# CONTENTS

# SYLLABUS

# DISCRETE MATHEMATICS

## BLOCK 1: ALGEBRAIC STRUCTURES

### Unit 1: Fundamental Concepts & Vectors

Groups, Rings, Fields, Spaces – linear, Dependence of Vector, Linear transformation, Bilinear forms, Eigen values and eigen vectors.

## BLOCK 2: GRAPH THEORY

### Unit 1: Fundamental Concepts, Algorithms & Applications

Basic terminologies of graph theory, Multigraphs and weighted graphs, Paths and circuits, Planar graphs, Trees and rooted trees, Spanning trees and cut sets, Colouring covering and portioning, Directed graphs, enumeration of graphs, Ideas on graphs theoretic algorithm and applications.

NOTES

# Block–1
# Algebraic Structures

## UNIT 1

# FUNDAMENTAL CONCEPTS AND VECTORS

**STRUCTURE**

NOTES

## 1.1. OBJECTIVES

After going through this unit, you will be able to discuss about various algebraic structures like groups, rings and field. Apart from this, you will be able to understand the concept of vector spaces, linear transformations and bilinear transformations.

## 1.2. INTRODUCTION

In the present units, we introduce the concept of algebraic system, binary operations and groups. The study of cyclic groups, normal groups, group homomorphism etc., help us in understanding various applications of computer science. Groups play an important role in coding theory. This unit also includes the concept of rings, integral domain, field and vector spaces.

We shall acquaint ourselves with the notion of a linear transformation (or linear function or mapping) and its various properties. The significance of linear transformations arises form the fact that we can pass from one vector space to another by means of linear transformations. Linear transformations are classified into (*i*) one-one or injective, (*ii*) onto or surjective and (*iii*) both one-one and onto or bijective. We shall also deal with isomorphism of vector spaces.

## 1.3. ALGEBRAIC STRUCTURES

If there exists a system such that it consists of a non-empty set and one or more operations on that set, then that system is called an algebraic system. It is generally denoted by (A, $op_1$, $op_2$, ..., $op_n$), where A is a non-empty set and $op_1$, $op_2$, ..., $op_n$ are operations on A.

An algebraic system is also called an **algebraic structure** because the operations on the set A define a structure on the elements of A.

## 1.4. BINARY OPERATIONS

Consider a non-empty set A and a function $f$ such that $f : A \times A \to A$ is called a binary operation on A. If $*$ is a binary operation on A, then it may be written as $a * b$.

A binary operation can be denoted by any of the symbols $+, -, *, \oplus, \Delta, \square, \vee, \wedge$ etc.

The value of the binary operation is denoted by placing the operator between the two operands.

*e.g.*, (*i*) The operation of addition is a binary operation on the set of natural numbers.

(*ii*) The operation of subtraction is a binary operation on set of integers. But, the operation of subtraction is not a binary operation on the set of natural numbers because the subtraction of two natural numbers may or may not be a natural number.

NOTES

(*iii*) The operation of multiplication is a binary operation on the set of natural numbers, set of integers and set of complex numbers.

(*iv*) The operation of set union is a binary operation on the set of subsets of a universal set. Similarly, the operation of set intersection is a binary operation on the set of subsets of a universal set.

**Tables of Operation**

Consider a non-empty finite set A = $\{a_1, a_2, a_3, ..., a_n\}$. A binary operation * on A can be described by means of table as shown in Fig. 1.

| * | $a_1$ | $a_2$ | $a_3$ | | $a_n$ |
|---|---|---|---|---|---|
| $a_1$ | $a_1*a_1$ | $a_1*a_2$ | | | |
| $a_2$ | $a_2*a_1$ | $a_2*a_2$ | | | |
| $a_3$ | | | $a_3*a_3$ | | |
| | | | | | |
| $a_n$ | | | | | $a_n*a_n$ |

**Fