad ae = (a_1, a_2, ..., a_n)(e_1, e_2, ..., e_n) = (a_1e_1, a_2e_2, ..., a_ne_n)$

$\quad = (a_1, a_2, ..., a_n) = a$

Also $\quad ea = (e_1, e_2, ..., e_n)(a_1, a_2, ..., a_n) = (e_1a_1, e_2a_2, ..., e_na_n)$

$\quad = (a_1, a_2, ..., a_n) = a$

$\therefore \quad ae = a = ea \quad \forall\, a \in G$

$\therefore \quad e = (e_1, e_2, ..., e_n)$ is the identity of G.

Existence of inverse. For $a = (a_1, a_2, ..., a_n)$, let $a' = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$, where a_i^{-1} is the inverse of a_i in the group G_i, $1 \le i \le n$.

Now $\quad aa' = (a_1, a_2, ..., a_n)(a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$

$\quad = (a_1a_1^{-1}, a_2a_2^{-1}, ..., a_na_n^{-1}) = (e_1, e_2, ..., e_n) = e.$

Also $\quad a'a = (a_1^{-1}, a_2^{-1}, ..., a_n^{-1})(a_1, a_2, ..., a_n)$

$\quad = (a_1^{-1}a_1, a_2^{-1}a_2, ..., a_n^{-1}a_n) = (e_1, e_2, ..., e_n) = e$

$\therefore \quad aa' = e = a'e$

$\therefore$ a' is the inverse of the element a of G.

$\therefore$ $G = G_1 \times G_2 \times ...... \times G_n$ is a group under the binary operation defined by

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n)$$

for $\quad (a_1, a_2, ..., a_n), (b_1, b_2, ..., b_n) \in G.$

This group is called the **group of external direct product** of the groups G_1, G_2, ..., G_n.

Remark. The external direct product $G_1 \times G_2 \times ...... \times G_n$ of the groups $G_1, G_2, ..., G_n$ is abelian if and only if the groups $G_1, G_2, ..., G_n$ are all abelian.

For example, let $G = \mathbf{R}^\circ \times \mathbf{R}^\circ \times \mathbf{R}^\circ$, where $\mathbf{R}^\circ$ is the set of all non-zero real numbers.

We know that $\mathbf{R}^\circ$ is a group under usual multiplication.

For $(a_1, a_2, a_3), (b_1, b_2, b_3) \in G$, we define $(a_1, a_2, a_3)(b_1, b_2, b_3) = (a_1b_1, a_2b_2, a_3b_3)$.

Under this binary operation, G is an abelian group. The identity of G is (1, 1, 1) and the inverse of the element (x, y, z) is G is $\left(\frac{1}{x}, \frac{1}{y}, \frac{1}{z}\right)$.

Example 1. *Let G_1 be the group of integers under usual addition and G_2 be the group of non-zero real numbers under usual multiplication. Show that the external direct product $G_1 \times G_2$ is a group.*

Sol. We have $\quad G_1 \times G_2 = \{(a_1, a_2) : a_1 \in \mathbf{Z}, a_2 \in \mathbf{R}^\circ\}$

For $\quad (a_1, a_2), (b_1, b_2) \in G_1 \times G_2$, define $(a_1, a_2)(b_1, b_2) = (a_1 + b_1, a_2b_2) \in G_1 \times G_2$.

Associativity. Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$.

$$\begin{aligned}\therefore\ (a_1, a_2)((b_1, b_2)(c_1, c_2)) &= (a_1, a_2)(b_1 + c_1, b_2c_2)\\ &= (a_1 + (b_1 + c_1), a_2(b_2c_2)) = ((a_1 + b_1) + c_1, (a_2b_2)c_2)\\ &= (a_1 + b_1, a_2b_2)(c_1, c_2) = ((a_1, a_2)(b_1, b_2))(c_1, c_2)\end{aligned}$$

$\therefore$ The product of $G_1 \times G_2$ is associative.

Existence of identity. $(0, 1) \in G_1 \times G_2$. Let $(a_1, a_2) \in G_1 \times G_2$.

Now $\quad (a_1, a_2)(0, 1) = (a_1 + 0, a_2 . 1) = (a_1, a_2)$

and $\quad (0, 1)(a_1, a_2) = (0 + a_1, 1.a_2) = (a_1, a_2)$.

$\therefore \quad (a_1, a_2)(0, 1) = (a_1, a_2) = (0, 1)(a_1, a_2)$

$\therefore$ (0, 1) is the identity of $G_1 \times G_2$.

Existence of inverse. Let $(a_1, a_2) \in G_1 \times G_2$.

$\therefore \quad a_1 \in \mathbf{Z}, a_2 \in \mathbf{R}^\circ$.

$\therefore \quad -a_1 \in \mathbf{Z}$ and $a_1 + (-a_1) = 0 = (-a_1) + a_1$

Also $\quad \frac{1}{a_2} \in \mathbf{R}^\circ$ and $a_2 . \frac{1}{a_2} = 1 = \frac{1}{a_2} . a_2$.

$$\text{Now } (a_1, a_2)\left(-a_1, \frac{1}{a_2}\right) = \left(a_1 + (-a_1), a_2 . \frac{1}{a_2}\right) = (0, 1)$$

$$\text{and} \quad \left(-a_1, \frac{1}{a_2}\right)(a_1, a_2) = \left((-a_1) + a_1, \frac{1}{a_2} . a_2\right) = (0, 1)$$

$\therefore \quad \left(-a_1, \frac{1}{a_2}\right)$ is the inverse of (a_1, a_2).

$\therefore \quad G_1 \times G_2$ is a group.

Let $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$.

$\therefore$ $(a_1, a_2)(b_1, b_2) = (a_1 + b_1, a_2 b_2) = (b_1 + a_1, b_2 a_2) = (b_1, b_2)(a_1, a_2)$

$\therefore$ The external direct product $G_1 \times G_2$ of groups G_1 and G_2 is an abelian group.

Example 2. *Show that $G_1 \times G_2$ is an abelian group if and only if G_1 and G_2 are both abelian groups.*

Sol. Let $(g_1, g_2), (g_1', g_2') \in G_1 \times G_2$.

$G_1 \times G_2$ is abelian

iff $(g_1, g_2). (g_1', g_2') = (g_1', g'_2)(g_1, g_2)$

iff $(g_1 g_1', g_2 g_2') = (g_1' g_1, g_2' g_2)$

iff $g_1 g_1' = g_1' g_1$ and $g_2 g_2', g_2' g_2$

iff G_1 and G_2 are both abelian.

$\therefore$ The result holds.

Example 3. *If G_1 and G_2 be two cyclic groups of orders 2 and 3 respectively then show that the external direct product $G_1 \times G_2$ of G_1 and G_2 is also a cyclic group.*

Sol. Let $G_1 = (a)$ and $G_2 = (b)$.

$\therefore$ $G_1 = \{e_1, a\}$ and $G_2 = \{e_2, b, b^2\}$,

where e_1 and e_2 are the identities of G_1 and G_2 respectively.

Now $G_1 \times G_2 = \{(e_1, e_2), (e_1, b), (e_1, b^2), (a, e_2), (a, b), (a, b^2)\}$

$\therefore$ The external direct product $G_1 \times G_2$ is a group of order 6.

Since G_1. G_2 are abelian, the group $G_1 \times G_2$ is also abelian.

We have $o(a) = 2, o(b) = 3$.

Now $(a, b) \in G_1 \times G_2$ and $(a, b) \neq (e_1, e_2)$

$$(a, b)^2 = (a^2, b^2) = (e_1, b^2) \neq (e_1, e_2)$$

$$(a, b)^3 = (a^3, b^3) = (a^3, e_2) = (ae_1, e_2) = (a, e_2) \neq (e_1, e_2).$$

$\therefore$ $o((a, b)) > 3$.

Since $o((a, b))$ must divide $o(G_1 \times G_2)$ *i.e.*, 6, we must have $o((a, b)) = 6$.

$\therefore$ The group $G_1 \times G_2$ of order 6 contains an element of order 6.

$\therefore$ The external direct product $G_1 \times G_2$ must be a cyclic group.

Example 4. *Let G be any group and $H = \{(a, a) : a \in G\}$. Show that H is a subgroup of the group of external direct product $G \times G$. Further H is normal iff G is abelian.*

Sol. We have $H = \{(a, a) : a \in G\}$.

Let e be the identity of G.

$\therefore$ $(e, e) \in H$ $\therefore$ $H \neq \phi$

Let $(a, a), (b, b) \in H$

Now $(a, a)(b, b)^{-1} = (a, a)(b^{-1}, b^{-1}) = (ab^{-1}, ab^{-1}) \in H$

$(\because \; a, b \in G \Rightarrow ab^{-1} \in G)$

$\therefore$ H is a subgroup of $G \times G$.

Let G be abelian.

Let $(a, a) \in H$ and $(g_1, g_2) \in G \times G$.

$$\therefore (g_1, g_2)(a, a)(g_1, g_2)^{-1} = (g_1 a, g_2 a)(g_1^{-1}, g_2^{-1}) = (g_1 a g_1^{-1}, g_2 a g_2^{-1})$$

$$= (a g_1 g_1^{-1}, a g_2 g_2^{-1}) = (ae, ae) = (a, a) \in H$$

$\therefore$ H is a normal subgroup of $G \times G$.

Conversely, let H be a normal subgroup of G × G.

Let $a, b \in G$. ∴ $(a, b) \in G \times G$

∴ $(a, b)(a, a)(a, b)^{-1} \in H$ (∵ $(a, a) \in H$)

$\Rightarrow (a, b)(a, a)(a^{-1}, b^{-1}) \in H \quad \Rightarrow (aaa^{-1}, bab^{-1}) \in H$

$\Rightarrow (a, bab^{-1}) \in H \quad \Rightarrow a = bab^{-1} \quad \Rightarrow ab = (bab^{-1})\, b$

$\Rightarrow ab = ba(b^{-1} b) \quad \Rightarrow ab = ba.$

∴ G is abelian.

∴ The result holds.

Example 5. *If $G_1, G_2, ..., G_n$ be n group then show that*

$$Z(G_1 \times G_2 \times ...... \times G_n) = Z(G_1) \times Z(G_2) \times ...... \times Z(G_n).$$

Sol. We have

$$G_1 \times G_2 \times ...... \times G_n = \{(a_1, a_2, ..., a_n) : a_i \in G_i,\ 1 \le i \le n\}.$$

Let $(z_1, z_2, ..., z_n) \in Z(G_1 \times G_2 \times ...... \times G_n)$

$$\Rightarrow (z_1, z_2, ..., z_n)(a_1, a_2, ..., a_n) = (a_1, a_2, ..., a_n)(z_1, z_2, ..., z_n)$$
$$\forall\ (a_1, a_2, ..., a_n) \in G_1 \times G_2 \times ...... \times G_n$$

$$\Rightarrow (z_1a_1, z_2a_2, ..., z_na_n) = a_1z_1, a_2z_2, ..., a_nz_n)$$

$$\Rightarrow z_1a_1 = a_1z_1, \quad z_2a_2 = a_2z_2, ..., z_na_n = a_nz_n$$

$$\Rightarrow z_1 \in Z(G_1), \quad z_2 \in Z(G_2), ..., z_n \in Z(G_n).$$

Similarly, we can show that

$$z_1 \in Z(G_1), z_2 \in Z(G_2), ..., z_n \in Z(G_n)$$

implies $(z_1, z_2, ..., z_n) \in Z(G_1 \times G_2 \times ...... \times G_n).$

∴ The result holds.

3.3. INTERNAL DIRECT PRODUCT

A group G is said to be the **internal direct product** of its normal subgroups $N_1, N_2, ..., N_n$ if

(*i*) $G = N_1N_2 ...... N_n$

(*ii*) Given $g \in G$ then $g = m_1m_2 ...... m_n$, $m_i \in N_i$ in a unique way.

Theorem 1. *Let a group G be the internal direct product of its normal subgroups $N_1, N_2, ..., N_n$.*

Prove that for $i \ne j$,

(*i*) $N_i \cap N_j = \{e\}$ (*ii*) $a \in N_i,\ b \in N_j \Rightarrow ab = ba.$

Proof. (*i*) Let $x \in N_i \cap N_j$

$\Rightarrow x \in N_i$ and $x \in N_j$

$x \in N_i \Rightarrow x = e_1 ...... e_{i-1}xe_{i+1} ...... e_{j-1}e_je_{j+1} ...... e_n$

$x \in N_j \Rightarrow x = e_1 ...... e_{i-1}e_ie_{i+1} ...... e_{j-1}xe_{j+1} ...... e_n,$

where each $e_t = e$ in the expressions of x.

Since every element of G has a unique representation in the form $m_1 m_2 \ldots\ldots m_n$, where $m_i \in N_i$, we have $x = e$.

$\therefore \qquad N_i \cap N_j = \{e\} \quad \text{for} \quad i \neq j.$

(*ii*) Let $a \in N_i$, $b \in N_j$, where $i \neq j$.

$a \in N_i \;\Rightarrow\; a \in G$ and N_j is normal.

$\therefore \qquad a^{-1}ba \in N_j$

$\Rightarrow \qquad b^{-1}a^{-1}ba \in N_j$, because $b^{-1} \in N_j$

Also, $\quad b \in N_j \;\Rightarrow\; b \in G \quad$ and $\quad N_i$ is normal.

$\therefore \qquad ba^{-1}b^{-1} \in N_i \qquad\qquad (\because \; a \in N_i \;\Rightarrow\; a^{-1} \in N_i)$

$\Rightarrow \qquad aba^{-1}b^{-1} \in N_i \qquad\qquad (\because \; a \in N_i)$

$\Rightarrow \qquad aba^{-1}b^{-1} \in N_i \cap N_j$

$\Rightarrow \qquad aba^{-1}b^{-1} = e$

$\Rightarrow \qquad ab\,(ba)^{-1} = e \;\Rightarrow\; ab = ba$

This completes the proof.

Example 6. *Let a group G be the internal direct product of its normal subgroups N_1, N_2. Show that*

(*i*) $N_1 \cap N_2 = \{e\}$ $\qquad\qquad$ (*ii*) $ab = ba$ *for* $a \in N_1$, $b \in N_2$.

Sol. (*i*) Let $\qquad x \in N_1 \cap N_2$

$\Rightarrow \qquad x \in N_1, x \in N_2$

We have $\qquad x = ex \quad$ and $\quad x = xe.$

Since every element of G has a unique representation in the form $m_1 m_2$, where $m_1 \in N_1$, $m_2 \in N_2$, we have $x = e$

$\therefore \qquad N_1 \cap N_2 = \{e\}.$

(*ii*) Let $a \in N$ and $b \in N_2$.

$a \in N_1 \qquad \Rightarrow \quad a \in G$

$\therefore \qquad aba^{-1} \in N_2$

$\Rightarrow \qquad aba^{-1} \in N_2 \qquad\qquad (\because \; b \in N_2 \;\Rightarrow\; b^{-1} \in N_2)$

Also, $\qquad b \in N_2 \qquad \Rightarrow \quad b \in G$

$\therefore \qquad ba^{-1}b^{-1} \in N_1 \qquad\qquad (\because \; a \in N_1 \;\Rightarrow\; a^{-1} \in N_1)$

$\Rightarrow \qquad aba^{-1}b^{-1} \in N_1 \qquad \Rightarrow \quad aba^{-1}b^{-1} \in N_1 \cap N_2$

$\Rightarrow \qquad aba^{-1}b^{-1} = e \qquad \Rightarrow \quad ab(ba) = e$

$\Rightarrow \qquad ab = ba.$

Theorem 2. *Let a group G be the internal direct product of its normal subgroups N_1, N_2, ..., N_n. Show that*

$$G \cong N_1 \times N_2 \times \ldots\ldots \times N_n.$$

Proof. Define $\phi : N_1 \times N_2 \times \ldots\ldots \times N_n \to G$ by

$\phi\,((a_1, a_2, \ldots\ldots, a_n)) = a_1 a_2 \ldots\ldots a_n \;\forall\; (a_1, a_2, \ldots\ldots, a_n) \in N_1 \times N_2 \times \ldots\ldots \times N_n.$

ϕ is the well defined. Let $(a_1, a_2, \ldots\ldots, a_n), (b_1, b_2, \ldots\ldots, b_n) \in N_1 \times N_2 \times \ldots\ldots \times N_n$

*We have adopted the definition of **internal direct product** as given by **Prof. I.N. Herstein**, in his book **'Topics in Algebra'**.

and $\qquad (a_1, a_2, \ldots\ldots a_n) = (b_1, b_2, \ldots\ldots, b_n).$

$\therefore \qquad a_i = b_i \quad \forall\, i,\ 1 \le i \le n$

$\Rightarrow \qquad a_1a_2 \ldots\ldots a_n = b_1b_2 \ldots\ldots b_n$

$\Rightarrow\ \phi((a_1, a_2, \ldots\ldots, a_n)) = \phi((b_1, b_2, \ldots\ldots, b_n)).$

$\therefore$ ϕ is well defined.

ϕ is a homomorphism. Let $(a_1, a_2, \ldots\ldots, a_n), (b_1, b_2, \ldots\ldots, b_n) \in N_1 \times N_2 \times \ldots\ldots \times N_n$.

$$\begin{aligned}\phi((a_1, a_2, \ldots\ldots, a_n)(b_1, b_2, \ldots\ldots, b_n)) &= \phi((a_1b_1, a_2b_2, \ldots\ldots a_nb_n))\\ &= (a_1b_1)(a_2b_2) \ldots\ldots (a_nb_n)\\ &= (a_1a_2 \ldots\ldots a_n)(b_1b_2 \ldots\ldots b_n) \qquad (\because\ x_ix_j = x_jx_i \text{ for } x_i \in N_i, x_j \in N_j)\\ &= \phi((a_1, a_2, \ldots\ldots, a_n))\ \phi((b_1, b_2, \ldots\ldots, b_n)).\end{aligned}$$

$\therefore$ ϕ is a homomorphism.

ϕ is one-one. Let $(a_1, a_2, \ldots\ldots, a_n), (b_1, b_2, \ldots\ldots, b_n) \in N_1 \times N_2 \times \ldots\ldots \times N_n$

and $\qquad \phi((a_1, a_2, \ldots\ldots, a_n)) = \phi((b_1, b_2, \ldots\ldots, b_n)).$

$\Rightarrow \qquad a_1a_2 \ldots\ldots a_n = b_1b_2 \ldots\ldots b_n.$

Since G is the internal direct product of $N_1, N_2, \ldots\ldots, N_n$, we have

$$a_1 = b_1,\ a_2 = b_2, \ldots\ldots\ a_n = b_n.$$

$\therefore \qquad (a_1, a_2, \ldots\ldots, a_n) = (b_1, b_2, \ldots\ldots, b_n).$

$\therefore$ ϕ is one-one.

ϕ is onto. Let $g \in G$. Since G is the internal direct product of $N_1, N_2, \ldots\ldots, N_n$, there exists $m_i \in N_i$, $1 \le i \le n$ such that

$$g = m_1m_2 \ldots\ldots m_n.$$

$\therefore \phi((m_1, m_2, \ldots\ldots, m_n)) = m_1m_2 \ldots\ldots m_n = g$

$\therefore$ ϕ is onto.

$\therefore$ ϕ is an isomorphism from $N_1 \times N_2 \times \ldots\ldots \times N_n$ onto G.

$\therefore N_1 \times N_2 \times \ldots\ldots \times N_n \cong G$

i.e., $\qquad \mathbf{G \cong N_1 \times N_2 \times \ldots\ldots \times N_n}.$

Theorem 3. *Prove that a group G is the internal direct product of its normal subgroups $N_1, N_2, \ldots\ldots, N_n$ if and only if*

(i) $G = N_1N_2 \ldots\ldots N_n$

(ii) $N_i \cap (N_1N_2 \ldots\ldots N_{i-1}N_{i+1} \ldots\ldots N_n) = \{e\}$ for $i = 1, 2, \ldots\ldots, n$.

Proof. Let G be the internal direct product of its normal subgroups $N_1, N_2, \ldots\ldots N_n$.

$\therefore \qquad G = N_1N_2 \ldots\ldots N_n. \quad \therefore$ (*i*) holds.

Let $\qquad d \in N_i \cap (N_1N_2 \ldots\ldots N_{i-1}N_{i+1} \ldots\ldots N_n)$

$\Rightarrow \qquad d \in N_i$ and $d = d_1d_2 \ldots\ldots d_{i-1}d_{i+1} \ldots\ldots d_n$, where $d_j \in N_j$.

$\Rightarrow\ e_1e_2 \ldots\ldots e_{i-1}\, de_{i+1} \ldots\ldots e_n = d_1d_2 \ldots\ldots d_{i-1}e_id_{i+1} \ldots\ldots d_n$, where each $e_k = e$.

Since representation of elements of G is unique, we have $d = e$, on comparing the *i*th factors. $\therefore$ (*ii*) holds.

Now we shall prove the converse. By (*i*), we have $G = N_1N_2 \ldots\ldots N_n$.

Let $g \in$ G and we have

$$g = x_1x_2 \ldots\ldots x_n \quad \text{and} \quad g = y_1y_2 \ldots\ldots y_{n'}$$

where $x_i, y_i \in N_i$ for $1 \leq i \leq n$.

$\therefore \qquad x_1x_2 \ldots\ldots x_n = y_1y_2 \ldots\ldots y_n$

$\Rightarrow \quad x_1^{-1}(x_1x_2 \ldots\ldots x_n)(y_2 \ldots\ldots y_n)^{-1} = x_1^{-1}(y_1y_2 \ldots\ldots y_n)(y_2 \ldots\ldots y_n)^{-1}$

$\Rightarrow \qquad (x_2 \ldots\ldots x_n)(y_n^{-1} \ldots\ldots y_2^{-1}) = (x_1^{-1}y_1)\, e$

$\Rightarrow \qquad (x_2y_2^{-1}) \ldots\ldots (x_ny_n^{-1}) = x_1^{-1}y_1 \qquad \ldots(1)$

$(\because \quad ab = ba \ \forall\ a \in N_i, b \in N_j)$

L.H.S of (1) is in $N_2N_3 \ldots\ldots N_n$ and R.H.S. is in N_1.

$\therefore \qquad x_1^{-1}y_1 = e \qquad$ (By Using (*ii*))

$\Rightarrow \qquad x_1 = y_1$

Similarly, we can show that

$$x_i = y_i \ \forall\ i = 2, 3, \ldots\ldots, n.$$

$\therefore \qquad x_1x_2 \ldots\ldots x_n = y_1y_2 \ldots\ldots y_n.$

$\therefore$ The representation of g is unique.

$\therefore$ G is the internal direct product of $N_1, N_2, \ldots\ldots, N_n$.

This completes the proof.

Example 7. *Let a group G be the internal direct product of its normal subgrups N_1, N_2. Show that*

$$G/N_1 \cong N_2 \text{ and } G/N_2 \cong N_1.$$

Sol. Since G is the internal direct product of N_1 and N_2, every element of G can be expressed uniquely as the product of elements of N_1 and N_2.

Define $\phi : G \to N_2$ by $\phi(n_1n_2) = n_2$ for $n_1n_2 \in G$.

Let $\qquad a_1a_2, b_1b_2 \in G$.

$\therefore \qquad \phi((a_1a_2)(b_1b_2)) = \phi(a_1(b_1a_2)b_2) = \phi(a_1b_2)(a_2b_2)) = a_2b_2 = \phi(a_1a_2)\ \phi(b_1b_2)$

$(a_2 \in N_2, b_1 \in N_1 \ \Rightarrow \ a_2b_1 = b_1a_2)$

$\therefore$ ϕ is a homomorhphism

Let $n_2 \in N_2$.

$\therefore$ $en_2 \in G$ and $f(en_2) = n_2$.

$\therefore$ ϕ is onto.

$\therefore$ By the **fundamental theorem of homomorphism,** we have

$$G/\ker \phi \cong N_2 \qquad \ldots(1)$$

Let $\qquad n_1n_2 \in \ker \phi$

$\Rightarrow \qquad \phi(n_1n_2) = e \ \Rightarrow \ n_2 = e \ \Rightarrow \ n_1n_2 = n_1e = n_1 \in N_1$

$\therefore \qquad \ker \phi \subseteq N_1$.

Let $\qquad n_1 \in N_1$.

$\therefore \qquad n_1e \in G$ and $\phi(n_1e) = e$.

$\therefore \qquad n_1e \in \ker \phi$ *i.e.,* $n_1 \in \ker \phi$

$\therefore \qquad N_1 \subseteq \ker \phi$.

$\therefore \qquad \ker \phi = N_1$.

$\therefore$ (1) $\Rightarrow \qquad G/N_1 \cong N_2$

Similarly, we can show that $G/N_2 \cong N_1$.

3.4. EXPONENT OF A GROUP

Let G be a finite group. If k is the largest among the orders of all elements of G, then k is called the **exponent** of G.

In other words, k is the exponent of the group G if there exists $a \in$ G such that $o(a) = k$ and no element of G has order exceeding k.

3.5. STRUCTURE THEOREM FOR FINITE ABELIAN GROUPS

Statement. *Every finite abelian group G can be expressed as the internal direct product $G_1 \times G_2 \times \ldots\ldots \times G_t$, where each G_i is a cyclic subgroup of G of order n_i such that n_{i+1}/n_i and the integers n_i are uniquely determined and $n_1 n_2 \ldots\ldots n_t = o(G)$.*

Proof. In the proof of this theorem we shall be using the following result relating to the order of elements of a group.

'The order of any element of a finite abelian group G divides the exponent of G'.

Now we begin with the proof of the 'structure theorem'.

Let G be a finite abelian group of order n (> 1).

We shall prove the result by using induction on o(G).

Let $n = 1$. In this case, the result holds trivially because G = $\{e\}$ and $\{e\}$ is a cyclic subgroup of G.

Let the result be true for all abelian groups of order less than n.

Let the exponent of G be n_1 and $g_1 \in$ G such that $o(g_1) = n_1$.

Let $G_1 = (g_1)$, the cyclic subgroup of G generated by g_1.

If G = G_1, then G itself is cyclic and we are done.

Let G ≠ G_1.

$\therefore$ G/G_1 contains elements other than $\bar{e}$ and $o(G/G_1) = \dfrac{o(G)}{o(G_1)} < n$.

$\therefore$ $1 < o(G/G_1) < n$. By induction hypothesis, let $G/G_1 = \overline{H}_2 \times \overline{H}_3 \times \ldots\ldots \times \overline{H}_t$, where each $\overline{H}_i$ is a cyclic subgroup of $\overline{G}$ (= G/G_1) of order n_i(> 1) such that n_{i+1}/n_i and the integers n_i are uniquely determined for $i = 2, 3, \ldots\ldots t-1$ and $n_2 n_3 \ldots\ldots n_t = n/n_1$ (= $o(G/G_1)$).

Let $\overline{H}_i = H_i/G_1$, where H_i is a subgroup of G containing G_1, $2 \le i \le t$. Let $h_i \in H_i$ be such that $\bar{h}_i = G_1 h_i$ is a generator of the cyclic subgroup $\overline{H}_i$.

Since $o(\overline{H}_i) = n_i$, we have $(\bar{h}_i)^{n_i} = \bar{e} = G_1$

i.e.,
$$(G_1 h_i)^{n_i} = G_1 \quad \text{or} \quad G_1 h_i^{n_i} = G_1 \quad \text{or} \quad h_i^{n_i} \in G_1 \ (= (g_1)).$$

$\therefore$ $h_i^{n_i} = g_1^{m_i}$ for some m_i such that $1 \le m_i \le n_1$. Let $\alpha_i = (m_i, n_1)$.

$\therefore$ $m_i = \alpha_i \beta_i$ and $n_1 = \alpha_i \gamma_i$ for some $\beta_i, \gamma_i \ge 1$ and $(\beta_i, \gamma_i) = 1$.

Now $\quad o(g_1) = n_1 = \alpha_i\gamma_i \;\Rightarrow\; o({g_1}^{\alpha_i}) = \gamma_i$

Since $(\beta_i, \gamma_i) = 1$, we have $o({g_1}^{\alpha_i\beta_i}) = \gamma_i$.

$$\Rightarrow \quad o({g_1}^{m_i}) = \gamma_i \;\Rightarrow\; o({h_i}^{n_i}) = \gamma_i$$

Also, $o(\overline{h}_i)/o(h_i)$.

$$\Rightarrow \; n_i/o(h_i) \;\Rightarrow\; o({h_i}^{n_i}) = \frac{o(h_i)}{n_i} \;\Rightarrow\; o(h_i) = n_i\, o({h_1}^{n_i}) = n_i\gamma_i$$

Since n_1 is the exponent of G, we have $o(h_i)/n_1$.

$\Rightarrow \; n_i\gamma_i/\alpha_i\gamma_i \;\Rightarrow\; n_i/\alpha_i \;\Rightarrow\; \alpha_i = n_i\delta_i$ for some $\delta_i \geq 1$.

$$\therefore \quad {h_i}^{n_i} = {g_1}^{m_i} = {g_1}^{\alpha_i\beta_i} = {g_1}^{n_i\delta_i\beta_i}$$

Define $\quad g_i = h_i(g_1)^{-\delta_i\beta_i} \quad \forall\; i = 2, 3, \ldots\ldots, t-1.$

$$\therefore \quad \overline{g}_i = G_1 g_i = G_1 h_i (g_1)^{-\delta_i\beta_i} = G_1 h_i = \overline{h_i}$$

and
$$\begin{aligned}{g_i}^{n_i} &= (h_i(g_1)^{-\delta_i\beta_i})^{n_i} = {h_i}^{n_i} {g_1}^{-\delta_i\beta_i n_i} = {h_i}^{n_i}({g_1}^{n_i\delta_i\beta_i})^{-1} = {h_i}^{n_i}{h_i}^{-n_i} \\ &= e\end{aligned}$$

$\therefore \quad o(g_i) = n_i,\; i = 2, 3, \ldots\ldots, t-1.$

Define $\quad H = (g_2)(g_3) \ldots\ldots (g_t)$

$\therefore$ H is a subgroup of G such that $o(H)/n_2 n_3 \ldots\ldots n_t$.

Let $\phi : G \to G/G_1$ be the natural homomorphism.

$$\begin{aligned}\therefore \quad \phi(H) &= \phi((g_2)(g_3) \ldots\ldots (g_t)) = \overline{(g_2)} \times \overline{(g_3)} \times \ldots\ldots \times \overline{(g_t)} \\ &= \overline{\overline{H}}_2 \times \overline{\overline{H}}_3 \times \ldots\ldots \times \overline{\overline{H}}_t = G/G_1\end{aligned}$$

Also $\quad f(H) = (HG_1)/G_1 \quad \therefore \quad G = HG_1 = G_1H = (g_1)(g_2)(g_3) \ldots\ldots (g_t).$

The fact that $\quad o(G) = n = n_1 n_2 n_3 \ldots\ldots n_t$

$\qquad = o(g_1)\, o(g_2)\, o(g_3) \ldots o(g_t)$ gives $G = (g_1) \times (g_2) \times \ldots\ldots \times (g_t)$.

Also $\quad o((g_i)) = o(g_i) = n_i$ such that n_{i+1}/n_i.

This completes the proof.

Remark. Keeping in view the scope of present book, we are accepting the uniqueness of the above representation.

SUMMARY

- The external direct product of groups is also a group.
- Let a group G be the internal direct product of its normal subgroups $N_1, N_2, \ldots\ldots, N_n$. Then for $i \neq j$, we have

  (*i*) $N_i \cap N_j = \{e\}$ $\qquad$ (*ii*) $a \in N_i,\, b \in N_j \;\Rightarrow\; ab = ba$.
- Let a group G be the internal direct product of its normal subgroups $N_1, N_2, \ldots\ldots, N_n$. Then $\quad G \cong N_1 \times N_2 \times \ldots\ldots \times N_n$.

- A group G is the internal direct product of its normal subgroup $N_1, N_2, ..., N_n$ if and only if

  (*i*) $G = N_1N_2 ...... N_n$

  (*ii*) $N_i \cap (N_1N_2 ...... N_{i-1}N_{i+1} ...... N_n) = \{e\}$ for $i = 1, 2, ..., n$.
- Every finite abelian group G can be expressed as the internal direct product $G_1 \times G_2 \times ...... \times G_t$, where each G_i is a cyclic subgroup of G of order n_i such that n_{i+1}/n_i and the integers n_i are uniquely determined and $n_1n_2 ...... n_t = o(G)$.

REVIEW QUESTIONS

1. We know that **Z** is an abelian group under usual addition. Show that **Z** × **Z** is also an abelian group.
2. Let G be the multiplicative group of non zero rational numbers. Show that $G \times G \times G$ is an abelian group. Also write the inverse of the element $(2, -5, 1/4)$ of $G \times G \times G$.
3. If G_1 and G_2 be any two groups, then show that $G_1 \times G_2 \cong G_2 \times G_1$.
4. If G_1, G_2 and G_3 be any three groups, then show that $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$.
5. Let a group G be the internal direct product of its normal subgroups N_1 and N_2. Show that $G \cong N_1 \times N_2$.

NOTES

UNIT 4

RINGS

STRUCTURE

4.0 LEARNING OBJECTIVES

After going through this unit, you should be able to:

- ring
- multiplicative inverse of an element
- field.

4.1. DEFINITION OF A RING

A non-empty set R with two binary operations denoted by '+' and '.' and called addition and multiplication respectively is said to be a **ring** if :

1. $a + (b + c) = (a + b) + c \quad \forall\ a, b, c \in R$

2. There is an element $0 \in R$ such that

$$a + 0 = a = 0 + a \quad \forall\ a \in R$$

3. For $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0 = (-a) + a$

4. $a + b = b + a \quad \forall\ a, b \in R$

5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall\ a, b, c \in R$

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

The element '0' is called the **additive identity** of the ring (R, +, .). The element '$-a$' is called the **additive inverse** of a.

The additive identity of the ring (R, +, .) is represented by '0' and it has nothing to do with the number zero.

In place of '+' and '.', the binary operations of the ring can very well be denoted by other symbols like $*$, o, ⊕, ⊙ etc.

Axioms **1—4** shows that (R, +) is an abelian group.

Axiom **5** states that the binary operation '.' is associative.

Axiom **6** states that the multiplication is distributive over addition.

Remark. The binary operations of a ring are generally taken as '+' and '.' but these operations have no bearing with the usual addition and multiplication of numbers.

4.2. COMMUTATIVE RING

A ring (R, +, .) is called a **commutative ring** if $a \cdot b = b \cdot a \quad \forall\ a, b \in R$.

Illustrations:

1. **Z, Q, R, C** are all commutative rings with respect to the usual addition and multiplication.

2. The set $\{a + ib : a, b \in \mathbf{Z}\}$ is called the set of **Gaussian integers** and is denoted as **Z**[i]. Under usual addition and multiplication, Z[i] is a commutative ring.

4.3. RING WITH UNIT ELEMENT

A ring (R, +, .) is called a **ring with unit element** if there exists an element '1' in R such that $a \cdot 1 = a = 1 \cdot a \quad \forall\ a \in R$.

The unit element of a ring is also called its **multiplication identity.**

4.4. RING WITHOUT ZERO DIVISORS

A ring (R, +, .) is called a **ring without zero divisors** if $a \cdot b = 0$ for $a, b \in R$ then either $a = 0$ or $b = 0$.

4.5. INTEGRAL DOMAIN

A ring (R, +, .) is called an **integral domain** if :

(*i*) the ring (R, +, .) is commutative

(*ii*) the ring (R, +, .) is without zero divisors.

In short, we can say that a commutative ring without zero divisors is an integral domain.

4.6. MULTIPLICATIVE INVERSE OF AN ELEMENT

Let (R, +, .) be a ring with unit element '1' and let a be any element of R. An element $b \in R$ is called the **multiplicative inverse** of a if

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

The multiplicative inverse of an element a is denoted by a^{-1}.

4.7. FIELD

A ring (R, +, .) is called a **field** if :

(*i*) the ring (R, +, .) is commutative

(*ii*) the ring (R, +, .) has unit element

(*iii*) every non-zero element of R has multiplicative inverse.

Equivalently, we can say that a non-empty set R with two binary operations '+' and '.' is a field if :

(*i*) (R, +) is an abelian group

(*ii*) $(R - \{0\}, .)$ is an abelian group

(*iii*) Multiplication '.' distributes over addition '+'.

Thus a non-empty set R with two binary operations '+' and '.' is a field if :

1. $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in R$

2. There is an element $0 \in R$ such that $a + 0 = a = 0 + a \quad \forall\, a \in R$

'0' is called the *additive identity* of R

3. For $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0 = (-a) + a$

$-a$ is called the *additive inverse* of a.

4. $a + b = b + a \quad \forall\, a, b \in R$

5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall\, a, b, c \in R$

6. There is an element $1 \in R$ such that $a \,.\, 1 = a = 1 \,.\, a \quad \forall\, a \in R$

'1' is called the *multiplicative identity* or *unit element* of R.

7. For $a\,(\neq 0) \in R$, there exist an element a^{-1} in R such that $a \,.\, a^{-1} = 1 = a^{-1} \,.\, a$

a^{-1} is called the *multiplicative inverse* of a.

8. $a \,.\, b = b \,.\, a \quad \forall\, a, b \in R$

9. $a \,.\, (b + c) = (a \,.\, b) + (a \,.\, c)$ and $(b + c) \,.\, a = (b \,.\, a) + (c \,.\, a) \quad \forall\, a, b, c \in R.$

Remark. In axiom **9**, we need writing only one equality, because the other follows by using axiom **8**.

4.8. DIVISION RING

A ring (R, +, .) is called a division ring if :

(*i*) the ring (R, +, .) has unit element

(*ii*) every non-zero element of R has multiplicative inverse.

Remark 1. A division ring is also called a **skew field.**

Remark 2. A commutative division ring is a field.

Example 1. *Let $R = \mathbf{Z}$, the set of integers and binary operations '+' and '.' be respectively the usual addition and multiplication of integers. Show that (R, +, .) is a ring.*

Sol. We have :

1. $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in \mathbf{Z}$

2. $0 \in \mathbf{Z}$ and $a + 0 = a = 0 + a \quad \forall\, a \in \mathbf{Z}$

3. For $a \in \mathbf{Z}$, we have $-a \in \mathbf{Z}$ and $a + (-a) = 0 = (-a) + a$

4. $a + b = b + a \quad \forall\, a, b \in \mathbf{Z}$

5. $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c \quad \forall\, a, b, c \in \mathbf{Z}$

6. $a \,.\, (b + c) = (a \,.\, b) + (a \,.\, c)$ and $(b + c) \,.\, a = (b \,.\, a) + (c \,.\, a) \quad \forall\, a, b, c \in \mathbf{Z}$

$\therefore$ (**Z**, +, .) is a ring.

Note 1. (**Z**, +, .) is also an integral domain, because

(*i*) $a \,.\, b = b \,.\, a \quad \forall\, a, b \in \mathbf{Z}$

(*ii*) $a \,.\, b = 0$ for $a, b \in \mathbf{Z}$ implies either $a = 0$ or $b = 0$.

Note 2. (**Z**, +, .) is not a field because $4\,(\neq 0) \in \mathbf{Z}$ and there is no integer k such that

$$4 \,.\, k = 1 = k \,.\, 4.$$

Example 2. *Let* **C** *be the set of complex numbers and binary operations '+' and '.' be respectively the usual addition and multiplication of complex numbers. Show that* (**C**, +, .) *is a ring.*

Sol. We have :

1. $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3 \quad \forall\, z_1, z_2, z_3 \in \mathbf{C}$

2. $0\,(= 0 + 0i) \in \mathbf{C}$ and $z + 0 = z = 0 + z \quad \forall\, z \in \mathbf{C}$

3. For $z\,(= a + ib) \in \mathbf{C}$, we have $-z\,(= -a - ib) \in \mathbf{C}$ and $z + (-z) = 0 = (-z) + z.$

4. $z_1 + z_2 = z_2 + z_1 \quad \forall\, z_1, z_2 \in \mathbf{C}$

5. $z_1 \,.\, (z_2 \,.\, z_3) = (z_1 \,.\, z_2) \,.\, z_3 \quad \forall\, z_1, z_2, z_3 \in \mathbf{C}$

6. $z_1 . (z_2 + z_3) = (z_1 . z_2) + (z_1 . z_3)$ and $(z_2 + z_3) . z_1 = (z_2 . z_1) + (z_3 . z_1)$ $\forall z_1, z_2, z_3 \in \mathbf{C}$

$\therefore$ $(\mathbf{C}, +, .)$ is a ring.

Note 1. $(\mathbf{C}, +, .)$ is also an integral domain, because

(*i*) the ring $(\mathbf{C}, +, .)$ is commutative

(*ii*) $z_1 . z_2 = 0$ for $z_1, z_2 \in \mathbf{C}$ implies either $z_1 = 0$ or $z_2 = 0$.

Note 2. $(\mathbf{C}, +, .)$ is also a field, because

(*i*) the ring $(\mathbf{C}, +, .)$ is commutative

(*ii*) $1 (= 1 + 0\, i) \in \mathbf{C}$ and $z.1 = z = 1.\, z\ \forall z \in \mathbf{C}$

(*ii*) Let $z (= a + ib)$ be a non-zero complex number.

$$\therefore \qquad a^2 + b^2 \neq 0$$

$$\therefore \qquad \frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2}\, i \in \mathbf{C} \text{ and}$$

$$(a + ib)\left(\frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2} i\right) = 1 = \left(\frac{a}{a^2+b^2} + \frac{(-b)}{a^2+b^2} i\right)(a + ib).$$

$\therefore$ Every non-zero element of $\mathbf{C}$ has a multiplicative inverse.

4.9. A PROPERTY OF FIELDS

Theorem 1. *Every field is an integral domain.*

Proof. Let $(F, +, .)$ be a field.

$\therefore$ $(F, +, .)$ is a commutative ring.

$\therefore$ It is sufficient to show that the ring $(F, +, .)$ is without zero divisors.

Let $a, b \in F$ and $a . b = 0$.

If $a = 0$, then we have nothing to prove.

Let $a \neq 0$. Since $(F, +, .)$ is a field, $\exists\, a^{-1} \in F : \quad a . a^{-1} = 1 = a^{-1} . a$

$$\therefore \qquad a . b = 0 \;\Rightarrow\; a^{-1} . (a . b) = a^{-1} . 0$$

$$\Rightarrow \qquad (a^{-1} . a) . b = 0 \;\Rightarrow\; 1 . b = 0 \;\Rightarrow\; b = 0.$$

$\therefore$ The ring $(F, +, .)$ is without zero divisors.

$\therefore$ $(F, +, .)$ is an integral domain.

Remark. The converse of above theorem is not true. For example, $(\mathbf{Z}, +, .)$ is an integral domain and it is not a field.

4.10. SCALAR MULTIPLE AND POWERS OF ELEMENTS OF A RING

Let $(R, +, .)$ be a ring.

For $a \in R$, we define

$$2a = a + a, \quad 3a = a + 2a, \;......,\; na = a + (n-1)a \text{ etc.}$$

and
$$a^2 = a . a, \quad a^3 = a . a^2, \;......,\; a^n = a . a^{n-1} \text{ etc.}$$

Remark 1. If $(R, +, .)$ is a ring then for the sake of simplicity, the product $a . b$ is written as ab for $a, b \in R$.

Remark 2. If (R, +, .) is a ring then for $a, b \in$ R, the element $a + (-b)$ is written as $a - b$.

Example 3. *Let R be a ring such that $x^2 = x \; \forall \; x \in R$. Show that R is commutative.*

Sol. Let $a, b \in$ R.

$\Rightarrow \quad (a + b)^2 = a + b \quad \Rightarrow \quad (a + b)(a + b) = a + b$

$\Rightarrow \quad a^2 + ab + ba + b^2 = a^2 + b^2 \Rightarrow \quad ab + ba = 0$ ...(1)

Also $\quad (x + x)^2 = x + x$

$\Rightarrow \quad (x + x)(x + x) = x + x \quad \Rightarrow \quad x^2 + x^2 + x^2 = x^2 + x^2$

$\Rightarrow \quad x^2 + x^2 = 0 \quad \Rightarrow \quad x + x = 0 \;\; \forall \; x \in$ R

$\therefore \quad (1) \Rightarrow \quad ab + ba = ba + ba$ $\quad (\because \; ba + ba = 0)$

$\Rightarrow \quad ab = ba$. $\therefore$ R is commutative.

Example 4. *Let (R, +, .) be a ring. Show that the ring is commutative if and only if*

$$(a + b)^2 = a^2 + 2ab + b^2 \quad \forall \; a, b \in R.$$

Sol. Let the ring (R, +, .) be commutative.

$\therefore \quad xy = yx \quad \forall \; x, y \in$ R

Now $\quad (a + b)^2 = (a + b)(a + b) = (a + b)a + (a + b)b = (aa + ba) + (ab + bb)$

$\quad = a^2 + ab + ab + b^2 = a^2 + 2ab + b^2$

$\therefore \quad (a + b)^2 = a^2 + 2ab + b^2 \quad \forall \; a, b \in$ R.

Conversely, let

$\quad (a + b)^2 = a^2 + 2ab + b^2 \quad \forall \; a, b \in$ R.

Let $x, y \in$ R.

$\therefore \quad (x + y)^2 = x^2 + 2xy + y^2 \quad \Rightarrow \quad (x + y)(x + y) = x^2 + xy + xy + y^2$

$\Rightarrow \quad (x + y)x + (x + y)y = x^2 + xy + xy + y^2$

$\Rightarrow \quad xx + yx + xy + yy = xx + xy + xy + yy$

$\Rightarrow \quad yx = xy$.

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

4.11. SUBRINGS

Let (R, +, .) be a ring. A non-empty subset S of R is called a **subring** of the ring (R, +, .) if S itself is a ring under the binary operations '+' and '.' of R.

Example 5. If (R, +, .) is a ring, then {0} and R are always subrings of R. These are called **improper subrings** of R. Other subrings, if any, are called **proper subrings** of R.

Example 6. **Z** is a subring of the ring (**Q**, +, .).

Example 7. **Q** is a subring of the ring (**R**, +, .).

4.12. TEST FOR A SUBRING

Theorem 2. *Let (R, +, .) be a ring. A non-empty subset S of R is a subring of R if and only if $a - b \in S$ and $ab \in S \quad \forall \; a, b \in S$.*

Proof. Let S be a subring of the ring (R, +, .).

$\therefore$ (S, +, .) is a ring. Let $a, b \in$ S.

$\therefore$ $-b$, being the additive inverse of b, is in S.

$\therefore$ $a + (-b)$ *i.e.*, $a - b$ is in S.

Also $ab \in$ S (∵ '.' is a binary operation on S)

$\therefore \quad a - b \in S, ab \in S \quad \forall\, a, b, \in S.$

Conversely, let $a - b \in S, ab \in S \quad \forall\, a, b \in S.$

'+' is associative because elements of S are also elements of R.

Let $a \in S$. $\therefore \quad a - a \in S \quad \Rightarrow \quad a + (-a) \in S \quad \Rightarrow \quad 0 \in S$

Let $x \in S$. $\therefore \quad x \in R$.

$\therefore \quad x + 0 = x = 0 + x$ (∵ R is a ring)

Let $a \in S$. $\therefore \quad 0 - a = -a \in S$

$\therefore$ For $a \in S, \exists -a \in S : a + (-a) = 0 = (-a) + a$

Also, $a, b \in S \Rightarrow a, -b \in S \Rightarrow a - (-b) \in S \Rightarrow a + b \in S.$

$\therefore$ '+' is a binary operation on S.

'.' is a binary operation on S because $ab \in S \quad \forall\, a, b \in S$.

'.' is associative because elements of S are also elements of R.

Distributive laws holds in S because elements of S are also elements of R.

$\therefore$ (S, +, .) is a ring. $\therefore$ S is a subring of the ring (R, +, .).

Example 8. *Show that the set of all even integers is a subring of the ring* (**Z**, +, .).

Sol. Let S = set of all even integers.

S ≠ ϕ because 0 (= 2(0)) ∈ S.

Let $2a, 2b \in S$.

$\therefore \quad 2a - 2b = 2(a - b) \in S \quad \text{and} \quad (2a)(2b) = 4ab = 2(2ab) \in S.$

$\therefore \quad 2a - 2b, (2a)(2b) \in S \quad \forall\, 2a, 2b \in S.$

$\therefore$ S is a subring of the ring (**Z**, +, .).

4.13. INTERSECTION OF SUBRINGS

Theorem 3. *The intersection of two subrings of a ring is also a subring of the ring.*

Proof. Let S_1 and S_2 be two subrings of a ring (R, +, .).

Let '0' be additive identity of the ring R.

$\Rightarrow \quad 0 \in S_1, 0 \in S_2 \quad \Rightarrow \quad 0 \in S_1 \cap S_2. \quad \therefore \quad S_1 \cap S_2 \neq \phi$

Let $a, \quad b \in S_1 \cap S_2$

$\Rightarrow \quad a, b \in S_1, a, b \in S_2 \quad \Rightarrow \quad a - b, ab \in S_1 \text{ and } a - b, ab \in S_2$

$\Rightarrow \quad a - b, ab \in S_1 \cap S_2$

$\therefore$ $S_1 \cap S_2$ is a subring of the ring (R, +, .).

NOTES

4.14. HOMOMORPHISM

A mapping ϕ of a ring R into a ring R′ is called, a **homomorphism** of R into R′ if (*i*) $\phi(a + b) = \phi(a) + \phi(b)$

(*ii*) $\phi(a \,.\, b) = \phi(a) \,.\, \phi(b)$

for all $a, b \in$ R.

The '+' and '.' signs occurring on the left hand side of (*i*) and (*ii*) are those of the ring R, and the '+' and '.' signs occurring on the right side of (*i*) and (*ii*) are those of the ring R′.

Remarks. (*i*) Shows that the ring homomorphism ϕ is a group homomorphism of the additive group (R, +) into additive group (R′, +).

4.15. HOMOMORPHIC IMAGE OF ADDITIVE IDENTITY AND ADDITIVE INVERSE

Theorem 4. *If ϕ is a ring homomorphism of ring R into ring R′, then*

(i) $\phi(0) = 0'$, where 0 and 0′ are the additive identities of the rings R and R′ respectively

(ii) $\phi(-a) = -\phi(a) \;\forall\; a \in R$.

Proof. (*i*) For $a \in$ R, we have

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

and
$$\phi(a) = 0' + \phi(a)$$

$$\therefore \quad \phi(0) + \phi(a) = 0' + \phi(a)$$

By cancellation law in the group $(R_1{}' +)$, we have $\phi(0) = 0'$.

(*ii*) For $a \in$ R, we have

$$\phi(a) + \phi(-a) = \phi(a + (-a)) = \phi(0) = 0'$$

and
$$\phi(-a) + \phi(a) = \phi((-a) + a) = \phi(0) = 0'$$

$$\therefore \quad \phi(a) + \phi(-a) = 0' = \phi(-a) + \phi(a)$$

$\therefore$ By definition $-\phi(a) = \phi(-a)$ *i.e.*, $\phi(-a) = -\phi(a)$.

Example 9. *If f is a homomorphism of ring R into ring R′ and g, a homomorphism of ring R′ into ring R″, show that gof is a homomorphism of ring R into ring R″.*

Sol. By definition *gof* is a mapping from R into R″.

For $a, b \in$ R, we have

$$(gof)(a + b) = g(f(a + b)) = g(f(a) + f(b))$$
$$= (g(f(a) + g(f(b)) = (gof)(a) + (gof)(b)$$

and
$$(gof)(ab) = g(f(ab)) = g(f(a)\, f(b))$$
$$= g(f(a))\, g(f(b)) = (gof)(a)(gof)(b)$$

$\therefore$ *gof* is a homomorphism of R into R″.

Theorem 5. *If ϕ is a ring homomorphism of ring R into ring R′, then $\phi(R)$ is a subring of the ring R′.*

Proof. $0 \in R \Rightarrow \phi(0)(= 0) \in \phi(R)$

$\therefore$ $\phi(R)$ is non-empty.

Let $\phi(a), \phi(b) \in \phi(R)$

$\Rightarrow$ $a, b \in R \Rightarrow a - b, ab \in R \Rightarrow \phi(a - b), \phi(ab) \in \phi(R)$

$$\phi(a - b) = \phi(a + (- b)) = \phi(a) + \phi(- b) = \phi(a) - \phi(b)$$

and $\phi(ab) = \phi(a) \phi(b)$

$\therefore$ $\phi(a), \phi(b) \in \phi(R) \Rightarrow \phi(a) - \phi(b), \phi(a) \phi(b) \in \phi(R)$

$\therefore$ $\phi(R)$ is a subring of R′.

Remark. '0' is representing the additive identity of rings R and R′ both.

4.16. KERNEL OF A RING HOMOMORPHISM

If ϕ is a homomorphism of ring R into ring R′, then the set $\{a \in R : \phi(a) = 0$, the additive identity of R′$\}$ is called the **kernel of the ring homomorphism** ϕ and written as **ker** ϕ.

Since $\phi(0) = 0$, so $0 \in \ker \phi$.

$\therefore$ ker ϕ is always a non-empty set.

Theorem 6. *If ϕ is a homomorphism of ring R to ring R′, then*

(*i*) *ker ϕ is a subgroup of R under addition.*

(*ii*) *$a \in$ ker ϕ and $r \in R$ then $ar, ra \in$ ker ϕ.*

Proof. (*i*) $\phi(0) = 0 \Rightarrow 0 \in \ker \phi$ $\therefore$ ker ϕ is non-empty.

Let $a, b \in \ker \phi$

$\therefore$ $\phi(a) = 0, \phi(b) = 0$

Now $\phi(a - b) = \phi(a + (- b)) = \phi(a) + \phi(- b) = \phi(a) + (- \phi(b))$

$$= \phi(a) - \phi(b) = 0 - 0 = 0$$

$\therefore$ $a - b \in \ker \phi$

$\therefore$ ker ϕ is a subgroup of R under addition.

(*ii*) Let $a \in \ker \phi$ and $r \in R$

$\therefore$ $\phi(ar) = \phi(a)\, \phi(r) = 0 \,.\, \phi(r) = 0$ $(\because \; a \in \ker \phi)$

and $\phi(ra) = \phi(r)\, \phi(a) = \phi(r) \,.\, 0 = 0$

$\therefore$ $ar, ra \in \ker \phi$.

Example 10. *Let $R = \{a + \sqrt{5}\, b : a, b \in \mathbf{Z}\}$ R is a ring under usual addition and multiplication of real numbers. Define $\phi : R \to R$ by $\phi\, (a + \sqrt{5}\, b) = a - \sqrt{5}\, b$. Show that ϕ is a homomorphism of R onto R and its kernel consists of 0 only.*

Sol. We have $R = \{a + \sqrt{5}\, b : a, b \in \mathbf{Z}\}$

Also $\phi(a + \sqrt{5}\, b) = a - \sqrt{5}\, b$

$$= a + \sqrt{5}\,(- b) \in R \quad \text{for} \quad a + \sqrt{5}\, b \in R$$

Let $a + \sqrt{5}\, b, c + \sqrt{5}\, d \in R$.

$$\therefore \quad \phi((a+\sqrt{5}\,b)+(c+\sqrt{5}\,d)) = \phi((a+c)+\sqrt{5}\,(b+d))$$
$$= (a+c)-\sqrt{5}\,(b+d) = (a-\sqrt{5}\,b)+(c-\sqrt{5}\,d)$$
$$= \phi(a+\sqrt{5}\,b)+\phi(c+\sqrt{5}\,d)$$

Also $\phi((a+\sqrt{5}\,b)(c+\sqrt{5}\,d)) = \phi((ac+5bd)+\sqrt{5}\,(ad+bc))$

and $= (ac+5bd)-\sqrt{5}\,(ad+bc)$

$$\phi(a+\sqrt{5}\,b)\,\phi(c+\sqrt{5}\,d) = (a-\sqrt{5}\,b)(c-\sqrt{5}\,d) = (ac+5bd)-\sqrt{5}\,(ad+bc)$$

$$\therefore \quad \phi((a+\sqrt{5}\,b)(c+\sqrt{5}\,d)) = \phi(a+\sqrt{5}\,b)\,\phi(c+\sqrt{5}\,d)$$

$\therefore$ $\phi : \text{R} \to \text{R}$ is a homomorphism.

Let $\qquad x+\sqrt{5}y \in \text{R}$

$\Rightarrow \qquad x, y \in \mathbf{Z} \;\Rightarrow\; x, -y \in \mathbf{Z} \;\Rightarrow\; x+\sqrt{5}\,(-y) \in \text{R}$

and $\qquad \phi(x+\sqrt{5}\,(-y)) = x-\sqrt{5}\,(-y) = x+\sqrt{5}\,y.$

$\therefore$ ϕ is onto

Let $\qquad x+\sqrt{5}y \in \ker\phi.$

$\therefore \qquad \phi(x+\sqrt{5}\,y) = 0 \quad i.e., \quad x-\sqrt{5}\,y = 0 \quad \text{or} \quad x = \sqrt{5}\,y$

Since $x, y \in \mathbf{Z}$, the equality $x = \sqrt{5}\,y$ is possible only when $x = 0, y = 0$.

$\therefore \qquad x+\sqrt{5}\,y = 0+\sqrt{5}\,(0) = 0 \quad \therefore \quad \ker\phi = \{0\}.$

4.17. ISOMORPHISM

A mapping ϕ of a ring R into a ring R′ is called an **isomorphism** if

(*i*) ϕ is a homomorphism *i.e.*,

$$\phi(a+b) = \phi(a)+\phi(b),\ \phi(a.b) = \phi(a).\phi(b) \quad \forall\ a\ , b \in \text{R}$$

(*ii*) ϕ is one-one

(*iii*) ϕ is onto.

Two rings are said to be **isomorphic** if there is an isomorphism from one ring onto the other.

Note. 1. A homomorphism $\phi : \text{R} \to \text{R}'$ is called an **epimorphism** if ϕ is onto.

2. A homomorphism $\phi : \text{R} \to \text{R}'$ is called a **monomorphism** if ϕ is one-one.

3. A homomorphism $\phi : \text{R} \to \text{R}'$ is called an **endomorphism** if R′ = R.

4. A homomorphism $\phi : \text{R} \to \text{R}$ is called an **automorphism** if ϕ is one-one and onto.

Example 11. *Let R be a ring with unit element '1'. Using its elements we form a ring $\overline{R}$ by defining $a \oplus b = a+b+1$ and $a \odot b = a+b+ab$ where $a, b \in R$, and the addition and multiplication on the right side of these relations are those of R. Show that rings R and $\overline{R}$ are isomorphic.*

Sol. Define $\phi : \text{R} \to \overline{\text{R}}$ by $\phi(a) = a-1$, $a \in \text{R}$.

ϕ is a homomorphism.

Let $a, b \in R$

$$\phi(a + b) = (a + b) - 1 = a + b - 1$$

and $$\phi(a) \oplus \phi(b) = \phi(a) + \phi(b) + 1 = (a - 1) + (b - 1) + 1 = a + b - 1$$

$\therefore$ $$\phi(a + b) = \phi(a) \oplus \phi(b).$$

Also $$\phi(ab) = (ab) - 1$$

and $$\phi(a) \odot \phi(b) = \phi(a) + \phi(b) + \phi(a)\,\phi(b)$$
$$= (a - 1) + (b - 1) + (a - 1)(b - 1) = ab - 1$$

$\therefore$ $$\phi(ab) = \phi(a) \odot \phi(b)$$

$\therefore$ ϕ is a homomorphism.

ϕ is one-one.

Let $a, b \in R$ and $\phi(a) = \phi(b)$.

$\Rightarrow$ $$a - 1 = b - 1 \Rightarrow a = b$$

$\therefore$ ϕ is one-one.

ϕ is onto.

Let $$a \in \overline{R}$$

$\Rightarrow$ $$a \in R \Rightarrow a + 1 \in R \text{ and } \phi(a + 1) = (a + 1) - 1 = a.$$

$\therefore$ ϕ is onto.

$\therefore$ ϕ is an isomorphism.

Example 12. *Let ϕ be an isomorphism of a ring R onto ring R'. If R is an integral domain, then show that R' is also an integral domain.*

Sol. Let $x, y \in R'$.

$\therefore$ $\exists\, a, b \in R$ such that $\phi(a) = x$, $\phi(b) = y$.

Now $xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\,\phi(a) = yx$ ($\because$ R is commutative)

$\therefore$ R' is commutative.

Let $xy = 0$ for $x, y \in R'$.

$\therefore$ $\exists\, a, b \in R$ such that $\phi(a) = x$, $\phi(b) = y$

$$xy = 0 \Rightarrow \phi(a)\,\phi(b) = 0 \Rightarrow \phi(ab) = \phi(0) \Rightarrow ab = 0$$

$\Rightarrow$ either $$a = 0 \text{ or } b = 0$$

Now $$a = 0 \Rightarrow \phi(a) = \phi(0) \Rightarrow x = 0$$

and $$b = 0 \Rightarrow \phi(b) = \phi(0) \Rightarrow y = 0.$$

$\therefore$ $$xy = 0 \Rightarrow \text{either } x = 0 \text{ or } y = 0$$

$\therefore$ R' is also an integral domain.

Example 13. *Let R be a ring with unit element 1 and $\phi : R \to R'$ be a homomorphism of ring R into an integral domain R' such that $\ker \phi \neq R$, then show that $f(1)$ is the unit element of R'.*

Sol. Let $r' \in R'$.

$\therefore$ $$\phi(1)r' = \phi(1.1)\ r' = \phi(1)\ \phi(1)r'$$

$\Rightarrow$ $$\phi(1)r' - \phi(1)\ \phi(1)r' = 0$$

$\Rightarrow$ $$\phi(1)\ [r' - \phi(1)r'] = 0$$

$\Rightarrow \qquad \phi(1) = 0 \quad \text{or} \quad r' - \phi(1)r' = 0$

$\phi(1) = 0 \;\Rightarrow\; 1 \in \ker\phi \;\Rightarrow\; \ker\phi = R$, which is impossible.

($\because$ An ideal containing the unit element always coincides with the ring)

$\therefore \qquad r' - \phi(1)r' = 0 \;\Rightarrow\; r' = \phi(1)r'$

$\Rightarrow \qquad \phi(1)r' = r' = r'\,\phi(1) \qquad\qquad (\because\ R' \text{ is com.})$

$\Rightarrow \qquad \phi(1)$ is the unit element of R′.

SUMMARY

- A non-empty set R with two binary operations denoted by '+' and '.' and called addition and multiplication respectively is said to be a **ring** if :
- $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in R$
- There is an element $0 \in R$ such that $\; a + 0 = a = 0 + a \quad \forall\, a \in R$
- For $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0 = (-a) + a$
- $a + b = b + a \quad \forall\, a, b \in R$
- $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c \quad \forall\, a, b, c \in R$
- $a \,.\, (b + c) = (a \,.\, b) + (a \,.\, c)$ and $(b + c) \,.\, a = (b \,.\, a) + (c \,.\, a) \quad \forall\, a, b, c \in R.$
- A ring (R, +, .) is called a **field** if :

  (*i*) the ring (R, +, .) is commutative

  (*ii*) the ring (R, +, .) has unit element

  (*iii*) every non-zero element of R has multiplicative inverse.
- Every field is an integral domain.
- Let (R, +, .) be a ring. A non-empty subset S of R is called a **subring** of the ring (R, +, .) if S itself is a ring under the binary operations '+' and '.' of R.
- The intersection of two subrings of a ring is also a subring of the ring.
- If ϕ is a homomorphism of ring R into ring R′, then the set $\{a \in R : \phi(a) = 0$, the additive identity of R′$\}$ is called the **kernel of the ring homomorphism** ϕ and write **ker** ϕ.

REVIEW QUESTIONS

1. Show that (**R**, +, .) is (*i*) a ring (*ii*) an integral domain (*iii*) a field, where the binary operations '+' and '.' are respectively usual addition and multiplication of real numbers.
2. Let $R = \{4n : n \in \mathbf{Z}\}$. Let the binary operations 'usual addition' and 'usual multiplication' be denoted by '+' and '.' respectively. Show that :

   (*i*) (R, +, .) is a commutative ring. (*ii*) (R, +, .) has no unit element.

   (*iii*) (R, +, .) is not an integral domain. (*iv*) (R, +, .) is not a field.
3. Let $R = \{a + \sqrt{2}\, b : a, b \in \mathbf{Q}\}$. Under usual addition and multiplication, show that :

   (*i*) (R, +, .) is a ring (*ii*) (R, +, .) is an integral domain

   (*iii*) (R, +, .) is a field.
4. Let $R = \{a + b\sqrt[3]{2}\ : a, b \in \mathbf{Q}\}$. Under usual addition and multiplication, show that (R, +, .) is not a ring.

5. Let $R = \{a + b\sqrt{5} : a, b \in \mathbf{Z}\}$. Under usual addition and multiplication, show that :

(*i*) (R, +, .) is commutative ring with unit element.

(*ii*) (R, +, .) is an integral domain.

(*iii*) (R, +, .) is not a field.

6. Let $R = \{0, 1, 2, 3, 4, 5\}$. Let ⊕ and ⊙ denote the operations 'addition modulo 6' and 'multiplication modulo 6' respectively. Show that :

(*i*) (R, ⊕, ⊙) is a commutative ring with unit element

(*ii*) (R, ⊕, ⊙) is not an integral domain.

(*iii*) (R, ⊕, ⊙) is not a field.

7. Show that $(\mathbf{N}, +, \times)$ is not a ring.

8. Show that the set **R** of real numbers is a subring of the ring (**C**, +, .).

9. Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, where $a, b \in \mathbf{Z}$ is a subring of the ring of all 2×2 matrices over integers under usual addition and multiplication of matrices.

10. Show that the set of matrices $\begin{bmatrix} a & 4 \\ 0 & 0 \end{bmatrix}$, where $a \in \mathbf{Z}$ is a not a subring of the ring of all 2×2 matrices over integers under usual addition and multiplication of matrices.

11. Let S be a subring of a ring R. Define $\phi : S \to R$ by $\phi(x) = x, x \in S$. Show that ϕ is a ring homomorphism for S into R.

12. Define $\phi : (\mathbf{Z}, +, .) \to (\mathbf{Q}, +, .)$ by $\phi(x) = \frac{x}{5}$. Show that ϕ is not a ring homomorphism.

13. Let R and R′ be rings. Define $\phi : R \to R'$ by $\phi(a) = 0$, $a \in R$. Show that ϕ is a ring homomorphism and $\ker \phi = R$.

14. Let R be a ring . Define $\phi : R \to R$ by $\phi(a) = a$, $a \in R$. Show that ϕ is a ring homomorphism and $\ker \phi = \{0\}$.

15. Let R be the ring of all continuous real valued functions defined on $[0, 4]$. Let ϕ be a mapping from the ring R into the ring **R** of real numbers defined by $\phi(f) = f(1)$, $f \in R$. Show that ϕ is a homomorphism of R onto **R**. Show that its kernel consists of all functions in R vanishing at $x = 1$.

16. Let ϕ be an isomorphism of a ring R onto ring R′. If R has a unit element then so do ring R′.

17. Let f be an isomorphism of a ring R onto ring R′. If R′ is an integral domain, then R is also an integral domain.

18. Let $R = \{2n : n \in \mathbf{Z}\}$ and define addition ⊕ and multiplication ⊙ in R by $a \oplus b = a + b$ and $a \odot b = \frac{ab}{2}$ for all $a, b \in R$. Under these operations, R is a ring. Show that this ring and the ring of integers are isomorphic.

NOTES

UNIT 5

IDEALS AND QUOTIENT RINGS

STRUCTURE

5.0. LEARNING OBJECTIVES

NOTES

After going through this unit, you should be able to:

- ideal, sum and product of two ideal
- maximal ideal, prime ideal
- ring, greatest common divisor (G.C.D)
- least common divisor (L.C.D)

5.1. INTRODUCTION

In this chapter, we shall define 'ideal' of a ring, an analog of the concept of 'normal subgroup' for a group. We shall take up different kinds of ideals like principal ideal, maximal ideal and prime ideal. We shall also consider quotient ring of a ring with respect to an ideal and the embedding of an integral domain in a field.

We shall end this chapter with the introduction of principal ideal rings and unique factorization domain.

5.2. IDEAL

Let R be a ring. A non-empty subset I of R is called a **left ideal** of R if

(*i*) I is a subgroup of R under addition *i.e.* $a - b \in I \quad \forall\ a, b \in I$

(*ii*) $ra \in I \quad \forall\ r \in R, a \in I$.

Let R be a ring. A non-empty subset I of R is called a **right ideal** of R if

(*i*) I is a subgroup of R under addition *i.e.* $a - b \in I \quad \forall\ a, b \in I$

(*ii*) $ar \in I \quad \forall\ r \in R, a \in I$.

Let R be a ring. A non-empty subset I of R is called an **ideal** (or **two sided ideal**) if it is both a left ideal and a right ideal.

Thus a non-empty set I of a ring R is an *ideal* of R if

(*i*) $a - b \in I \quad \forall\ a, b \in I$

(*ii*) $ra, ar \in I \quad \forall\ r \in R, a \in I$.

Every ideal of a ring is also a subring of R but a subring of R may not be an ideal of R. This is because if I is an ideal of R, then $r, s \in I \Rightarrow \ r \in I, s \in R \ \Rightarrow \ rs \in I$. An ideal requires a stronger closure property than a subring. For example, the set **Z** of integers is a subring of the ring (**Q**, +,.). However **Z** is not an ideal of (**Q**, +, .) because $2 \in \mathbf{Z}, \frac{1}{3} \in \mathbf{Q}$ but $2\left(\frac{1}{3}\right) = \frac{2}{3} \notin \mathbf{Z}$.

If the ring R is commutative, then every left (resp. right) ideal of R is a right (resp. left) ideal. Thus, in a commutative ring every left (or right) ideal is an ideal.

If R is a ring then {0} and R are always ideals of R. These are called **improper ideals.** Any other ideal of R other then improper ideals is called a **proper ideal.**

A ring having no proper ideal is called a **simple ring.**

Example 1. *Let* $R = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbf{Z}\right\}$. *R is a ring under usual addition and multiplication.*

Let $I = \left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, a, b \in \mathbf{Z}\right\}$. *Show that I is a left ideal of R but not a right ideal of R.*

Sol. $I = \left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathbf{Z}\right\}$ $\quad I \neq \phi$, because $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in I$.

Let $\quad \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \in I$

$\therefore \quad \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in I$

Let $\quad \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in R.$

$\therefore \quad \begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} pa+qb & 0 \\ ra+sb & 0 \end{bmatrix} \in I$

$\therefore$ I is a left ideal of R.

Also, $\quad \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap & aq \\ bp & bq \end{bmatrix}$, which may not be in I.

$\therefore$ I is not a right ideal.

Example 2. *Let R be a ring with unit element 1. If I is an ideal of R and* $1 \in I$, *then show that* $I = R$.

Sol. Since I is an ideal of R, we have $I \subseteq R$.

Let $r \in R$. $\therefore \quad r.1 \in I \quad$ *i.e.,* $\quad r \in I$

$\therefore \quad R \subseteq I.$

Combining, we get $\quad I = R.$

Example 3. *Let* $\phi : R \to R'$ *be a ring homomorphism. If A is an ideal of R, then show that* $\phi(A)$ *is an ideal of* $\phi(R)$.

Sol. $\quad \phi(A) = \{\phi(a) : a \in A\}$

$0 \in A \;\Rightarrow\; \phi(0) \in \phi(A) \quad \therefore \phi(A)$ is non-empty.

Let $\quad \phi(a), \phi(b) \in \phi(A)$

$\therefore \quad \phi(a) - \phi(b) = \phi(a-b) \in \phi(A) \qquad (\because \; a, b \in A \;\Rightarrow\; a - b \in A)$

Let $\phi(r) \in \phi(R)$, where $r \in R$.

$\therefore \quad \phi(r)\,\phi(a) \in \phi(ra) \in \phi(A) \quad$ and $\quad \phi(a)\,\phi(r) = \phi(ar) \in \phi(A)$

$(\because \; r \in R, a \in A \;\Rightarrow\; ra, ar \in A)$

$\therefore \quad \phi(A)$ is an ideal of $\phi(R)$.

Example 4. *Let R be a ring and L is a left ideal of R. Show that the set* $\lambda(L) = \{x \in R : xa = 0 \;\forall\; a \in L\}$ *is an ideal of R.*

Sol. $\quad 0 \in R \;$ and $\; 0.a = 0 \quad \forall\; a \in L.$

$\Rightarrow \quad 0 \in \lambda(L) \;\Rightarrow\; \lambda(L) \neq \phi$

Let $x_1, x_2 \in \lambda(L)$. $\;\therefore\; x_1a = 0, \; x_2a = 0 \quad \forall \quad a \in L$

Now $\quad (x_1 - x_2)a = (x_1 + (-x_2))a = x_1a + (-x_2a) = x_1a - x_2a = 0 - 0 = 0$

$\Rightarrow \quad (x_1 - x_2)a = 0 \;\forall\; a \in L \;\Rightarrow\; x_1 - x_2 \in \lambda(L).$

NOTES

Let $r \in R$ and $x \in \lambda(L)$. $\therefore$ $xa = 0 \quad \forall\, a \in L$

Now $\quad (rx)a = r(xa) = r.0 = 0 \quad \forall\, a \in L$

$\therefore \quad rx \in \lambda(L)$

$\therefore$ $\lambda(L)$ is a left ideal of R.

Also $\quad (xr)a = x(ra) = 0 \qquad (\because \; r \in R, a \in L \;\Rightarrow\; ra \in L)$

$\Rightarrow \quad (xr)a = 0 \quad \forall\, a \in L \;\Rightarrow\; xr \in \lambda(L)$

$\therefore$ $\lambda(L)$ is a right ideal of R.

$\therefore$ $\lambda(L)$ is an ideal of R.

Theorem 1. *The Kernel of a homomorphism of a ring R into a ring R′ is an ideal of R.*

Proof. Let $\phi : R \to R'$ be a homomorphism.

$0 \in \ker \phi$, because $f(0) = 0$. $\quad\therefore$ $\ker \phi$ is non-empty.

Let $\quad a, b \in \ker \phi \quad \therefore \quad \phi(a) = 0, \quad \phi(b) = 0.$

Now $\quad \phi(a - b) = \phi(a + (-b)) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = 0 - 0 = 0$

$\therefore \quad a - b \in \ker \phi$

Let $r \in R$ and $a \in \ker \phi$. $\quad\therefore \quad \phi(a) = 0$

$\phi(ra) = \phi(r)\,\phi(a) = \phi(r).0 = 0 \quad$ and $\quad \phi(ar) = \phi(a)\,\phi(r) = 0.\phi(r) = 0$

$\therefore$ $ra, ar \in \ker \phi$.

$\therefore$ $\ker \phi$ is an ideal of R.

Theorem 2. *A field cannot have any proper ideal.*

Proof. Let F be a field and I be an ideal of F.

Let $I \neq (0) \quad \therefore \quad \exists\, a (\neq 0) \in I$

$a \in I \;\Rightarrow\; a \in F$ and F being a field, we have $a^{-1} \in F$.

$\therefore \quad aa^{-1} \in I \qquad (\because \;$ I is an ideal$)$

$\Rightarrow \quad 1 \in I \;\Rightarrow\; (1)\,x \in I \quad \forall \quad x \in F$

$\Rightarrow \quad x \in I \quad \forall \quad x \in F$

$\Rightarrow \quad F \subseteq I \quad$ *i.e.*, $\quad I = F$

$\therefore$ F cannot have any proper ideal.

Example 5. *Show that a homomorphism of a field into a ring is either one-one or takes each element to 0.*

Sol. Let $\phi : F \to R$ be a homomorphism of a field F into a ring R.

$\therefore$ $\ker \phi$ is an ideal of F. Since F is a field, F has no proper ideal.

$\therefore \quad \ker \phi = (0) \quad$ or $\quad \ker \phi = F$

Let $\text{ke}\, \phi = (0)$ Let $a, b \in F$ and $\phi(a) = \phi(b)$.

$\Rightarrow \quad \phi(a) - \phi(b) = 0 \;\Rightarrow\; \phi(a - b) = 0 \;\Rightarrow\; a - b \in \ker \phi$

$\Rightarrow \quad a - b = 0 \;\Rightarrow\; a = b$

$\therefore$ ϕ is one-one.

Let $\quad \ker \phi = F \quad \therefore \quad \phi(a) = 0 \quad \forall \quad a \in F.$

$\therefore$ The result holds.

Theorem 3. *If a commutative ring with unit element has no proper ideal then it is a field.*

Proof. Let R be a commutative ring with unit element '1' and having no proper ideal.

In order to show that R is a field it is sufficient to show that every non-zero element of R has multiplicative inverse.

NOTES

Let $a(\neq 0) \in$ R.

Define $\quad Ra = \{ra : r \in R\}$

$0 \in R \Rightarrow (0)r (= 0) \in Ra. \quad \therefore \quad Ra \neq \phi$

Let $\quad r_1a, r_2a \in Ra$

$\Rightarrow \quad r_1a - r_2a = r_1a + (-r_2a) = (r_1 + (-r_2))a = (r_1 - r_2)a \in Ra$

$(\because \quad r_1 - r_2 \in R)$

For $\quad r \in R, \quad r(r_1a) = (rr_1)a \in Ra \qquad (\because \quad rr_1 \in R)$

$\therefore$ Ra is a left ideal of R. $\therefore$ Ra is an ideal of R, because R is commutative.

Now $Ra \neq (0)$, because $1.a = a(\neq 0) \in Ra$. $\therefore$ We have Ra = R.

$\Rightarrow \quad 1 \in Ra \Rightarrow 1 = xa$ for some $x \in$ R

$\therefore$ x is the multiplicative inverse of a.

$\therefore$ Every non-zero element of R has multiplicative inverse. $\therefore$ R is a field.

Corollary. Let R be a ring with unity such that R has no right ideal except {0} and R. Prove that R is a division ring.

[**Hent.** For $a(\neq 0) \in$ R, show that aR is a right ideal].

Theorem 4. *Let A and B be two left ideals of a ring R. A ∪ B is a left ideal of R if and only if either A ⊆ B or B ⊆ A.*

Proof. A and B are left ideals of the ring R.

Let $A \subsetneq B$ or $B \subsetneq A$

$A \subsetneq B \Rightarrow A \cup B = B$ and $B \subsetneq A \Rightarrow A \cup B = A$

$\therefore$ If either case, A ∪ B is an ideal of R.

Conversely, let A ∪ B be an ideal of R. If possible, let $A \not\subseteq B$ and $B \not\subseteq A$.

$\therefore \quad \exists\, x \in A, x \notin B$ and $y \in B, y \notin A$

$x \in A \Rightarrow x \in A \cup B$ and $y \in B \Rightarrow y \in A \cup B$

$\therefore \quad x - y \in A \cup B$

$\Rightarrow \quad x - y \in A$ or $x - y \in B$

Let $\quad x - y \in A$

$\therefore \quad x - (x - y) \in A$ or $y \in A$, which is absurd.

Similarly, $x - y \in$ A is impossible.

$\therefore$ Our supposition is wrong.

$\therefore$ Either $A \subseteq B$ or $B \subsetneq A$.

Illustration. Let R be the ring of integers.

The sets $A = \{2n : n \in \mathbf{Z}\}$ and $B = \{5n : n \in \mathbf{Z}\}$ are both ideals of R.

Here $\quad 2 \in A, 5 \in B$

$\therefore \quad 2, 5 \in A \cup B$

Let A ∪ B be an ideal of R.

$\Rightarrow \quad 2 - 5 \in A \cup B \Rightarrow -3 \in A \cup B$

This is impossible.

$\therefore$ $A \cup B$ is not an ideal of R. This has happened because neither $A \subseteq B$ nor $B \subsetneq A$.

NOTES

5.3. SUM OF TWO IDEALS

If A and B are two ideals of a ring R, then their sum A + B is defined as follows:

$$A + B = \{a + B : a \in A \quad \text{and} \quad b \in B\}.$$

Theorem 5. *Prove that the sum of two left ideals of a ring is also a left ideal of the ring.*

Proof. Let A and B be two left ideals of a ring R.

$\therefore$ By definition,

$$A + B = \{A + b : a \in A \quad \text{and} \quad b \in B\}.$$

$$0 \in A, 0 \in B \Rightarrow 0 + 0 (= 0) \in A + B \quad \therefore \quad A + B \neq \phi$$

Let $a_1 + b_1, a_2 + b_2 \in A + B$, where $a_1, a_2 \in A$ and $b_1, b_2 \in B$.

$\therefore$ $a_1 - a_2 \in A$ and $b_1 - b_2 \in B$

$\therefore$ $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in A + B$

Let $r \in R$ and $a + b \in A + B$.

$\therefore$ $r \in R, a \in A, b \in B$

$\therefore$ $ra \in A$ and $rb \in B$

$\therefore$ $r(a + b) = ra + rb \in A + B$

$\therefore$ A + B is a left ideal of R.

Remark 1. The sum of two right ideals of a ring is also a ringht ideal of the ring.

Remark 2. The sum of a left ideal and a right ideal may not be a left (or right) ideal of the ring.

Example 6. *If I_1 and I_2 are two left ideals of a ring R, then show that I_1 is a left ideal of the ring $I_1 + I_2$.*

Sol. Since I_1, I_2 are left ideals of R, their sum $I_1 + I_2$ is also a left ideal of R.

Let $a_1 + a_2, a_1' + a_2' \in I_1 + I_2$, where $a_1, a_1' \in I_1$ and $a_2, a_2' \in I_2$.

$\therefore$ $a_1 + a_2 \in R$ and so $(a_1 + a_2)(a_1' + a_2') \in I_1 + I_2$

$\therefore$ $I_1 + I_2$ is a subring of R and hence a ring in itself.

We have $a_1 - a_1' \in I_1 \quad \forall\, a_1, a_1' \in I_1$

Let $a_1 + a_2 \in I_1 + I_2$ and $a_1' \in I_1$

$\Rightarrow$ $a_1 + a_2 \in R, a_1' \in I_1$

$\Rightarrow$ $(a_1 + a_2)a_1' \in I_1$

$\therefore$ I_1 is a left ideal of $I_1 + I_2$.

5.4. PRODUCT OF TWO IDEALS

If A and B are two ideals of a ring R, then their product AB is defined as follows:

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, n \in N \right\}$$

NOTES

Theorem 6. *Prove that the product of two ideals of a ring is also an ideal of the ring.*

Proof. Let A and B be two ideals of a ring R.

∴ By definition

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, n \in N \right\}$$

$$0 \in A, 0 \in B \;\Rightarrow\; 0.0\ (= 0) \in AB \quad \therefore \quad AB \neq \phi$$

Let $\sum_{i=1}^{m} a_i b_i, \sum_{i=1}^{n} a_i' b_i' \in AB$, where $a_i, a_i' \in A$, $b_i, b_i' \in B$.

$\therefore \; \sum_{i=1}^{m} a_i b_i - \sum_{i=1}^{n} a_i' b_i' = \sum_{i=1}^{m} a_i b_i + \sum_{i=1}^{n} (-a_i') b_i' \in AB$, being finite sum of products.

Let $r \in R$.

$$\therefore \qquad r\left(\sum_{i=1}^{m} a_i b_i\right) = \sum_{i=1}^{m} r(a_i b_i) = \sum_{i=1}^{m} (r a_i) b_i \in AB \quad (\because r \in R, a_i \in A \Rightarrow r a_i \in A)$$

$$\text{Also} \qquad \left(\sum_{i=1}^{m} a_i b_i\right) r = \sum_{i=1}^{m} (a_i b_i) r = \sum_{i=1}^{m} a_i (b_i r) \in AB \quad (\because r \in R, b_i\, B \Rightarrow b_i r \in B)$$

∴ AB is an ideal of R.

Remark. In proving the above theorem, we have used only the following facts:

(*i*) A is a **left** ideal of R.

(*ii*) B is a **right** ideal of R.

Example 7. *If A and B are two ideals of a ring R then show that the ideal AB of R is contained in the ideal A ∩ B of R.*

Sol. We have $\quad AB = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, n \in N \right\}$

and $\qquad A \cap B = \{x : x \in A, x \in B\}.$

Let $\sum_{i=1}^{n} a_i b_i \in AB$, where $a_i \in A$, $b_i \in B$, $n \in N$.

$$b_i \in B \;\Rightarrow\; b_i \in R \;\Rightarrow\; a_i b_i \in A\ \forall\ i \qquad [\because \text{A is a right ideal of R}]$$

$$a_i \in A \;\Rightarrow\; a_i \in R \;\Rightarrow\; a_i b_i \in B\ \forall\ i \qquad [\because \text{B is a left ideal of R}]$$

$$\therefore \qquad a_i b_i \in A \cap B\ \forall\ i$$

$$\therefore \quad \sum_{i=1}^{n} a_i b_i \in A \cap B \qquad [\because A \cap B \text{ is an ideal of R}]$$

$$\therefore \qquad AB \subseteq A \cap B.$$

5.5. IDEAL GENERATED BY A SET

NOTES

Let R be a ring and S, a non-empty subset of R. An ideal A of R is said to be **generated** by S if A is the smallest ideal of R containing S. Alternatively,

(*i*) $S \subseteq A$ and

(*ii*) for any ideal I of R, $S \subseteq I$ implies $A \subseteq I$.

We write A = (S) or A = < S >

Theorem 7. *If A and B are two ideals of a ring R, then the ideal generatd by the set $A \cup B$ is equal to the ideal A + B i.e., $(A \cup B) = A + B$.*

Proof. $a \in A \Rightarrow a = a + 0 \in A + B \quad \therefore \quad A \in A + B$

$b \in B \Rightarrow b = 0 + b \in A + B \quad \therefore \quad B \in A + B$

$\therefore \quad A \cup B \subseteq A + B$

Let I be an ideal of R such that $A \cup B \subseteq I$.

Let $a + b \in A + B$, where $a \in A$, $b \in B$.

$\Rightarrow \quad a, b \in A \in B$

$\Rightarrow \quad a, b \in I \qquad (\because \; A \cup B \subseteq I)$

$\Rightarrow \quad a + b \in I \qquad (\because \; I \text{ is an ideal})$

$\therefore \quad A + B \subseteq I$

$\therefore$ A + B is the ideal generated by $A \cup B$ *i.e.*, $(A \cup B) = A + B$.

5.6. PRINCIPAL IDEAL

Let R be a ring. An ideal of R generated by a singleton set is called a **principal ideal.**

Let $S = \{a\}$, $a \in R$ and A be the ideal generated by S. We say that the ideal A is generated by a and write A = (*a*) or as A = < *a* >. Thus, A is the samkllest ideal of R containing *a*.

Example 8. *Let R be a commulative ring and A, an ideal of R. Let $a \in A$ be such that $b \in A \Rightarrow b = ra$ for some $r \in R$. Show that A = (a).*

Sol. We have $a \in A$. Let I be an ideal of R such that $a \in I$.

Let $b \in A$. $\therefore \exists\, r \in R : b = ra$. Since I is an ideal of R and $a \in I$, $r \in R$, we have $ra \in I$.

$\Rightarrow \quad b \in I \Rightarrow A \subseteq I$

$\therefore$ A is the smallest ideal of R containing *a*.

$\therefore \quad A = (a)$.

Theorem 8. *Let a be an element of a ring R with unit element. Prov that*

$$(a) = \left\{ \sum_{i=1}^{n} r_i a s_i : r_i, s_i \in R, n \in \mathrm{N} \right\}$$

Proof. Let $\quad A = \left\{ \sum_{i=1}^{n} r_i a s_i : r_i, s_i \in R, n \in \mathrm{N} \right\}.$

NOTES

$$1 \in R \;\Rightarrow\; 1.a.1\,(=a) \in A \quad \therefore \quad A \neq \phi \text{ and } a \in A$$

Let $\displaystyle\sum_{i=1}^{m} r_i a s_i, \sum_{i=1}^{n} r_i{}' a s_i{}' \in A$

$$\therefore \quad \sum_{i=1}^{m} r_i a s_i - \sum_{i=1}^{n} r_i{}' a s_i{}' = \sum_{i=1}^{m} r_i a s_i + \sum_{i=1}^{n} (-r_1{}')\, a s_i{}' \in A, \text{ being a finite sum.}$$

Let $r \in R$.

$$\therefore \quad r\left(\sum_{i=1}^{m} r_i a s_i\right) = \sum_{i=1}^{m} r(r_i a s_i) = \sum_{i=1}^{m} (r r_i)\, a s_i \in A$$

and
$$\left(\sum_{i=1}^{m} r_i a s_i\right) r = \sum_{i=1}^{m} (r_i a s_i) r = \sum_{i=1}^{m} r_i a (s_i r) \in A$$

$\therefore$ A is an ideal of R containing a.

Let I be any ideal of R containing a. We shall show that $A \subseteq I$.

Let $r_i, s_i \in R$ for $i = 1, 2, \ldots\ldots, n$ and $n \in \mathbf{N}$.

$$a \in I,\ r_i \in R \quad \Rightarrow \quad r_i a \in I,\ 1 \le i \le n$$

$$r_i a \in I,\ s_i \in R \quad \Rightarrow \quad r_i a s_i \in I,\ 1 \le i \le n$$

$$\therefore \quad \sum_{i=1}^{n} r_i a s_i \in I$$

$$\therefore \quad A \subseteq I$$

$\therefore$ A is the smallest ideal of R containing a.

$$\therefore \quad A = (a)$$

$$\therefore \quad \mathbf{(a)} = \left\{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{r_i a s_i : r_i, s_i \in R, n \in N}\right\}$$

Corollary. Let R be a commutative ring with unit element and $a \in R$.

$$\therefore \quad (a) = \left\{\sum_{i=1}^{n} r_i a s_i : r_i, s_i \in R, n \in \mathbf{N}\right\}$$

Now
$$\sum_{i=1}^{n} r_i a s_i = \sum_{i=1}^{n} a r_i s_i = a\left(\sum_{i=1}^{n} r_i s_i\right) = ar, \text{ for some } r \in R.$$

$$\therefore \quad \mathbf{(a) = \{ar : r \in R\}.}$$

For example, let R be the ring of integers under usual addition and multiplication.

Here $\quad (2) = \{2n : n \in R\}$

This is the principal ideal of R generated by 2.

Theorem 9. *Let a be an element of a comutative ring R with unit element. Prove that $(a) = \{ar : r \in R\}$.*

Proof. Let $\quad A = \{ar : r \in R\}$

$$1 \in R \;\Rightarrow\; a = a.1 \in A \quad \therefore \quad A \neq \phi \text{ and } a \in A$$

Let $\quad ar_1, ar_2 \in A$

$$\therefore \quad ar_1 - ar_2 = a(r_1 - r_2) \in A \qquad [\because \; r_1 - r_2 \in R)$$

Let $\quad ar_1 \in A$ and $r \in R$

$\therefore \quad (ar_1)r = a(r_1r) \in R$ and $r(ar_1) = (ar_1)r = a(r_1\, r) \in R \qquad (\because$ R is com.)

$\therefore$ A is an idal of R containing a.

Let I be any ideal of R containing a. We shall show that $A \subseteq I$.

$$a \in I \Rightarrow ar \in I \quad \forall\, r \in R \Rightarrow A \subseteq I \qquad (\because \text{ I is an ideal})$$

$\therefore$ A is the principal ideal generated by a *i.e.*, $A = (a)$.

$$\therefore \qquad (a) = \{ar : r \in R\}.$$

5.7. PRINCIPAL IDEAL DOMAIN

An integral domain R with unit element is called a **principal ideal domain** if each of its ideal is principal.

In other words, if A is an ideal of a principal ideal domain R, then there exists $a \in R$ such that

$$A = (a) = \{ar : r \in R\}.$$

A principal ideal domain (PID) is also known as a principal ideal ring.

Example 9. *Show that every field is a principal ideal domain.*

Sol. Let F be a field.

$\therefore$ F is a commutative ring with unit element.

Let $\quad a \neq 0$ and $ab = 0$ for some $a, b \in F$.

$$a \neq 0 \Rightarrow a^{-1} \text{ exists}$$

$$\therefore \qquad a^{-1}(ab) = a^{-1}0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow 1.b = 0 \Rightarrow b = 0$$

$\therefore$ F has no zero divisor.

$\therefore$ F is an integral domain.

Since F is a field, its only ideals are (0) and F.

For $\quad x \in F, \; x = 1.x \in (1) \quad \therefore \; F = (1)$

$\therefore$ Every idal of F is a principal ideal.

$\therefore$ F is a principal ideal domain.

$\therefore$ Every field is a principal ideal domain.

Example 10. *Show that the set of integers* **Z** *is a principal ideal domain under usual addition and multiplication.*

Sol. We know that **Z** is a commutative ring with unit element '1'. Also, $ab = 0$ is possible in **Z** only when at least one of a and b is zero.

$\therefore$ There are no zero divisors in **Z.**

$\therefore$ **Z** is an integral domain with unit element.

Let A be any idal of **Z**. If A is the null ideal, then A = (0), so A is a principal ideal. Now let us assume that $A \neq (0)$.

$\therefore \; \exists$ at least one $a(\neq 0) \in A$.

$$a \in A \Rightarrow -a \in A$$

Since either a or $-a$ is positive, A contains positive integers. Let n be the least positive integer in A. We shall show that $A = (n)$.

$$n \in A \;\Rightarrow\; nr \in A \;\; \forall r \in \mathbf{Z} \;\Rightarrow\; (n) \subseteq A$$

Let m be any element of A. By the division algorithm in **Z**, there exist integers q and r such that $m = nq + r$, where $r = 0$ or $0 < r < n$.

$$n \in A \text{ and } q \in \mathbf{Z} \;\Rightarrow\; nq \in A$$

$$\Rightarrow \qquad m - nq \in A \;\Rightarrow\; r \in A \qquad (\because \; m = nq + r \;\Rightarrow\; r = m - nq)$$

Since n is the least positive integer in A, so $0 < r < n$ is impossible.

$\therefore$ $\qquad r = 0$

$\therefore$ $\qquad m = nq \;\Rightarrow\; m \in (n) \;\Rightarrow\; A \subseteq (n)$

$\therefore$ $\qquad A = (n) \quad \therefore \quad$ A is a principal ideal.

$\therefore$ Every ideal of **Z** is a principal ideal.

$\therefore$ **Z** is a principal ideal domain.

Remark. We know that every field is a PID The converse of this is not true, because **Z** is a PID and it is not a field.

5.8. MAXIMAL IDEAL

An ideal M ($\neq$ R) of a ring R is called a **maximal ideal** of R if whenever A is an ideal of R such that $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.

In other words, an ideal M($\neq$ R) of ring R is a maximal ideal if there does not exist any ideal between M and R.

Example 11. *Show that an ideal of the ring of integers* **Z** *is maximal if and only if it is generated by some prime integer.*

Sol. Let p be a prime integer and $A = (p)$.

Now $\qquad A \neq Z \qquad\qquad (\because \; 1 \notin A)$

Let B be an ideal of **Z** and $A \subseteq B \subseteq \mathbf{Z}$.

Since **Z** is a PID, $\exists\, b \in \mathbf{Z} : B = (b)$.

$$A \subseteq B \;\Rightarrow\; p \in (b) \;\Rightarrow\; p = bq \text{ for some } q \in \mathbf{Z}$$

Since p is prime, either $b = 1$ or $q = 1$.

$b = 1 \Rightarrow B = \mathbf{Z}$ and $q = 1 \Rightarrow p = b.\ 1 = b \Rightarrow A = B$

$\therefore$ $\qquad$ Either $B = A$ or $B = \mathbf{Z}$.

$\therefore$ A is a maximal ideal of **Z**.

Conversely, let M be a maximal ideal of **Z**.

Since **Z** is a PID, $\exists\, m \in \mathbf{Z} : M = (m)$.

We assume that $m > 0$, because $(m) = (-m)$.

If possible, let m be not a prime integer.

$\therefore$ $\exists\, a(\neq 1), b(\neq 1) \in \mathbf{Z}$ such that $m = ab$

$$m = ab \;\Rightarrow\; m \in (a) \;\Rightarrow\; M \subseteq (a)$$

Also $(a) \neq \mathbf{Z}$, because $a \neq 1$.

$\therefore$ $\qquad M \subseteq (a) \subset Z$

$\Rightarrow$ $\qquad (a) = M \qquad\qquad (\because \;$ M is maximal$)$

$\Rightarrow$ $\qquad A \in M \;\Rightarrow\; a = mc$ for some $c \in \mathbf{Z}$.

$\Rightarrow \qquad m = ab = (mc)b = m(cb) \;\Rightarrow\; 1 = cb$

This is impossible because $b \neq 1$.

$\therefore$ Our supposition is wrong. $\therefore$ m is a prime integer.

NOTES

5.9. PRIME IDEAL

An ideal P of a commutative ring R is called a **prime ideal** of R if $ab \in$ P, $a, b \in$ R implies that $a \in$ P or $b \in$ P.

Illustrations (*i*) Let R be an integral domain. Let P = (0).

Let $ab \in (0)$ for $a, b \in$ R

$\therefore$ $ab = 0$. Since R is an integral domain, either $a = 0$ or $b = 0$.

$\therefore$ Either $a \in$ P or $b \in$ P.

$\therefore$ (0) is a prime ideal of R.

(*ii*) Let **Z** be the ring of integers.

$\therefore$ **Z** is a commutative ring with unit element.

Let p be a prime number.

$\therefore \qquad (p) = \{pn : n \in \mathbf{Z}\}$

Let $\qquad ab \in (p)$ for $a, b \in \mathbf{Z}$

$\Rightarrow \qquad p/ab \;\Rightarrow\; p/a$ or $p/b \qquad (\because\; p$ is prime)

$\Rightarrow \qquad a \in (p)$ or $b \in (p)$.

$\therefore$ (p) is a prime ideal of Z.

(*iii*) Let R be the commutative ring of even integers. We know that (4) is a maximal ideal or R.

We have $2 \in$ R and $2 \times 2 = 4 \in (4)$. Here $2 \notin (4)$.

$\therefore$ (4) is not a prime ideal of R.

Example 12. *Give an example of a finite commutative ring in which every maximal ideal need not be a prime ideal.*

Sol. Let R = {0, 2, 4, 6}. R is a commutative ring under addition and multiplication modulo 8.

Let $\qquad$ M = {0, 4}

M is an ideal of R. Let I be an ideal of R such that M $\subsetneq$ I $\subseteq$ R.

$\therefore$ I is a subgroup of R under addition modulo 8.

$\Rightarrow \; o(\text{I})/o(\text{R}) \;\Rightarrow\; o(\text{I}) = 1$ or 2 or 4

$o(\text{I}) = 1$ is impossible because $\text{M} \subsetneq \text{I}$

$o(\text{I}) = 2 \;\Rightarrow\; \text{I} = \text{M}$

$o(\text{I}) = 4 \;\Rightarrow\; \text{I} = \text{R}$

$\therefore$ M is maximal ideal.

Now $\qquad 2 \otimes_8 6 = 4 \in$ M and $2 \notin$ M, $6 \notin$ M.

$\therefore$ M is not a prime ideal.

Example 13. *Show that every non-zero prime ideal of a principal ideal domain is a maximal ideal.*

Sol. Let P be a non-zero prime ideal of a principal ideal domain R.

Let $a(\neq 0) \in$ R and P = (a).

Let Q = (b) be an ideal of R such that $P \subseteq Q \subseteq R$.

$$a \in P \;\Rightarrow a \in Q \;\Rightarrow\; a = br \text{ for some } r \in R.$$

$$\Rightarrow br \in P \;\Rightarrow\; b \in P \quad \text{or} \quad r \in P$$

Let $\quad b \in P \;\; \therefore \;\; br' \in P \;\; \forall \;\; r'\, R$

$\Rightarrow \qquad Q \subseteq P \;\Rightarrow\; P = Q.$

Let $\quad r \in P \;\; \therefore \;\; r = ar''$ for some $r'' \in R$

$\therefore \qquad r = ar'' \;\Rightarrow\; r = (br)\, r'' \;\Rightarrow\; r(1 - br'') = 0$

$\Rightarrow \qquad 1 - br'' = 0 \qquad (\because \;\; r = 0 \;\Rightarrow\; a = b.0 = 0$, which is impossible)

$\Rightarrow \qquad br'' = 1 \;\Rightarrow\; 1 \in (b) \;\Rightarrow\; Q = R$

$\therefore \qquad P \subseteq Q \subseteq R \;\Rightarrow\;$ either Q = P or Q = R.

∴ P is a maximal ideal of R.

5.10. QUOTIENT RING

Let R be a ring and U, an ideal of R.

∴ U can be considered as a subgroup of the abelian group R under addition. Since, the group R is abelian, a right coset U + a of U in R is same as the left coset a + U.

∴ It is sufficient to say that U + a is a coset of U in R.

Let R/U denote the set of all distinct cosets of U in R.

$$\therefore \qquad R/U = \{U + a : a \in R\}$$

We define addition and multiplication in R/U as follows:

$$(U + a) + (U + a) = U + (a + b)$$

and $\qquad (U + a)(U + b) = U + ab \quad$ for $\quad U + a,\, U + b \in R/U.$

Operations on R/U are well defined.

Let $\qquad U + a = U + a' \quad$ and $\quad U + b = U + b'$

Now $\qquad a \in U + a \;\Rightarrow\; a \in U + a' \;\Rightarrow\; a = u_1 + a'$ for some $u_1 \in U$

$\qquad b \in U + b \;\Rightarrow\; b \in U + b' \;\Rightarrow\; b = u_2 + b'$ for some $u_2 \in U$

$\therefore \qquad a + b = (u_1 + a') + (u_2 + b') = u_1 + u_2 + a' + b'$

$\Rightarrow \qquad U + a + b = U + u_1 + u_2 + a' + b' \qquad$ ...(1)

Since U is an ideal of R, we have $u_1 + u_2 \in U$.

$\therefore \qquad U + u_1 + u_2 = U$

∴ (1) $\Rightarrow\; U + (a + b) = U + (a' + b')$

⇒ Addition in R/U is well defined.

Also $\qquad ab = (u_1 + a')\,(u_2 + b') = u_1u_2 + u_1b' + a'u_2 + a'b'$

$\Rightarrow \qquad U + ab = U + u_1u_2 + u_1b' + a'u_2 + a'b' \qquad$ ...(2)

Since U is an ideal of R, we have $u_1u_2, u_1b', a'u_2 \in$ U.

$\Rightarrow \qquad u_1u_2 + u_1b' + a'u_2 \in$ U

$\Rightarrow \qquad$ U $+ u_1u_2 + u_1b' + a'u_2 =$ U

$\therefore$ (2) $\Rightarrow \qquad$ U $+ ab =$ U $+ a'b'$

$\Rightarrow$ Multiplication in R/U is well defined.

Associativity of addition.

Let $\qquad$ U $+ a$, U $+ b$, U $+ c \in$ R/U.

$$(\mathrm{U} + a) + [(\mathrm{U} + b) + (\mathrm{U} + c)] = (\mathrm{U} + a) + (\mathrm{U} + b + c) = \mathrm{U} + a + (b + c)$$

Also $[(\mathrm{U} + a) + (\mathrm{U} + b)] + (\mathrm{U} + c) = (\mathrm{U} + a + b) + (\mathrm{U} + c = \mathrm{U} + (a + b) + c$

$\therefore \qquad (\mathrm{U} + a) + [(\mathrm{U} + b) + (\mathrm{U} + c)] = [(\mathrm{U} + a) + (\mathrm{U} + b)] + (\mathrm{U} + c)$

$(\because \quad a + (b + c) = (a + b) + c)$

$\therefore$ Addition is associative.

Existence of additive identity. Let U $+ a \in$ R/U.

$$0 \in \mathrm{U} \Rightarrow \mathrm{U} + 0 \in \mathrm{R/U}$$

Now $\qquad (\mathrm{U} + a) + (\mathrm{U} + 0) = \mathrm{U} + a + 0 = \mathrm{U} + a$

and $\qquad (\mathrm{U} + 0) + (\mathrm{U} + a) = \mathrm{U} + 0 + a = \mathrm{U} + a$

$\therefore$ U + 0 *i.e.,* U is the additive identity of R/U.

Existence of additive inverse. Let U $+ a \in$ R/U.

$\Rightarrow \qquad a \in \mathrm{R} \Rightarrow -a \in \mathrm{R} \Rightarrow \mathrm{U} + (-a) \in \mathrm{R/U}$

Now $\qquad (\mathrm{U} + a) + (\mathrm{U} + (-a)) = \mathrm{U} + (a + (-a)) = \mathrm{U} + 0 = \mathrm{U}$

and $\qquad (\mathrm{U} + (-a)) + (\mathrm{U} + a) = \mathrm{U} + ((-a) + (-a) + a) = \mathrm{U} + 0 = \mathrm{U}$

$\therefore$ U $+ (-a)$ is the additive inverse of U $+ a$.

Commutativity of addition. Let U $+ a$, U $+ b \in$ R/U.

$\therefore \qquad (\mathrm{U} + a) + (\mathrm{U} + b) = \mathrm{U} + a + b = \mathrm{U} + b + a = (\mathrm{U} + b) + (\mathrm{U} + a)$

$\therefore$ Addition is commutative.

Associativity of multiplication. Let U $+ a$, U $+ b$, U $+ c \in$ R/U.

$$(\mathrm{U} + a)\ [(\mathrm{U} + b)\ (\mathrm{U} + c)] = (\mathrm{U} + a)\ (\mathrm{U} + bc) = \mathrm{U} + a(bc)$$

Also $\quad [(\mathrm{U} + a)(\mathrm{U} + b)](\mathrm{U} + c) = (\mathrm{U} + ab)(\mathrm{U} + c) = \mathrm{U} + (ab)c$

$\therefore \qquad (\mathrm{U} + a)\ [(\mathrm{U} + b)(\mathrm{U} + c)] = [(\mathrm{U} + a)(\mathrm{U} + b)]\ (\mathrm{U} + c) \qquad (\because \quad a(bc) = (ab)c)$

$\therefore$ Multiplication is associative.

Distributivity of multiplication over addition. Let U $+ a$, U $+ b$, U $+ c \in$ R/U.

$$\begin{aligned}(\mathrm{U} + a)\ [(\mathrm{U} + b) + (\mathrm{U} + c)] &= (\mathrm{U} + a)(\mathrm{U} + b + c) = \mathrm{U} + a(b + c) = \mathrm{U} + ab + ac\\ &= (\mathrm{U} + ab) + (\mathrm{U} + ac)\\ &= (\mathrm{U} + a)(\mathrm{U} + b) + (\mathrm{U} + a)(\mathrm{U} + c)\end{aligned}$$

Similarly, we can show that

$$[(\mathrm{U} + b) + (\mathrm{U} + c)](\mathrm{U} + a) = (\mathrm{U} + b)(\mathrm{U} + a) + (\mathrm{U} + c)(\mathrm{U} + a)$$

$\therefore$ R/U is a ring. This ring is called the **quotient ring** of R with respect to the ideal U of R.

NOTES

Theorem 10. *Let U be an ideal of a ring R and R / U, the quotient ring of R with respect to the ideal U.*

(*i*) *If R is commutative then so is R / U.*

(*ii*) *If R has unit element '1', then R / U has unit element U + 1.*

Proof. (*i*) Let U + a, U + b ∈ R/U.

$$(U + a)(U + b) = U + ab = U + ba = (U + b)\ (U + a)$$

$$(\because\quad ab = ba)$$

∴ R/U is commutative.

(*ii*) Let U + a ∈ R/U.

$$(U + a)(U + 1) = U + a(1) = U + a$$

and $$(U + 1)(U + a) = U + (1)a = U + a$$

∴ $$(U + a)(U + 1) = U + a = (U + 1)(U + a)$$

∴ U + 1 is the unit element of R/U.

Theorem 11. *Let U be an ideal of a ring R. Define $\phi : R \to R / U$ by $\phi(a) = U + a$ $\forall\ a \in R$. Show that*

(*i*) *φ is a homomorphism of R onto R / U*

(*ii*) *ker φ = U.*

Proof. We have $\phi : R \to R/U$ defined by $\phi(a) = U + a \quad \forall \quad a \in R$.

(*i*) Let $a, b \in R$.

∴ $$\phi(a + b) = u + a + b = (U + a) + (U + b) = \phi(a) + \phi(b)$$

and $$\phi(ab) = U + ab = (U + a)\ (U + b) = \phi(a)\ \phi(b)$$

∴ φ is a homomorphism.

Let $$U + a \in R/U.$$

∴ $$a \in R \quad \text{and} \quad \phi(a) = U + a$$

∴ φ is onto.

(*ii*) Let $u \in U$.

∴ $$\phi(u) = U + u = U = \text{zero of } R/U$$

⇒ $$u \in \ker \phi \quad \Rightarrow \quad U \subseteq \ker \phi.$$

Conversely, Let $a \in \ker \phi$.

∴ $$\phi(a) = U \quad \text{or} \quad U + a = U.$$

∴ $$0 + a \in U + a \quad \Rightarrow \quad 0 + a \quad i.e., \quad a \in U$$

⇒ $$\ker \phi \subseteq U. \quad \therefore \quad \ker \phi = U.$$

Remark. Part (*i*) says that *every quotient ring of a ring is a homorphic image of the ring under consideration.*

5.11. THE FUNDAMENTAL THEOREM OF HOMOMORPHISM

Statement. *Let φ be a homomorphism of a ring R onto a ring R′. Then R / ker φ ≅ R′.*

Proof. φ is a homomorphism of ring R onto ring R′. Let U be the kernel of the homorphism φ.

$\therefore$ U is an ideal of ring R.

$\therefore$ R/U is a quotient ring of R.

Define $\psi : R/U \to R'$ by $\psi(U + a) = \phi(a) \in R' \quad \forall \quad U + a \in R/U$.

ψ is well defined. Let $U + a, U + b. \in R/U$ and $U + a = U + b$.

Let $a = u + b$ for some $u \in U$.

$\therefore \quad a = 0 + a \in U + a \quad \Rightarrow \quad a \in U + b$.

$\therefore \quad a - b = u$ and thus $a - b \in U$

$\therefore \qquad \phi(a - b) = 0 \qquad (\because \quad U = \ker \phi)$

$\Rightarrow \qquad \phi(a) + \phi(-b) = 0 \quad \Rightarrow \quad \phi(a) - \phi(b) = 0 \quad \Rightarrow \quad \phi(a) = \phi(b)$

$\Rightarrow \qquad \psi(U + a) = \psi(U + b).$

$\therefore \quad \psi$ is well defined.

ψ is a homomorphism. Let $U + a, U + b \in R/U$.

$$\psi((U + a) + (U + b)) = \psi(U + a + b) = \phi(a + b)$$
$$= \phi(a) + \phi(b) = \psi(U + a) + \psi(U + b)$$

and
$$\psi((U + a)(U + b)) = \psi(U + ab) = \phi(ab) = \phi(a)\,\phi(b)$$
$$= \psi(U + a)\,\psi(U + b)$$

$\therefore \quad \psi$ is homomorphism.

ψ is one-one. Let $U + a, U + b \in R/U$ and $\psi(U + a) = \psi(U + b)$.

$\Rightarrow \qquad \phi(a) = \phi(b) \qquad \Rightarrow \quad \phi(a) - \phi(b) = 0$

$\Rightarrow \qquad \phi(a) + \phi(-b) = 0 \qquad \Rightarrow \quad \phi(a + (-b)) = 0$

$\Rightarrow \qquad \phi(a - b) = 0 \qquad \Rightarrow \quad a - b \in \ker \phi \quad$ *i.e.,* $\quad a - b \in U$

Let $\qquad a - b = u, \quad u \in U$

$\Rightarrow \qquad a = u + b \qquad \Rightarrow \quad U + a + U + u + b = U + b$

$\therefore \qquad \psi(U + a) = \psi(U + b) \qquad \Rightarrow \quad U + a = U + b$

$\therefore \quad \psi$ is one-one.

ψ is onto. Let $a' \in R'$. Since $\phi : R \to R'$ is onto, there exists $a \in R$ such that $\phi(a) = a'$.

$\therefore \qquad U + a \in R/U \quad$ and $\quad \psi(U + a) = \phi(a)' = a'$

$\therefore \quad \psi$ is onto.

$\therefore \quad \psi$ is a one-one homomorphism of R/U onto R′.

$\therefore \qquad R/U \cong R' \quad$ *i.e.,* $\quad$ **R/ker φ ≅ R′**.

5.12. FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

Let D be an integral domain with at least two elements. Let $D_o = D - \{0\}$. $\therefore \quad D_o \neq \phi$

Define a relation ~ on $D \times D_o$ as follows :

$(a, b) \sim (c, d)$ if and only if $ad = bc$.

~ is an equivalence relation.

Let $\qquad (a, b) \in D \times D_o$.

We have $\qquad ab = ba. \quad \therefore \quad (a, b) \sim (a, b) \quad \forall \ (a, b) \in D \times D_o$

$\therefore \quad \sim$ is reflexive.

NOTES

Let $\quad (a, b), (c, d) \in D \times D_o \quad$ and $\quad (a, b) \sim (c, d)$.

$\Rightarrow \qquad ad = bc \quad \Rightarrow \quad cb = da \quad \Rightarrow \quad (c, d) \sim (a, b)$

$\therefore \quad \sim$ is symmetric.

Let $(a, b), (c, d), (e, f) \in D \times D_o$ and $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$.

$\Rightarrow \qquad ad = bc \quad$ and $\quad cf = de$

$\Rightarrow \qquad (ad)f = (bc)f \quad \Rightarrow \quad adf = b(cf)$

$\Rightarrow \qquad adf = b(de) \quad \Rightarrow \quad (af)d = (be)d$

$\Rightarrow \qquad af = be \qquad (\because \quad d \neq 0$ and D is an integral domain)

$\Rightarrow \qquad (a, b) \sim (e, f)$

$\therefore \quad \sim$ is transitive.

$\therefore \quad$ The relation $\sim$ on $D \times D_o$ is an equivalence relation.

$\therefore \quad$ The relation $\sim$ partitions the set $D \times D_o$ into mutually disjoint equivalence classes.

For $(a, b) \in D \times D_o$, let $\frac{a}{b}$ denote the equivalence class of (a, b).

$$\therefore \qquad \frac{a}{b} = \{(c, d) \in D \times D_o : (c, d) \sim (a, b)\}$$

Let F be the family of all these equivalence classes.

Let $\qquad \frac{a}{b}, \frac{c}{d} \in F \quad$ and $\quad \frac{a}{b} = \frac{c}{d}$

Since $\sim$ is reflexive, $(a, b) \in \frac{a}{b}$.

$$\Rightarrow \qquad (a, b) \in \frac{c}{d} \quad \Rightarrow \quad (a, b) \sim (c, d) \quad \Rightarrow \quad ad = bc$$

$\therefore \quad$ If $\frac{a}{b}, \frac{c}{d} \in F$ and are equal then, we have $ad = bc$.

Conversely, let $ad = bc$, where $a, b, c, d \in D$ and $b \neq 0$, $d \neq 0$.

$$\Rightarrow \qquad (a, b) \sim (c, d) \quad \Rightarrow \quad (a, b) \in \frac{c}{d} \quad \Rightarrow \quad \frac{a}{b} = \frac{c}{d} \qquad \left(\because \quad (a, b) \in \frac{a}{b}\right)$$

$\therefore \quad$ The elements $\frac{a}{b}, \frac{c}{d}$ of F are equal if and only if $ad = bc$.

We define addition and multiplication in F as follows.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad \text{for} \quad \frac{a}{b}, \frac{c}{d} \in F.$$

Operations on F are well defined.

Let $\qquad \frac{a}{b} = \frac{a'}{b'} \quad$ and $\quad \frac{c}{d} = \frac{c'}{d'}$

$\Rightarrow \qquad ab' = ba' \quad$ and $\quad cd' = dc' \qquad$ ...(1)

(1) $\Rightarrow \qquad ab'dd' = ba'dd' \quad$ and $\quad bb'cd' = bb'dc'$

$\Rightarrow \qquad ab'dd' + bb'cd' = ba'dd' + bb'dc'$

$\Rightarrow \qquad adb'd' + bcb'd' = a'd'bd + b'c'bd$

$\Rightarrow \qquad (ad + bc)b'd' = (a'd' + b'c')bd$

$$\Rightarrow \qquad \frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'} \quad \Rightarrow \quad \frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}.$$

(By equality of elements of F)

$\Rightarrow$ Addition in F is well defined.

(1) $\Rightarrow$ $\quad ab'cd' = ba'dc' \quad \Rightarrow \quad (ac)(b'd') = (a'c')(bd)$

$$\Rightarrow \qquad \frac{ac}{bd}=\frac{a'c'}{b'd'} \quad \Rightarrow \quad \frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}.$$

(By equality of elements of F)

$\Rightarrow$ Multiplication in F is well defined.

Now we shall show that (F, +, .) is a field.

Let $\quad a(\neq 0) \in \text{D}. \quad \therefore \quad \frac{0}{a}, \frac{a}{a} \in \text{F}$

$$\frac{0}{a}=\frac{a}{a} \quad \Rightarrow \quad (0)a = aa \quad \Rightarrow \quad aa = 0 \quad \Rightarrow a = 0$$

($\because$ D is an I.D.)

This is impossible.

$\therefore \quad \frac{0}{a} \neq \frac{a}{a}$. Thus, F has at least two elements.

Addition is associative. Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \text{F}$.

$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\left(\frac{cf+de}{df}\right)=\frac{adf+b\,(cf+de)}{b(df)}=\frac{adf+bcf+bde}{bdf}$$

Also, $\quad \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+bde}{(bd)f}=\frac{adf+bcf+bde}{bdf}$

$$\therefore \qquad \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\left(\frac{a}{b}+\left(\frac{c}{d}\right)+\frac{e}{f}\right).$$

Existence of additive identity. Let $\frac{a}{b} \in \text{F}$. For $\quad k(\neq 0) \in \text{D}, \quad \frac{0}{k} \in \text{F}$.

Now $\qquad \frac{a}{b}+\frac{0}{k}=\frac{ak+b(0)}{bk}=\frac{ak}{bk}=\frac{a}{b} \qquad (\because \quad akb = bka)$

and $\qquad \frac{0}{k}+\frac{a}{b}=\frac{(0)b+ka}{kb}=\frac{ka}{kb}=\frac{a}{b}.$

$$\therefore \qquad \frac{a}{b}+\frac{0}{k}=\frac{a}{b}=\frac{0}{k}+\frac{a}{b}$$

$\therefore \quad \frac{0}{k}$ is the additive identity of F.

Here note that $\frac{0}{k}=\frac{0}{\lambda}$ for any $\lambda(\neq 0) \in \text{D}$ because $(0)\lambda = 0(k)$.

Existence of additive inverse. Let $\frac{a}{b} \in$ F.

$$\Rightarrow \qquad a \in \text{D} \ \Rightarrow \ -a \in \text{D} \ \Rightarrow \ \frac{-a}{b} \in \text{F}$$

Now $$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{bb} = \frac{ab - ab}{b^2} = \frac{0}{b^2}$$

and $$\frac{-a}{b} + \frac{a}{b} = \frac{(-a)\,b + ba}{bb} = \frac{-ab + ab}{b^2} = \frac{0}{b^2}.$$

$$\therefore \qquad \frac{a}{b} + \frac{-a}{b} = \frac{0}{b^2} = \frac{-a}{b} + \frac{a}{b}$$

$\therefore$ $\frac{-a}{b}$ is the additive inverse of $\frac{a}{b}$.

Here note that $\frac{0}{b^2} = \frac{0}{k}$ for any $k(\neq 0) \in$ D.

Addition is commutative. Let $\frac{a}{b}, \frac{c}{d} \in$ F.

$$\therefore \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b}$$

$\therefore$ (F, +) is an abelian group.

Multiplication is associative. Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in$ F.

$$\frac{a}{b}\left(\frac{c}{d}.\frac{e}{f}\right) = \frac{a}{b}.\frac{ce}{df} = \frac{ace}{bdf} = \frac{ac}{bd}.\frac{e}{f} = \left(\frac{a}{b}.\frac{c}{d}\right).\frac{e}{f}$$

$$\therefore \qquad \frac{a}{b}.\left(\frac{c}{d}.\frac{e}{f}\right) = \left(\frac{a}{b}.\frac{c}{d}\right).\frac{e}{f}.$$

Existence of multiplicative identity. Let $\frac{a}{b} \in$ F. For $k(\neq 0) \in$ D, $\frac{k}{k} \in$ F.

Now $$\frac{a}{b}.\frac{k}{k} = \frac{ak}{bk} = \frac{a}{b} \quad \text{and} \quad \frac{k}{k}.\frac{a}{b} = \frac{ka}{kb} = \frac{a}{b}$$

$$\therefore \qquad \frac{a}{b}.\frac{k}{k} = \frac{a}{a} = \frac{k}{k}.\frac{a}{b}$$

$\therefore$ $\frac{k}{k}$ is the multiplicative identity of F.

Here note that $\frac{k}{k} = \frac{\lambda}{\lambda}$ for any $\lambda(\neq 0) \in$ D, because $k\lambda = k\lambda$.

Existence of multiplicative inverse. Let $\frac{a}{b} \in$ F and $\frac{a}{b} \neq \frac{0}{k}$ for any $k(\neq 0)$ $\in$ D.

$\Rightarrow$ $a \neq 0$ for otherwise $\frac{a}{b} = \frac{0}{b}$ and $\frac{0}{b}$ is equal to $\frac{0}{k}$ $\Rightarrow$ $\frac{b}{a} \in$ F.

Now $\frac{a}{b}.\frac{b}{a}=\frac{ab}{ba}=\frac{ab}{ab}$ and $\frac{b}{a}.\frac{a}{b}=\frac{ba}{ab}=\frac{ab}{ab}$

$$\therefore \quad \frac{a}{b}.\frac{b}{a}=\frac{ab}{ab}=\frac{b}{a}.\frac{a}{b}$$

$\therefore$ $\frac{b}{a}$ is the multiplicative inverse of $\frac{a}{b}$.

Here note that $\frac{ab}{ab}$ is the multiplicative identity because $\frac{ab}{ab}=\frac{k}{k}$ for any $k(\neq 0)$ $\in$ D.

Multiplication is commutative. Let $\frac{a}{b},\frac{c}{d}\in$ F.

$$\therefore \quad \frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}.\frac{a}{b}.$$

$\therefore$ (F, .) is an abelian group.

Distributivity. Let $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in$ F.

$$\frac{a}{b}.\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}.\frac{cf+de}{df}=\frac{a\,(cf+de)}{bdf}=\frac{acf+ade}{bdf}$$

Also $\frac{a}{b}.\frac{c}{d}+\frac{a}{b}.\frac{e}{f}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{acbf+bdae}{bdbf}=\frac{(acf+ade)b}{(bdf)b}=\frac{acf+ade}{bdf}$

$$\therefore \quad \frac{a}{b}.\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}.\frac{c}{d}+\frac{a}{b}.\frac{e}{f}.$$

Second distributive law holds as a consequence of commutative law of multiplication.

$\therefore$ (F, +, .) is a field.

This field is called the **field of quotient of the integral domain D.**

5.13. EMBEDDING OF A RING

A ring R is said to be **embedded** in a ring R′ if there exists an isomorphism of R into R′.

If R is embedded in R′ then R′ is called an **over-ring** or **extension** of R.

Theorem 12. *Every integral domain with at least two elements can be embedded in a field.*

Proof. Let D be an integral domain containing at least two elements.

Let $D_o = D - \{0\}$. $\therefore$ $D_o \neq \phi$

Define a relation ~ on D × D_o as follows :

$(a, b) \sim (c, d)$ if and only if $ad = bc$.

$\therefore$ ~ is an equivalence relation.

$\therefore$ The relation ~ partitions the set $D \times D_o$ into mutually disjoint equivalence classes. For $(a, b) \in D \times D_o$, let $\frac{a}{b}$ denote the equivalence class of (a, b).

$$\therefore \qquad \frac{a}{b} = \{(c, d) \in D \times D_o : (c, d) \sim (a, b)\}$$

Let F be the family of all these equivalence classes.

In F, the elements $\frac{a}{b} = \frac{c}{d}$ iff $(a, b) \sim (c, d)$ iff $ad = bc$.

For $\frac{a}{b}, \frac{c}{d} \in F$, we define addition and multiplication as follows :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Under these operations, F is a field. This field is called the field of quotients of the integral domain D.

Let k be any arbitrary but fixed non-zero element of D.

Define $\phi : D \to F$ by $\phi(a) = \frac{ak}{k} \quad \forall\, a \in D$.

ϕ is well defined. Let $a, b \in D$

$$\therefore \qquad \phi(a) = \frac{ak}{k}, \quad \phi(b) = \frac{bk}{k}.$$

$$a = b \;\Rightarrow\; akk = kbk \;\Rightarrow\; \frac{ak}{k} = \frac{bk}{k}$$

$\therefore$ ϕ is well defined.

ϕ is a homomorphism. Let $a, b \in D$.

$$\phi(a + b) = \frac{(a + b)k}{k}$$

$$\text{Also} \qquad \phi(a) + \phi(b) = \frac{ak}{k} + \frac{bk}{k} = \frac{akk + kbk}{kk}$$

$$= \frac{(a + b)kk}{kk} = \frac{(a + b)k}{k}.$$

$$\therefore \qquad \phi(a + b) = \phi(a) + \phi(b)$$

$$\text{Also,} \qquad \phi(ab) = \frac{(ab)k}{k} = \frac{abkk}{kk} = \frac{ak}{k} = \frac{bk}{k} = \phi(a)\,\phi(b)$$

$\therefore$ ϕ is a homomorphism.

ϕ is one-one. Let $a, b \in D$ and $\phi(a) = \phi(b)$.

$$\Rightarrow \qquad \frac{ak}{k} = \frac{bk}{k} \;\Rightarrow\; akk = kbk$$

$$\Rightarrow \qquad k(a - b) = 0 \;\Rightarrow\; k(a - b) = 0 \;\Rightarrow\; a - b = 0 \quad (\because \;\; \text{D is an I.D.})$$

$\therefore$ ϕ is one-one.

$\therefore$ ϕ is a one-one homomorphism on D into F.

$\therefore$ ϕ is an isomorphism of D into F.

$\therefore$ The integral domain D is embedded in the field of quotients of the integral domain D.

$\therefore$ Every integral domain with at least two elements can be embedded in a field. This completes the proof.

5.14. UNIT

Let R be a commutative ring with unit element. An element $a\ (\neq 0) \in$ R is called a **unit** in R if there exist an element $b \in$ R such that $ab = 1$.

For example, let F be a field and $a\ (\neq 0) \in$ F.

Let b be the multiplicative inverse of a.

$\therefore \qquad ab = 1.$

$\therefore$ a is a unit in F.

$\therefore$ Every non-zero element in a field is a unit.

Remark. The 'unit' and 'unit element' are different concepts. A commutative ring with unit element may have more than one units but its unit element is unique.

Illustrations

1. ± 1 are the only units in the ring of integers **Z**.

2. ± 1 and $\pm i$ are the only units in the ring **Z**$[i]$, where **Z**$[i] = \{x + iy : x, y \in \mathbf{Z}\}$. This is so because we have

$$(1)(1) = 1, (-1)(-1) = 1, (i)(-i) = 1.$$

5.15. DIVISIBILITY IN A COMMUTATIVE RING

Let $a(\neq 0)$, b be elements of a commutative ring R. a is said to **divide** b if there exits $c \in$ R such that $b = ac$.

We shall use the symbol a/b to represent the fact that a divides b and $a \nmid b$ to mean that a does not divide b.

If a divides b, then we say that a is a **factor** of b. Further a is called a **proper factor** of b if a and c are both non-units, where $b = ac$.

For example, 2/10 in the ring of integers **Z**, because $5 \in$ **Z** and $10 = 2.5$. Here 2 is a proper factor of 10 because 2 and 5 are both non-units in **Z**.

Remark. An element $a \in$ R is a unit if and only if a divides 1.

Theorem 13. *If a, b, c be elements of a commutative ring R, then*

(*i*) $a/b,\ b/c \ \Rightarrow\ a/c$

(*ii*) $a/b,\ a/c \ \Rightarrow\ a/(b \pm c)$

(*iii*) $a/b \ \Rightarrow\ a/bd \ \ \forall \ \ d \in R.$

Proof. (*i*) $\qquad a/b \ \Rightarrow\ b = ax$ for some $x \in$ R

$\qquad b/c \ \Rightarrow\ c = by$ for some $y \in$ R

Now $\qquad c = by = (ax)y = a(xy) \ \Rightarrow\ a/c. \qquad (\because\ xy \in$ R$)$

(*ii*) $a/b \Rightarrow b = ax$ for some $x \in$ R

$a/c \Rightarrow c = ay$ for some $y \in$ R

Now $b \pm c = ax \pm ay = a(x \pm y) \Rightarrow a/(b \pm c)$. $(\because x \pm y \in \text{R})$

(*iii*) $a/b \Rightarrow b = ax$ for some $x \in$ R

$\Rightarrow bd = (ax)d = a(xd) \Rightarrow a/bd$. $(\because xd \in \text{R})$

5.16. GREATEST COMMON DIVISOR (G.C.D.)

Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $d \in$ R is called the **greatest common divisor (g.c.d.)** of a and b if

(*i*) d/a, d/b

(*ii*) whenever $c(\neq 0) \in$ R is such that c/a and c/b then c/d.

we write $d = (a, b)$ whenever d is the g.c.d. of a and b.

5.17. LEAST COMMON MULTIPLE (L.C.M.)

Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $l \in$ R is called the **least common multiple (l.c.m.)** of a and b if

(*i*) a/l, b/l

(*ii*) whenever $c(\neq 0) \in$ R is such that a/c and b/c then l/c.

We write $l = [a, b]$ whenever l is the l.c.m. of a and b.

5.18. ASSOCIATE

Let R be a commutative ring with unit element. An element a of R is said to be an **associate** of $b \in$ R if $a = ub$ for some unit u in R.

If a is an associate of b, then b is an associate of a because $a = ub$ implies $b = u^{-1}a$.

If $a \in$ R, then all the associates of a can be obtained by multiplying different units of the ring by a.

For example, the ring of integer **Z** has only two units 1, – 1.

$\therefore$ For any $a(\neq 0) \in$ **Z**, the associates of a are $a(= 1.a)$ and $-a(= (-1)a)$.

Remark. If a and b are associates then $a = u_1 b$ and $b = u_2 a$ for some units u_1, and u_2.

Theorem 14. *Let R be an integral domain with unit element. Two non-zero elements a, b of R are associates if and only if a/b and b/a.*

Proof. Let non-zero elements a, b of R be associates.

$\therefore$ $\exists$ a unit $u \in$ R : $a = ub$.

$$a = ub \Rightarrow u^{-1}a = u^{-1}(ub) \Rightarrow b = u^{-1}a$$

Now $a = ub \Rightarrow b/a$ and $b = u^{-1}a \Rightarrow a/b$.

NOTES

Conversely, let a/b and b/a.

$a/b \Rightarrow b = ax$ for some $x \in R$

$b/a \Rightarrow a = by$ for some $y \in R$

$\therefore \quad b = ax = (by)x = b(xy)$

$\Rightarrow \quad b - b(xy) = 0 \Rightarrow b.1 - b(xy) = 0 \Rightarrow b(1 - xy) = 0$

$\Rightarrow \quad 1 - xy = 0$ $\qquad$ ($\because$ $b \neq 0$ and R is an I.D.)

$\Rightarrow \quad xy = 1 \Rightarrow x$ and y are units in R.

$\therefore$ a and b are associates.

Example 14. *Let R be an integral domain with unit element and $d_1 = (a, b)$. Show that an element d_2 of R is also equal to (a, b) if and only if d_1 and d_2 are associates.*

Sol. We have $\quad d_1 = (a. b)$.

Let $\quad d_2 = (a, b)$

$\therefore \quad d_1/a, d_1/b, d_2/a, d_2/b, d_1/d_2, d_2/d_1$

Let $\quad d_2 = xd_1$ and $d_1 = yd_2$

$\Rightarrow \quad d_2 = x(yd_2) \Rightarrow 1.d_2 - (xy)d_2 = 0$

$\Rightarrow \quad (1 - xy)d_2 = 0 \Rightarrow 1 - xy = 0$ $\qquad$ ($\because$ $d_2 \neq 0$)

$\Rightarrow \quad xy = 1$

$\therefore$ x, y are both units.

$\therefore$ $d_2 = xd_1$ implies that d_1 and d_2 are associates.

Converselty, let d_1 and d_2 be associates.

$\therefore \quad d_1 = ud_2$ for some unit u in R.

We have $\quad (a, b) = d_1$

$\Rightarrow \quad d_1/a, d_1/b \Rightarrow ud_2/a, ud_2/b \Rightarrow d_2/a, \; d_2/b$

Let $\quad c/a, c/b. \; \therefore \; c/d_1$ $\qquad$ ($\because$ $d_1 = (a, b)$)

$\Rightarrow \quad c/ud_2 \Rightarrow vc/vud_2 \Rightarrow vc/d_2 \Rightarrow c/d_2$

(Since u is a unit, $\exists\, v \in$ R: $uv = 1$)

$\therefore \quad d_2 = (a, b)$

$\therefore$ The result holds.

Example 15. *If R is a PID, then show that any two non-zero elements $a, b \in R$ have l.c.m. in R.*

Sol. Let $\quad A = (a)$ and $B = (b)$.

$\therefore$ $A \cap B$ is also an ideal of R.

Let $\quad A \cap B = (l)$.

$l \in A \cap B \Rightarrow l \in A \Rightarrow l = ax$, for some $x \in R$

$l \in A \cap B \Rightarrow l \in B \Rightarrow l = by$, for some $y \in R$

$\therefore \quad a/l$ and b/l

Let $\quad a/c, b/c$ for some $c \in R$.

$\Rightarrow \quad c = a\lambda, \; c = b\mu$ for some $\lambda, \mu \in R$

$\Rightarrow \quad c \in (a), \; c \in (b) \Rightarrow c \in A \cap B \Rightarrow c \in (l)$

$\Rightarrow \quad c = ul$ for some $u \in R$ some $u \in R \Rightarrow l/c$

$\therefore$ $a/l,\ b/l$ and $a/c,\ b/c \ \Rightarrow\ l/c$

$\therefore$ l is the l.c.m. of a and b.

NOTES

5.19. PRIME ELEMENT

Let R be a commutative ring with unit element. A non-zero, non-unit element $p \in$ R is called a **prime element** of R if for every a, b in R, p/ab implies p/a or p/b.

Remark. A non-zero, non-unit element $p \in$ R is not prime if there exists a pair of elements a, $b \in$ R such that p/ab and $p \nmid a$, $p \nmid b$.

5.20. IRREDUCIBLE ELEMENT

Let R be a commutative ring with unit element. A non-zero, non-unit element $p \in$ R is called an **irreducible element** of R if for every a, b in R, $p = ab$ implies either a or b is a unit.

Remark 1. A non-zero, non-unit element $p \in$ R is not irreducible if there exists a pair of elements a, b, $\in$ R such that $p = ab$, where $a \in d$, b are both non-unit elements of R. In other words, a and b are proper factors of the non-irreducible element p of R.

$\therefore$ An irreducible element of a ring cannot have a proper factor.

Remark 2. In the ring of integers **Z**, every prime number is both a prime element and an irreducible element.

Remark 3. The ring $\{a + \sqrt{5}bi : a, b \in \mathbf{Z}\}$ is also denoted by $\mathbf{Z}[\sqrt{5}i]$.

Remark 4. if $a + \sqrt{5}\,bi$ is a unit of R, then there exists $c + \sqrt{5}\,di \in$ R such that

$$(a + \sqrt{5}\,bi)(c + \sqrt{5}\,di) = 1 \quad \Rightarrow \quad (a^2 + 5b^2)\,(c^2 + 5d^2) = 1$$

$$\Rightarrow \qquad a^2 + 5b^2 = 1 \quad \Rightarrow \quad a = \pm 1,\ b = 0$$

$$\Rightarrow \qquad a + \sqrt{5}\,bi = \pm 1 + (\sqrt{5}\ .\ 0)i = \pm 1.$$

$\therefore$ The units of R are ± 1.

Theorem 15. *If R is an integral domain with unit element, then every prime element is also an irreducible element.*

Proof. Let p be a prime element of R.

$\therefore$ $p \neq 0$ and p is not a unit.

Let $p = ab$, for some a, $b \in$ R.

$$\Rightarrow \qquad ab = p.1 \quad \Rightarrow \quad p/ab \quad \Rightarrow \quad p/a \quad \text{or} \quad p/b$$

Let $\quad p/a. \quad \therefore \quad a = p\lambda$ for some $\lambda \in$ R

$$\therefore \qquad p = ab \quad \Rightarrow \quad p = (p\lambda)b \quad \Rightarrow \quad p.1 = p(\lambda b) \quad \Rightarrow \quad p(1 - \lambda b) = 0$$

$$\Rightarrow \qquad 1 - \lambda b = 0 \qquad\qquad (\because \quad p \neq 0 \text{ and R is an I.D.})$$

$$\Rightarrow \qquad \lambda b = 1 \quad \Rightarrow \quad b \text{ is a unit.}$$

Similarly, if p/b then a is a unit.

$\therefore$ p is an irreducible element.

Remark. The converse of this theorem is not true. But if the integral domain with unit element happens to be a principal ideal ring, then the converse is also true.

5.21. UNIQUE FACTORIZATION DOMAIN (UFD)

NOTES

An integral domain R with unit element is called a **unique factorization domain** if :

(*i*) Every non-zero, non-unit element in R can be written as the product of finite number of irreducible element of R.

(*ii*) The decomposition in (*i*) is unique up to the order and associates of the irreducible elements.

Example 16. *Let R be a commutative ring with unit element. Show that every prime element in R generates a prime ideal of R.*

Sol. Let p be a prime element in R.

$\therefore$ p is non-zero and non-unit element and for every $a, b \in$ R, $p/ab \Rightarrow p/a$ or p/b. Let $cd \in (p)$, the ideal generated by p.

$\Rightarrow \quad \exists\, r \in \text{R} : cd = pr$

$\Rightarrow \quad p/cd \Rightarrow p/c$ or p/d $\qquad (\because$ p is a prime element of R)

$\Rightarrow \quad c = px$ or $d = py$ for some $x, y \in$ R

$\Rightarrow \quad c \in (p)$ or $d \in (p)$

$\therefore$ (p) is a prime ideal of R.

Example 17. *Show that the ring of integers is a UFD.*

Sol. The ring of integers, Z is an integral domain with unit element.

$\therefore$ Every prime in **Z** is an irreducible element of **Z**. The units in Z are only -1 and 1.

Let n be an integer other than $0, -1, 1$.

$\therefore$ n can be expressed as the product of finite number of prime elements and hence irreducible elements.

The expression is unique except for order and sign.

$\therefore$ **Z** is a UFD.

SUMMARY

- The kernel of a homomorphism of a ring R into a ring R′ is an ideal of R.
- Let $\phi : \text{R} \to \text{R}'$ be a homomorphism of ring R into ring R′. If A is an ideal of R then $f(\text{A})$ is an ideal of $\phi(\text{R})$.
- A field cannot have any proper ideal.
- If a commutative ring with unit element has no proper ideal then it is a field.
- If A_1 and B_2 are two left (resp. right) ideals of a ring R, then $\text{A}_1 + \text{B}_2$ and $\text{A}_1 \cap \text{B}_2$ are also left (resp. right) ideals of R.
- Let R be a ring and S, a non-empty subset of R. An ideal A of R is said to be generated by S if A is the smallest ideal of R containing S.
- Let R be a ring. An ideal of R generated by a singlton set is called a principal ideal. If the ideal A is generated by the set $\{a\}$, then we write $\text{A} = (a)$ or as $\text{A} = <a>$.
- Let ϕ be a homomorphism of a ring R onto a ring R′. Then R/ker $\phi \cong$ R′.
- If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R if and only if R/M is a field.

- If R is a commutative ring and P is an ideal of R, then P is a prime ideal of R if and only if R/P is an integral domain.
- Every integral domain having at least two elements can be embedded in a field.
- Let R be an integral domain with unit element. Two non-zero elements a, b of R are associates if and only if a/b and b/a.
- If R is an integral domain with unit element, then every prime element is also an irreducible element.
- If R is a principal ideal domain, then every irreducible element is also a prime element.

REVIEW QUESTIONS

1. Let R be a ring and a ∈ R. Show that $Ra = \{ra : r \in R\}$ is a left ideal of R.
2. Let R be a commutative ring and $a \in$ R. Show that the set aR = $\{ar : r \in R\}$ is an ideal of R.
3. Let R be a ring and $a \in$ R. Show that the set $r(a) = \{x \in R : ax = 0\}$ is a right ideal of R.
4. Show that **Z** is a subring of the ring (**R**, +, .) but neither a left ideal nor a right ideal of (**R**, +, .).
5. Let $R = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbf{Z}\right\}$. Show that the set $\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbf{Z}\right\}$ is a right ideal of R.
6. The set $R = \left\{\begin{bmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{bmatrix} : a, b, c, d, e, f, g \in \mathbf{Z}\right\}$ is a ring under matrix addition and multiplication. Show that :

   $A = \left\{\begin{bmatrix} 0 & 0 & a \\ 0 & 0 & b \\ 0 & 0 & 0 \end{bmatrix} : a, b \in \mathbf{Z}\right\}$ is an ideal of R but $B = \left\{\begin{bmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} : a \in \mathbf{Z}\right\}$ is not an ideal of R.

   Further B is an ideal of the ring A.
7. Show that the subset A of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. $a, b \in \mathbf{Z}$ forms a subring of the ring R of all 2 × 2 matrices having integral elements. Also show that A is neither a left ideal of R nor a right ideal of R.
8. In the commutative ring (**Q**, + .), show that 4 divides 9.
9. If a/b and a/c in a commutative ring R, then show that

   $a/(mb + nc^2) \quad \forall \quad m, n \in \mathbf{Z}.$
10. Show that 1 and – 1 are the only units in the ring of integers.
11. If a is a unit in a commutative ring R with unit element, then a^{-1} is also a unit in R.
12. Show that the product of two units in a commutative ring with unit element is also a unit.
13. Let R be a commutative ring with unit element. Show that the relation in R defined by 'is an associate of' is an equivalence relation.
14. If p, q are prime elements in an integral domain R with unit element such that p/q, then show that p and q are associates.
15. Show that 1 + i is an irreducible element of the ring **Z**[i].

NOTES

UNIT 6

EUCLIDEAN RINGS

STRUCTURE

6.0. LEARNING OBJECTIVES

After going through this unit, you should be able to:

- euclidean ring.

6.1. INTRODUCTION

In this chapter, we shall introduce Euclidean rings. We shall prove that every Euclidean ring is a principal ideal ring as well as a unique factorization domain. In the last, we shall prove a theorem regarding the maximal ideals of a Euclidean rings.

6.2. EUCLIDEAN RING

An integral domain R is called a **Euclidean ring** if for every $a\ (\neq 0) \in$ R, there is defined a non negative integer $d(a)$ such that :

(*i*) $d(a) \leq d(ab)\ \forall\ a(\neq 0),\ b(\neq 0) \in$ R.

(*ii*) Given $a\ (\neq 0),\ b(\neq 0) \in$ R, there exist elements $q, r \in$ R such that $a = bq + r$, where either $r = 0$ or $d(r) < d(b)$.

The condition (*i*) given above can also be written as $d(b) \le d(ab)$. Also, $d(a)$ is defined only for non-zero elements of R. In other words, $d(0)$ is not defined. An Euclidean ring is also known as a **Euclidean domain**.

NOTES

Remark. If $a = 0$ and $b \ne 0$, we can write $a = b.0 + 0$ or $a = bq + r$, where $q = 0$, $r = 0$.

$\therefore$ The requirement (*ii*) is trivially true when $a = 0$.

Example 1. *Show that the set of integer* **Z** *is a Euclidean ring under usual addition and multiplication.*

Sol. We know that **Z** is a commutative ring.

Also, $ab = 0$ is possible in **Z** only when at least one of a and b is zero.

$\therefore$ **Z** has no zero divisor.

$\therefore$ **Z** is an integral domain.

For every $a(\ne 0) \in$ **Z**, we define $d(a) = |\, a \,|$. $\therefore$ $d(a)$ is a non-negative integer.

(*i*) For non-zero integers a, b, we have

$$|\,a\,| \le |\,a\,|\,|\,b\,| = |\,ab\,| \quad i.e., \ d(a) \le d(ab)$$

$$(\because \ b \ne 0 \ \Rightarrow \ |\,b\,| \ge 1)$$

$$\therefore \qquad d(a) \le d(ab) \ \forall \ a(\ne 0), b(\ne 0) \in \mathbf{Z}.$$

(*ii*) Let $a(\ne 0), b(\ne 0) \in \mathbf{Z}$

Dividing a by b, there exist integers q and r such that

$$a = bq + r, \quad \text{where} \quad 0 \le r < |\,b\,|.$$

$$\begin{aligned} \text{Now} \qquad 0 \le r < |\,b\,| \quad &\Rightarrow \quad r = 0 \quad \text{or} \quad 0 < r < |\,b\,| \\ &\Rightarrow \quad r = 0 \quad \text{or} \quad |\,r\,| < |\,b\,| \\ &\Rightarrow \quad r = 0 \quad \text{or} \quad d(r) < d(b). \end{aligned}$$

$\therefore$ For non-zero elements a, b of **Z**, there exist $q, r \in$ **Z** such that $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$.

$\therefore$ **Z** is a Euclidean ring.

Example 2. *Show that the integral domain* **Q** *of rational number with* $d(a) = |\, a \,| \ \forall \ a \ (\ne 0) \in$ **Q** *is not a Euclidean domain.*

Sol. $$a = \frac{2}{5}, b = \frac{3}{5}$$

$$\therefore \qquad d(a) = d\left(\frac{2}{5}\right) = \left|\frac{2}{5}\right| = \frac{2}{5}$$

and $$d(ab) = d\left(\frac{2}{5} \cdot \frac{3}{5}\right) = d\left(\frac{6}{25}\right) = \left|\frac{6}{25}\right| = \frac{6}{25}$$

$$\therefore \qquad d(a) \not\le d(ab), \text{ because } \frac{2}{5} \not\le \frac{6}{25}.$$

$\therefore$ **Q** is not a Euclidean ring.

Example 3. *Show that every field is a Euclidean domain.*

Sol. Let F be a field.

$\therefore$ F is a commutative ring.

Let $a \neq 0$ and $ab = 0$ for some $a, b \in$ F.

$a \neq 0 \;\Rightarrow\; a^{-1}$ exists.

$$\therefore \qquad a^{-1}(ab) = a^{-1}0 \;\Rightarrow\; (a^{-1}a)\, b = 0 \;\Rightarrow\; 1b = 0 \;\Rightarrow\; b = 0$$

$\therefore$ F has no zero divisor.

$\therefore$ F is an integral domain.

For every $a(\neq 0) \in$ F, we define $d(a)$ = the integer '1'.

$\therefore$ $d(a)$ is a non-negative integer.

(*i*) For non-zero elements a, b of F, we have $d(a) = 1$ and $d(ab) = 1$.

$$\therefore \qquad d(a) \leq d(ab).$$

(*ii*) Let $a(\neq 0), b(\neq 0) \in$ F.

$$\therefore \qquad a = 1 \,.\, a = (bb^{-1})\, a = b(b^{-1}a) = b(b^{-1}a) + 0$$

$\Rightarrow$ $a = bq + r$, where $q = b^{-1}a \in$ F and $r = 0$.

$\therefore$ F is a Euclidean domain.

$\therefore$ Every field is a Euclidean domain.

Remark. In the above example, the '1' involved in the relation $a^{-1}a = 1$ is the unit element *i.e.*, the multiplicative identity of the field F whereas the '1' involved in the relation $d(a) = 1$ is first positive integer.

Theorem 1. *Every Euclidean ring is a principal ideal domain.*

Proof. Let R be a Euclidean ring.

$\therefore$ R is an integral domain. In order to prove that R is a principal ideal domain, we should show R possesses unit element and every ideal of R is a principal ideal.

Let A be any ideal of R. If A is the null ideal, then A = (0), so A is a principal ideal.

Now let us assume that A $\neq$ (0).

Since R is a Euclidean domain, so for every $a(\neq 0) \in$ R, there is defined a non-negative integer $d(a)$ such that

(*i*) $d(a) \leq d(ab)\ \forall\ a(\neq 0), b(\neq 0) \in$ R

(*ii*) Given $a(\neq 0), b(\neq 0) \in$ R, there exists elements $q, r \in$ R such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

$$\text{Let} \qquad \text{M} = \{d(x) : x(\neq 0) \in \text{A}\}$$

$\therefore$ M is a non-empty set of non-negative integers.

Let $b(\neq 0) \in$ A be such that $d(b)$ is the least element of M. We shall show that A = (b).

$$b \in \text{A} \;\Rightarrow\; br \in \text{A}\ \forall\ r \in \text{R} \;\Rightarrow\; (b) \subseteq \text{A}$$

Let y be any element of A. If $y = 0$, then $y \in (b)$, so let $y \neq 0$.

$\therefore$ Given $y(\neq 0), b(\neq 0) \in$ R, there exists elements $q, r \in$ R such that $y = bq + r$, where $r = 0$ or $d(r) < d(b)$.

$$y \in \text{A} \text{ and } b \in \text{A} \;\Rightarrow\; y \in \text{A} \text{ and } bq \in \text{A} \;\Rightarrow\; y - bq \in \text{A}$$

$\Rightarrow \quad r \in A \qquad (\because \quad y = bq + r \quad \Rightarrow \quad r = y - bq)$

If possible, let $r \neq 0 \quad \therefore \quad d(r) < d(b)$

By definition of b, $\qquad d(b) \leq d(r)$.

This is a contradiction $\quad \therefore \quad r = 0$.

$\Rightarrow \qquad y = bq \quad \Rightarrow \quad y \in (b) \quad \Rightarrow \quad A \subseteq (b)$

$\therefore \quad A = (b) \quad \therefore \quad$ A is a principal ideal.

$\therefore \quad$ Every ideal of R is a principal ideal.

Now, we shall show that R has a unit element.

In particular, R itself is an ideal of R.

$\therefore \quad \exists\, a \in R : R = (a)$.

Also $\quad a \in R. \quad \therefore \quad \exists\, b \in R : ab = a$

Let x be any element of R.

$\Rightarrow \quad x \in (a) \quad \Rightarrow \quad x = ay$ for some $y \in R$

Now $\qquad xb = (ay)b = (ya)b = y(ab) = ya = ay = x$

$\Rightarrow \qquad xb = x \qquad (\because \quad$ R is commutative)

$\Rightarrow \qquad xb = x = bx$

$\therefore \quad b$ is the unit element of R.

$\therefore \quad$ R is a principal ideal domain.

Theorem 2. *If R be a Euclidean ring, then any two non-zero elements a and b in R have a greatest common divisor d in R and $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.*

Proof. Let $\qquad A = \{xa + yb : x, y \in R\}$

$$0x + 0y = 0 + 0 = 0 \in A. \quad \therefore \quad A \neq \phi$$

Let $\qquad x_1 a + y_1 b,\ x_2 a + y_2 b \in A$.

$\therefore \qquad (x_1 a + y_1 b) - (x_2 a + y_2 b) = (x_1 - x_2)a + (y_1 - y_2)b \in A$

$(\because \quad x_1, x_2, y_1, y_2 \in R \quad \Rightarrow \quad x_1 - x_2, y_1 - y_2 \in R)$

Also, $\quad r \in R \quad \Rightarrow \quad r(x_1 a + y_1 b) = (rx_1)\, a + (ry_1)\, b \in R$

$(\because \quad x_1, y_1 \in R \quad \Rightarrow rx_1, ry_1 \in R)$

$\therefore \quad$ A is an ideal of R. Since every Euclidean ring is a principal ideal domain, the ideal A of R is a principal ideal.

Let $\qquad A = (d)$, for some $d \in R$.

Also $\qquad d = 1.d \in (d)$ *i.e.*, A

$(\because \quad$ a PID always have unit element)

$\therefore \qquad d = \lambda a + \mu b \quad$ for some $\lambda, \mu \in R$.

Now $\qquad a = 1.a + 0.b \quad$ and $\quad b = 0.a + 1.b$

$\therefore \qquad a, b \in A$ *i.e.*, (d)

$\Rightarrow \qquad a = md, b = nd \quad$ for some $m, n \in R$

$\Rightarrow \quad d/a, d/b \quad$ Now, let $c/a, c/b$

$\Rightarrow \quad c/\lambda a, c/\mu b \quad \Rightarrow \quad c/(\lambda a + \mu b) \quad \Rightarrow \quad c/d$

$\therefore \qquad d =$ g.c.d. of (a, b) and $d = \lambda a + \mu b$, where $\lambda, \mu \in R$.

This completes the proof.

Theorem 3. *Let R be a Euclidean ring and a, b be non-zero elements of R. Show that :*

(i) $d(a) = d(ab)$ if b is a unit *(ii) $d(a) < d(ab)$ if b is not a unit.*

Proof. We have $d(a) \leq d(ab)$. ...(1)

(*i*) Let b be a unit in R.

$\therefore$ There exists $c \in$ R : $bc = 1$

$\therefore$ $a = a(1) = a(bc) = (ab)\, c$

$\Rightarrow$ $d(a) = d((ab)\, c) \geq d(ab) \quad \Rightarrow \quad d(a) \geq d(ab)$ ...(2)

(1) and (2) $\Rightarrow$ $d(a) = d(ab)$.

(*ii*) Let b be not a unit in R.

Since $a \neq 0$, $b \neq 0$ and R is an I.D., we have $ab \neq 0$.

$\therefore$ For $a \neq 0$, $ab \neq 0$, $\exists\, q, r \in$ R such that

$a = (ab)\, q + r$, where $r = 0$ or $d(r) < d(ab)$

$r = 0 \Rightarrow a = (ab)\, q \Rightarrow a(1 - bq) = 0 \Rightarrow 1 - bq = 0$ $(\because \; a \neq 0)$

$\Rightarrow bq = 1 \quad \Rightarrow$ b is a unit in R.

This is impossible. $\therefore$ $r \neq 0$

$\therefore$ $d(r) < d(ab)$

$a = (ab)\, q + r \Rightarrow r = a - abq \Rightarrow r = a(1 - bq)$

$\Rightarrow d(r) = d(a(1 - bq)) \geq d(a) \Rightarrow d(a) \leq d(r)$

$\Rightarrow d(a) \leq d(r) < d(ab) \Rightarrow d(a) < d(ab)$.

Theorem 4. *Every Euclidean ring is a unique factorization domain.*

Proof. Let R be a Euclidean ring.

$\therefore$ R is an integral domain. We know that every ideal of a Euclidean ring is a principal ideal.

$\therefore$ R being an ideal of R is principal.

$\therefore$ $\exists\, a \in$ R : R $= (a)$.

Also $a \in$ R $\therefore$ $\exists\, b \in$ R : $ab = a$

Let x be any element of R.

$\Rightarrow x \in (a) \Rightarrow x = ay$ for some $y \in$ R.

Now $xb = (ay)\, b = (ya)\, b = y(ab) = ya = ay = x$

$\Rightarrow xb = x \Rightarrow xb = x = bx$ ($\because$ R is commutative)

$\therefore$ b is the unit element of R.

$\therefore$ The Euclidean ring R is a principal ideal domain.

Since R is given to be a Euclidean ring, for every $a(\neq 0) \in$ R, there is defined a non-negative integer $d(a)$ such that

(*i*) $d(a) \leq d(ab)\ \forall\ a(\neq 0), b(\neq 0) \in$ R

(*ii*) Given $a(\neq 0)$, $b(\neq 0) \in$ R, there exists elements $q, r \in$ R such that $a = bq + r$, where either $r = 0$ or $d(r) < d(b)$.

Now we shall show that

(*i*) Every non-zero, non-unit element in R can be written as the product of finite number of irreducible elements of R.

(*ii*) The decomposition in (*i*) is unique upto the order and associates of the irreducible elements.

We denote the unit element of R by '1'

For $x \in R$, $d(1) \le d(1.x) = d(x)$

$\therefore$ $d(1)$ is the minimum value of the d-function.

Let a be any non-zero element in R. $\therefore$ $d(a) \ge d(1)$.

If $d(a) = d(1)$, then a must be a unit in R and so (*i*) and (*ii*) holds trivially. Let $d(a) \ge d(1)$. We suppose that (*i*) and (*ii*) are true for all $x \in$ R such that $d(x) < d(a)$. If a an irreducible element of R, then the result holds trivially. So suppose that a is not an irreducible element.

$\therefore$ $\exists\, b, c \in$ R : $a = bc$ and b, c are non-units.

$$\therefore \quad d(b) < d(bc) \quad \text{and} \quad d(c) < d(bc)$$

$$\Rightarrow \quad d(b) < d(a) \quad \text{and} \quad d(c) < d(a) \qquad (\because \quad a = bc)$$

$\therefore$ By induction hypothesis, b and c can be written as the products of finite number of irreducible elements of R.

$$\text{Let} \quad b = p_1p_2 \ldots\ldots p_m \quad \text{and} \quad c = p_{m+1}\, p_{m+2} \ldots\ldots p_n$$

$$\therefore \quad a = bc = p_1p_2 \ldots\ldots p_m\, p_{m+1}p_{m+2} \ldots\ldots p_n$$

$$\text{i.e.,} \quad a = p_1p_2 \ldots\ldots p_n$$

$\therefore$ (*i*) holds. Let a be also equal to the product of irreducible elements p_1', p_2', $\ldots\ldots p'_{n'}$.

$$\therefore \quad p_1p_2 \ldots\ldots p_n = p_1'p_2' \ldots\ldots p'_{n'} \qquad \ldots(1)$$

Since the Euclidean ring R is a principal ideal domain, every irreducible element in R is a prime element.

$\therefore$ $p_1, p_2, \ldots\ldots p_n, p_1', p_2', \ldots\ldots p'_{n'}$ are prime elements.

Now p_1 divides $p_1p_2 \ldots\ldots p_n$.

$\therefore$ p_1 divides $p_1'p_2' \ldots\ldots p'_{n'}$

p_1 divides at least one of p_1', $'p_2'$, $\ldots\ldots p'_{n'}$.

Without loss of generality, let p_1/p_1'

$\therefore$ $p_1' = up_1$ for some $u \in$ R.

Since p_1' is irreducible, either u or p_1 is a unit.

$\therefore$ u is a unit, because p_1 being a prime cannot be a unit.

$\therefore$ $p_1' = up_1$ implies that p_1 and p_1' are associates.

$\therefore$ (1) $\Rightarrow$ $p_1p_2 \ldots\ldots p_n = up_1p_2' \ldots\ldots p'_{n'}$

Since R is an integral domain and $p_1 \ne 0$, we cancel p_1.

$$\therefore \quad p_2p_3 \ldots\ldots p_n = up_2'p_3' \ldots\ldots p'_{n'} \qquad \ldots(2)$$

Now we can repeat the above argument on the relation (2) with p_2. If $n < n'$, then after n steps, the L.H.S. of (1) becomes 1 while the R.H.S. of (1) reduces to the product of n units in R and $(n' - n)$ prime numbers. Since prime numbers are not units in R, the product on the R.H.S. cannot be 1.

$\therefore$ $n < n'$ is impossible.

Similarly $n' < n$ is impossible.

$$\therefore \quad n = n'$$

Also every p is associate of same p' and so every p' is associate of same p.

NOTES

This completes the proof.

Theorem 5. *An ideal A of a Euclidean ring R is maximal iff A is generated by some prime element of R.*

Proof. Let $A = (p)$, where p is a prime element of R. Let B be an ideal of R such that $A \subseteq B \subsetneq R$. Since every Euclidean ring is a principal ideal domain, the ideal B is a principal ideal.

Let $B = (b)$ for some $b \in R$.

$A \subseteq B \Rightarrow p \in B \Rightarrow p = br$ for some $r \in R$.

Since p is prime and R is an I . D, so p is irreducible.

$\therefore \quad p = br \quad \Rightarrow \quad$ either b or r is a unit.

Let b be a unit $\quad \therefore \quad bc = 1$ for some $c \in R$

$\Rightarrow \quad 1(= bc) \in B \quad \Rightarrow \quad B = R.$

Let r be a unit $\quad \therefore \quad rs = 1$ for some $s \in R$

$\therefore \qquad p = br \quad \Rightarrow \quad ps = brs = b.1 = b \quad \Rightarrow \quad b \in (p) \quad \Rightarrow \quad B \subseteq A$

$\Rightarrow \qquad B = A$

$\therefore$ Either $\qquad B = A \quad$ or $\quad B = R. \quad \therefore \quad$ The ideal A is maximal.

Conversely, let A be a maximal ideal of R. Since R is a Euclidean ring, $A = (p)$ for same $p \in R$. We shall show that p is prime. If possible let p be not prime.

$\therefore \quad p$ is not irreducible.

$\therefore \quad \exists\, m, n \in R\, ; p = mn$ and neither m nor n is a unit in R.

$$p = mn \quad \Rightarrow \quad (p) \subseteq (m) \subseteq R.$$

Since (p) is maximal, either $(m) = (p) \quad$ or $\quad (m) = R.$

$$(m) = (p) \quad \Rightarrow \quad m \in (p) \quad \Rightarrow \quad m = kp \text{ for some } k \in R$$

$$\Rightarrow \quad p = mn = kpn$$

$$\Rightarrow \quad 1 = kn \quad \Rightarrow \quad n \text{ is a unit.} \qquad (\because \quad p \neq 0 \text{ and R is an I.D.})$$

This is impossible. $\quad \therefore \quad (m) \neq (p).$

$$(m) = R \quad \Rightarrow \quad 1 \in (m) \quad \Rightarrow \quad 1 = xm \text{ for some } x \in R \quad \Rightarrow \quad m \text{ is a unit.}$$

This is impossible $\quad \therefore \quad (m) \neq R.$

$\therefore \quad$ Our supposition is wrong.

$\therefore \quad p$ is a prime element in R.

SUMMARY

- Every Euclidean ring is a principal ideal domain.
- If R be a Euclidean ring, then any two none-zero elements a and b in R have a greatest common divisior d in R and $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.
- If R is a Euclidean ring and a, b be non-zero elements of R, then
  (*i*) $d(a) = d(ab)$ if b is *a* unit
  (*ii*) $d(a) < d(ab)$ if b is not *a* unit.
- Every Euclidean ring is a unique factorization domain.
- An ideal A of *a* Euclidean ring R is *a* maximal ideal iff A is generated by some prime element of R.

NOTES

REVIEW QUESTIONS

1. Let a, b, c be any three elements of a Euclidean ring R and $(a, b) = 1$. If a/bc then show that a/c.
2. Show that a non-zero element a in a Euclidean domain R is a unit iff $d(a) = d(1)$.
3. Let R be a Euclidean ring and a, b are non-zero elements of R. If $d(a) < d(ab)$, show that b is not a unit.
4. Let R be a Euclidean ring and a, b are non-zero elements of R. If a and b are associates. show that $d(a) = d(b)$.
5. Show that every Euclidean ring possesses unit element.
6. Let R be a Euclidean ring and A be an ideal of R. Show that there exists an element $a_0 \in \mathrm{R}$ such that $\mathrm{A} = \{a_0 r : r \in \mathrm{R}\}$.

NOTES

UNIT

7

POLYNOMIAL RINGS

STRUCTURE

7.0. LEARNING OBJECTIVES

After going through this unit, you should be able to:

- polynomial over a ring
- degree of a polynomial
- sum and product of polynomial
- classification of polynomial.

7.1. INTRODUCTION

In this chapter, we shall prepare rings of polynomials using elements of a ring as their coefficients. We shall end this chapter after obtaining a method, called

Eisenstein Criterion, of deciding whether a polynomial over integers is irreducible or not, over the rational numbers.

NOTES

7.2. POLYNOMIAL OVER A RING

Let R be a ring. An infinite sequence $(a_0, a_1, a_2, ...)$ of elements of R is said to be a **polynomial** over R if only finitely many terms a_i are non-zero elements of R.

In other words, there exists a non-negative integer n such that $a_i = 0 \; \forall \; i > n$.

For example $(4, 0, 3, 5, a_4, a_5, ...)$ with $a_n = 0 \; \forall \; n > 3$ is a polynomial over the ring of integers.

7.3. USUAL NOTATION FOR POLYNOMIALS

Let $(a_0, a_1, a_2, ...)$ be a polynomial over a ring R. This polynomial is denoted by $\mathbf{a_0 + a_1x + a_2x^2 + ...}$. Here x is only a symbol and is called an **indeterminate.** Also, $x^2, x^3, ...$ are symbols. The elements $a_0, a_1, a_2, ...$ are called the **coefficients** of the polynomial. The different formal power symbols $x, x^2, x^3, ...$ are meant just to indicate the position of the corresponding coefficients. The symbol '+' connecting the terms in the polynomial $a_0 + a_1x + a_2x^2 + ...$ has no bearing with the 'addition' of the ring R. Also, the zero appearing in a polynomial is the zero element of the ring.

If in the polynomial $(a_0, a_1, a_2, ...)$, $a_i = 0 \; \forall \; i > n$, then this polynomial is also written as $\sum\limits_{i=0}^{n} a_i x^i$.

In the notation of $(a_0, a_1, a_2, ...)$ as $a_0 + a_1x + a_2x^2 + ...$, it is also assumed that if $a_i = 0$ for some i, then the corresponding terms a_ix^i *i.e.*, $0x^i$ need not be written.

If $(a_0, a_1, a_2, ...)$ is a polynomial over a ring R such that n is the largest non-negative integer with $a_n \neq 0$, then a_0 is called the **constant term** of the polynomial and a_n is called the **leading coefficient** of the polynomial. We can write this polynomial as $a_0 + a_1x + a_2x^2 + ... + a_nx^n$. A polynomial $(a_0, a_1, a_2, ...)$ is called a **constant polynomial** if $a_i = 0 \; \forall \; i > 0$.

For example, $(1, 5, 0, 0, 7, 0, 9, a_7, a_8, ...)$ where $a_7 = a_8 = ... = 0$ is a polynomial over the ring **Z**, because only finitely many terms are non-zero. This polynomial can also be written as $1 + 5x + 0x^2 + 0x^3 + 7x^4 + 0x^5 + 9x^6 + 0.x^7 + 0.x^8 + ...$ or simply as $1 + 5x + 7x^4 + 9x^6$.

7.4. POLYNOMIAL RING OVER A RING

Let R be a ring. Let R[x] denote the set of all polynomials over the ring R.

$\therefore$ $\quad$ $R[x] = \{(a_0, a_1, a_2, ...) : a_i \in R$ and only finitely many a_i are non-zero$\}$

Equivalently,

$R[x] = \{a_0 + a_1x + a_2x^2 + ... : a_i \in R$ and only finitely many a_i are non-zero$\}$.

or $$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in R \text{ and for some non-negative integer } n,\ a_m = 0 \quad \forall\ m > n \right\}$$

NOTES

We shall show that R[x] is a ring. We define equality, addition and multiplication in R[x].

Let $f = (a_0, a_1, a_2, ...), g = (b_0, b_1, b_2, ...) \in R[x]$.

We define $f = g$ if and only if $a_i = b_i$ for $i = 0, 1, 2, ...$

We define $f + g = (c_0, c_1, c_2, ...)$, where $c_i = a_i + b_i \quad \forall\ i$

$\therefore$ In order to add two polynomials, we add the corresponding coefficients.

We define $fg = (d_0, d_1, d_2, ...)$,

where $d_i = a_0b_i + a_1b_{i-1} + ... + a_{i-1}\, b_1 + a_ib_0 \quad \forall\ i$

$\therefore$ In particular, $d_0 = a_0b_0, \quad d_1 = a_0b_1 + a_1b_0, \quad d_2 = a_0b_2 + a_1b_1 + a_2b_0, ...$

Since R is a ring, each c_i and d_i is in R.

Let m and n be non-negative integers such that

$$a_i = 0 \quad \forall\ i > m \quad \text{and} \quad b_i = 0 \quad \forall\ i > n$$

$\therefore$ For $i > \max(m, n)$, $c_i = a_i + b_i = 0 + 0 = 0$

$\therefore$ Only finitely many c_i are non-zero.

$\therefore$ $f + g \in R[x]$.

For $i > m + n$,

$$d_i = a_0b_i + a_1b_{i-1} + ... + a_mb_{i-m} + a_{m+1}b_{i-m-1} + ...\ a_{i-1}b_1 + a_ib_0$$
$$= a_00 + a_10 + ... + a_m0 + 0b_{i-m-1} + ... + 0b_1 + 0b_0 = 0 + 0 + ... + 0 = 0$$

$\therefore$ Only finitely many d_i are non-zero.

$\therefore$ $fg \in R[x]$.

In order to write fg in terms of the indeterminate x, we write f and g separately in terms of x and multiply these and use the formula $x^\lambda x^\mu = x^{\lambda+\mu}$.

Thus, if $$f = \sum_{i=0}^{m} a_ix^i \quad \text{and} \quad g = \sum_{i=0}^{n} b_ix^i\ ,$$

then $$f + g = \sum_{i=0}^{\max(m,n)} (a_i + b_i)\, x^i$$

and $$fg = \sum_{i=0}^{m+n} (a_0b_i + a_1b_{i-1} + ... + a_{i-1}b_1 + a_ib_0)\, x^i.$$

$\therefore$ Addition and multiplication in R[x] are well defined.

Addition is associative.

Let $f = (a_0, a_1, a_2, ...), g = (b_0, b_1, b_2, ...), h = (c_0, c_1, c_2, ...) \in R[x]$.

$$\therefore \quad f + (g + h) = (a_0, a_1, a_2, ...) + [(b_0, b_1, b_2, ...) + (c_0, c_1, c_2, ...)]$$
$$= (a_0, a_1, a_2, ...) + (b_0 + c_0, b_1 + c_1, b_2 + c_2, ...)$$
$$= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), ...)$$
$$= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, (a_2 + b_2) + c_2, ...)$$

$= (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...) + (c_0, c_1, c_2, ...)$

$= [(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...)] + (c_0, c_1, c_2, ...) = (f + g) + h.$

Existence of additive identity. Let $f = (a_0, a_1, a_2, ...) \in R[x]$.

NOTES

Let $i = (0, 0, 0, ...) \in R[x]$.

$\therefore \quad f + i = (a_0, a_1, a_2, ...) + (0, 0, 0, ...)$

$= (a_0 + 0, a_1 + 0, a_2 + 0, ...) = (a_0, a_1, a_2, ...) = f$

Similarly, $i + f = f$. $\quad \therefore \quad f + i = f = i + f$.

$\therefore$ i is the additive identity.

Existence of additive inverse. Let $f = (a_0, a_1, a_2, ...) \in R[x]$.

$\Rightarrow \quad a_0, a_1, a_2, ... \in R \;\Rightarrow\; -a_0, -a_1, -a_2, ... \in R$

$\Rightarrow \quad (-a_0, -a_1, -a_2, ...) \in R[x]$.

We denote this element of $R[x]$ by $-f$.

$\therefore \quad f + (-f) = (a_0, a_1, a_2, ...) + (-a_0, -a_1, -a_2, ...)$

$= (a_0 - a_0, a_1 - a_1, a_2 - a_2, ...) = (0, 0, 0, ...) = i$

Similarly, $\quad (-f) + f = i$

$\therefore \quad f + (-f) = i = (-f) + f$.

$\therefore$ $-f$ is the additive inverse of f.

Addition is commutative. It is left as an exercise.

Multiplication is associative.

Let $\quad f = (a_0, a_1, a_2, ...), g = (b_0, b_1, b_2, ...), h = (c_0, c_1, c_2, ...) \in R[x]$.

$\therefore \quad f(gh) = (a_0, a_1, a_2 ......) [(b_0, b_1, b_2, ...)(c_0, c_1, c_2, ...)]$

$= (a_0, a_1, a_2, ...)(b_0c_0, b_0c_1 + b_1c_0, b_0c_2 + b_1c_1 + b_2c_0, ...)$

$= (a_0(b_0 c_0), a_0(b_0c_1 + b_1c_0) + a_1(b_0c_0), ...)$

Also $\quad (fg)h = [(a_0, a_1, a_2, ...)(b_0, b_1, b_2, ...)](c_0, c_1, c_2, ...)$

$= (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, ...)(c_0, c_1, c_2, ...)$

$= ((a_0b_0) c_0, (a_0b_0)c_1 + (a_0b_1 + a_1b_0)c_0, ...)$

$= (a_0(b_0c_0), a_0(b_0c_1) + a_0(b_1c_0) + a_1(b_0c_0), ...)$

$= (a_0(b_0c_0), a_0(b_0c_1 + b_1c_0) + a_1(b_0c_0), ...)$

$\therefore \quad f(gh) = (fg)h$.

Similarly, we can show that $f(g + h) = fg + fh$ and $(g + h)f = gf + hf$.

$\therefore$ $R[x]$ is a ring.

Corollary 1. If R is a cummutative ring then $R[x]$ is also a cummutative ring.

Corollary 2. If R is a ring with unit element 1 then $R[x]$ is also a ring with unit element and the unit element is $(1, 0, 0, ...)$.

Example 1. *Show that the ideal (x) of the ring Z[x] is a prime ideal but not a maximal ideal.*

Sol. Let $\quad f(x), g(x) \in Z[x]$ such that $f(x)\, g(x) \in (x)$.

$\therefore$ There exists $h(x) \in Z[x] : f(x)\, g(x) = xh(x)$ ...(1)

Let $\quad f(x) = a_0 + a_1x + ... + a_mx^m,$

$g(x) = b_0 + b_1x + ... + b_nx^n$

and $\quad h(x) = c_0 + c_1x + ... + c_px^p.$

$\therefore$ Comparing the constant terms in (1), we get $a_0b_0 = 0$

$\Rightarrow$ $a_0 = 0$ or $b_0 = 0$ ($\because$ **Z** is an I.D.)

$a_0 = 0 \Rightarrow f(x) = a_1x + \ldots\ldots + a_mx^m = x(a_1 + \ldots\ldots + a_mx^{m-1}) \in (x)$

$b_0 = 0 \Rightarrow g(x) = b_1x + \ldots\ldots + b_nx^n = x(b_1 + \ldots\ldots + b_nx^{n-1}) \in (x)$

$\therefore$ Either $f(x) \in (x)$ or $g(x) \in (x)$.

$\therefore$ (x) is a prime ideal of $\mathbf{Z}[x]$.

Now we shall show that (x) is not a maximal ideal of $\mathbf{Z}[x]$.

$(x) \neq \mathbf{Z}[x]$ because $2 \in \mathbf{Z}[x]$ but $2 \notin (x)$.

Let A be the ideal of $\mathbf{Z}[x]$ generated by 3 and x.

$3 \notin (x)$ because $3 \neq xf(x)$ for any $f(x) \in \mathbf{Z}[x]$.

$\therefore$ $(x) \subset \mathrm{A}$

Also, $4 \in \mathbf{Z}[x]$ and 4 cannot be expressed as $3\phi(x) + x\psi(x)$ for any $\phi(x), \psi(x)$ in $\mathbf{Z}[x]$.

$\therefore$ $\mathrm{A} \subset \mathbf{Z}[x]$

$\therefore$ (x) is not a maximal ideal of $\mathbf{Z}[x]$ because $(x) \subset \mathrm{A} \subset \mathbf{Z}[x]$.

7.5. DEGREE OF A POLYNOMIAL

Let R be a ring.

Let $f = (a_0, a_1, a_2, \ldots\ldots)$ *i.e.*, $a_0 + a_1x + a_2x^2 + \ldots\ldots$ be a non-zero polynomial over R.

$\therefore$ Only finitely many a_i are non-zero. If for a non-negative integer n, $a_n \neq 0$ and $a_m = 0 \ \forall \ m > n$, we say that the **degree** of the polynomial f is n and write deg $f = n$.

If degree of a polynomial is zero then we say that it is a constant polynomial. The degree of zero polynomial is not defined.

Illustrations. (*i*) $2 + 3x^2 + 7x^5$ is a polynomial of degree 5 over the ring of integers.

(*ii*) 4 is a polynomial of degree 0 over the ring of integers. This is a constant polynomial.

Remark. If a polynomial f over a ring R is expressed in terms of the indeterminate x, then we generally write f as $f(x)$.

7.6. DEGREE OF SUM AND PRODUCT OF POLYNOMIALS

Let $f(x) = a_0 + a_1x + \ldots\ldots + a_mx^m, \ a_m \neq 0$

and $g(x) = b_0 + b_1x + \ldots\ldots + b_nx^n, \ b_n \neq 0$

be polynomials over a ring R.

$\therefore$ deg $f(x) = m$ and deg $g(x) = n$

We have $$f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i)x^i$$

$$\therefore \quad \deg(f(x) + g(x)) \begin{cases} = \max(m, n) & \text{if } m \neq n \\ = m & \text{if } m = n \text{ and } a_m + b_n \neq 0 \\ < m & \text{if } m = n \text{ and } a_m + b_n = 0 \end{cases}$$

$\therefore$ In general, $\mathbf{deg\ (f(x) + g(x)) \leq max\ \{deg\ f(x),\ deg\ g(x)\}}$.

Also $$f(x)\,g(x) = \sum_{i=0}^{m+n} (a_0b_i + a_1b_{i-1} + \text{......} + a_{i-1}b_1 + a_ib_0)\, x^i$$

$$\therefore \qquad \deg\,(f(x)\,g(x)) \begin{cases} = m+n & \text{if } a_mb_n \neq 0 \\ < m+n & \text{if } a_mb_n = 0. \end{cases}$$

$\therefore$ In general, $\mathbf{deg\,(f(x)\,g(x)) \le deg\,f(x) + deg\,g(x).}$

Remark. If R is an integral domain, then $a_mb_n \neq 0$ whenever $a_m \neq 0$, $b_n \neq 0$.

$\therefore$ We have $\mathbf{deg\,(f(x)\,g(x)) = deg\,f(x) + deg\,g(x).}$

Theorem 1. *If R is an integral domain then R[x] is also an integral domain.*

Proof. R is given to be an integral domain.

$\therefore$ R is a commutative ring.

$\therefore$ R[x] is also a commutative ring.

Let $$f(x) = a_0 + a_1x + \text{......} + a_mx^m,\ a_m \neq 0$$

and $$g(x) = b_0 + b_1x + \text{......} + b_nx^n,\ b_n \neq 0$$

be any two non-zero elements in R[x].

Since R is an integral domain and a_m, $b_n \neq 0$, so $a_mb_n \neq 0$.

The product $f(x)\,g(x)$ of $f(x)$ and $g(x)$ will contain the term $a_mb_n\,x^{m+n}$.

$\therefore \qquad f(x)g(x) \neq 0 \qquad\qquad (\because \quad a_mb_n \neq 0)$

$\therefore \qquad f(x) \neq 0,\ g(x) \neq 0 \ \Rightarrow\ f(x)g(x) \neq 0.$ $\therefore$ R[x] is an I.D.

Theorem 2. *If F is a field then F[x] is an integral domain and not a field.*

Proof. F is given to be a field.

$\therefore$ F is a commutative ring.

$\therefore$ F[x] is a commutative ring.

Let $ab = 0$, $a \neq 0$ in F.

$\Rightarrow \qquad a^{-1}(ab) = a^{-1}0 \ \Rightarrow\ b = 0.$ $\therefore$ F is an I.D.

Let $$f(x) = a_0 + a_1x + \text{......} + a_mx^m,\ a_m \neq 0$$

and $$g(x) = b_0 + b_1x + \text{......} + b_nx^n,\ a_n \neq 0$$

be any two non-zero elements in R[x].

Since F is an integral domain and a_m, $b_n \neq 0$, so $a_mb_n \neq 0$.

The product $f(x)\,g(x)$ of $f(x)$ and $g(x)$ will contain the term $a_mb_nx^{m+n}$.

$\therefore \qquad f(x)\,g(x) \neq 0 \qquad\qquad (\because \quad a_mb_n \neq 0)$

$\therefore \qquad f(x) \neq 0, g(x) \neq 0 \ \Rightarrow\ f(x)\,g(x) \neq 0.$ $\therefore$ F[x] is an integral domain.

Let $f(x)(\neq 0) \in$ F and deg $f(x) \geq 1$. The unit element of F is the constant polynomial '1'.

If possible, let multiplicative inverse of $f(x)$ exists and let it be $g(x)$.

$\therefore \qquad f(x)\,g(x) = 1 \qquad$ ...(1)

This shows that $g(x) \neq 0$, for otherwise we would have

$$f(x)\,g(x) = f(x)\,.\,0 = 0 \neq 1.$$

Since F is an integral domain, we have

$$\deg\,(f(x)\,g(x)) = \deg f(x) + \deg g(x) \geq 1$$

$\therefore$ (1) is impossible, because deg (1) = 0.

$\therefore$ A non-zero element in F[x] may not have multiplicative inverse in F[x].

$\therefore$ F[x] is not a field.

Remark. Only non zero constant polynomials are invertible in F[x].

Theorem 3. (Division Algorithm). *If F is a field then for any two polynomials $f(x)$, $g(x) \in F[x]$, $g(x) \neq 0$, there exist polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)\, q(x) + r(x)$, where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$.*

NOTES

Proof. $f(x)$, $g(x)$ are elements of F[x] and $g(x) \neq 0$.

If deg $f(x) <$ deg $g(x)$, then we write $f(x) = g(x) \,.\, 0 + f(x)$.

$\therefore$ $f(x) = g(x)\, q(x) + r(x)$, where $q(x) = 0$ and $r(x) = f(x)$.

$\therefore$ deg $r(x) <$ deg $g(x)$.

So, let us assume that deg $f(x) \geq$ deg $g(x)$.

We shall prove that result by using induction on deg $f(x)$.

If deg $f(x) = 0$, then deg $g(x) = 0$ *i.e.*, $g(x)$ is a non-zero constant and $(g(x))^{-1} \in$ F

($\because$ F is a field)

We write $f(x) = (g(x)\, (g(x))^{-1})\, f(x) + 0.$

$\therefore$ $f(x) = (g(x)((g(x))^{-1}\, f(x)) + 0.$

$\therefore$ $f(x) = g(x)\, q(x) + r(x)$, where $q(x) = (g(x))^{-1}\, f(x)$ and $r(x) = 0$.

Let the result be true for all polynomials on the left of the relation '$f(x) = g(x)\, q(x) + r(x)$', whose degree is less than deg $f(x)$.

Let $f(x) = a_0 + a_1x + \ldots\ldots + a_mx^m,\ a_m \neq 0$ ...(1)

and $g(x) = b_0 + b_1x + \ldots\ldots + b_nx^n,\ b_n \neq 0$ ...(2)

and $m \geq n$.

Since F is a field, $b_n^{-1} \in$ F.

Multiplying (2) by $a_mb_n^{-1}x^{m-n}$, we get

$$a_mb_n^{-1}x^{m-n}\, g(x) = a_mb_n^{-1}b_0x^{m-n} + a_mb_n^{-1}b_1x^{m-n+1} + \ldots\ldots + a_mb_n^{-1}b_{n-1}x^{m-1} + a_mx^m \quad \ldots(3)$$

Subtracting (3) from (1), we find that $f(x) - a_mb_n^{-1}x^{m-n}\, g(x) = f_1(x)$, say, is a polynomial which is either zero or is of degree $< m$.

If $f_1(x) = 0$ then $f(x) - a_mb_n^{-1}x^{m-n}\, g(x) = 0$,

$\therefore$ $f(x) = g(x)\, (a_mb_n^{-1}x^{m-n}) + r(x)$, where $r(x) = 0$.

Now, let deg $f_1(x) < m$.

$\therefore$ By the induction hypothesis, $\exists\ q_1(x)$, $r_1(x) \in$ F[x] such that

$$f_1(x) = g(x)\, q_1(x) + r_1(x),$$

where $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$.

$\Rightarrow$ $f(x) - a_mb_n^{-1}x^{m-n}\, g(x) = g(x)\, q_1(x) + r_1(x)$

$\Rightarrow$ $f(x) = g(x)(a_mb_n^{-1}x^{m-n} + q_1(x)) + r_1(x)$

$\Rightarrow$ $f(x) = g(x)\, q(x) + r(x)$,

where $q(x) = a_mb_n^{-1}x^{m-n} + q_1(x)$ and $r(x) = r_1(x)$.

$\therefore$ The result is true for $f(x)$. ($\because$ $r(x) = 0$ or deg $r(x) <$ deg $g(x)$)

$\therefore$ For given $f(x), g(x) \in F[x]$, and $g(x) \neq 0$ there exists $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)\, q(x) + r(x), \text{ where } r(x) = 0 \quad \text{or} \quad \deg r(x) < \deg g(x)).$$

$\therefore$ The division algorithm holds in F[x].

Caution. The 'division algorithm' holds in F[x], only when F is a field.

Theorem 4. *If F is a field then F[x] is a Euclidean ring.*

Proof. F is given to be a field.

$\therefore$ F is an integral domain.

$\Rightarrow$ F[x] is an integral domain.

For every $f(x)$ $(\neq 0) \in$ F[x] we define $d(f(x)) = \deg f(x)$.

$\therefore$ $d(f(x))$ is a non-negative integer.

Let $\quad f(x)\ (\neq 0), g(x)\ (\neq 0) \in F[x]$

$\therefore \quad \deg (f(x)\, g(x)) = \deg f(x) + \deg g(x) \qquad (\because \text{ F is an I.D.})$

$\Rightarrow \quad \deg f(x) \leq \deg (f(x)\, g(x))$

$\Rightarrow \quad d(f(x)) \leq d(f(x)\, g(x)) \quad \forall\, f(x)\ (\neq 0), g(x)\ (\neq 0) \in F[x].$

Let $f(x)$ $(\neq 0)$, $g(x)$ $(\neq 0) \in$ F[x]. By **division algorithm,** there exists polynomials $q(x)$ and $r(x)$ in F[x] such that

$$f(x) = g(x)\, q(x) + r(x), \text{ where either } r(x) = 0 \text{ or } \deg r(x) < \deg g(x)$$

$\therefore \quad f(x) = g(x)\, q(x) + r(x)$, where either $r(x) = 0$ or $d(r(x)) < (g(x))$

$\therefore$ F[x] is a Euclidean ring.

Corollary. Since every Euclidean ring is a PID, the Euclidean ring F[x] is also a PID.

Theorem 5. *If F is a field then F[x] is a principal ideal domain.*

Proof. F is given to be a field.

$\therefore$ F is an integral domain with unit element.

$\Rightarrow$ F[x] is an integral domain with unit element.

Now, we shall show that every ideal of F[x] is principal ideal.

Let A be any ideal of F[x]. If A is the null ideal, then A = (0), so A is a principal ideal.

Now let us assume that A $\neq$ (0).

$\therefore$ There exists a non-zero polynomials in A. Let $g(x)$ be a non-zero polynomial of lowest degree m belonging to A. We shall show that A = $(g(x))$. Let $f(x)$ be any element of A.

$\therefore$ By division algorithm, there exists polynomials $q(x)$ and $r(x)$ in F[x] such that

$$f(x) = g(x)\, q(x) + r(x), \text{ where } r(x) = 0 \text{ or } \deg r(x) < \deg g(x).$$

Now $\quad f(x) \in A \quad \text{and} \quad g(x)\, q(x) \in A \qquad (\because$ A is an ideal of F[x])

$\therefore \quad f(x) - g(x)\, q(x) \in A \quad$ *i.e.,* $r(x) \in A$

$\therefore$ deg $r(x)$ cannot be less than deg $g(x)$.

$\therefore \quad r(x) = 0.$

$\Rightarrow \quad f(x) = g(x)\, q(x)$

$\therefore$ Every element of A is some multiple of $g(x)$. $\quad \therefore \quad A = (g(x))$

$\therefore$ A is a principal ideal.

$\therefore$ F[x] is a principal ideal domain.

NOTES

Example 2. *Show that* **Z**[*x*] *is not a PID.*

Sol. To show that **Z**[*x*] is not a PID., it is sufficient to show an ideal of **Z**[*x*] which is not a principal ideal.

Let A be the ideal of **Z**[*x*] generated by 3 and *x*. If possible, let $A = (f(x))$ for some $f(x) \in \mathbf{Z}[x]$.

$3, x \in A \Rightarrow 3 = f(x)\, g(x)$ and $x = f(x)\, h(x)$

for some elements $g(x)$ and $h(x)$ of **Z**[*x*].

$3 = f(x)\, g(x) \Rightarrow \deg (3) = \deg f(x) + \deg g(x) \quad (\because \ \mathbf{Z} \text{ is an I.D.})$

$\Rightarrow \quad 0 = \deg f(x) + \deg g(x)$

$\Rightarrow \quad \deg f(x) = 0, \quad \deg g(x) = 0$

$\therefore$ $f(x)$ and $g(x)$ are constants.

$\therefore$ Either $f(x) = 1, \ g(x) = 3$ or $f(x) = -1, \ g(x) = -3$

or $f(x) = 3, \ g(x) = 1$ or $f(x) = -3, \ g(x) = -1.$

$f(x) = 1 \Rightarrow A = (1) \quad \therefore \ \phi(x) \in \mathbf{Z}[x]$

$\Rightarrow \quad \phi(x) = 1 \Rightarrow \phi(x) \in A \quad \therefore \ A = \mathbf{Z}[x]$

$f(x) = -1 \Rightarrow A = (-1) \quad \therefore \ \phi(x) \in \mathbf{Z}[x]$

$\Rightarrow \quad \phi(x) = (-1)(-\phi(x)) \in A \quad \therefore \ A = \mathbf{Z}[x]$

$\therefore \quad f(x) = \pm 1 \Rightarrow A = \mathbf{Z}[x] \quad \therefore \ 4 \in A \qquad (\because \ 4 \in \mathbf{Z}[x])$

$\Rightarrow \quad 4 = 3\psi_1(x) + x\psi_2(x)$ for some $\psi_1(x), \psi_2(x) \in \mathbf{Z}[x]$

$\Rightarrow \quad 4 = 3a$ for some $a \in \mathbf{Z}$, which is impossible $\quad \therefore \ f(x) \neq \pm 1$

$f(x) = 3 \Rightarrow x = 3h(x) \Rightarrow x = 3(\lambda_0 + \lambda_1 x + \ldots\ldots + \lambda_n x^n)$, say

$(\because \ x = f(x)\, h(x))$

$\Rightarrow \quad 1 = 3\lambda_1$, which is impossible $\quad \therefore \ f(x) \neq 3$. Similarly, $f(x) \neq -3$.

$\therefore$ Our supposition is wrong. $\quad \therefore$ A is not a principal ideal of **Z**[*x*].

$\therefore$ **Z**[*x*] is not a PID.

7.7. POLYNOMIAL IN n VARIABLES OVER A RING

Let R be a ring. Let $x_1, x_2, \ldots\ldots, x_n$ be *n* variables.

Let $R_1 = R[x_1]$, the ring of polynomials in x_1 over the ring R.

$R_2 = R_1[x_2]$, the ring of polynomials in x_2 over the ring R_1

$R_3 = R_2[x_3]$, the ring of polynomials in x_3 over the ring R_2.

....

$R_n = R_{n-1}[x_n]$, the ring of polynomials in x_n over ring the R_{n-1}.

The ring R_n is called the ring of polynomials in *n* variables $x_1, x_2, \ldots\ldots, x_n$ over the ring R and is denoted by $R[x_1, x_2, \ldots\ldots, x_n]$.

The elements of $R[x_1, x_2, \ldots\ldots, x_n]$ are of the form $\sum a_{i_1} a_{i_2} \ldots\ldots a_{i_n} x_1^{i_1} x_2^{i_2} \ldots\ldots x_n^{i_n}$, where equality and addition are defined coefficientwise and multiplication is defined by the use of distributive law and the rule of exponents :

$$(x_1^{i_1} x_2^{i_2} \ldots\ldots x_n^{i_n})(x_1^{j_1} x_2^{j_2} \ldots\ldots x_n^{j_n}) = x_1^{i_1+j_1} x_2^{i_2+j_2} \ldots\ldots x_n^{i_n+j_n}.$$

Theorem 6. *If R is an integral domain then $R[x_1, x_2, ..., x_n]$ is also an integral domain.*

Proof. R is given to be an integral domain. We shall prove the result by using induction on the number of variables.

Let $n = 1$. Since R is an integral domain, so $R[x_1]$ is also an integral domain.

$\therefore$ The result is true for $n = 1$.

Let the result be true for $n - 1$ variables.

$\therefore$ $R[x_1, x_2, ..., x_{n-1}]$ is an integral domain.

$\Rightarrow$ $R[x_1, x_2, ..., x_{n-1}][x_n]$ is an integral domain.

$\Rightarrow$ $R[x_1, x_2, ... x_n]$ is an integral domain.

$\therefore$ The result is true for any number of variables.

Theorem 7. *If R is a unique factorization domain, then $R[x_1, x_2, ..., x_n]$ is also a unique factorization domain.*

Proof. R is given to be a unique factorization domain. We shall prove the result by using induction on the number of variables.

Let $n = 1$. Since R is a unique factorization domain, $R[x_1]$ is also a unique factorization domain*.

$\therefore$ The result is true for $n = 1$. Let the result be true for $n - 1$ variables.

$\therefore$ $R[x_1, x_2, ..., x_{n-1}]$ is a unique factorization domain.

$\Rightarrow$ $R[x_1, x_2, ..., x_{x-1}][x_n]$ is a unique factorization domain.

$\Rightarrow$ $R[x_1, x_2, ..., x_n]$ is a unique factorization domain.

$\therefore$ The result is true for any number of variables.

7.8. IRREDUCIBLE POLYNOMIAL

Let F be a field. A polynomial $p(x) \in F[x]$ is called an **irreducible polynomial** over F if for every $a(x), b(x) \in F[x]$,

$$p(x) = a(x)\, b(x) \Rightarrow \text{ either } a(x) \text{ or } b(x) \text{ has degree '0'}.$$

Ilustrations :

(*i*) The polynomial $x^2 - 5$ of $\mathbf{Q}[x]$ is irreducible over **Q** and not over **R** because

$$x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5}).$$

(*ii*) The polynomial $x^2 + 4$ of $\mathbf{R}[x]$ is irreducible over **R** and not over **C** because

$$x^2 + 4 = (x + 2i)(x - 2i).$$

Example 3. *Let F be a field. Show that every irreducible element of F[x] is an irreducible polynomial of F[x] and conversely.*

Sol. Let $f(x)$ be any irreducible element of $F[x]$. If possible, let $f(x)$ be a reducible polynomial.

$\therefore$ $\exists\, g(x), h(x) \in F[x]$ such that $f(x) = g(x)\, h(x)$ and $\deg g(x) > 0$, $\deg h(x) > 0$.

$\Rightarrow$ $g(x), h(x) \notin F$

$\Rightarrow$ $g(x), h(x)$ cannot be units of F

*We have accepted this result, keeping in view the scope of this book.

$\Rightarrow$ $g(x)$, $h(x)$ cannot be units of F[x] ($\because$ Units of F and F[x] are same)

$\therefore$ $f(x)$ cannot be an irreducible element of F[x]. This is absurd.

$\therefore$ $f(x)$ is an irreducible polynomial.

Conversely, let $f(x)$ be an irreducible polynomial of F[x].

$\therefore$ $f(x)$ is not a constant polynomial. $\therefore$ $f(x)$ is not a unit of F[x].

Let $f(x) = g(x)\, h(x)$, where $g(x), h(x) \in$ F[x].

Since $f(x)$ is an irreducible polynomial, either $g(x)$ or $h(x)$ is a constant polynomial.

Let $g(x) = g_0 \in$ F

Since $g_0 \neq 0$, $g_0^{-1} \in$ F

$\therefore$ g_0 is a unit in F $\therefore$ g_0 is a unit in F[x]

$\therefore$ $f(x)$ is an irreducible element of F[x].

Note. From now onward, we shall be restricting ourselves to polynomials over the field of rational numbers **Q**. In other words, we shall be considering polynomials belonging to **Q**[x] only.

7.9. CONTENT OF A POLYNOMIAL

Let $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n$ be a polynomial with $a_0, a_1, \ldots\ldots a_n \in$ Z. The greatest common divisor (g.c.d.) of the integers $a_0, a_1, \ldots\ldots, a_n$ is called the **content** of the polynomial $f(x)$.

For example, let $f(x) = 4 + 10x - 8x^3$.

The g.c.d. of 4, 10, 0, – 8 is 2.

$\therefore$ The content of $f(x)$ is 2.

7.10. PRIMITIVE POLYNOMIAL

Let $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n$ be a polynomial with $a_0, a_1, \ldots\ldots a_n \in$ Z. If the greatest common divisor of $a_0, a_1, \ldots\ldots, a_n$ is 1 then $f(x)$ is called a **primitive polynomial.** The content of a primitive polynomial is 1. For example, the polynomial $3 + 4x + 7x^2$ is a primitive polynomial, because g.c.d. of 3, 4, 7 is 1.

Remark. Let $f(x) = a_0 + a_1x + \ldots\ldots a_nx^n$ be a polynomial with integer coefficients. $f(x)$ may or may not be primitive. Let $f(x)$ be not primitive.

Let c = g.c.d. $(a_0, a_1, \ldots\ldots, a_n)$ be the content of $f(x)$. $\therefore$ $c > 1$.

Also, $c/a_0, c/a, \ldots\ldots c/a_n$.

Let $a_0 = cb_0, a_1 = cb_1, \ldots\ldots, a_n = cb_n$ for integers $b_0, b_1, \ldots\ldots, b_n$.

Also g.c.d. $(b_0, b_1, \ldots\ldots, b_n) = 1$

$\therefore$ The polynomial

$b_0 + b_1x + \ldots\ldots + b_nx^n$ is primitive.

Now $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n = c(b_0 + b_1x + \ldots\ldots + b_nx^n)$

$\therefore$ **f(x) = (content of f(x)). (a primitive polynomial).**

Theorem 8. *The product of two primitive polynomials is also a primitive polynomial.*

Proof. Let $\quad f(x) = a_0 + a_1x + ... + a_mx^m$

and $\quad g(x) = b_0 + b_1x + ... + b_nx^n$

be two primitive polynomials.

$\therefore$ By definition,

$$f(x)\,g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + ... + a_mb_nx^{m+n}$$

If possible, let $f(x)\,g(x)$ be not primitive.

$\therefore$ All the coefficients of $f(x)\,g(x)$ would be divisible by some integer larger than 1 and hence by some prime number p, because there always exists a prime factor of a positive integer larger than 1.

Since $f(x)$ and $g(x)$ are both primitive, p cannot divide each and every coefficient of $f(x)$ and $g(x)$.

Let a_j and b_k be the first coefficients of $f(x)$ and $g(x)$ respectively which p does not divide.

$\therefore \quad p/a_0, p/a_1, ... p/a_{j-1}, b \nmid a_j$ and $p/b_0, p/b_1, ... p/b_{k-1}\, p \nmid b_k$.

In $f(x)\,g(x)$, the coefficient of x^{j+k}

$$= (a_0b_{j+k} + a_1b_{j+k-1} + ...+ a_{j-1}b_{k+1}) + a_jb_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + ... + a_{j+k}b_0)$$

By the choice of a_j, we have $p/(a_0b_{j+k} + a_1b_{j-k-1} + ... + a_{j-1}b_{k+1})$

By the choice of b_k, we have $p/(a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + ... + a_{j+k}b_0)$

By the choice of p, it divides all coefficients of $f(x)\,g(x)$.

$\therefore$ p must divide a_jb_k. Since p is prime, either p/a_j or p/b_k.

This contradicts the choice of a_j and b_k.

$\therefore$ Our supposition is wrong.

$\therefore$ The product $f(x)\,g(x)$ is also a primitive polynomial.

Theorem 9. (Gauss Lemma). *If the primitive polynomial f(x) can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.*

Proof. Let $f(x) = g(x)\,h(x)$, where $g(x)$ and $h(x)$ are polynomials having rational coefficients. By clearing denominators and taking out common factors we can then write

$f(x) = (a/b)\,g_1(x)\,h_1(x)$, where a and b are integers and the polynomials $g_1(x)$ and $h_1(x)$ are primitive.*

$$\Rightarrow \qquad bf(x) = ag_1(x)\,h_1(x).$$

Since $f(x)$ is primitive, the content of $bf(x)$ is $b(1)$ *i.e.*, b.

Similarly, the content of $ag_1(x)\,h_1(x)$ is a.

*For example, let $f(x) = 3 + 6x - x^2 - 2x^3$.

$f(x)$ is also equal to the product of polynomials $\frac{4}{3} + \frac{8}{3}x$ and $\frac{9}{4} - \frac{3}{4}x^2$.

$$\therefore \qquad f(x) = \left(\frac{4}{3} + \frac{8}{3}x\right)\left(\frac{9}{4} - \frac{3}{4}x^2\right)$$

$$= \frac{4}{3}(1 + 2x)\,\frac{3}{4}(3 - x^2) = \frac{1}{1}\,(1 + 2x)(3 - x^2).$$

$\therefore$ We must have $b = a$.

$\therefore$ $f(x) = (1/1)\, g_1(x)\, h_1(x)$ *i.e.*, $f(x) = g_1(x)\, h_1(x)$.

$\therefore$ $f(x)$ can be factored as the product of two polynomials having integer coefficients.

7.11. THE EISENSTEIN CRITERION

Statement. *Let $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n$ be a polynomial with integer coefficients. Suppose that for some prime number p, $p^2 \nmid a_0$, p/a_0, p/a_1, p/a_2, ..., p/a_{n-1}, $p \nmid a_n$.*

Then $f(x)$ is irreducible over the rationals.

Proof. We have $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n$.

Let $c = \text{g.c.d.}(a_0, a_1, \ldots\ldots, a_n)$ and $a_0 = cb_0, a_1 = cb_1, \ldots\ldots, a_n = cb_n$

$\therefore$ $f(x) = c(b_0 + b_1x + \ldots\ldots + b_nx^n) = cg(x)$, say.

$\therefore$ $g(x)$ is a primitive polynomial. If $f(x)$ is itself primitive, then we take $c = 1$ and $g(x) = f(x)$.

$$p \nmid a_n \;\Rightarrow\; p \nmid cb_n \;\Rightarrow\; p \nmid c, p \nmid b_n$$

$$p/a_0 \;\Rightarrow\; p/cb_0 \;\Rightarrow\; p/b_0 \qquad (\because\; p \nmid c)$$

Similarly, p/b_1, p/b_2, ... , p/b_{n-1}.

$$p^2 \nmid a_0 \;\Rightarrow p^2 \nmid c^2b_0^{\,2} \;\Rightarrow\; p^2 \nmid b_0^{\,2} \qquad (\because\; p \nmid c \;\Rightarrow\; p^2 \nmid c^2)$$

$\therefore$ $p^2 \nmid b_0$, p/b_0, p/b_1, p/b_2, ... p/b_{n-1}, $p \nmid b_n$.

If possible, let the primitive polynomial $g(x)$ be reducible over rationals.

$\therefore$ The primitive polynomial $g(x)$ can be factored as the product of two polynomials having rational coefficients.

$\therefore$ By **Gauss Lemma**, the primitive polynomial $g(x)$ can be factored as the product of two polynomials having integer coefficients.

Let $g(x) = (c_0 + c_1x + \ldots\ldots + c_rx^r)(d_0 + d_1x + \ldots\ldots + d_sx^s)$, where the c's and d's are integers and $r, s > 0$.

Comparing constant terms, we get $b_0 = c_0d_0$.

$\therefore$ $p/b_0 \;\Rightarrow\; p/c_0d_0 \;\Rightarrow\; p/c_0$ or p/d_0.

If possible, let p/c_0 and p/d_0 both.

$\therefore$ $c_0 = \lambda p$, $d_0 = \mu p$ for some integers λ, μ.

$\Rightarrow$ $b_0 = c_0d_0 = \lambda\mu p^2 \;\Rightarrow\; p^2/b_0$, which is impossible.

$\therefore$ p cannot divide c_0, d_0 both. Let p/c_0 and $p \nmid d_0$.

We claim that p cannot divide all c's. If possible, let p divide all c's.

$\Rightarrow$ $p/(c_0 + c_1x + \ldots\ldots + c_rx^r) \;\Rightarrow\; p/g(x)$

$\Rightarrow$ $p/(b_0 + b_1x + \ldots\ldots + b_{n-1}x^{n-1} + b_nx^n)$

$\Rightarrow$ p/b_n $\quad(\because\; p/b_0, p/b_1, \ldots\ldots, p/b_{n-1} \;\Rightarrow\; p/b_0 + b_1x + \ldots\ldots + b_{n-1}x^{n-1})$

This is impossible.

$\therefore$ p cannot divide all c's. Let c_k be the first c not divisible by p, $k \le r < n$.

∴ p divides $c_0, c_1 ......, c_{k-1}$.

Now $\quad b_k = c_0d_k + c_1d_{k-1} + c_2d_{k-2} + ... + c_{k-1}\,d_1 + c_kd_0$

We have $\quad p/b_k, p/c_0, p/c_1, p/c_2, ..., p/c_{k-1}$

∴ $\quad p/(b_k - (c_0d_k + c_1d_{k-1} + c_2d_{k-2} + ... + c_{k-1}d_1))$

⇒ $p/c_kd_0 \Rightarrow p/c_k$ or p/d_0. This is impossible, because we have $p \nmid c_k, p \nmid d_0$.

∴ Our supposition is wrong.

∴ The primitive polynomial $g(x)$ is not reducible over rationals.

∴ $g(x)$ is irreducible over rationals.

∴ $f(x)$, being a constant multiple of an irreducible polynomial is also irreducible over rationals.

Example 4. *Show that the polynomial $x^4 - 4x + 2$ is irreducible over* **Q.**

Sol. Let $\quad f(x) = x^4 - 4x + 2$

∴ $\quad f(x) = 2 + (-4)x + 0x^2 + 0x^3 + x^4$

Let $\quad a_0 = 2, a_1 = -4, a_2 = 0, a_3 = 0, a_4 = 1.$

Let $\quad p = 2$. This is a prime number.

Now $\quad (2)^2 \nmid 2, 2/2, 2/(-4), 2/0, 2/0, 2 \nmid 1$

∴ $\quad p^2 \nmid a_0, p/a_0, p/a_1, p/a_2, p/a_3, p \nmid a_4$

∴ By **Eisenstein criterion**, the given polynomial is irreducible over **Q.**

Example 5. *Show that the polynomial $x^n - p$ is irreducible over* **Q.** *Here p is some prime number.*

Sol. Let $\quad f(x) = x^n - p.$

∴ $\quad f(x) = -p + 0x + 0x^2 + ... + 0x^{n-1} + 1.x^n$

Here $\quad a_0 = -p, a_1 = 0, a_2 = 0, ..., a_{n-1} = 0, a_n = 1$

We have $\quad p^2 \nmid (-p), p/-p, p/0, p/0, ..., p/0, p \nmid 1.$

∴ By **Eisenstein criterion** the given polynomial is irreducible over **Q.**

Example 6. *Let p be a prime number and $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$. Show that $f(x)$ is irreducible over* **Q.**

Sol. We have

$$f(x) = x^{p-1} + x^{p-2} + ... + x + 1.$$

$$\Rightarrow \quad f(x) = 1 + x + ... + x^{p-2} + x^{p-1}$$

$$= \frac{1(1-x^p)}{1-x} = \frac{x^p - 1}{x-1}$$

Replacing x by $x + 1$, we get

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{(1+x)^p - 1}{x}$$

$$= \frac{1}{x}\,[1 + {}^pC_1x + {}^pC_2x^2 + ... + {}^pC_px^p - 1]$$

$$= \frac{x}{x}[{}^pC_1 + {}^pC_2x + \ldots\ldots + {}^pC_px^{p-1}]$$

$$= p + \frac{p(p-1)}{2}x + \ldots\ldots + x^{p-1}$$

Let $\qquad a_0 = p, a_1 = \frac{p(p-1)}{2}, \ldots\ldots, a_{p-1} = 1$

$\therefore$ $p^2 \nmid a_0, p/a_0, p/a_1, \ldots\ldots p \nmid a_{p-1}$

$\therefore$ By **Eisenstein criterion** $f(x + 1)$ is irreducible over **Q.**

If possible, let $f(x)$ be not irreducible over **Q.**

$\therefore$ $\qquad f(x) = g(x)\,h(x)$ for some $g(x)\,h(x) \in$ **Q**$[x]$ with deg $g(x) > 1$, deg $h(x) > 1$.

$\therefore$ $\qquad f(x + 1) = g(x + 1)\,h(x + 1)$ and deg $g(x + 1) > 1$, deg $h(x + 1) > 1$.

$\therefore$ $f(x + 1)$ is not irreducible over **Q.** This is impossible.

$\therefore$ Our supposition is wrong.

$\therefore$ $f(x)$ *i.e.*, the given polynomial is irreducible over **Q.**

SUMMARY

- If R is a ring then the set of polynomials R$[x]$ over R is also a ring.
- If the ring R is commutative, then R$[x]$ is also commutative.
- If the ring R has unit element then R$[x]$ also has unit element.
- If R is an integral domain, then R$[x]$ is also an integral domain.
- If F is a field then F$[x]$ is an integral domain and not a field.
- If F is a field then F$[x]$ is a Euclidean ring.
- If F is a field then F$[x]$ is a principal ideal ring.
- If R is an integral domain then R$[x_1, x_2, \ldots\ldots, x_n]$ is also as integral domain.
- If R is a unique factorization domain then R$[x_1, x_2, \ldots\ldots, x_n]$ is also a unique factorization domain.
- The product of two primitive polynomials is also primitive.
- **Gauss Lemma.** If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.
- **Eisenstein Criterion.** Let $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n$ be a polynomial with integer coefficients. Suppose that for some prime number p, $p^2 \nmid a_0$, $p/a_0, p/a_1, p/a_2, \ldots\ldots p/a_{n-1}, p \nmid a_n$. Then $f(x)$ is irreducible over the rationals.

REVIEW QUESTIONS

1. If R is a ring and $f, g, h \in$ R$[x]$, then show that :

(*i*) $f(g + h) = fg + fh$ $\qquad$ (*ii*) $(g + h)f = gf + hf$.

2. If R is a commutative ring and $f, g \in$ R$[x]$, then show that $fg = gf$.

3. If R is a ring with unit element 1, then show that R$[x]$ is a ring with unit element $(1, 0, 0, 0, \ldots\ldots)$.

4. Let R[x] be the ring of polynomials over a ring R. Show that $R' = \{(a, 0, 0, \ldots\ldots) : a \in R\}$ *i.e.* the set of all constant polynomials is a subring of R[x] and R is isomorphic to R′.
5. If R is a ring, show that it can be embedded in the ring R[x].
6. If R is an integral domain with unit element, then every unit in R is a unit in R[x] and every unit in R[x] is a unit in R.
7. Let R be a an integral domain with unit element. Show that if a is an irreducible element of R then a is also an irreducible element of R[x].
8. Let R be a commutative ring with unit element. If (x) is a prime ideal of R[x] then show that R is an integral domain.
9. Let **R**[x] be the ring of polynomials over the ring of real numbers. Let $A = \{f(x) \in \mathbf{R}[x] : f(0) = 0 = f(1)\}$. Show that A is an ideal of **R**[x] and the quotient ring **R**[x]/A is not an integral domain.
10. If F is a field then for any two polynomials $f(x), g(x) \in F[x]$, $g(x) \neq 0$, there exists unique polynomials $q(x)$ and $r(x)$ in F[x] such that $f(x) = g(x)\, q(x) + r(x)$, where $r(x) = 0$ or deg $r(x)$ < deg $g(x)$. This is called **'the division algorithm'**.

NOTES

UNIT 8

VECTOR SPACES

STRUCTURE

8.0. LEARNING OBJECTIVES

NOTES

After going through this unit, you should be able to:

- field, subfield, binary operation
- vector space, subspace, sum of two space and subspace.

8.1. INTRODUCTION

Before we go to the concept of vector space, we first define field, subfield, internal and external binary operations.

8.2. FIELD

A non-empty set F containing at least two elements and with two binary operations, denoted additively (+) and multiplicatively (.), is called a field if

(*i*) F is an abelian group w.r.t. addition (+).

(*ii*) The set of all non-zero elements F—{0} is an abelian group w.r.t. multiplication (.).

(*iii*) The multiplication distributes over addition

i.e., $a(b + c) = ab + ac$

and $(b + c)a = ba + ca$ $\bigg\}$ $a, b, c \in$ F.

A field with addition and multiplication compositions is written as : (F, +, .).

Note that the multiplicative inverse of a non-zero element of a field is unique.

Some examples of number fields are :

(Q, +, .), (R, +, .) and (C, +, .).

8.3. SUBFIELD

A subset S (containing more than one element) of a field F is called a subfield of F if S is a field w.r.t. the addition and multiplication in F.

For example,

(*i*) The field (Q, +, .) is a subfield of the field (R, +, .).

(*ii*) The field (R, +, .) is a subfield of (C, +, .).

8.4. INTERNAL BINARY OPERATION

*If in a non-empty set S, $a * b \in S$ for all $a, b \in S$ and $a * b$ is unique, we say that the binary operation * is an internal binary operation on S.*

8.5. EXTERNAL BINARY OPERATION

NOTES

Let V and F be two non-empty sets. If $v * \alpha \in V$ for each $v \in V$ and $\alpha \in F$, and $v * \alpha$ is unique, then $*$ is called an external binary operation on V over F.

In the external binary operation, v is an element of V, α is an element of F and $v * \alpha$ is an element of V.

8.6. VECTOR SPACES

So far, we have studied algebraic structures such as groups, rings or fields which involve only internal binary operations, *i.e.*, binary operations in which the element associated to an ordered pair of elements of the underlying set is an element of the set. Now, we are going to introduce a new algebraic structure called Vector Space, which involves an external binary operation. The motivation for this algebraic system is the set of vectors, where vectors can be added and can be multiplied by scalars (reals or complex) to produce vectors.

We now, define the concept of a vector space over a field F.

8.7. DEFINITION

Definition. *Let (F, +, .) be a field. Then, a non-empty set V together with two binary operations called vector addition '+' (internal composition in V) and scalar multiplication '.' (external composition) is called a vector space over the field F if the following conditions are satisfied :*

1. (V, +) is an abelian group i.e.,

(*i*) V is closed w.r.t. '+' *i.e.,* $u, v \in V \Rightarrow u + v \in V$

(*ii*) Addition is commutative : $u + v = v + u, \forall u, v \in V$

(*iii*) Addition is associative :

$u + (v + w) = (u + v) + w, \quad \forall u, v, w \in V$

(*iv*) Existence of identity : There is a unique vector $\mathbf{0}$ in V, called the zero vector, such that $u + \mathbf{0} = u = \mathbf{0} + u \quad \forall u \in V$

(*v*) Existence of inverse :

For each vector u in V, there is a unique vector $-u$ in V such that $u + (-u) = \mathbf{0} = (-u) + u$

2. The scalar multiplication, '.' which associates for each

$u \in V$ and $a \in F$, a unique vector $au \in V$ satisfies :

(*i*) $1. u = u, \quad \forall u \in V$

(*ii*) $a(u + v) = au + av, \quad \forall u, v \in V, a \in F$

(*iii*) $(a + b)u = au + bu, \quad \forall u \in V$ and $a, b \in F$

(*iv*) $(ab)(u) = a(bu), \quad \forall u \in V$ and $a, b \in F$.

Elements of F are called scalars and those of V are called vectors.

Thus, a vector space is a composite of '*a* field', '*a* set of vectors' and two operations with certain properties.

We say *V is a vector space over the field F* and is denoted by V(F) but when there is no chance of confusion, we just refer to the vector space as V.

Vector space is also called the linear space.

8.8. A PLANE VECTOR IS AN ORDERED PAIR (a_1, a_2) OF REAL NUMBERS

A space vector is an ordered triplet (a_1, a_2, a_3) of real numbers.

We do not make any distinction between the plane vector (a_1, a_2) and the directed line segment $\overrightarrow{OP}$, where O is the origin and P is the point whose cartesian coordinates are (a_1, a_2). In fact, we write $(a_1, a_2) = \overrightarrow{OP}$.

In this case the vector (a_1, a_2) is also called the position vector of P. Similarly, in the case of space vectors, we write $(a_1, a_2, a_3) = \overrightarrow{OP}$. The vector (0, 0, 0) is the zero vector is space.

The set of all plane vectors (*i.e.*, the set of all ordered pairs of real numbers) is denoted by V_2. The set of all space vectors (*i.e.*, the set of all ordered triplets of real numbers) is denoted by V_3. Since V_2 is cartesian product R × R, we also denote V_2 by R^2. Similarly,

$$V_3 = R \times R \times R = R^3.$$

Two plane vectors (a_1, a_2) and (b_1, b_2) are equal iff $a_1 = b_1$and $a_2 = b_2$.

Two space vectors (a_1, a_2, a_3) and (b_1, b_2, b_3) are equal iff $a_1 = b_1$, $a_2 = b_2$, $a_3 = b_3$.

Addition of vectors in V_2 is defined by $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$ for all vectors (a_1, a_2), (b_1, b_2) ∈ V_2.

Multiplication of vectors in V_2 by a real number λ is defined as

$$\lambda(a_1, a_2) = (\lambda a_1, \lambda a_2), \text{ for } (a_1, a_2) \in V_2 \text{ and } \lambda \in R.$$

Likewise, we define addition and scalar multiplication in V_3.

Proceeding exactly as in the above example, we see that V_2 and V_3 are vector spaces over R.

8.9. VISUALISATION OF A VECTOR SPACE INVOLVES THE FOLLOWING FIVE STEPS

(*i*) Consider a non-empty set V.

(*ii*) Define a binary operation on V and call it vector addition.

(*iii*) Define scalar multiplication on V.

(*iv*) Define equality in V.

(*v*) Check that V forms an abelian group w.r.t. vector addition and that scalar multiplication satisfies the four properties mentioned in the definition of vector space.

NOTES

Proceeding on the lines of V_2, and V_3, we now generalize to the set of all ordered n-tuples in the following example.

Example 1. *Consider the set R^n (also denoted by R_n) of all ordered n-tuples of real numbers defined by*

$$R^n = \{X = (x_1, x_2, ..., x_n) \mid x_i \text{ is real}, i = 1, 2, 3, ..., n\}.$$

Prove that R^n is a vector space over R w.r.t. usula addition and scalar multiplication defined in R^n.

Sol. The n-tuple $X = (x_1, x_2, ..., x_n)$ is called an n-vector, x_i is called the ith coordinate or component of X. O = (0, 0, ..., 0) is called the null vector.

We define addition and scalar multiplication among n-tuples as follows :

If $X = (x_1, x_2, ..., x_n)$ and $Y = (y_1, y_2, ..., y_n)$ then we define

$$X + Y = (x_1 + y_1, x_2 + y_2, ... x_n + y_n).$$

This (coordinate wise) addition is called vector addition.

If λ is a real number, we define $\lambda X = (\lambda x_1, \lambda x_2, ... \lambda x_n)$ and *is called (coordinate wise) scalar multiplication* (λ is called a scalar).

Two vectors X and Y are equal iff $x_i = y_i$, $i = 1, 2, 3 ...., n$.

Now, we check that the set R^n of all ordered n-tuples of real numbers is a vector space over R under coordinate-wise vector addition and scalar multiplication :

Now, (1) R^n forms an abelian group under vector addition.

For, (*i*) X + Y = Y + X (commutative law of addition)

(*ii*) X + (Y + Z) = (X + Y) + Z (associative law of addition)

(*iii*) There is an n-tuple O = (0, 0, ..., 0) called the zero vector such that

$$X + O = X = O + X, \forall X \in R^n.$$

(*iv*) For each X in R^n, there exists a unique Y in R^n such that

$$X + Y = O = Y + X$$

Y is denoted by $-X$ and is the vector $-X = (-x_1, -x_2, ..., -x_n)$ if $X = (x_1, x_2, ..., x_n)$.

(2) The scalar multiplication satisfies the following properties :

(*i*) $1.X = X$, $\forall X \in R^n$

(*ii*) $a(X + Y) = aX + aY$, $\forall X, Y \in R^n$ and $a \in R$

(*iii*) $(a + b)X = aX + bX$, $\forall X \in R^n$ and $a, b \in R$

(*iv*) $(ab)X = a(bX)$, $\forall X \in R^n$ and $a, b \in R$

Hence R^n is a vector space over R.

Note that R^n is a vector space over R but R^n is not a vector space over C, the field of complex numbers. For, suppose λ is a non-real complex number, then $\lambda X = (\lambda x_1, \lambda x_2, ..., \lambda x_n)$ is not in R^n because the numbers λx_i are non-real complex and R^n contains only n-tuples of real numbers.

The special cases $n = 2$ and $n = 3$, give the vector spaces

$$R^2 = V_2 \quad \text{and} \quad R^3 = V_3.$$

The special case $n = 1$ gives the vector space V_1, which is nothing but the space of real numbers, where addition is the ordinary addition of real numbers and scalar multiplication is the ordinary multiplication of real numbers.

Example 2. *Show that the set $M_{m,n}$ (R) of all m × n matrices with matrix addition and scalar multiplication is a vector space over R.*

Sol. We shall denote the set $M_{m,n}$(R) briefly by M in our solution.

Composition : Matrix addition is an internal binary composition in the set M.

We know that sum of two matrices of the same order $m \times n$ is always defined and is a matrix of order $m \times n$ and hence belongs to the same set M.

Also **multiplication of a matrix** $A = [a_{ij}]_{m \times n}$ by a *scalar* α $(\alpha \in R)$ is a matrix $\alpha A = [\alpha a_{ij}]_{m \times n}$ and hence belongs to the same set M.

Now, **(I) The set M is an abelian group under addition as shown below :**

(*i*) **Commutativity**

Let $A = [a_{ij}]_{m \times n}$ and $B = [b_{ij}]_{m \times n}$ be two matrices belonging to the set M.

Then $A + B = B + A$ [∵ Matrix addition is commutaitve]

(*ii*) **Associativity**

Let $A = [a_{ij}]_{m \times n}$, $B = [b_{ij}]_{m \times n}$ and $C = [c_{ij}]_{m \times n}$ be three matrices belonging to the set M.

Then $(A + B) + C = A + (B + C)$ [∵ Matrix addition is associative]

(*iii*) **Existence of Identity**

Let $A = [a_{ij}]_{m \times n}$ be any matrix belonging to the set M.

Then, there exists a $m \times n$ null matrix $O_{m \times n}$ in M such that

$$A + O = O + A = A$$

(*iv*) **Existence of Inverse**

Let $A = [a_{ij}]_{m \times n}$ belong to the set M.

∴ Matrix $-A = [-a_{ij}]_{m \times n}$ also belongs to the set M such that $A + (-A) = (-A) + A = 0$ [∵ $a_{ij} \in R \Rightarrow -a_{ij} \in R$]

Hence the set M is an abelian group under addition.

Properties of Scalar Multiplication

(II) From the properties of matrices, it follows that scalar multiplication satisfies the following properties :

(*i*) $1.A = A, \forall A \in M$

(*ii*) $\alpha(A + B) = \alpha A + \alpha B, \forall \alpha \in R$ and $A, B \in M$

(*iii*) $(\alpha + \beta) A = \alpha A + \beta A, \forall \alpha, \beta \in R$ and $A \in M$

(*iii*) $(\alpha\beta) A = \alpha(\beta A) \forall \alpha, \beta \in R$ and $A \in M$

Thus the set M satisfies all the postulates of the vector space.

Hence $M_{m,n}$(R) = M, the set of all $m \times n$ matrices over R is a vector space.

Example 3. *Show that any field forms a vector space over itself.*

Sol. Let F be any field.

Let V = F.

Since F is a field, F has two binary compositions defined in it say addition (+) and multiplication (.).

Addition composition of F is vector addition in V and multiplication composition in F is scalar multiplication.

Now (I), (V, +) is an abelian group (∵ V = F is a field).

(II) From the field properties of F, it follows that scalar multiplication satisfies :

(*i*) $1 \,.\, u = u \qquad \forall\, u \in V$

(*ii*) $a(u + v) = au + av \qquad \forall\, u, v \in V, a \in F$

(*iii*) $(a + b)\, u = au + bu \qquad \forall\, u \in V$ and $a, b \in F$

(*iv*) $(ab)\, u = a(bu) \qquad \forall\, u \in V$ and $a, b \in F$.

Hence, V is a vector space over F.

Example 4. *Let H be a subfield of a given field F. Show that F can be regarded as a vector space over H.*

Sol. Let us take the usual addition in the field F as vector addition. Let us define the scalar multiplication in the following way :

If $u \in F$ and $a \in H$, then au may be taken as the product of these elements as already defined in the field F.

Now, (I) F is an abelian group under vector addition.

(II) From the field properties of F, it follows that the scalar multiplication satisfies the following properties :

(*i*) $1 \,.\, u = u \qquad \forall\, u \in F$ and $1 \in H$

(*ii*) $a(u + v) = au + av \qquad \forall\, u, v \in F$ and $a \in H$

(*iii*) $(a + b)\, u = au + bu \qquad \forall\, u \in F$ and $a, b \in H$

(*iv*) $(ab)\, u = a(bu) \qquad \forall\, u \in F$ and $a, b \in H$

Hence, F is a vector space over the subfield H.

Note. The field R of all real numbers is a subfield of the field C of all complex numbers. So C is a vector space over R*. But, note that R is not a vector space over C because R is not closed w.r.t. scalar multiplication. For example, $2 \in R$, $3 + 2i \in C$ but $2\,(3 + 2i)$ does not belong to R.

8.10. SOME GENERAL PROPERTIES OF A VECTOR SPACE

If V is a vector space over a field F and **0** is the zero of V and 0 is the zero of the field F, then

(*i*) $a\mathbf{0} = \mathbf{0}, \qquad \forall\, a \in F$

(*ii*) $0u = \mathbf{0}, \qquad \forall\, u \in V$

(*iii*) $(-1)\, u = -u, \qquad \forall\, u \in V$

(*iv*) $a(-u) = -(au) = (-a)\, u, \qquad \forall\, a \in F, u \in V$

(*v*) $a(u - v) = au - av, \qquad \forall\, a \in F, u, v \in V$

(*vi*) If $a\, u = \mathbf{0}$, then $a = 0$ or $u = \mathbf{0}$.

Proof. (*i*) Let $u \in V$.

Then $au = a(u + \mathbf{0}) = au + a\mathbf{0}$

$\Rightarrow \quad a\mathbf{0} = \mathbf{0}$

(*ii*) $\quad 0 + 0 = 0, 0 \in F$

$\Rightarrow \quad (0 + 0) = u = 0u, \forall\, u \in V$

NOTES

$\Rightarrow \qquad 0u + 0u = 0u$

$\Rightarrow \qquad 0u = \mathbf{0}$

(*iii*) $\qquad (-1)\,u + u = (-1)\,u + 1.\,u = (-1+1)\,u = 0u = \mathbf{0}$

$\Rightarrow \qquad (-1)\,u = -u.$

Proofs of others are left to the reader as an exercise.

VECTOR SUBSPACE

Sometimes we are not interested in the entire region of a vector space, but are interested in only a particular part of it. For example, we may be interesting in one-dimensional lines or two-dimensional planes in the three dimensional vector space V_3, especially on those lines or planes which pass through origin. Such lines or planes form a vector space on their own. Such cases lead to a new concept known as vector-subspace which we shall, now introduce.

8.11. VECTOR SUBSPACE

A non-empty subset W of a vector space V over a field F is called a subspace of V if W is a vector space over F under the same operations of vector addition and scalar multiplication as in V.

Following example illustrate the concept of a subspace :

Example 5. *Consider the vector space*

$$V = R^3 = \{(x_1, x_2, x_3) \mid x_i \in R\}$$

of all ordered triplets of real numbers over R under the operations of coordinate-wise addition and coordinate-wise scalar multiplication.

Let $\qquad W = \{(x_1, x_2, 0) \mid x_1, x_2 \in R\} \subseteq V.$

Then W is a subspace of V.

Sol. Let $u = (x_1, x_2, 0)$ and $v = (y_1, y_2, 0)$ be any two elements of W.

Then, $u + v = (x_1 + y_1, x_2 + y_1, 0)$ and $au = (ax_1, ax_2, 0)$ belong to W for $a \in$ R.

The zero element $(0, 0, 0) \in$ W.

Negative of u is $-u = (-x_1, -x_2, 0) \in$ W.

Other laws of associativity and commutativity for addition, distributive laws and scalar axiom $1.u = u$, etc. are all true in W, because elements of W are elements of V and in V all these laws are true. Hence, W is a subspace of V.

In the above example, we note that to prove that W is a subspace of V, we explicitly checked only the followings :

(*i*) The sum of any two vectors in W is in W. *i.e.*, W is closed w.r.t. vector addition.

(*ii*) The scalar multiple of any vector in W is in W. *i.e.*, W is closed w.r.t. scalar multiplication.

(*iii*) The existence of **0** in W and the existence of a negative for each element in W.

The other axioms were not explicitly checked, because this, as the following theorem shows, was not necessary. In fact, the theorem shows that even (*iii*) need not have been checked.

Theorem 1. *The necessary and sufficient condition for a non-empty subset W of a vector space V (F) to be a sub-space of V is that W is closed w.r.t. vector addition and scalar multiplication in V.*

Proof. (1) *The condition is necessary.* If W is a sub-space of V, then W is a vector space and therefore, W is closed w.r.t. vector addition and scalar multiplication.

(2) *The condition is sufficient i.e., if W is closed w.r.t. vector addition and scalar multiplication in V, then W is a vector sub-space of V.*

If $u \in \mathrm{W}$ and $1 \in \mathrm{F}$, then $-1 \in \mathrm{F}$ and $(-1)\,u \in \mathrm{W}$

($\because$ W is closed under scalar multiplication)

But, $\quad (-1)\,u = -(1.u) = -u$

Hence, $\quad u \in \mathrm{W} \;\Rightarrow\; -u \in \mathrm{W},\ \forall\, u \in \mathrm{W}.$

Now, $\quad u \in \mathrm{W}, -u \in \mathrm{W} \;\Rightarrow\; u + (-u) = \mathbf{0} \in \mathrm{W}$

(Since W is closed w.r.t. vector addition).

Commutativity and associativity also hold good as they hold in $\mathrm{V} \supseteq \mathrm{W}$.

$\therefore$ (W, +) is an abelian group.

Other postulates of vector space hold good in case of W as they hold in $\mathrm{V} \supseteq \mathrm{W}$.

Hence, W is a vector subspace of V.

Theorem 2. *A non-empty subset W of V is a subspace of a vector space V(F), if and only if for each pair of vectors $u, v \in W$ and each scalar $a \in F$, the vector $au + v \in W$.*

Proof. (*i*) Let W be a subspace of V.

Let $u, v \in \mathrm{W}$ and $\alpha \in \mathrm{F}$

Now, $\alpha \in \mathrm{F}$ and $u \in \mathrm{W} \;\Rightarrow\; \alpha u \in \mathrm{W}$

$\alpha u \in \mathrm{W}, v \in \mathrm{W} \;\Rightarrow\; \alpha u + v \in \mathrm{W}.$

(*ii*) Let W be a non-empty subset of V such that $au + v \in \mathrm{W}$ for all vectors $u, v \in \mathrm{W}$ and all scalars $a \in \mathrm{F}$. Since W is non-empty, there is a vector $w \in \mathrm{W}$ and hence $(-1)\,w + w = \mathbf{0}$ is in W. If u is any vector in W and a is any scalar, then the vector $au = au + \mathbf{0}$ is in W. In particular $(-1)\,u = -u$ is in W. Finally, if $u, v \in \mathrm{W}$, then $u + v = 1u + v$ is in W.

Hence W is a subspace of V.

Theorem 3. *The necessary and sufficient conditions for any non-empty subset W(F) to be a subspace of V(F) are :*

(*i*) $u, v \in W \quad \Rightarrow u - v \in W$

(*ii*) $a \in F$ *and* $u \in W \quad \Rightarrow au \in W.$

Proof. (1) *Conditions are necessary*

Let W be a subspace of V(F).

$$\therefore \quad u, v \in \mathrm{W} \;\Rightarrow\; u, -v \in \mathrm{W} \qquad \text{(Inverse property of W).}$$
$$\Rightarrow\; u + (-v) \in \mathrm{W} \qquad (\because \text{ W is closed w.r.t. } +)$$
$$\Rightarrow\; u - v \in \mathrm{W}$$

As W is closed w.r.t. scalar multiplication,

$$a \in \mathrm{F}, u \in \mathrm{W} \Rightarrow au \in \mathrm{W}.$$

So, the conditions are necessary.

(2) *Conditions are sufficient*

Let W be a subset of V(F) such that

(*i*) $u, v \in W \quad \Rightarrow \quad u - v \in W$

(*ii*) $\alpha \in F, u \in W \quad \Rightarrow \quad \alpha u \in W$.

Second condition implies :

Now $\quad u \in W, 1 \in F \quad \Rightarrow \quad u \in W, -1 \in F \quad \Rightarrow \quad (-1)\, u \in W \quad \Rightarrow \quad -u \in W.$

i.e., additive inverse of each element of W exists in W.

Taking $v = u$, the first condition implies.

$$u \in W, u \in W \quad \Rightarrow \quad u - u \in W, \textit{i.e.}, \mathbf{0} \in W.$$

Thus, identity element exists in W.

All other postulates hold good in W as they hold in V.

Hence, W is a subspace of V.

8.12. PROPER AND IMPROPER SUBSPACES

Every vector space V(F) has two subspaces, namely :

(*i*) W = {0} consisting of the single element zero and is called *null space* or *zero space*.

(*ii*) W = V, the vector space itself.

These two subspaces are called *improper subspaces of V*. All other subspaces, if any, are called *proper subspaces of V*.

Example 6. *Let $V = R^3$ be the three dimensional space. Let $W = \{(x, y, z) \mid ax + by + cz = 0 \,;\, x, y, z \in R\}$, a, b, c being fixed real numbers. Show that W is a subspace of V.*

Sol. Let $\quad u = (x_1, y_1, z_1), v = (x_2, y_2, z_2)$ be any two elements of W and $\alpha \in R$.

Now, $\quad \alpha u + v = \alpha(x_1, y_1, z_1) + (x_2, y_2, z_2) = (\alpha x_1, \alpha y_1, \alpha z_1) + (x_2, y_2, z_2)$

$$= (\alpha x_1 + x_2, \alpha y_1 + y_2, \alpha z_1 + z_2) \qquad \ldots(1)$$

Also, $\quad ax_1 + by_1 + cz_1 = 0 \quad$ and $\quad ax_2 + by_2 + cz_2 = 0$

$\Rightarrow \qquad \alpha(ax_1 + by_1 + cz_1) + (ax_2 + by_2 + cz_2) = 0$

$\Rightarrow \qquad a(\alpha x_1 + x_2) + b(\alpha y_1 + y_2) + c(\alpha z_1 + z_2) = 0 \qquad \ldots(2)$

From (1) and (2), it follows that $\alpha u + v \in W$

Hence, W is a subspace of V.

Remark. The above example shows that any plane passing through the origin is a subspace of R^3.

Example 7. *Let V be the vector space of all square matrices of second order over R.*

Let $W = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \Big/ a, b \in R \right\}$ *be the set of all second order diagonal matrices over R. Show that W is a subspace of V.*

Sol. Let $u = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}, v = \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix}$ be any two elements of W and $\alpha \in R$.

Then, $\alpha u + v = \alpha \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} + \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1\alpha & 0 \\ 0 & b_1\alpha \end{bmatrix} + \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix}$

$= \begin{bmatrix} a_1\alpha + a_2 & 0 \\ 0 & b_1\alpha + b_2 \end{bmatrix} \in \text{W}$. $(\because\ a_1\alpha + a_2, b_1\alpha + b_2 \in \text{R})$

Hence, W is a subspace of V.

8.13. SOME MORE EXAMPLES ON SUBSPACES

1. (*i*) $\text{W} = \{(x, 0) \mid x \in \text{R}\}$ is a subspace of $\text{V}_2(\text{R})$.

In fact, W represents x-axis and is a part of the plane.

(*ii*) $\text{W} = \{(0, y) \mid y \in \text{R}\}$ is a subspace of $\text{V}_2(\text{R})$.

2. Let $\text{V} = \text{R}^3$ be the three dimensional space.

Then, (*i*) $\text{W} = \{(0, y, z) \mid y, z \in \text{R}\}$ is a subspace of V.

This in fact represents the plane $x = 0$.

(*ii*) $\text{W} = \{(x, 2x, x) \mid x \in \text{R}\}$ is a subspace of V.

3. The n-square symmetric matrices form a subspace of the space of all n-square matrices over F.

4. The set of all scalar multiples of a given element u_0 of a vector space V(F) is a subspace of V.

Note. *If W is a subspace of V(F) and θ is zero in W and* **0** *is zero in V, then θ and* **0** *coincide.*

(For, $0\theta \in \text{W}$. But $0u = \mathbf{0}$, $\forall\ u \in \text{V}$

So, in particular $0\theta = \mathbf{0}$

Hence $\mathbf{0} \in \text{W}$

$\therefore$ **0** acts as zero in W and hence is zero in W. Thus, θ and **0** coincide).

Example 8. *Show that* $W = \{(a, b, c) \mid a, b, c \in Q\}$ *is not a subspace of* $V_3(R)$.

Sol. Since $\text{Q} \subseteq \text{R}$, W is a subset of $\text{V}_3(\text{R})$.

Now, $u = (1, 2, 3) \in \text{W}$ and $\alpha = \sqrt{3} \in \text{R}$ but

$\alpha u = (\sqrt{3}, 2\sqrt{3}, 3\sqrt{3}) \notin \text{W}$. $(\because\ \sqrt{3} \notin \text{Q})$

$\therefore$ W is not closed under scalar multiplication.

Hence, W is not a subspace of $\text{V}_3(\text{R})$.

Example 9. *If V is the set of all 2 × 2 matrices over R, then prove that (i) the set of all 2 × 2 singular matrices (ii) the set of all matrices A for which* $A^2 = A$, *are not subspaces of V.*

Sol. (*i*) Let W be the set of all 2 × 2 singular matrices.

Now, $\text{A} = \begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix}, \text{B} = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix} \in \text{W}$. $(\because\ |\text{A}| = 0, |\text{B}| = 0)$

But, $\text{A} + \text{B} = \begin{bmatrix} 5 & 0 \\ 0 & 3 \end{bmatrix} \notin \text{W}$ $\left(\because\ \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} = 15 \neq 0\right)$

$\therefore$ W is not a subspace of V.

(*ii*) Let W be the set of all matrices A for which $A^2 = A$.

Then $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in W. \qquad (\because \quad I^2 = I)$$

NOTES

But, $$I + I = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \notin W \qquad \left[\because \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \neq \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}\right]$$

8.14. LINEAR COMBINATION OF VECTORS

For a vector space V(F), if $u, v \in$ V and $a, b \in$ F, then

$$a\ddot{u} + bv \in V.$$

In general, $a_1v_1 + a_2v_2 + \ldots\ldots + a_nv_n \in$ V, for $v_i \in$ V and $a_i \in$ F, ($i = 1, 2, \ldots\ldots, n$). This leads to the following definition :

8.15. DEFINITION

A vector $v \in V$ is said to be a linear combination (L.C.) of the vectors $v_1, v_2, \ldots\ldots, v_n \in V$ if there exist scalars $a_1, a_2, \ldots\ldots, a_n \in F$ such that $v = a_1 v_1 + a_2v_2 + \ldots\ldots + a_nv_n$.

Examples. (*i*) If $v_1 = (1, 1, 1)$, $v_2 = (1, 0, 1)$, $v_3 = (1, 0, 0)$, then the vector $v = (8, 3, 7)$ is a linear combination of the vectors v_1, v_2 and v_3 as is clear from

$$v = 3v_1 + 4v_2 + v_3.$$

(*ii*) Zero vector **0** is always a linear combination of any finite number of vectors $v_1, v_2, \ldots\ldots, v_n$, because

$$\mathbf{0} = 0v_1 + 0v_2 + \ldots\ldots + 0v_n.$$

(*iii*) If $v_1 = (1, 0, 0)$, $v_2 = (0, 1, 0)$, $v_3 = (0, 0, 1)$, then any vector in space v_3 can be expressed as a linear combination of v_1, v_2 and v_3. For instance, the vector $v = (4, 5, 7)$ can be written as

$$v = 4v_1 + 5v_2 + 7v_3$$

v_1, v_2, v_3 are called unit vectors in V_3.

In the space v_n(R), then n vectors $(1, 0, 0, \ldots\ldots 0)$, $(0, 1, 0, \ldots\ldots, 0)$, ..., $(0, 0, \ldots\ldots, 0, 1)$ are unit vectors.

(*iv*) If $v_1 = (1, 0, 0)$, $v_2 = (1, 2, 0)$ and $v = (2, -1, 1)$, then v is not a linear combination of v_1 and v_2 since any linear combination of v_1 and v_2 must have its last component zero.

Example 10. *Write the vector* $v = \begin{bmatrix} 3 & -1 \\ 1 & -2 \end{bmatrix}$ *in the vector space of 2 × 2 matrices as a linear combination of*

$$v_1 = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, v_2 = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, v_3 = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}.$$

Sol. Let $$v = a_1v_1 + a_2v_2 + a_3v_3 \; ; a_1, a_2, a_3 \in R \qquad \ldots(1)$$

$$\Rightarrow \quad \begin{bmatrix} 3 & -1 \\ 1 & -2 \end{bmatrix} = a_1\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} + a_2\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} + a_3\begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + a_2 + a_3 & a_1 + a_2 - a_3 \\ -a_2 & -a_1 \end{bmatrix}$$

NOTES

By definition of equality of two matrices, we have

$$a_1 + a_2 + a_3 = 3,$$
$$a_1 + a_2 - a_3 = -1,$$
$$-a_2 = 1, a_1 = 2.$$

Solving these, we get $a_1 = 2$, $a_2 = -1$, $a_3 = 2$.

Putting these values of a_1, a_2, a_3 in eqn. (1),

$$v = 2v_1 - v_2 + 2v_3.$$

8.16. SPAN OF A SET

The span (or linear span) of a subset S of a vector space V is the set of all finite linear combinations of S.

In other words, if S is a subset of V, the span of S is the set

$\{a_1u_1 + a_2u_2 + \ldots\ldots + a_nu_n \mid a_1, a_2, \ldots\ldots, a_n$ any scalars, n positive integer ; $u_1, u_2, \ldots\ldots, u_n \in$ S$\}$

The span of S is denoted by $<$ S $>$

If S contains only a finite number of elements $u_1, u_2, \ldots\ldots, u_n$ say, then $<$ S $>$ is also written as $< u_1, u_2, \ldots\ldots, u_n >$.

For example, in the vector space V_3, take the set

$$W = \{(1, 0, 0), (0, 1, 0)\}.$$

Any linear combination of a finite number of elements of W is of the form a $(1, 0, 0) + b\ (0, 1, 0) = (a, b, 0)$.

The set of all such linear combinations is $<$ W $>$.

Actually, $<$ W $> = \{(a, b, 0) \mid a, b$ are scalars$\}$. It is a subspace of V_3. In fact, it is true in all cases and prove this assertion in the form of following theorem :

Theorem 4. *The set of all linear combinations of a given non-empty subset of a vector space V(F) is a subspace of V.*

Proof. Let $\{v_1, v_2, \ldots\ldots, v_r\}$ be the given set of vectors $\in$ V(F).

Let W denote the set of all linear combinations of given set of vector

$$W \neq \phi \qquad [\because \quad v_1 = 1.\ v_1 + 0.v_2 + 0.v_3 + \ldots\ldots + 0.v_r \text{ is a linear combination of } v_1, v_2, v_3, \ldots\ldots, v_r \text{ and hence} \in W]$$

Let $\qquad u = a_1v_1 + a_2v_2 + \ldots + a_rv_r$

and $\qquad v = b_1v_1 + b_2v_2 + \ldots + b_rv_r$

be any two linear combinations of the given set of vectors.

Then, $\qquad u + v = (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \ldots\ldots + (a_r + b_r)v_r$

is also a linear combination of the vectors.

Also, $\qquad ku = (ka_1)v_1 + (ka_2)v_2 + \ldots\ldots + (ka_r)v_r$,

where k is some scalar.

Thus, the set W of all linear combinations of the given set of vectors is closed under vector addition and scalar multiplication.

Hence, W is a subspace of V(F).

Remark. It should be noted (proved above in proving $W \neq \phi$) that all the vectors of the spanning or generating set of a sub-space W also belong to W.

8.17. DEFINITION

A space which arises as a set of all linear combinations of any given set of vectors, is said to be generated (or spanned) by the given set of vectors. The given set of vectors is said to be the set of generators of the space.

One can see that a set of vectors $v_1, v_2, \ldots\ldots, v_r$ of a vector space V is a generating set of a subspace W of V if

(*i*) $v_1, v_2, \ldots\ldots, v_r \in W$

(*ii*) $w \in W$ implies there exist scalars $a_1, a_2, \ldots\ldots, a_r$ in F such that

$$w = a_1v_1 + a_2v_2 + \ldots\ldots + a_rv_r$$

A subspace W of V is said to be finitely generated if we can find a generating set for W consisting of finitely many elements.

The space generated by the vectors $v_1, v_2, \ldots\ldots, v_r$ is denoted by $< v_1, v_2, \ldots\ldots, v_r >$.

Note. The space $< v_1, v_2, \ldots\ldots, v_r >$ does not depend on the order of vectors and on how often any vector is repeated in the sequence

For example,

$$< (1, 0), (0, 1), (1, 2) > = < (1, 0), (0, 1) >$$

Examples. (*i*) {(1, 0), (0, 1)} is a generating set of the two dimensional vector space R^2 as any vector (x, y) in R^2 can be written as

$$x(1, 0) + y(0, 1).$$

(*ii*) {(1, 0, 0), (0, 1, 0), (0, 0, 1)} is a generating set of 3-dimensional vector space R^3 because any vector (x, y, z) can be written as

$$x(1, 0, 0) + y(0, 1, 0) + z(0, 0, 1).$$

(*iii*) Let $V = R^3$, $W = \{(x, y, 0) \mid x, y \in R\}$

Then, {(1, 0, 0), (0, 1, 0)} is a generating set for W. Another generating set for W is {(1, 0, 0), (2, 3, 0)}.

(*iv*) The vectors $v_1 = (1, 1, 1)$, $v_2 = (1, 2, 3)$, $v_3 = (1, 3, 2)$ and $v_4 = (3, 2, 1)$ span R^3.

For, any vector (x, y, z) of R^3 can be expressed as

$$(x, y, z) = a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4$$

i.e., $$(x, y, z) = a_1(1, 1, 1) + a_2(1, 2, 3) + a_3(1, 3, 2) + a_4(3, 2, 1)$$

which implies

$$a_1 + a_2 + a_3 + 3a_4 = x$$
$$a_1 + 2a_2 + 3a_3 + 2a_4 = y$$
$$a_1 + 3a_2 + 2a_3 + a_4 = z$$

These equations are consistent as these are three equations in four unknowns.

Hence, the vectors v_1, v_2, v_3, v_4 span R^3.

(v) In $V_2 = R^2$, $(3, 7)$ belongs to $< (1, 2), (0, 1) >$ but does not belong to $< (1, 2), (2, 4) >$.

Sol. $(3, 7)$ belongs to $< (1, 2), (0, 1) >$ if it is a linear combination of $(1, 2)$ and $(0, 1)$, *i.e.*, if

$$(3, 7) = a_1(1, 2) + a_2(0, 1) = (a_1, 2a_1 + a_2)$$

for some suitable $a_1, a_2 \in R$.

This is possible if $a_1 = 3$ and $2a_1 + a_2 = 7$

Solving these equations, we get $a_1 = 3$, $a_2 = 1$

Thus, $(3, 7) = 3(1, 2) + 1(0, 1)$.

Hence, $(3, 7) \in < (1, 2), (0, 1) >$.

Again, if $(3, 7) \in < (1, 2), (2, 4) >$, then

$$(3, 7) = a_1 (1, 2) + a_2(2, 4) = (a_1 + 2a_2, 2a_1 + 4a_2)$$

for some suitable a_1 and a_2.

This implies $a_1 + 2a_2 = 3$, $2a_1 + 4a_2 = 7$.

But, these equations do not have a common solution.

Hence, $(3, 7) \notin < (1, 2), (2, 4) >$.

(vi) In the complex vector space V_2 (C), $(1 + i, 1 - i)$ belongs to $< (1 + i, 1), (1, 1, - i) >$.

Sol. $< (1 + i, 1), (1, 1, - i) >$ is the space of all linear combinations of $(1 + i, 1)$, $(1, (1 - i))$

$$= \{\alpha(1 + i, 1) + \beta(1, (1, - i)) \mid \alpha, \beta \text{ are complex numbers}\}$$
$$= \{(\alpha + \beta + \alpha i, \alpha + \beta - \beta i) \mid \alpha, \beta \text{ are complex numbers}\}.$$

Now, $(1 + i, 1 - i) \in < (1 + i, 1), (1, 1, - i) >$.

if $(1 + i, 1, - i) = (\alpha + \beta + \alpha i, \alpha + \beta - \beta i)$ for some α, β

i.e. if $1 + i = \alpha + \beta + \alpha i$ and $1 - i = \alpha + \beta - \beta i$

i.e. if $1 + i = \alpha(1 + i) + \beta$ and $1 - i = \alpha + \beta (1 - i)$

i.e. if (solving for α, β), $\alpha = 1 + i$, $\beta = 1 - i$

Hence, $(1 + i, 1 - i) \in < (1 + i, 1), (1, 1, - i) >$.

Remark. *A non-null space always contains an infinite number of elements. So, the space generated by a non-empty set S always has an infinite number of elements. But, S itself may be a finite set.*

Example 11. *Show that the set $\{(1, 2, 3), (0, 1, 2), (0, 0, 1)\}$ which is a sub-set of $V_3 = R^3$ generates or spans the entire vector space V.*

Sol. Let $S = \{(1, 2, 3), (0, 1, 2), (0, 0, 1)\}$ be the given set.

Let (a, b, c) be any vector belonging to

$$V_3 = R^3.$$

Consider $(a, b, c) = \alpha(1, 2, 3) + \beta(0, 1, 2) + \gamma (0, 0, 1)$

$$= (\alpha, 2\alpha + \beta, 3\alpha + 2\beta + \gamma)$$

$$\therefore \quad \alpha = a \quad \text{...(1)}$$

$$2\alpha + \beta = b \quad \text{...(2)}$$

$$3\alpha + 2\beta + \gamma = c \quad \text{...(3)}$$

Putting $\alpha = a$ from (1) in (2),

$$2a + \beta = b \text{ or } \beta = b - 2a.$$

Putting values of α and β in Eqn. (3),

$$3a + 2b - 4a + \gamma = c \quad \text{or } \gamma = a - 2b + c$$

$\therefore$ $\exists$ α, β, γ such that

the vector (a, b, c) is a linear combination of vectors (1, 2, 3) (0, 1, 2) and (0, 0, 1).

Therefore $(a, b, c) \in L(S)$

Hence $V_3 \subseteq L(S)$ ...(1)

Of course $L(S) \subseteq V_3$ ...(2)

[Because every linear combination of vectors of S belongs to V_3]

From (1) and (2), we have $V_3 = L(S)$.

Theorem 5. *If S is a non-empty subset of a vector space V, then < S > is the smallest subspace of V containing S.*

Proof. By the above theorem < S > is a subspace.

It contains S because each element u of S can be written as $1u$. *i.e.*, a finite linear combination of S. To show that < S > is the smallest subspace containing S, we shall show that if T is any other subspace containing S, then T contains < S > also.

So, let a subspace T contains S.

Now, any element of < S > is of the form $a_1u_1 + a_2u_2 + \ldots\ldots + a_nu_n$, where a_i's are scalars, u_i's are in S and n is a positive integer. Since $S \subseteq T$ each $u_i \in T$. Since T is a subspace, $a_1u_1 + a_2u_2 + \ldots + a_nu_n \in T$. Thus each element of < S > is in T.

Remark. $< \phi > = \{0\}$.

Cor. *If $v_1, v_2, \ldots, v_r$; $w_1, w_2, \ldots\ldots, w_s$ are vectors in a vector space V such that each w_i is a linear combination of $v_1, v_2, \ldots\ldots, v_r$, then $< w_1, w_2, \ldots\ldots, w_s > \subseteq < v_1, v_2, \ldots\ldots, v_r >$.*

INTERSECTION AND SUM OF VECTOR SPACES

Theorem 6. *The intersection of two subspaces of a vector space V(F) is a subspace of V.*

Proof. Let W_1 and W_2 be two subspaces of V(F).

$W_1 \cap W_2 \neq \phi$ as zero vector of V belongs to both W_1 and W_2.

Let $u, v \in W_1 \cap W_2$ and $a \in F$.

Now, $u, v \in W_1 \cap W_2 \Rightarrow u, v \in W_1$ and $u, v \in W_2$.

$u, v \in W_1 ; a \in F \Rightarrow au + v \in W_1$ [$\because$ W_1 is subspace]

and $u, v \in W_2 ; a \in F \Rightarrow au + v \in W_2$ [$\because$ W_2 is subspace]

$au + v \in W_1, au + v \in W_2 \Rightarrow au + v \in W_1 \cap W_2$.

Thus, $u, v \in W_1 \cap W_2, a \in F \Rightarrow au + v \in W_1 \cap W_2$

Hence, $W_1 \cap W_2$ is a subspace of V(F).

The result can be generalized to any number of subspaces. More precisely, if $W_1, W_2, \ldots\ldots, W_n$ are n -subspaces of V, then their intersection $W_1 \cap W_2 \cap \ldots\ldots \cap W_n$ is also a subspace of V.

Note. The union of two subspaces may not be a subspace.

For example, let $W_1 = x$-axis and $W_2 = y$-axis in $V_2 (= R^2)$. Here, $(1, 0) \in W_1$ and $(0, 1) \in W_2$. So, (1, 0) and (0, 1) belong to $W_1 \cup W_2$. But, $(1, 0) + (0, 1) = (1, 1) \notin W_1 \cup W_2$. Therefore, $W_1 \cup W_2$ is not closed w.r.t. addition. Hence, $W_1 \cup W_2$ is not a subspace of V_2.

However, if one of the subspaces is a subset of the other, then the union of two subspaces is a subspace. This is proved in the following theorem :

Theorem 7. *The Union of two subspaces of a vector space is a subspace of the vector speae if and only if either is contained in the other.*

Proof. Let W_1 and W_2 be two subspaces of V over a field F.

If $W_1 \subseteq W_2$, then $W_1 \cup W_2 = W_2$ and hence $W_1 \cup W_2$ is a subspace.

If $W_2 \subseteq W_1$, then $W_1 \cup W_2 = W_1$ and hence $W_1 \cup W_2$ is a subspace.

Conversely, let $W_1 \cup W_2$ be a subspace.

We shall show that either $W_1 \subseteq W_2$ or $W_2 \subseteq W_1$.

Suppose if possible, neither W_1 is a subset of W_2 nor W_2 is a subset of W_1.

Then, there exists an element $u \in W_1$ but $u \notin W_2$ ...(1)

and there exists an element $v \in W_2$ but $v \notin W_1$ ...(2)

Now, $u \in W_1 \Rightarrow u \in W_1 \cup W_2$

and $v \in W_2 \Rightarrow v \in W_1 \cup W_2$

As $u, v \in W_1 \cup W_2$, therefore, $u + v \in W_1 \cup W_2$

($\because$ $W_1 \cup W_2$ is a vector space)

Now, $u + v \in W_1 \cup W_2 \Rightarrow u + v \in W_1$ or $u + v \in W_2$.

Case (*i*) $u + v \in W_1$

Also, $u \in W_1$

$\therefore$ $(u + v) - u = v \in W_1$, which contradicts (2).

Case (*ii*) $u + v \in W_2$

Also $v \in W_2$

$\therefore$ $(u + v) - v = u \in W_2$, which contradicts (1)

Thus, in both the cases we arrive at a contradiction.

Therefore, our supposition is wrong.

Hence, either $W_1 \subseteq W_2$ or $W_2 \subseteq W_1$.

We have seen that $W_1 \cup W_2$ is not in general a subspace. However, $< W_1 \cup W_2 >$ is the smallest subspace of V containing $W_1 \cup W_2$. Moreover, one can see that $< W_1 \cup W_2 >$ consists of elements of the type $u + v$, $u \in W_1$ and $v \in W_2$.

8.18. LINEAR SUM OF TWO SUBSPACES

Let W_1 and W_2 be two subspaces of the vector space V(F). Then, the linear sum of W_1 and W_2 is denoted by $W_1 + W_2$ and is the set of all possible sums $u + v$ where $u \in W_1$ and $v \in W_2$.

i.e., $$W_1 + W_2 = \{u + v \mid u \in W_1 \text{ and } v \in W_2\}.$$

For Example : Let $$V = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in R \right\}.$$

Then clearly V is a vector space of all 2×2 matrices over R w.r.t. usula vector addition and scalar multiplication defined in matrices.

Let
$$W_1 = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \middle| a, c, d \in \mathrm{R} \right\},$$
$$W_2 = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| a, b \in \mathrm{R} \right\}.$$

Then, one can easily see that W_1, W_2 are two subspaces of V.

$$\therefore \quad W_1 + W_2 = \left\{ \begin{pmatrix} 2a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathrm{R} \right\}$$

Obviously, $\quad W_1 \subseteq W_1 + W_2$

$(\because \; u \in W_1, \mathbf{0} \in W_2 \Rightarrow u + \mathbf{0} = u \in W_1 + W_2, \forall \, u \in W_1)$

Similarly, $\quad W_2 \subseteq W_1 + W_2$.

Hence, $\quad W_1 \cup W_2 \subseteq W_1 + W_2$.

Theorem 8. *Linear sum $W_1 + W_2$ of two subspaces W_1 and W_2 of a vector space V(F) is a subspace of V(F).*

Proof. Let $u, v \in W_1 + W_2$ and a any arbitrary scalar in F.

Then, $\exists \, u_1, v_1 \in W_1$ and $u_2, v_2 \in W_2$ such that

$$u = u_1 + u_2 \text{ and } v = v_1 + v_2.$$

$$\therefore \quad au + v = a(u_1 + u_2) + (v_1 + v_2) = (au_1 + v_1) + (au_2 + v_2)$$

Since $\quad au_1 + v_1 \in W_1$ and $au_2 + v_2 \in W_2$

$(\because \; W_1$ and W_2 are subspaces$)$

$$\therefore \quad (au_1 + v_1) + (au_2 + v_2) \in W_1 + W_2$$
$$\Rightarrow \quad a(u_1 + u_2) + (v_1 + v_2) \in W_1 + W_2$$
$$\Rightarrow \quad au + v \in W_1 + W_2$$

Thus, $u, v \in W_1 + W_2, a \in F \Rightarrow au + v \in W_1 + W_2$.

Hence, $W_1 + W_2$ is a subspace of V.

Remark. One can show that if $W_1, W_2, \ldots, W_n$ are subspaces of V(F), then $W_1 + W_2 + \ldots + W_n$ is also a subspace of V.

Theorem 9. *If W_1 and W_2 are two subspaces of a vector space V(F), then*

$$W_1 + W_2 = < W_1 \cup W_2 >$$

i.e., *linear sum of W_1 and W_2 is the subspace generated by the union of W_1 and W_2.*

Proof. Clearly, $\quad W_1 \subseteq W_1 + W_2$ and $W_2 \subseteq W_1 + W_2$

$$\therefore \quad W_1 \cup W_2 \subseteq W_1 + W_2$$

Since $< W_1 \cup W_2 >$ is the smallest subspace containing $W_1 \cup W_2$, therefore,

$$< W_1 \cup W_2 > \subseteq W_1 + W_2 \qquad \ldots(1)$$

Conversely, let $u + v \in W_1 + W_2$ where $u \in W_1$, $v \in W_2$.

$$\therefore \quad 1.u + 1.v = u + v \in < W_1 \cup W_2 >$$
$$\therefore \quad W_1 + W_2 \subseteq < W_1 \cup W_2 > \qquad \ldots(2)$$

$\therefore$ From (1) and (2),

$$W_1 + W_2 = < W_1 \cup W_2 >.$$

Remarks. *(i) If W_1 and W_2 are two subspaces of V(F) then $W_1 \cap W_2$ is a subspace of V and is the largest subspace contained in W_1 as well as W_2.*

(ii) $W_1 + W_2$ contains W_1 as well as W_2 and is the smallest subspace of V that contains both W_1 and W_2.

(iii) $W_1 + W_1 = W_1$ and if $W_1 \subseteq W_2$ then $W_1 + W_2 = W_2$.

(iv) The operations of forming the sum of subspaces is associative and commutative. If $W_1, W_2, \ldots\ldots, W_n$ are subspaces of V then $W_1 + W_2 + \ldots\ldots + W_n$ is, irrespective of any bracketing that might be inserted and irrespective of the order of the summands, the set of all vectors in V expressible as (a vector in W_1) + (a vector in W_2) + ... + (a vector in W_n).

8.19. DIRECT SUM OF SUBSPACE

Let V be a vector space over a field F. Let $W_1, W_2, \ldots, W_n$ be subspaces of V. Then, each vector in the sum $W_1 + W_2 + \ldots\ldots + W_n$ can be expressed in atleast one way in the form

(a vector in W_1) + (a vector in W_2) + ... + (a vector in W_n). In most of the cases, we can express a vector of $W_1 + W_2 + \ldots\ldots + W_n$ in more than one way. In case we can express **each vector** in $W_1 + W_2 + \ldots\ldots + W_n$ in **exactly one** way as :

(a vector in W_1) + (a vector in W_2) + ... + (a vector in W_n), then we call the sum $W_1 + W_2 + \ldots + W_n$ of subspaces $W_1, W_2, \ldots\ldots, W_n$ as the **direct sum** of subspaces $W_1, W_2, \ldots\ldots, W_n$ and we write it as $W_1 \oplus W_2 \oplus \ldots \oplus W_n$.

For example : *(i)* In R^3 (R), $W_1 = <(1, 0, 0)>$, $W_2 = <(0, 1, 0)>$, $W_3 = <(0, 0, 1)>$ are subspaces of R^3(R). Any vector $(a, b, c) \in R^3$ can be uniquely written as $(a, b, c) = (a, 0, 0) + (0, b, 0) + (0, 0, c)$ where $(a, 0, 0) \in W_1$, $(0, b, 0) \in W_2$, $(0, 0, c) \in W_3$.

Then, $R^3 = W_1 \oplus W_1 \oplus W_3$.

(ii) If V is a finite dimensional vector space and $(e_1, e_2, \ldots\ldots, e_n)$ is a basis of V, then

$$V = <e_1> \oplus <e_2> \oplus \ldots\ldots \oplus <e_n>.$$

The following example, shows the difference between the linear sum and the direct sum of two sub-spaces.

Example. (i) Consider the vector space V_3(R).

Then, $W_1 = \{(a, b, 0) \mid a, b \in R\}$, $W_2 = \{(0, 0, c) \mid c \in R\}$, are subspaces. (Show !).

Now any vector $(a, b, c) \in V_3(R)$ can be written as

$$(a, b, c) = (a, b, 0) + (0, 0, c) \qquad \ldots(1)$$

where, $\qquad (a, b, 0) \in W_1$ and $(0, 0, c) \in W_2$.

Moreover, any vector $(a, b, c) \in V_3(R)$ can be written in form (1) uniquely as the sum of elements of W_1 and W_2.

Hence, $\qquad V_3(R) = W_1 \oplus W_2$.

(ii) Take $\qquad W_1 = \{(a, b, 0) \mid a, b \in R\}$

and $\qquad W_2 = \{(0, b, c) \mid b, c \in R\}$.

Then, W_1 and W_2 are subspaces in V_3(R). (Show !)

Now, any vector $(a, b, c) \in V_3(R)$ can be written as

$$(a, b, c) = \left(a, \frac{b}{2}, 0\right) + \left(0, \frac{b}{2}, c\right) \qquad \ldots(1)$$

$$\left(\text{where}\left(a, \frac{b}{2}, 0\right) \in W_1 \text{ and} \left(0, \frac{b}{2}, c\right) \in W_2\right)$$

NOTES

$$\therefore \qquad V_3(R) = W_1 + W_2$$

Further, any vector $(a, b, c) \in V_3(R)$ can also be written as

$$(a, b, c) = \left(a, \frac{3b}{4}, 0\right) + \left(0, \frac{b}{4}, c\right) \qquad ...(2)$$

$$\left(\text{where}\left(a, \frac{3b}{4}, 0\right) \in W_1 \text{ and} \left(0, \frac{b}{4}, c\right) \in W_2\right)$$

(1) and (2) show that elements of V cannot be uniquely expressed as sum of elements of W_1 and W_2. Hence. $V_3(R)$ is the linear sum of two subspaces W_1 and W_2 but is not direct sum of two subspaces W_1 and W_2.

A simplified criterion for a sum of subspaces to be the direct sum is given in the following theorem.

Theorem 10. *Let W_1, W_2, ..., W_n be n subspaces of V(F). Suppose that the only way to express* **0** *in the form $w_1 + w_2 + ... + w_n$ with $w_i \in W_i$ for each i, is to take every $w_i =$* **0**. *Then the sum $W_1 + W_2 + ... +W_n$ is a direct sum.*

Proof. Let w be an arbitrary vector in $W_1 + W_2 + ... + W_n$.

Let, if possible, w can be written in two different forms :

$$w = u_1 + u_2 + ... + u_n = v_1 + v_2 + ... + v_n \qquad ...(1)$$

where, for each i, $u_i \in W_i$ and $v_i \in W$.

The two expressions for w are identical.

From (1), $\qquad (u_1 - v_1) + (u_2 - v_2) + ... + (u_n - v_n) = \mathbf{0}$

$\Rightarrow \qquad u_1 - v_1 = \mathbf{0}, u_2 - v_2 = \mathbf{0}, ..., u_n - v_n = \mathbf{0}$

(by given hypothesis)

$\Rightarrow \qquad u_i = v_i, \quad \text{for} \quad i = 1, 2, ..., n.$

$\Rightarrow$ The two expressions for w are identical.

Hence, the sum of subspaces is the direct sum.

Following theorem gives a very simple criterion for the sum of two only subspaces to be the direct sum.

Theorem 11. *If W_1 and W_2 are two subspaces of V(F), then $W_1 + W_2$ is a direct sum if and only if $W_1 \cap W_2 = \{$***0***$\}$.*

Proof. (*i*) Let $W_1 + W_2$ be a direct sum.

To show : $\qquad W_1 \cap W_2 = \{\mathbf{0}\}$

Let $\qquad w \in W_1 \cap W_2 \Rightarrow w \in W_1 \quad \text{and} \quad w \in W_2$

Now, $\qquad w \in W_2 \Rightarrow -w \in W_2 \qquad (\therefore \quad W_2 \text{ is a subspace})$

$\therefore \qquad w + (-w) = \mathbf{0}$

Thus, **0** can be expressed as sum of a vector in W_1 and a vector in W_2 in two ways : $\mathbf{0} = w_1 + (-w_1)$ and $\mathbf{0} = \mathbf{0} + \mathbf{0}$.

But $W_1 + W_2$ being the direct sum (given). there is only one way to express **0** as sum of a vector in W_1 and a vector in W_2.

$\therefore$ w (and $-w$) must be $\mathbf{0}$.

Hence, no vector other than $\mathbf{0}$ can belong to $W_1 \cap W_2$. But, $W_1 \cap W_2$ being a subspace of V, contains $\mathbf{0}$.

$\therefore$ $W_1 \cap W_2 = \{\mathbf{0}\}$.

(*ii*) Conversely, let $W_1 \cap W_2 = \{\mathbf{0}\}$.

We further suppose that $\mathbf{0} = w_1 + w_2$ where $w_1 \in W_1$ and $w_2 \in W_2$.

$\therefore$ $w_1 = -w_2$ and hence $w_1 \in W_2$ ($\because$ $w_2 \in W_2$ and W_2 is a subspace)

Therefore, $w_1 \in W_1 \cap W_2$.

$\Rightarrow$ $w_1 = \mathbf{0}$ ($\because$ $W_1 \cap W_2 = \{\mathbf{0}\}$)

Hence, $w_2 (= -w_1) = \mathbf{0}$

This proves that the only way to express $\mathbf{0}$ as the sum of a vector in W_1 and a vector in W_2 is to take both these vectors equal to $\mathbf{0}$.

Hence. $W_1 + W_2$ is a direct sum.

Theorem 12. *Let W_1 and W_2 be two subspaces of a vector space V(F). Then, $V = W_1 \oplus W_2$ if any two of the following conditions hold*

1. *$V = W_1 + W_2$* 2. *$W_1 \cap W_2 = \{0\}$*
3. *dim V = dim W_1 + dim W_2*

Proof. (*i*) Let (1) and (2) hold.

Since $W_1 \cap W_2 = \{\mathbf{0}\}$

$\therefore$ The sum $W_1 + W_2$ is a direct sum.

$\therefore$ From (1), it follows that $V = W_1 \oplus W_2$

(*ii*) Let (1) and (3) hold.

Then, from (3), dim V = dim W_1 + dim W_2

$\Rightarrow$ dim $(W_1 + W_2)$ = dim W_1 + dim W_2 ($\because$ by (1), $V = W_1 + W_2$)

$\Rightarrow$ dim W_1 + dim W_2 − dim $(W_1 \cap W_2)$ = dim W_1 + dim W_2

($\because$ dim $(W_1 + W_2)$ = dim W_1 + dim W_2 − dim $(W_1 \cap W_2)$. To be proved later)

$\Rightarrow$ dim $(W_1 \cap W_2) = 0$ $\Rightarrow$ $W_1 \cap W_2 = \{\mathbf{0}\}$.

$\therefore$ (2) also holds. Hence by part (*i*), $V = W_1 \oplus W_2$.

(*iii*) Let (2) and (3) hold.

Since by (2), $W_1 \cap W_2 = \{\mathbf{0}\}$, therefore $W_1 + W_2$ is a direct sum.

$\therefore$ dim $(W_1 \oplus W_2)$ = dim W_1 + dim W_2 = dim V (By condition (3))

Since $W_1 \oplus W_2$ is a subspace of V, it follows that $V = W_1 \oplus W_2$.

8.20. COMPLEMENTARY SUBSPACES

If $V = W_1 \oplus W_2$, then the two subspaces W_1 and W_2 of the vector space V(F) are said to be complementary subspaces.

Remark 1. *A vector space V is said to be the direct sum of n subspaces $W_1, W_2, \ldots\ldots, W_n$ (of V) iff each element $v \in V$ can be uniquely written as :*

$$v = w_1 + w_2 + \ldots\ldots + w_n \text{ where } w_i \in W_i,\ i = 1, 2, \ldots\ldots, n.$$

We write $V = W_1 \oplus W_2 \oplus \ldots\ldots \oplus W_n$.

Remark 2. *If $(e_1, e_2, \ldots\ldots e_m)$ is a basis of W_1 and $(f_1, f_2, \ldots\ldots f_n)$ is a basis of W_2 then*

(i) $(e_1, e_2, \ldots\ldots e_m, f_1, f_2, \ldots\ldots f_n$ is a basis of $W_1 \oplus W_2$

(ii) dim $(W_1 \oplus W_2)$ = dim W_1 + dim W_2

(iii) The result of (i) and (ii) can be generalized to more than two subspaces.

LINEAR INDEPENDENCE OF VECTORS

NOTES

8.21. DEFINITION

Let V be a vector space over F. Vectors $v_1, v_2, ..., v_n \in V$, are said to be linearly dependent (L.D.) over F if there exist scalars $a_1, a_2, ..., a_n$ in F, not all zero such that

$$a_1v_1 + a_2v_2 + ... + a_nv_n = \mathbf{0}.$$

Here, **0** *on the right hand side indicates the null vector.*

Vectors which are not linearly dependent are called linearly independent (L.I.).

In fact, vectors $v_1, v_2, ..., v_n$ are **linearly independent** if and only if

$$a_1v_1 + a_2v_2 + ... + a_nv_n = \mathbf{0},\ a_i \in \text{F}$$

implies $\qquad a_1 = a_2 = ... = a_n = 0.$

i.e., zero solution is the only solution.

If $S = \{v_1, v_2, ..., v_n\}$, then we say that the set S is L.I. or L.D. according as the vectors $v_1, v_2, ..., v_n$ are L.I. or L.D.

An infinite subset S of V is said to be L.I. if every finite subset of S is L.I.

Remark 1. *A set containing only zero vector is linearly dependent*

Let $\qquad S = \{0\}$

Consider $\qquad a.0 = 0$

This equation is satisfied by $a = 0$ and also by non-zero values to a.

$\therefore$ The set $S = \{0\}$ is a L.D. set.

Remark 2. *A singleton set of a non-zero vector of V(F) is linearly independent.*

Let $S = \{\alpha\}$ where α is a non-zero vector of V(F).

Consider $\qquad a\,\alpha = 0.$

This equation is satisfied only by $a = 0$.

$\therefore$ The set $S = \{\alpha\}$ is linearly independent.

Remark 3. *Now we remind the reader of the few results on consistency and solutions of linear equations.*

We know that matrix form of linear equations is AX = B.

Case I. Matrix B ≠ O, the equations are said to be **Non-Homogeneous.**

If A is non-singular ; then unique solution is $X = A^{-1}B$.

If A is singular and (Adj. A)B ≠ O ; then

no solution *i.e.*, equations are inconsistent

If A is singular and (Adj. A)B = O ; then

Infinitely many solutions.

Case II. Matrix B = O, then equations are said to be homogeneous (AX = O)

If A is non-singular, then only zero solution

If A is singular (*i.e.* | A | = 0) ; then infinitely many solutions. (Here also zero solution is one of the solutions).

One may define : *A set of vectors $\{v_1, v_2, ..., v_n\}$ is L.D. if one of the vectors can be expressed as a L.C. of the others.* Note that if a set of vectors (with $n \geq 2$) is L.D., it may not be true that each of the vectors in the sequence is expressible as a L.C. of the others.

For example, in $\{(1, 0), (0, 1), (0, 2)\}$, $(0, 2)$ is expressible in terms of $(1, 0)$ and $(0, 1)$ but $(1, 0)$ cannot be expressed as a L.C. of $(0, 1)$ and $(0, 2)$.

($\because$ all combinations of $(0, 1)$ and $(0, 2)$ are of the type $(0, \alpha)$)

Moreover, a set containing a repetition is always L.D.

For example, $\{u_1, u_1, u_3, ..., u_n\}$ is L.D.

because $$1.u_1 + (-1)u_1 + 0.u_3 + ... + 0u_n = \mathbf{0}.$$

Example 12. *Show that the set of vectors $\{(1, 2, 0), (0, 3, 1), (-1, 0, 1)\}$ in $V_3(Q)$ is L.I. (where Q is the field of rationals).*

Sol. Suppose $a(1, 2, 0) + b(0, 3, 1) + c(-1, 0, 1) = \mathbf{0} = (0, 0, 0)$ where $a, b, c \in Q$.

$\Rightarrow$ $$(a - c, 2a + 3b, b + c) = (0, 0, 0)$$

$\Rightarrow$ $$a - c = 0, 2a + 3b = 0, b + c = 0$$

From first and last equations

$$a = c, b = -c$$

But $2a + 3b = 2c - 3c \neq 0$ unless $c = 0$

$\therefore$ $a = 0, b = 0, c = 0$ is the only solution.

Hence, the given vectors are L.I.

Or

Matrix form of the above linear homogeneous equations is

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 3 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Now, $$\begin{vmatrix} 1 & 0 & -1 \\ 2 & 3 & 0 \\ 0 & 1 & 1 \end{vmatrix} = 1\,(3 - 0) - 0 - (2 - 0) = 1 \neq 0$$

Hence $a = 0, b = 0, c = 0$ is the only solution.

Hence the given vectors form a L.I. set.

Example 13. *If V is the vector space of all 2×3 matrices over R, show that the matrices*

$$A = \begin{bmatrix} 2 & 1 & -1 \\ 3 & -2 & 4 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 & -3 \\ -2 & 0 & 5 \end{bmatrix},$$

and $$C = \begin{bmatrix} 4 & -1 & 2 \\ 1 & -2 & 3 \end{bmatrix} \text{ form a L.I. set.}$$

Sol. Suppose $aA + bB + cC = O$ where $a, b, c \in R$

$\Rightarrow$ $$a\begin{bmatrix} 2 & 1 & -1 \\ 3 & -2 & 4 \end{bmatrix} + b\begin{bmatrix} 1 & 1 & -3 \\ -2 & 0 & 5 \end{bmatrix} + c\begin{bmatrix} 4 & -1 & 2 \\ 1 & -2 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$\Rightarrow$ $$\begin{bmatrix} 2a + b + 4c & a + b - c & -a - 3b + 2c \\ 3a - 2b + c & -2a - 2c & 4a + 5b + 3c \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\Rightarrow \quad 2a + b + 4c = 0,\ a + b - c = 0,\ -a - 3b + 2c = 0 \qquad \text{...(1)}$$

and
$$3a - 2b + c = 0,\ -2a - 2c = 0,\ 4a + 5b + 3c = 0 \qquad \text{...(2)}$$

NOTES

Solving equations in (1), we get

$$a = b = c = 0$$

which obviously satisfy the 3 equations in (2) also.

Hence, the given matrices form a L.I. set.

Example 14. *If X_1, X_2, ..., X_r is a linearly independent system of $n \times 1$ column vectors and A is an $n \times n$ non-singular matrix, show that AX_1, AX_2, ..., AX_r are linearly independent.*

Sol. Suppose $a_1AX_1 + a_2AX_2 + ... + a_rAX_r = O$ for some scalars $a_1, a_2, ..., a_r$.

$$\Rightarrow \quad A(a_1X_1) + A(a_2X_2) + ... + A(a_rX_r) = O$$

$$\Rightarrow \quad A(a_1X_1 + a_2X_2 + ... + a_rX_r) = O \qquad \text{...(1)}$$

Since A is non-singular, A^{-1} exists.

Pre-multiplying both sides of (1) by A^{-1}, we have

$$A^{-1}A(a_1X_1 + a_2X_2 + ... + a_rX_r) = A^{-1}O$$

$$\Rightarrow \quad (A^{-1}A)(a_1X_1 + a_2X_2 ...... + a_rX_r) = O$$

$$\Rightarrow \quad a_1X_1 + a_2X_2 + ... + a_rX_r = O \qquad (\because \ AA^{-1} = I)$$

$\Rightarrow \quad a_1 = a_2 = ... = a_r = 0$, since $X_1, X_2, ..., X_r$ are linearly independent.

Hence, $AX_1, AX_2, ..., AX_r$ are linearly independent.

Example 15. *Consider the vector space P(x) of all polynomials over the field F and show that the infinite set $S = \{1, x, x^2, x^3, ...\}$ is L.I.*

Sol. Let $S_m = \{x^{n_1}, x^{n_2}, ..., x^{n_m}\}$ be any finite subset of S. Then for scalars a_1, a_2 ......, a_m, consider the linear combination

$$a_1x^{n_1} + a_2x^{n_2} + ... + a_mx^{n_m}$$

By definition of zero polynomial and the equality of two polynomials,

$$a_1x^{n_1} + a_2x^{n_2} + ... + a_mx^{n_m} = 0 \qquad \text{...(1)}$$

iff
$$a_1 = a_2 = ... = a_m = 0$$

where 0 on the right of (1) is a zero polynomial.

Hence, any finite subset of S is L.I.

$\therefore$ S is L.I.

Example 16. *Show that the vectors*

$$u = (1 + i,\ 2i),\ v = (1,\ 1 + i)$$

in $V_2(C)$ are L.D. but in $V_2(R)$ are L.I.

Sol. Two vectors are dependent if one is a multiple of the other.

Thus u and v are dependent if for some number $\alpha + i\beta \in$ C,

$$u = (\alpha + i\beta)v$$

i.e., if $\quad (1 + i, 2i) = (\alpha + i\beta)\,(1, 1 + i) = (\alpha + i\beta, \alpha - \beta + i\,(\alpha + \beta))$

i.e., if $\quad \alpha + i\beta = 1 + i \quad$ and $\quad \alpha - \beta + i\,(\alpha + \beta) = 2i$

i.e., if $\quad \alpha = 1, \beta = 1$

Thus, $u = (1 + i)v$. Hence, u, v are L.D.

(*ii*) If $u, v \in V_2(R)$, then u is not a multiple of v because $1 + i \notin R$. Thus, u, v are L.I.

NOTES

Theorem 13. *Any set which contains the null vector* **0** *is linearly dependent.*

Proof. Let $\{v_1, v_2, ..., v_r\}$ be a set of vectors containing the null vector **0** over V. Let $v_i = \mathbf{0}$.

Then, $0v_1 + 0v_2 + ... + 0v_{i-1} + 1.v_i + 0v_{i+1} + ...+ 0v_r = \mathbf{0}$ is a linear combination of vectors with not all coefficients zero. Hence, the set is linearly dependent.

Theorem 14. *If a vector v is a linear combination of vectors $v_1, v_2, ..., v_r$, then $\{v, v_1, v_2, ..., v_r\}$ is a linearly dependent set.*

Proof. Since v is a linear combination of vectors $v_1, v_2, ..., v_r$

$\therefore$ There exist scalars $a_1, a_2, ... a_r$ such that

$$v = a_1v_1 + a_2v_2 + ... + a_rv_r$$

$$\Rightarrow \qquad (-1)v + a_1v_1 + a_2v_2 + ... + a_rv_r = \mathbf{0}$$

which shows that there is at least one non-zero coefficient (-1).

Hence, the set $\{v, v_1, v_2, ..., v_r\}$ is a linearly dependent set.

Remark. *Coefficients may not be zero in a linear combination.*

Theorem 15. *If $\{v_1, v_2, ..., v_r\}$ is a linearly independent set and $\{v, v_1, v_2, ..., v_r\}$ is a linearly dependent set, then v is a linear combination of the vectors $v_1, v_2, ..., v_r$.*

Proof. Since the set $\{v, v_1, v_2, ..., v_r\}$ is linearly dependent.

$\therefore$ there exist scalars $a, a_1, a_2, ..., a_r$ not all zero, such that

$$av + a_1v_1 + a_2v_2 + ... + a_rv_r = \mathbf{0} \qquad ...(1)$$

Case (*i*) $a \neq 0$

Dividing (1) by a and rewriting, we have

$$v = \left(\frac{-a_1}{a}\right) v_1 + \left(\frac{-a_2}{a}\right) v_2 + ... + \left(\frac{-a_r}{a}\right) v_r$$

$\Rightarrow$ v is a linear combination of vectors $v_1, v_2, ... v_r$

Case (*ii*) $\qquad a = 0$

From (1), $\quad a_1v_1 + a_2v_2 + ... + a_rv_r = \mathbf{0}$

$\Rightarrow$ $a_1 = a_2 = ... = a_r = 0$, since the vectors $v_1, v_2, ..., v_r$ are linearly independent.

This contradicts that the scalars $a, a_1, a_2, ..., a_r$ are not all zero.

Hence, $a \neq 0$ and v is a linear combination of vectors $v_1, v_2, ..., v_r$.

Theorem 16. *The set of non-zero vectors $v_1, v_2, ..., v_r$ from a vector space V is linearly dependent if and only if there exists some vector v_i which is a linear combination of the preceeding vectors $v_1, v_2, ..., v_{i-1}$.*

Proof. Suppose v_i is a linear combination of the preceeding vectors $v_1, v_2, ..., v_{i-1}$.

i.e., $\qquad v_i = a_1v_1 + a_2v_2 + ... + a_{i-1} v_{i-1}$, for scalars $a_1, a_2, ... a_{i-1}$

From this, we have the relation

$$a_1v_1 + a_2v_2 + ... + a_{i-1} v_{i-1} + (-1) v_i + 0 v_{i-1} + ... + 0v_r = \mathbf{0}$$

which has at least one coefficient, namely (-1) non-zero.

$\Rightarrow$ the vectors $v_1, v_2, ..., v_r$ are linearly dependent.

Conversely, let the vectors $v_1, v_2, \ldots\ldots, v_r$ be linearly dependent.

$\therefore$ there exist scalars $a_1, a_2, \ldots\ldots, a_r$ not all zero such that

$$a_1v_1 + a_2v_2 + \ldots + a_rv_r = \mathbf{0} \qquad \ldots(1)$$

NOTES

Let i be the largest subscript for which $a_i \neq 0$ (*i.e.*, $a_{i+1}, a_{i+2}, \ldots\ldots$ are all zero).

Case I. i ≠ 1

Then, (1) can be written as

$$a_1v_1 + a_2v_2 + \ldots\ldots + a_{i-1}v_{i-1} + a_iv_i = \mathbf{0}$$

Since $a_i \neq 0$, we can rewrite it as

$$v_i = \left(\frac{-a_1}{a_i}\right)v_1 + \left(\frac{-a_2}{a_i}\right)v_2 + \ldots\ldots + \left(\frac{-a_{i-1}}{a_i}\right)v_{i-1}$$

$\Rightarrow$ v_i is a linear combination of the preceeding vectors $v_1, v_2, \ldots\ldots, v_{i-1}$.

Case II. When $i = 1$, we have $a_1v_1 = \mathbf{0}$ with $a_1 \neq 0$.

$\therefore$ $v_1 = \mathbf{0}$ which is a contradiction to the given hypothesis that all vectors are not zero.

Remark. *The above theorem provides us a method to decide whether a given set of vectors is linearly dependent or not.* Following example illustrates this.

Example 17. *Show that the vectors (1, 2), (1, 1), (3, 4) and (7, 9) in R^2 are linearly dependent.*

Sol. Clearly $a(1, 2) \neq (1, 1)$ for any scalar a.

Now $\quad a(1, 2) + b(1, 1) = (3, 4)$

$\Rightarrow \quad a + b = 3$ and $2a + b = 4$

Solving, we have $a = 1, b = 2$

$\therefore$ (3, 4) is a linear combination of (1, 2) and (1, 1).

Hence, the given set of vectors is linearly dependent.

Cor. 1. *If the vectors $v_1, v_2, \ldots\ldots, v_r$ generate a subspace W of a vector space V and v_i is a linear combination of the remaining $r - 1$ vectors, then the remaining $r - 1$ vectors $v_1, v_2, \ldots\ldots, v_{i-1}, v_{i+1}, \ldots\ldots, v_r$ also generate the same subspace W.*

To illustrate the corollary, consider three vectors (1, 1), (1, 2), (3, 5) in R^2.

A linear combination of these vectors is

$$a(1, 1) + b(1, 2) + c(3, 5) \qquad \ldots(1)$$

for some scalars a, b, c.

Since $\quad (3, 5) = 1(1, 1) + 2(1, 2)$

$\therefore$ (1) can be rewritten as

$$a(1, 1) + b(1, 2) + c[1(1, 1) + 2(1, 2)] = (a + c)(1, 1) + (b - 2c)(1, 2).$$

$\therefore$ Every linear combination of the 3 vectors (1, 1), (1, 2), (3, 5) can be expressed as a linear combination of 2 vectors (1, 1) and (1, 2).

Hence, the space generated by the 3 given vectors is the same as that generated by the vectors (1, 1) and (1, 2).

NOTES

Cor. 2. *Any finite generating set S of vectors not all zero contains a subset of linearly independent vectors, which also generates the same space.*

For, we can delete from the set S, any vector which is a null vector or which is a linear combination of the vectors proceeding it. The remaining subset will also generate the same space and will be linearly independent.

Theorem 17. *Every subset of a linearly independent set is linearly independent.*

Proof. Let $\{v_1, v_2, ..., v_n\}$ be a linearly independent set.

Let, if possible, $\{v_1, v_2, ..., v_k\}$, $k < n$, be a linearly dependent subset of $\{v_1, v_2, ..., v_n\}$.

Then there exist scalars $a_1, a_2, ..., a_k$, *not all zero,* such that

$$a_1v_1 + a_2v_2 + ... + a_kv_k = \mathbf{0}.$$

$$\Rightarrow \quad a_1v_1 + a_2v_2 + ... + a_kv_k + 0v_{k+1} + ... + 0v_n = \mathbf{0}.$$

and the scalars $a_1, a_2, ..., a_k, 0, ... 0$ are not all zero.

$\Rightarrow$ the vectors $v_1, v_2, ..., v_n$ are linearly dependent. But, this contradicts the given hypothesis that the vectors $v_1, v_2, ..., v_n$ are linearly independent.

Hence, the set $\{v_1, v_2, ..., v_k\}$ is a linearly independent set.

Similarly, any other subset of $\{v_1, v_2, ..., v_n\}$ is linearly independent.

Cor. *Every super set of a linearly dependent set is linearly dependent.*

Proof. Let A be a set of linearly dependent vectors. Let B be a super set of A.

Let, if possible, B be linearly independent. Then, A being a subset of a linearly independent set B, is linearly independent. This contradicts the given hypothesis that A is linearly dependent.

Hence, B is linearly dependent.

Theorem 18. *The non-zero rows in an echlon matrix form a L.I. set.*

Proof. If the echlon matrix is O, then the set of non-zero rows is ϕ and hence L.I.

So, consider the case when there is at least one non-zero row in the echlon matrix. Let its non-zero rows be (in order from the top downwards) $R_1, R_2, ... R_l$.

Suppose $a_1R_1 + a_2R_2 + ... + a_lR_l = O$ for some scalars $a_1, a_2, ..., a_l$.

Each side of this equation is a row matrix. Pick out from each side the entry in the position where R_1 has the leading entry and where therefore, the lower rows $R_2, R_3, ..., R_l$ of the echlon matrix have zeros.

Hence, a_1x (leading entry of R_1) = 0.

$$\Rightarrow \quad a_1 = 0.$$

$$\therefore \quad a_2R_2 + ... + a_lR_l = O.$$

Now, consider the position where R_2 has leading entry (and therefore, $R_3, ..., R_l$ have zeros). Hence, we deduce that $a_2 = 0$. Proceeding like this, we find that

$a_3 = a_4 = ... = a_l = 0$. Thus, all the coefficients $a_1, a_2, ..., a_l$ are zero.

$\therefore$ The set $\{R_1, R_2, ... R_l\}$ is L.I.

BASES AND DIMENSION OF A VECTOR SPACE

NOTES

8.22. BASIS

Definition. *Let V be a vector space. A set of vectors $v_1, v_2, \ldots\ldots, v_n \in V$ is called a basis of V if*

(*i*) the vectors $v_1, v_2, \ldots\ldots, v_n$ are linearly independent

(*ii*) $v_1, v_2, \ldots\ldots, v_n$ span V

(*i.e.* any vector $v \in$ V can be expressed as a linear combination of the vectors $v_1, v_2, \ldots\ldots, v_n$).

The space V is finite dimensional if it has a finite basis. If V is not finite dimensional, it is called infinite dimensional.

The vector space $V_0 = \{\mathbf{0}\}$ is zero dimensional.

Note. *ϕ is taken as basis of $\{\mathbf{0}\}$ since $< \phi > = \{\mathbf{0}\}$ and ϕ is L.I. Note further that $\{\mathbf{0}\}$ is not a basis of $\{\mathbf{0}\}$ since the set $\{\mathbf{0}\}$ is L.D.*

Remark. Basis of a vector space is **not unique** but the number of vectors in a **basis** is unique.

Examples. (*i*) The set of vectors (1, 0, 0), (0, 1, 0) and (0, 0, 1) is a basis for the vector space R^3.

Sol. For, $a\,(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1) = \mathbf{0}$, $a, b, c \in$ R

$\Rightarrow \qquad (a, b, c) = \mathbf{0} = (0, 0, 0)$

$\Rightarrow \qquad a = 0, b = 0, c = 0$

$\Rightarrow$ the vectors (1, 0, 0), (0, 1, 0) and (0, 0, 1) are linearly independent.

Also, any vector (x, y, z) of R^3 can be written as a linear combination of these vectors, namely

$$(x, y, z) = x(1, 0, 0) + y(0, 1, 0) + z(0, 0, 1).$$

Hence, these vectors form a basis.

(*ii*) The set of 3 vectors (1, 1, 1), (1, 2, 3) and (1, 4, 2) is a basis for the vector space R^3.

Sol. First, we show that these vectors are linearly independent.

Now, if for some scalars a, b, c

$$a(1, 1, 1) + b(1, 2, 3) + c(1, 4, 2) = \mathbf{0}$$

then, $\qquad (a + b + c, a + 2b + 4c, a + 3b + 2c) = \mathbf{0} = (0, 0, 0)$

$\Rightarrow \qquad a + b + c = 0$

$$a + 2b + 4c = 0 \quad \text{and} \quad a + 3b + 2c = 0$$

Solving these equations, we find that $a = 0, b = 0, c = 0$.

$\therefore$ the three vectors (1, 1, 1), (1, 2, 3) and (1, 4, 2) are linearly independent.

Secondly, we show that any vector (x, y, z) of R^3 can be expressed as a linear combination of given vectors.

Now, $\qquad (x, y, z) = p(1, 1, 1) + q(1, 2, 3) + r(1, 4, 2) \qquad \ldots(1)$

$\Rightarrow \qquad (x, y, z) = (p + q + r, p + 2q + 4r, p + 3q + 2r)$

NOTES

$$\Rightarrow \qquad p + q + r = x$$

$$p + 2q + 4r = y \quad \text{and} \quad p + 3q + 2r = z$$

Solving these three equations for p, q and r, we find that

$$p = -\tfrac{1}{5}\ (2x + y + 3z),$$

$$q = -\tfrac{1}{5}\ (2x + y + 3z),$$

$$r = -\tfrac{1}{5}\ (x - 2y + z).$$

As, $x, y, z \in \mathrm{R}$; $p, q, r \in \mathrm{R}$.

For these values of p, q, r, we get from (1), (x, y, z) as a linear combination of (1, 1, 1), (1, 2, 3) and (1, 4, 2). Hence, the vectors (1, 1, 1), (1, 2, 3) and (1, 4, 2) form a basis of R^3.

(*iii*) In the vector space R^n, the vectors $e_1 = (1, 0, 0, ..., 0)$, $e_2 = (0, 1, 0, ... 0)$, ..., $e_n = (0, 0, 0, ..., 0, 1)$ form a basis.

Sol. For, if $\qquad a_1e_1 + a_2e_2 + ... + a_ne_n = \mathbf{0}$

then $\qquad a_1 = 0, a_2 = 0, ... a_n = 0$

so the set of vectors $e_1, e_2, ..., e_n$ is linearly independent.

Also, any vector $(x_1, x_2, ..., x_n) \in \mathrm{R}^n$ can be expressed as

$$(x_1, x_2, ..., x_n) = x_1e_1 + x_2e_2 + ... + x_ne_n.$$

The vectors $e_1, e_2, ..., e_n$ are called unit vectors and are said to form the *standard basis* of R^n.

(*iv*) One can see that the set of vectors

$$(1, 0, 0, ..., 0), (1, 1, 0, ..., 0) ..., (1, 1, ..., 1) \text{ is also a basis of } \mathrm{R}^n.$$

(*v*) The vectors $v_1 = (1, 1, 1)$, $v_2 = (1, 2, 3)$ and $v_3 = (3, 2, 1)$ are not a basis of R_3 because $v_3 = 4v_1 - v_2$.

(*vi*) In the vector space $\mathrm{P}_n(\mathrm{R})$ of all polynomials of degree n over the field of reals, the set $\{1, x, x^2, ..., x^n\}$ of polynomials is a basis of $\mathrm{P}_n(\mathrm{R})$.

Sol. Firstly these vectors are L.I.

For, $\quad a_1 \,.\, 1 + a_2x + a_3x^2 + ... + a_nx^n = \mathbf{0}$

[where $a_1, a_2, ..., a_n \in \mathrm{R}$ and $\mathbf{0}$ on right is the zero polynomial].

By definition of zero polynomial and equality of polynomials, we have

$$a_1 = a_2 = ... = a_n = 0.$$

Secondly, if $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ is any polynomial in $\mathrm{P}_n(\mathrm{R})$, then $f(x)$ can be thought of as a linear combination of polynomials $1,\ x,\ x^2, ..., x^n$.

Hence, the set $\{1, x, x^2, ..., x^n\}$ of polynomials is a basis of $\mathrm{P}_n(\mathrm{R})$.

(*vii*) The set $\{1, x, x^2, ..., x^n, x^{n+1}, ...\}$ is a natural basis for the vector space of polynomials of any arbitrary degree over R or C.

(*viii*) The set $\{(1, 0, 0), (1, 1, 0), (1, 1, 1), (0, 1, 0)\}$ of vectors spans $\mathrm{V}_3(\mathrm{R})$ but is not a basis.

Sol. Let (a, b, c) be any vector of $\mathrm{V}_3(\mathrm{R})$.

Let us examine whether we can express it as a linear combination of given vectors or not.

Now, $\qquad (a, b, c) = a_1(1, 0, 0) + a_2(1, 1, 0) + a_3(1, 1, 1) + a_4(0, 1, 0)$

$$= (a_1 + a_2 + a_3, a_2 + a_3 + a_4, a_3)$$

$$\Rightarrow \qquad a_1 + a_2 + a_3 = a,\ a_2 + a_3 + a_4 = b,\ a_3 = c.$$

Solving these equations, we get

$$a_1 = a - a_2 - a_3 = a + a_4 - b,\ a_2 = b - a_3 - a_4 = b - c - a_4,\ a_3 = c.$$

In particular, taking $a_4 = 0$, we find

$$(a, b, c) = (a - b)(1, 0, 0) + (b - c)(1, 1, 0) + c(1, 1, 1) + 0(0, 1, 0).$$

Thus, (a, b, c) has been expressed as a L.C. of the given vectors.

But, the given set is not L.I. because

$$1(1, 0, 0) + (-1)(1, 1, 0) + 0(1, 1, 1) + (0, 1, 0) = (0, 0, 0)$$

Hence, the given set is not a basis.

(*ix*) If V is the vector space of all ordered pairs of complex numbers over the field R, then the set S = {(1, 0), (*i*, 0), (0, 1), (0, *i*)} is a basis of V.

Sol. Firstly, to show that S is L.I.

Now, $a_1(1, 0) + a_2(i, 0) + a_3(0, 1) + a_4(0, i) = \mathbf{0}$

(where $a_1, a_2, a_3, a_4 \in$ R)

$$\Rightarrow \qquad (a_1 + ia_2,\ a_3 + ia_4) = (0, 0)$$

$$\Rightarrow \qquad a_1 + ia_2 = 0,\ a_3 + ia_4 = 0$$

$$\Rightarrow \qquad a_1 = 0 = a_2,\ a_3 = 0 = a_4$$

Hence, S is L.I.

Secondly, to show that S spans V.

Let u be any elt. of V.

$$\therefore \qquad u = (a + ib,\ c + id),\ a, b, c, d \in \text{R}.$$

$$= a(1, 0) + b(i, 0) + c(0, 1) + d(0, i)$$

showing that u is a L.C. of elements of S.

Hence, S is a basis of V.

(*x*) If M_2 is the vector space of all 2 × 2 matrices over R, then the set S = {A_1, A_2, A_3, A_4} where $A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $A_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $A_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ is a basis of M_2.

Sol. (*i*) Any element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of M_2 can be written as :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$\therefore$ S generates M_2

(*ii*) *A_1, A_2, A_3, A_4 are L.I.*

For, $\quad \alpha_1\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \alpha_2\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \alpha_3\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \alpha_4\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$\Rightarrow \qquad \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow \alpha_1 = 0,\ \alpha_2 = 0,\ \alpha_3 = 0,\ \alpha_4 = 0.$$

By a basis of a sub-space W of a vector space V, we mean a basis of W as a vector space under the induced operations.

Remarks. (*i*) The basis of a vector space need not be unique as is clear from the above example.

(*ii*) Every basis of a vector space V is a generating set for V but not conversely, since a generating set need not be linearly independent.

(*iii*) A basis of a vector space is a linearly independent set but a linearly independent set of vectors need not be a basis of V since these linearly independent vectors may not span V.

8.23. COORDINATE VECTOR

If the set $B = \{v_1, v_2, ..., v_n\}$ is a basis of a vector space V(F), then a vector $v \in V$ can be written as

$$v = a_1v_1 + a_2v_2 + ... + a_nv_n.$$

for some scalars $a_1, a_2, ..., a_n$. The coefficients $a_1, a_2, ..., a_n$ in the linear combination of v are called coordinates of v relative to the basis B. The vector $(a_1, a_2, ..., a_n)$ is called the coordinate vector of v relative to the basis B and is denoted by $[v]_B$.

The coordinates of a vector relative to the standard basis are simply called the coordinates of the vector.

It is important to note that the vectors in a basis must be in a particular order and, as a matter of fact, the basis $\{v_1, v_2, ..., v_n\}$ is considered to be different from the basis $\{v_2, v_1, ..., v_n\}$. This is because the coordinates of a vector v in V(F) in terms of these basis are respectively $(a_1, a_2, ..., a_n)$ and $(a_2, a_1, ..., a_n)$ which are obviously different unless $a_1 = a_2$. *Hence, a basis will always imply an ordered basis in the sense we have given.*

Theorem 19. *A set of vectors $v_1, v_2, ..., v_n \in V$ is a basis of V if and only if each element of V can be uniquely expressed as a linear combination of $v_1, v_2, ..., v_n$.*

Proof. (*i*) Let $v_1, v_2, ..., v_n$ be a basis for V. If $v \in$ V, then by the definition of the basis of V, there exist scalars $a_1, a_2, ..., a_n$ such that

$$v = a_1v_1 + a_2v_2 + ... + a_nv_n \qquad ...(1)$$

Let, if possible, $\quad v = b_1v_1 + b_2v_2 + ... + b_nv_n \qquad ...(2)$

be another linear combination of $v_1, v_2, ..., v_n$.

(1)—(2) gives $\quad \mathbf{0} = v - v = (a_1 - b_1)v_1 + (a_2 - b_2)v_2 + ... + (a_n - b_n)v_n$

Since $v_1, v_2, ..., v_n$ are linearly independent, we have

$$a_1 - b_1 = 0,\ a_2 - b_2 = 0,\ ......,\ a_n - b_n = 0$$

i.e., $\quad a_1 = b_1,\ a_2 = b_2,\ ......,\ a_n = b_n.$

Thus, each element v of V can be uniquely expressed as a linear combination of $v_1, v_2, ..., v_n$.

(*ii*) **Conversely,** let each element of V be uniquely expressed as a linear combination of $v_1, v_2, ..., v_n$. This implies, in particular that $v_1, v_2, ..., v_n$ span V.

To show that $v_1, v_2, ..., v_n$ are linearly independent, let

$$a_1v_1 + a_2v_2 + ... + a_nv_n = \mathbf{0}$$

Also, $\quad 0v_1 + 0v_2 + ... + 0v_n = \mathbf{0}$

Thus, the null vector **0** has been written as a linear combination in two ways.

Therefore, our assumption of unique representation implies that

$$a_1 = a_2 = ... = a_n = 0.$$

Hence, $v_1, v_2, ..., v_n$ are linearly independent.

Next theorem shows that if V is a finitely generated vector space, then from a given generating set of V, we can choose subset which forms a basis of V.

Theorem 20. *If $v_1, v_2, \ldots\ldots v_r$ generate a vector space V, then there exists a subset of $v_1, v_2, \ldots\ldots, v_r$ which is a basis of V.*

Proof. If $v_1, v_2, \ldots\ldots, v_r$ are linearly independent, then these already form a basis of V.

If these are linearly dependent, then some v_i is a linear combination of the remaining vectors

$$v_1, v_2, \ldots\ldots, v_{i-1}, v_{i+1}, \ldots\ldots, v_r.$$

Since each v in V is linear combination of $v_1, v_2, \ldots\ldots, v_r$, v_i is a linear combination of $v_1, v_2, \ldots\ldots, v_{i-1}, v_{i+1}, \ldots\ldots, v_r$. Thus, on removing the element v_i from the given set, we still get a generating set for V. If this subset is linearly independent, it is a basis of V, otherwise we repeat the argument. After a finite number of steps, we obtain a subset of $v_1, v_2, \ldots\ldots, v_r$ which is linearly independent and is a generating set for V and hence is a basis of V.

Theorem 21. *If $v_1, v_2, \ldots\ldots, v_n$ is a generating set of a vector space V, then any $n + 1$ vectors in V are linearly dependent.*

Or

If $v_1, v_2, \ldots\ldots v_n$ form a basis in V then any $n + 1$ vectors in V are linearly dependent.

Proof. Without any loss of generality, we suppose that the vectors $v_1, v_2, \ldots\ldots, v_n$, are L.I. because otherwise, we can find a subset of $v_1, v_2, \ldots\ldots, v_n$, which is L.I. and generate V.

Let $w_1, w_2, \ldots\ldots, w_{n+1}$ be any $n + 1$ vectors in V.

Since $v_1, v_2, \ldots\ldots, v_n$ generate V, we have

$$w_1 = a_{11}v_1 + a_{12}v_2 + \ldots\ldots + a_{1n}v_n$$
$$w_2 = a_{21}v_1 + a_{22}v_2 + \ldots\ldots + a_{2n}v_n$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$w_{n+1} = a_{n+1,1}v_1 + a_{n+1,2}v_2 + \ldots\ldots + a_{n+1,n}v_n$$

for some scalars a_{ij}.

To show that $w_1, w_2, \ldots\ldots, w_{n+1}$ are linearly dependent, we have to show that there exists scalars $c_1, c_2, \ldots\ldots, c_{n+1}$, not all zero such that

$$c_1w_1 + c_2w_2 + \ldots\ldots + c_{n+1}w_{n+1} = \mathbf{0} \qquad \ldots(1)$$

i.e.,
$$\sum_{i=1}^{n+1} c_iw_i = \mathbf{0}$$

i.e.,
$$\sum_{i=1}^{n+1} c_i\left(\sum_{j=1}^{n} a_{ij}v_j\right) = \mathbf{0}$$

i.e.,
$$\sum_{j=1}^{n}\left(\sum_{i=1}^{n+1} a_{ij}c_j\right)v_j = \mathbf{0}$$

This is so if
$$\sum_{i=1}^{n+1} a_{ij}c_i = 0,\ 1 \le j \le n \qquad (\because v_i \text{ are L.I.}) \qquad \ldots(2)$$

Now, (2) is a system of n homogeneous equations in $n + 1$ unknowns c_i and hence has a non-trivial solution, *i.e.*, there exist $c_1, c_2, \ldots\ldots, c_{n+1}$ not all zero such that (2) and hence (1) is true.

Hence, $w_1, w_2, \ldots\ldots, w_{n+1}$ are linearly dependent.

Cor. *If V is a finitely generated vector space, then the maximum number of linearly independent elements in V is finite.*

Proof. If V has a generating set of n elements, then any set of linearly independent vectors in V has at the most n elements.

The following theorem shows that every finitely generated vector space has a basis.

Theorem 22. (*Existence Theorem*) : *If V is a finitely generated vector space, then any maximal set of linearly independent vectors in V is a basis of V.*

Proof. Consider sets of linearly independent vectors in V. By the above corollary, the number of elements in any such set is bounded by a fixed number. Among these, choose the one with maximum number of elements. Let $\{v_1, v_2, \ldots\ldots, v_n\}$ be such a set. We shall show that $\{v_1, v_2, \ldots\ldots, v_n\}$ is a basis of V.

By our choice, $v_1, v_2, \ldots\ldots, v_n$ are linearly independent. Let $v \in$ V be any element, then by the maximality of $v_1, v_2, \ldots\ldots, v_n$, the set consisting of $v_1, v_2, \ldots\ldots, v_n$ and v is a linearly dependent set.

Therefore, it follows that v is a linear combination of $v_1, v_2, \ldots\ldots v_n$. Hence, $v_1, v_2, \ldots\ldots, v_n$ is a basis of V.

Theorem 23. (*Invariance of the Number of Elements in a Basis*) : *If V is a finitely generated vector space, then any two basis of V have the same number of elements.*

Proof. Let $v_1, v_2, \ldots\ldots, v_r$ and $w_1, w_2, \ldots\ldots, w_s$ be two bases of V.

Suppose $s < r$. Then $v_1, v_2, \ldots\ldots, v_r$ are linearly dependent (Theorem 44), a contradiction.

$\therefore$ $\qquad s \nless r.$

Similarly, $\qquad r \nless s.$

Hence, $\qquad r = s.$

8.24. DIMENSION OF A VECTOR SPACE

Definition. *The number of vectors in a basis of a finitely generated vector space is called the dimension of the vector space V and is denoted by dim V.*

The dimension of a null vector space V *i.e.*, V = {0} is defined to be **zero**.

Dimension of a non-zero vector space is a natural number greater than or equal to 1.

If dim V is n, then we say that V is an n-dimensional vector space. **The dimensions of the spaces R, R^2 and R^n are 1, 2 and n respectively.** That is why we call R^n an n-dimensional vector space. The dimension of the vector space of polynomials of degree $\leq n$ is $n + 1$ because $1, x, x^2, \ldots\ldots, x^n$ is a basis of the vector space.

Vector space of all polynomials with coefficients in F is an infinite dimensional vector space.

A vector space of dimension r consisting of n-vectors is generally denoted by $V_n^r(F)$. When $r = n$, we denote by $V_n(F)$ for $V_n^r(F)$.

Remark. *Since we can choose a basis of a vector space V from a given generating set, dimension of V is less than or equal to the number of elements in any generating set. Further, since any maximal set of linearly independent elements of V forms a basis of V, we see that any linearly independent set has at the most n elements if dim V is n.*

Theorem 24. (*Extension Theorem*) : *If V is a finitely generated vector space, then any set of linearly independent vectors $v_1, v_2, ..., v_r$ in V, can be extended to a basis of V.*

Proof. Let V(F) be a finitely generated vector space over F.

$\therefore$ V has finite dimension n (say).

Let $B = \{u_1, u_2, ..., u_n\}$ be a basis of V.

Let $A = \{v_1, v_2, ..., v_m\}$ be any L.I. set of vectors in V.

We shall show that A can be extended to form a basis for V.

Write $$B_1 = A \cup B = \{v_1, v_2, ..., v_m, u_1, u_2, ..., u_n)$$

Since $B_1 \supseteq B$, and B_1, is a basis.

$\therefore$ B_1 is L.D.

$\Rightarrow$ There exists a vector in B_1, which is a linear combination of the preceding vectors and that vector cannot be any one of the v_i's ($\because$ A is L.I.). Therefore, that must be one of the u_i's. Let that u_i be u_k. Then u_k is a linear combination of $v_1, v_2, ..., v_m, u_1, u_2, ..., u_{k-1}$.

After removing u_k from the set B_1, we denote the remaining set by B_2.

$$\therefore \quad B_2 = \{v_1, v_2, ..., v_m, u_1, u_2, ..., u_{k-1}, u_{k+1}, ..., u_n\}$$

and B_2 spans V.

($\because$ If $u \in V$, can be expressed as a linear combination of elements of B_1 and in this linear combination, u_k can be written as a linear combination of $v_1, v_2, ..., v_m, u_1, u_2, ..., u_{k-1}$, so u can be written as a linear combination of $v_1, v_2, ..., v_m, u_1, u_2, ..., u_{k-1}\ u_{k+1}, ..., u_n$).

If B_2 is L.I., then B_2 is a basis of V.

If B_2 is L.D., then we repeat the same procedure as we have done for B_1 to get a new set. We continue this process till we get a set B′ containing vectors $v_1, v_2, ..., v_m$ such that B′ is L.I. and spans V.

Thus, B′ is an extended set of A and is a basis of V. Thus, any linearly independent set in V can be extended to form a basis of V.

Example 18. *Find the basis for R^3, which contains the vectors (1, 2, 3) and (2, 1, 0).*

Sol. The set of vectors (1, 0, 0), (0, 1, 0) and (0, 0, 1) is a standard basis of R^3.

Consider the linearly dependent set of vectors (1, 2, 3), (2, 1, 0), (1, 0, 0), (0, 1, 0) and (0, 0, 1).

We start from left.

{(1, 2, 3)} being a singleton set of non-zero vector is L.I.

First two vectors (1, 2, 3) and (2, 1, 0) are linearly independent because neither vector is a multiple of the other.

NOTES

So, consider the first 3 vectors. The relation

$$a(1, 2, 3) + b(2, 1, 0) + c(1, 0, 0) = \mathbf{0}$$

implies $$a + 2b + c = 0$$

$$2a + b = 0 \quad \text{and} \quad 3a = 0$$

Matrix form of these homogeneous equations is

$$\begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ 3 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Since $$\begin{vmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ 3 & 0 & 0 \end{vmatrix} = 3\,(0 - 1) = -3 \neq 0$$

The given equations have only null solution.

$\therefore$ $$a = 0,\ b = 0,\ c = 0 \text{ is the only solution.}$$

Therefore, the vectors (1, 2, 3), (2, 1, 0) and (1, 0, 0) are linearly independent and hence form a basis of R^3.

Example 19. *Find a largest linearly independent set of vectors contained in the set {(– 1, 0, 1), (– 1, 1, 2), (1, 2, 0), (3, 1, 2), (1, 1, 4)} as a subset of R^3.*

Sol. Let $$S = \{(-1, 0, 1), (-1, 1, 2), (1, 2, 0), (3, 1, 2)\ (1, 1, 4)\}.$$

We start from left to right.

{(– 1, 0, 1)} being a singleton set of non-zero vector is L.I.

Since (– 1, 1, 2) ≠ a (– 1, 0, 1) for any scalar a.

$\therefore$ (– 1, 0, 1) and (– 1, 1, 2) are linearly independent.

Now, $$a(-1, 0, 1) + b(-1, 1, 2) + c(1, 2, 0) = \mathbf{0}$$

$\Rightarrow$ $$-a - b + c = 0$$

$$b + 2c = 0 \quad \text{and} \quad a + 2b = 0$$

Solving these, we have

$$a = 0,\ b = 0,\ c = 0.$$

$\therefore$ The vectors (– 1, 0, 1), (– 1, 1, 2) and (1, 2, 0) are linearly independent.

We know that (By Art. 44) every set of $(n + 1)$ or more vectors of an n-dimensional vector space is L.D.

Also we know that dimension of R^3 is 3.

$\therefore$ Every set of **four** vectors and **five** vectors of R^3 is **L.D.**

Hence, the largest linearly independent subset of **S** is

$$\{(-1, 0, 1), (-1, 1, 2), (1, 2, 0)\}.$$

Remark 1. A largest linearly independent subset may not be unique. For instance, in the above example, one can verify that the set {(– 1, 0, 1), (– 1, 1, 2), (3, 1, 2)} is another largest linearly independent subset of S.

Theorem 25. *The sequence of non-zero rows in an echlon matrix E is a basis of the row space of E and of every matrix equivalent to E.*

Proof. If E = O, then the set of non-zero rows of E is ϕ and the result is true because the only matrix row equivalent to E is O whose row space is {**0**}. If E ≠ O, then the set of non-zero rows in E spans the row space of E and this set is L.I. Hence, this set is a basis of the row space of E and therefore, of the row space of every matrix row equivalent to E.

This theorem provides a very efficient method for dealing with numerical problems but, it must be kept in mind that this method usually produces a basis which is not a subset of the given spanning set as is clear from the following example :

Example 20. *Find a basis of the subspace of R^4 spanned by the set*

{(1, 0, 1, 2), (2, 3, 0, 1), (– 1, 1, 1, – 2), (1, 5, 3, – 1)}. Find its basis and dimension.

Sol. Consider the given vectors as row matrices.

∴ The subspace W spanned by the given vectors is the row space of the matrix

$$A = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \\ -1 & 1 & 1 & -2 \\ 1 & 5 & 3 & -1 \end{bmatrix}.$$

Reduce A to echelon matrix E (where leading entry in a row may not be 1) given by

$$E = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 8 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ (Verify !)}$$

Then, the set of non-zero rows of E is a basis of W. So, the basis is {(1, 0, 1, 2), (0, 1, 2, 0), (0, 0, 8, 3)}. Hence dimension is 4.

Example 21. *Extend {(1, 2, 3, 4), (0, 0, 5, 6)} to a basis for R^4.*

Sol. Consider the given vectors as row matrices.

Write down an echelon matrix whose rows include the given vectors, namely,

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 5 & 6 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

(Leading entry in a row in echelon form may not be 1)

The rows of this matrix written in any order form a L.I. set of 4-vectors and since dim (R^4) = 4.

∴ This is a basis of R^4 and is an extension of the given L.I. set.

Theorem 26. *If W is a sub-space of a finite dimensional vector space V, then dim W ≤ dim V. Equality holds only when W = V.*

Proof. Let B = {v_1, v_2, ..., v_n} be a basis for V.

Then, B generates V and has n elements.

Any set of L.I. vectors in V and therefore, any set of L.I. vectors in W, cannot have more than n vectors. Hence, dim W ≤ dim V.

When dim W = dim V, a basis for W, is a set of n L.I. vectors of V, whose dimension is also n. So, B is also a basis for V. This means V = < B > = W.

Theorem 27. *If W_1 and W_2 are two sub-spaces of a finite dimensional vector space V, then dim ($W_1 + W_2$) = dim W_1 + dim W_2 – dim ($W_1 \cap W_2$).*

Proof. Let dim $W_1 = m$, dim $W_2 = p$, dim ($W_1 \cap W_2$) = r, and dim V = n.

Then, $m \leq n, p \leq n, r \leq n.$

Let $\{v_1, v_2, ..., v_r\}$ be a basis for $W_1 \cap W_2$.

This is a L.I. set in $W_1 \cap W_2$ and therefore, in W_1 as well as W_2. So, it can be extended to a basis for W_1, say

NOTES

$$\{v_1, v_2, ..., v_r, u_{r+1}, ..., u_m\} \quad ...(1)$$

and to a basis for W_2, say

$$\{v_1, v_2, ..., v_r, w_{r+1}, ... w_p\} \quad ...(2)$$

We shall show that the set

$$A = \{v_1, v_2, ..., v_r\, u_{r+1}, u_{r+2}, ..., u_m; w_{r+1}, ..., w_p\}$$

is a basis for $W_1 + W_2$.

To show that A is a basis for $W_1 + W_2$, we shall show (*i*) A is L.I. in $W_1 + W_2$ (*ii*) $< A > = W_1 + W_2$.

To prove (*i*), let us assume that

$$\sum_{i=1}^{r} a_i v_i + \sum_{i=r+1}^{m} b_i u_i + \sum_{i=r+1}^{p} c_i w_i = 0 \quad ...(3)$$

$$\Rightarrow \quad \sum_{i=1}^{r} a_i v_i + \sum_{i=r+1}^{m} b_i u_i = - \sum_{i=r+1}^{p} c_i w_i \quad ...(4)$$

$$= v \text{ (say).}$$

The vector $v \in W_1$ as L.H.S. is in W_1.

v is also in W_2, since R.H.S. of (4) is in W_2.

Thus, $v \in W_1 \cap W_2$.

Therefore, v can be expressed uniquely in terms of $v_1, v_2, ..., v_r$

($\because$ $\{v_1, v_2, ..., v_r\}$ is a basis for $W_1 \cap W_2$)

$$\therefore \quad v = \sum_{i-1}^{r} d_i v_i \text{ for suitable } d_i\text{'s} \quad ...(5)$$

Hence, from (4), $$\sum_{i=1}^{r} d_i v_i + \sum_{i=r+1}^{p} c_i w_i = 0 \quad ...(6)$$

But $\{v_1, v_2, ..., v_r, w_{r+1}, ... w_p\}$ is L.I.

So, each d_i's and c_i's is zero.

Putting $c_{r+1} = c_{r+2} = ... = c_p = 0$ in (4), we have

$$\sum_{i=1}^{r} a_i v_i + \sum_{i=r+1}^{m} b_i u_i = 0 \quad ...(7)$$

But $\{v_1, v_2, ..., v_r, u_{r+1}, ..., u_m\}$ is L.I.

So, each of a_i's and b_i's is zero.

$\therefore$ equation (3) implies that each scalar involved is zero. Hence, A is L.I.

To prove (*ii*), let $w \in W_1 + W_2$ be any element.

Then, $w = u + v$ where $u \in W_1$ and $v \in W_2$.

$$\therefore \qquad w = \sum_{i=1}^{r} a_i v_i + \sum_{i=r+1}^{m} b_i u_i + \sum_{i=1}^{r} a_i' v_i + \sum_{i=r+1}^{p} b_i' w_i \qquad ...(8)$$

for suitable scalars a_i's, b_i's, a_i''s, b_i''s.

From (8), we find that $w \in \langle A \rangle$.

Hence, $\quad W_1 + W_2 \subseteq \langle A \rangle$.

Since $\quad A \subseteq W_1 + W_2$

$\therefore \quad \langle A \rangle \subseteq W_1 + W_2$

Hence, $\quad W_1 + W_2 = \langle A \rangle$.

Now, dim $(W_1 + W_2)$ is the number of elements in A

$$= r + (m - r) + (p - r) = m + p - r$$

$$= \dim W_1 + \dim W_2 - \dim (W_1 \cap W_2).$$

This completes the proof.

Cor 1. *If a finite dimensional vector space $V(F)$ is the direct sum of its sub-spaces W_1 and W_2 then $\dim V = \dim W_1 + \dim W_2$.*

[For. Let $\quad V = W_1 \oplus W_2$

$\Rightarrow \quad V = W_1 + W_2 \quad$ and $\quad W_1 \cap W_2 = \{0\}$

Now $\quad \dim V = \dim (W_1 + W_2)$

$$= \dim W_1 + \dim W_2 - \dim (W_1 \cap W_2)$$

$$= \dim W_1 + \dim W_2 - 0$$

$$= \dim W_1 + \dim W_2 \qquad (\because \quad W_1 \cap W_2 = \{0\})$$

Example 22. *In $R^3(R)$, let W_1 and W_2 be the sub-spaces generated by $\{(1, 0, -1), (2, 1, 3)\}$ and $\{(-1, 2, 2), (2, 2, -1), (2, -1, 2), (3, 0, 3)\}$ respectively. Find the dimensions of W_1, W_2, $W_1 \cap W_2$ and $W_1 + W_2$.*

Sol. Since the set $\{(1, 0, -1), (2, 1, 3)\}$ generates W_1 and it has only two elements, so that $\dim W_1 \leq 2$.

Since $\quad (1, 0, -1) \neq \alpha(2, 1, 3)$ for any $\alpha \in R$

$\therefore$ The given set $\{(1, 0, -1), (2, 1, 3)\}$ is L.I. and hence is a basis of W_1.

$\therefore \quad \dim W_1 = 2.$

Since W_2 is a sub-space of $R^3(R)$.

$\therefore \quad \dim W_2 \leq \dim R^3(R) = 3.$

Since the set $\{(-1, 2, 2), (2, 2, -1), (2, -1, 2), (3, 0, -3)\}$ generates W_2, the maximum L.I. subset of it is a basis of W_2.

Now, $\{(2, 2, -1), (2, -1, 2), (3, 0, -3)\}$ is a L.I. set (verify !) and is a maximal L.I. set also.

$\therefore \quad \dim W_2 = 3.$

Since $\quad \dim W_2 = \dim R^3(R).$

$\therefore \quad W_2 = R^3.$

Now, $\quad W_1 \cap W_2 = W_1 \cap R^3 = W_1.$

$\therefore \quad \dim W_1 \cap R^3 = \dim W_1 = 2.$

$\therefore \quad \dim (W_1 + W_2) = \dim W_1 + \dim W_2 - \dim (W_1 \cap W_2) = 3 + 2 - 2 = 3.$

NOTES

8.25. IDENTICAL SPACES

Definition. *Two vector spaces V_1 and V_2 (of the same dimension) are called identical spaces if and only if every vector of V_1 is a vector of V_2 and conversely, i.e.,* if and only if each is a subspace of the other.

Example 23. *Show that the vector space spanned by the vectors $v_1 = (1, 2, 1)$, $v_2 = (1, 2, 3)$ and $v_3 = (3, 6, 5)$ and the vector space spanned by the vector $w_1 = (0, 0, 1)$ and $w_2 = (1, 2, 5)$ are identical.*

Sol. Since $(1, 2, 3) \neq a(1, 2, 1)$ for any real number a.

$\therefore$ v_1 and v_2 are linearly independent.

But, $\qquad v_3 = 2v_1 + v_2.$

$\therefore$ The space spanned by v_1, v_2, v_3 is the same as that of v_1 and v_2.

$\therefore$ The vectors v_1, v_2, v_3 span a space V_1 (say) of dimension two.

Since $(0, 0, 1) \neq t(1, 2, 5)$ for any real number t.

$\therefore$ The vectors w_1 and w_2 are linearly independent and span a space V_2 (say) of dimension two.

Next, we see that $\qquad w_1 = \frac{1}{2}v_2 - \frac{1}{2}v_1$

and $\qquad w_2 = 2v_2 - v_1$

and $\qquad v_1 = w_2 - 4w_1$

$\qquad v_2 = w_2 - 2w_1.$

Now, any vector $aw_1 + bw_2$ of V_2 is a vector

$$(\tfrac{1}{2}a + 2b)v_2 - (\tfrac{1}{2}a + b)\, v_1 \text{ of } V_1$$

and any vector $cv_1 + dv_2$ of V_1 is a vector

$$(c + d)w_2 - (4c + 2d)w_1 \text{ of } V_2.$$

Hence the spaces V_1 and V_2 are identical.

Example 24. *If $v_1 = (1, 2, 1)$, $v_2 = (3, 1, 5)$ and $v_3 = (3, -4, 7)$ are vectors in R^3, prove that the subspaces spanned by $S = \{v_1, v_2\}$ and $T = \{v_1, v_2, v_3\}$ are same.*

Sol. Let $\qquad W_1 = L(S) \quad \text{and} \quad W_2 = L(T)$

To show : $\qquad W_1 = W_2$

Now, $\qquad S \subseteq T \Rightarrow L(S) \subseteq L(T) \Rightarrow W_1 \subseteq W_2 \qquad ...(1)$

Let $\qquad v_3 = av_1 + bv_2\,;\ a, b \in R.$

$\Rightarrow \qquad (3, -4, 7) = a(1, 2, 1) + b(3, 1, 5) = (a + 3b, 2a + b, a + 5b)$

$\Rightarrow \qquad a + 3b = 3,\ 2a + b = -4,\ a + 5b = 7$

Solving we get, $\qquad a = -3,\ b = 2$

$\therefore \qquad v_3 = -3v_1 + 2v_2 \qquad ...(2)$

Let $\qquad v \in W_2 = L(T)$

$\therefore \qquad v = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3,\ \alpha_i \in R$

$$= \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3(-3v_1 + 2v_2) \qquad \text{[By (2)]}$$
$$= (\alpha_1 - 3\alpha_3)v_1 + (\alpha_2 + 2\alpha_3)v_2$$

$\Rightarrow$ $v \in W_1 = L(S)$

NOTES

Hence $W_2 \subseteq W_1$ ...(3)

$\therefore$ from (1) and (2), $W_1 = W_2$.

QUOTIENT SPACE

8.26. COSETS

Let W be a subspace of a vector space V(F). For any element $v \in V$, the subset of V defined by

$\{v + w \mid w \in W\}$ is called the left coset of W generated by v and is denoted by $v + W$.

Similarly, the subset of V defined by

$\{w + v \mid w \in W\}$ is called the right coset of W generated by v and is denoted by $W + v$.

As the vector space V(F) is commutative w.r.t. addition '+',

$$v + w = w + v, \ \forall \ v \in V \text{ and } w \in W$$

so that $v + W = W + v$; *i.e.*, the right cosets of W become identical with the left cosets of W. Hereafter, each is called a coset of W in V generated by v.

If $v \in W$, then $v + w \in W$ for each $w \in W$ ($\because$ W is a sub-space.)

$\therefore$ $v + W = \{v + w \mid w \in W\} = \{u \mid u \in W\} = W$ (where $v + w = u$).

Hence W itself is a coset generated by any one element of W.

In particular, $W = \mathbf{0} + W$, where $\mathbf{0}$ is the additive identity in V.

Thus, all cosets of W with the elements of V which are also elements of W are identical with the coset W and cosets by the elements of V which are not elements of W are different.

Theorem 28. *If W is a sub-space of a vector space V(F) and $u, v \in V$, then $u + W = v + W$ iff $u - v \in W$.*

Proof. (*i*) Let $u + W = v + W$.

By definition of equality of two sets, it means that if $u + w_1 \in u + W$, then there must be some element $v + w_2$ in $v + W$ such that

$$u + w_1 = v + w_2, \text{ where } w_1, w_2 \in W$$

$$\Rightarrow \quad u - v = w_2 - w_1$$

As $w_1, w_2 \in W$ and W is a sub-space, $w_2 - w_1 \in W$.

Hence, $u - v \in W$.

(*ii*) Conversely, let $u - v \in W$ for $u, v \in V$.

Now, for $w_1 \in W$,

$$u + w_1 = \mathbf{0} + u + w_1 = v - v + u + w_1$$

$= v + (u - v) + w_1 = v + w_2$ where $w_2 = (u - v) + w_1 \in W$

$(\because u - v \in W$ and $w_1 \in W \Rightarrow (u - v) + w_1 \in W)$

NOTES

$\therefore \qquad u + w_1 = v + w_2$ for $w_2 \in W$

$\Rightarrow \qquad u + w_1 \in v + W$

$\Rightarrow \qquad u + W \subseteq v + W.$

Similarly, $\qquad v + W \subseteq u + W.$

Hence, $\qquad \mathbf{u + W = v + W.}$

Let us now consider the set $\{u + W \mid u \in V\}$ of all cosets of a sub-space W in a vector space V(F). This set is denoted by V/W. In this set of cosets, we define addition (+) and scalar multiplication (.) as follows :

$$(u + W) + (v + W) = (u + v) + W, \text{ for } u, v \in V$$

and $\qquad \alpha.(u + W) = \alpha.u + W, \quad \forall\, \alpha \in F, u \in V.$

(which we just write $\alpha(u + W) = \alpha u + W$).

Note that in $(u + W) + (v + W)$, '+' is some sort of addition of two sets, while in $u + W$, '+' is another type of addition and in $(u + v) + W$, '+' in $u + v$ is the vector addition of elements of V. Similar is the case with scalar multiplication ' . '.

In the following theorem, we shall prove that the set of cosets V/W is a vector space w.r.t. the addition and scalar compositions defined above.

Theorem 29. *If W is a subspace of a vector space V(F), then the set V/W $= \{u + W / u \in V\}$ of all cosets of W in V is a vector space over F w.r.t. addition and scalar compositions defined by :*

$$(u + W) + (v + W) = (u + v) + W, u, v \in V$$

and $\qquad \alpha(u + W) = \alpha u + W, \forall\, \alpha \in F, u \in V.$

Proof. For $u, v \in V$, $u + v \in V$ and $\alpha u \in V$, and hence $(u + v) + W$ and $\alpha u + W$ are certainly in V/W.

First of all, it is necessary to show that the two compositions are well defined, *i.e.*, they are independent of the particular representative chosen to denote a coset.

To show that addition is well defined, *i.e.*, show that if $u + W = u' + W$ for $u, u' \in V$ and $v + W = v' + W$ for $v, v' \in V$, then

$$(u + v) + W = (u' + v') + W.$$

Now, $\qquad u + W = u' + W \;\Rightarrow\; u - u' \in W$

and $\qquad v + W = v' + W \;\Rightarrow\; v - v' \in W.$

Since W is a subspace, therefore,

$$u - u' \in W \quad \text{and} \quad v - v' \in W$$

$\Rightarrow \quad (u - u') + (v - v') \in W \qquad (\because$ W is a sub-space)

$\Rightarrow \quad (u + v) - (u' + v') \in W$

$\Rightarrow \quad (u + v) + W = (u' + v') + W \qquad$ (By the Theorem 54)

$\Rightarrow \quad (u + W) + (v + W) = (u' + W) + (v' + W)$

showing that addition is well defined.

To show that scalar multiplication is well defined

Now, $\qquad u + W = u' + W \;\Rightarrow\; u - u' \in W \qquad$ (By Theorem 54)

$\Rightarrow \qquad \alpha(u - u') \in W$ for $\alpha \in F \qquad (\because$ W is a sub-space)

$$\Rightarrow \quad au - au' \in W$$
$$\Rightarrow \quad au + W = au' + W$$

Hence, $u + W = u' + W$ and $a \in F \Rightarrow au + W = au' + W$

NOTES

showing that scalar multiplication is well defined.

Now to show that V/W is a vector space, we have to verify the axioms for a vector space as below :

Addition satisfies the following properties :

1. Associativity. For $u, v, w \in V$,

$$\begin{aligned}[(u+W)+(v+W)]+(w+W) &= [(u+v)+W]+(w+W) && \text{(By def. of addition)}\\ &= (u+v+w)+W && \text{(By def. of addition)}\\ &= (u+W)+[(v+w)+W] && \text{(By def. of addition)}\\ &= (u+W)+[(v+W)+(w+W)] && \text{(By def. of addition)}\end{aligned}$$

$\therefore$ Addition is associative.

2. Commutativity. For $u, v \in V$,

$$\begin{aligned}(u+W)+(v+W) &= (u+v)+W && \text{(By def. of addition)}\\ &= (v+u)+W && (\because \text{ V is commutative})\\ &= (v+W)+(u+W) && \text{(By def. of addition)}\end{aligned}$$

$\therefore$ addition is commutative.

3. Existence of additive identity

$\mathbf{0} + W \in V/W$ for $\mathbf{0} \in V$ such that for

$u + W \in V/W$, $(\mathbf{0} + W) + (u + W) = (\mathbf{0} + u) + W = u + W$

($\mathbf{0}$ being additive identity in V)

Hence, $\mathbf{0} + W(= W)$ is the additive identity in V/W.

4. Existence of inverse. For each $u + W \in V/W$.

$\exists\ (-u) + W \in V/W$ such that

$$\begin{aligned}(u+W)+((-u)+W) &= u+(-u)+W = \mathbf{0}+W && (\because \ u+(-u)=\mathbf{0} \text{ in V})\\ &= W.\end{aligned}$$

Thus, $-u + W$ is the additive inverse of $u + W$.

Scalar multiplication satisfies the following properties :

Let $u + W, v + W \in V/W$ and $a, b \in F$. Then,

(i) $$\begin{aligned}a[(u+W)+(v+W)] = a[(u+v)+W] &= a(u+v)+W\\ &= (au+av)+W\\ &= (au+W)+(av+W)\\ &= a(u+W)+a(v+W)\end{aligned}$$

(ii) $$\begin{aligned}(a+b)(u+W) &= (a+b)u+W = (au+bu)+W\\ &= (au+W)+(bu+W) = a(u+W)+b(u+W)\end{aligned}$$

(iii) $$\begin{aligned}ab(u+W) &= (ab)u+W\\ &= a(bu)+W = a(bu+W) = a[b(u+W)].\end{aligned}$$

(iv) $$1.(u+W) = (1.u)+W = u+W.$$

Hence, V/W is a vector space over F.

8.27. QUOTIENT SPACE

The vector space V/W formed of all cosets in V(F) of a sub-space W and defined above, is called the quotient space of V w.r.t. W.

NOTES

DIMENSION OF A QUOTIENT SPACE

Theorem 30. *If W is an m-dimensional sub-space of an n-dimensional vector space V(F), then dimension of the quotient space V/W is n-m.*

i.e. $\quad dim\ (V/W) = dim\ V - dim\ W.$

Proof. Let the set $\ B = \{u_1, u_2, ..., u_m\} \subseteq V$

be a basis of W, where $m \le n$. Then B can be extended to a basis of V. Let the set

$$B_1 = \{u_1, u_2, ..., u_m, u_{m+1}, ..., u_n\}$$

be a basis of V.

Consider the set S of all cosets of W by vectors u_{m+1} , $u_{m+2}, ..., u_n \in V$ (but not in W).

i.e., $$S = \{u_{m+1} + W, u_{m+2} + W, ..., u_n + W\} \subseteq V/W.$$

We claim that. S is a basis for V/W.

To prove it, firstly, we show that S is L.I.

Let $\ a_{m+1}, a_{m+2}, ..., a_n \in$ F such that

$$\sum_{i=m+1}^{n} a_i(u_i + W) = \hat{0}$$ (where $\hat{0}$ is the additive identity in V/W and is infact W).

$\Rightarrow \quad a_{m+1}\ (u_{m+1} + W) + a_{m+2}\ (u_{m+2} + W) + ... + a_n\ (u_n + W) = W$

$\Rightarrow \quad (a_{m+1}\ u_{m+1} + W) + (a_{m+2}\ u_{m+2} + W) + ... + (a_nu_n + W) = W$

(By scalar multiplication composition in V/W)

$\Rightarrow \quad (a_{m+1}\ u_{m+1} + a_{m+2}\ u_{m+2} + ... + a_nu_n) + W = W$

$\Rightarrow \quad (a_{m+1}\ u_{m+1} + a_{m+2}\ u_{m+2} + ... + a_nu_n \in W$

$\Rightarrow$ $(a_{m+1}\ u_{m+1} + a_{m+2}\ u_{m+2} + ... + a_nu_n$ can be expressed as a linear combination of elements of B $\quad (\because \quad$ B is a basis of W)

$\Rightarrow \quad (a_{m+1}\ u_{m+1} + a_{m+2}\ u_{m+2} + ... + a_nu_n$
$= b_1u_1 + b_2u_2 + ... + b_mu_m$ for some b_i's $\in$ F.

$$\Rightarrow \quad \sum_{i=m+1}^{n} a_iu_i + \sum_{i=1}^{m} (-b_i)\ u_i = 0.$$

$\Rightarrow \quad a_{m+1} = 0, a_{m+2} = 0, ..., a_n = 0$ and $b_1 = 0, b_2 = 0, ..., b_m = 0$

$(\because \quad B_1$ is a basis of V)

$\Rightarrow \quad$ S is L.I.

Secondly, to show that V/W = L(S).

Consider any element $u + W$(for $u \in V$) of V/W.

Then, $$u + W = \left(\sum_{i=1}^{n} a_i u_i\right) + W \qquad (\because \ B_1 \text{ is a basis of } V)$$

$$= \left(\sum_{i=1}^{m} a_i u_i\right) + \left(\sum_{i=m+1}^{n} a_i u_i\right) + W = \sum_{i=m+1}^{n} a_i u_i + W$$

$$\left[\because \ \sum_{i=1}^{m} a_i u_i \text{ being the linear combination of elements of the basic set B of W, is in W.}\right]$$

$$= \sum_{i=m+1}^{n} a_i (u_i + W),$$

which is a linear combination of elements of S.

$\therefore$ $u + W \in L(S)$.

Hence, $V/W \subseteq L(S)$.

Also, $L(S) \subseteq V/W$.

Hence, $V/W = L(S)$.

Therefore, S is a basis of V/W.

$\therefore$ dim (V/W) is the number of elements in S.

i.e., dim (V/W) = $n - m$ = dim V – dim W.

Example 25. *If W is a sub-space of $V = V_3(R)$ generated by {(1, 0, 0), (1, 1, 0)}, find V/W and its basis.*

Sol. Clearly (1, 0, 0) and (1, 1, 0) are L.I. and therefore, form a basis of W.

This basis can be extended to a basis for V.

One can check that (1, 0, 0), (1, 1, 0) and (0, 0, 1) are L.I. and hence form a basis of V.

$$\therefore \quad V/W = \{u + W \mid u \in V\}$$
$$= \{a(0, 0, 1) + W \mid a \in F\}$$
$$(\because \quad (1, 0, 0) \text{ and } (1, 1, 0) \text{ are in W})$$

One of its basis is {(0, 0, 1) + W}.

SUMMARY

- A non-empty set F containing at least two elements and with two binary operations, denoted additively (+) and multiplicatively (.), is called a field
- A subset S (containing more than one element) of a field F is called a subfield of F if S is a field w.r.t. the addition and multiplication in F.
- The necessary and sufficient condition for a non-empty subset W of a vector space V (F) to be a sub-space of V is that W is closed w.r.t. vector addition and scalar multiplication in V.
- A vector $v \in V$ is said to be a linear combination (L.C.) of the vectors $v_1, v_2, \ldots\ldots v_n \in V$ if there exist scalars $a_1, a_2, \ldots\ldots, a_n \in F$ such that $v = a_1 v_1 + a_2 v_2 + \ldots\ldots + a_n v_n$.

- The span (or linear span) of a subset S of a vector space V is the set of all finite linear combinations of S.
- A space which arises as a set of all linear combinations of any given set of vectors, is said to be generated (or spanned) by the given set of vectors. The given set of vectors is said to be the set of generators of the space.
- Vectors which are not linearly dependent are called linearly independent (L.I.)
- The non-zero rows in an echlon matrix form a L.I. set.
- The number of vectors in a basis of a finitely generated vector space is called the dimension of the vector space V and is denoted by dim V.
- Two vector spaces V_1 and V_2 (of the same dimension) are called identical spaces if and only if every vector of V_1 is a vector of V_2 and conversely, *i.e.*, if and only if each is a subspace of the other.

REVIEW QUESTIONS

1. (*a*) Define a vector space and give one example of a vector space over the field of reals.

   (*b*) Define vector space and show that the set C of all complex numbers is a vector space over the set R of all reals w.r.t. usual addition and scalar multiplication.

2. Prove that R is a vector space over the field Q of rationals where vector addition is defined by

   $u + v = u + v, \forall u, v \in R$ and scalar multiplication is defined by :

   $a. u = au$ where $a \in Q, u \in R$.

3. Let R^+ be the set of all positive real numbers. Define the operations of addition and scalar multiplication as follows :

   $$u + v = u. v, \forall u, v \in R^+$$

   $$au = u^a, \ \forall u \in R^+ \text{ and } a \in R.$$

   Show that R^+ is a real vector space (*i.e.*, vector space over R).

4. Prove that the set of all diagonal matrices of same order over R, is a vector space w.r.t. matrix addition and scalar multiplication.

5. Show that the set of all matrices of the form $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$ where $x, y \in C$, is a vector space over C w.r.t. matrix addition and scalar multiplication.

6. Show that

   (*i*) C is a vector space over C (*ii*) C is a vector space over R

   (*iii*) R is not a vector space over C (*iv*) Q is not a vector space over R

   under usual operations of addition and scalar multiplication.

7. Show that the set $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$ is a vector space over Q w.r.t. the compositions :

   $$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c + (b + d)\sqrt{2})$$

   and $$\alpha(a + b\sqrt{2}) = a\alpha + b\alpha\sqrt{2}$$

   where a, b, c, d and α are all rational numbers.

8. Show that $W = \{(x, y) \mid ax + by = 0, x, y \in R\}$ where a, b are fixed real numbers, is a subspace of R^2.

9. Show that $W = \left\{\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \middle| x \in R\right\}$ is a subspace of the vector space V, of all 2 × 2 real matrices.

10. Write the vector $\alpha = (1, -2, 5)$ as a linear combination of vectors $\alpha_1 = (1, 1, 1)$, $\alpha_2 = (1, 2, 3)$ and $\alpha_3 = (2, -1, 1)$ in the vector space $V_3(R)$.

11. Express the matrix $\begin{bmatrix} 2 & 0 \\ 4 & -5 \end{bmatrix}$ as a linear combination of the matrices

$$A = \begin{bmatrix} 0 & -3 \\ 2 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix} \text{ and } C = \begin{bmatrix} 2 & 3 \\ 0 & 5 \end{bmatrix}.$$

12. For what value of k will the vector $\alpha = (1, k, 5)$ in $V_3(R)$ is a linear combination of vectors $\beta = (1, -3, 2)$ and $\gamma = (2, -1, 1)$.

13. Can the polynomial $3x^2 - 5x + 7$ be expressed as a linear combination of the polynomials $2x^2 + 7x - 3$ and $x^2 + 3x - 5$?

14. Show that in R^3, the subspace

$W = \{(0, y, z) \mid y, z \in R\}$ is generated by

(*i*) (0, 2, – 1) and (0, 1, 2) (*ii*) (0, 2, 3) and (0, 3, 5).

15. If $v_1 = (2, -1, 0)$, $v_2 = (1, 2, 1)$ and $v_3 = (0, 2, -1)$, show that v_1, v_2, v_3 are linearly independent. Express the vectors (3, 2, 1), (1, 1, 1) as a linear combination of v_1, v_2, v_3.

16. Show that the vectors $v_1 = (2, 3, -1, -1)$, $v_2 = (1, -1, -2, -4)$, $v_3 = (3, 1, 3, -2)$, $v_4 = (6, 3, 0, -7)$ form a linearly dependent set. Also, express one of them as a linear combination of the others.

17. In the vector space of polynomials of degrees ≤ 4, which of the following sets are linearly independent ?

(*i*) $x + 1, x^3 - x + 1, x^3 + 2x + 1$ (*ii*) $x^3 + 1, x^3 - 1, x, x^4 - x$

(*iii*) $1 + x, x + x^2, x^2 + x^3, x^3 + x^4, x^4 - 1$.

18. Show that the three row vectors as well as the three column vectors of the matrix

$$\begin{bmatrix} 2 & 3 & 1 \\ 7 & -6 & 17 \\ 5 & 2 & 7 \end{bmatrix}$$

are linearly dependent.

19. Find the relation on a, b, c such that the matrix $\begin{bmatrix} a & -b \\ b & c \end{bmatrix}$ is a linear combination of

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}; \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}.$$

20. A set of vectors is linearly dependent. Show that at least one member of the set is a linear combination of the remaining ones.

21. Let u, v, w be elements of a vector space V(F) and $a, b \in F$.

Show that u, v, w are L.D. iff $u + av + bw, v, w$ are L.D.

22. Show that the 4 vectors

(1, 0, 0), (0, 1, 0), (0, 0, 1) and (1, 1, 1) in $V_3(C)$ are L.D. but any three of them are L.I.

23. Find a if the vectors $\begin{bmatrix} 1 \\ -1 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ -3 \end{bmatrix}, \begin{bmatrix} a \\ 0 \\ 1 \end{bmatrix}$ are linearly dependent.

24. Test for L.I. of vectors

(0, 1, 0, 1, 1) ; (1, 0, 1, 0, 1) ; (0, 1, 0, 1, 1) ; (1, 1, 1, 1, 1) over $V_5(Q)$.

25. Show that the following sets of vectors constitute a basis of R^3.

(*i*) (4, 3, 2) (2, 1, 0), (– 1, 1, – 1) (*ii*) (– 1, 1, 0) (0, 3, – 3), (2, 0, 1)

(*iii*) (2, – 1, 0), (3, 5, 1), (1, 1, 2).

26. Show that the following sets of vectors are basis for R^4.

(*i*) (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)

(*ii*) (1, 0, 0, 0), (1, 2, 0, 0), (1, 2, 3, 0), (1, 2, 0, 4).

27. Determine a basis of the sub-space spanned by the vectors

(– 3, 1, 2), (0, 1, 3), (2, 1, 0), (1, 1, 1).

28. Extend the following sets of vectors to form a basis of R^3:

(*i*) (0, 1, 2), (2, – 1, 4) (*ii*) (1, 2, 3), (2, – 2, 0).

29. Extend the set {(3, – 1, 2)} to two different basis for $V_3(R)$.

30. (*a*) Show that in R^n, any $n + 1$ vectors are linearly dependent. Hence, deduce that if v_1, v_2, ..., v_n in R^n are linearly independent, then every v in R^n is a linearly combination of v_1, v_2, ..., v_n.

(*b*) If V is a n-dimensional vector space, then prove that every set of $(n + 1)$ vectors in V is linearly dependent.

[**Hint.** It is Art. 50]

31. Show that any set v_1, v_2, ..., v_r of linearly independent vectors in R^n can be extended to a basis of R^n.

32. Show that the subspace generated by (0, 0, 1) and (1, 1, 1) is of dim 2.

33. If W is the subspace of the vector space $V = V_2(R)$ generated by (1, 2), find then the quotient space V/W and its basis.

34. If W is a subspace of the vector space $V = V_3(R)$ generated by {(1, 0, 0), (0, 0, 1)}, find the quotient space V/W and its basis.

35. If V is the vector space of all 2 × 2 matrices over R and

$$W = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} a, b, c \in R \right\}$$

Then find a basis of V/W.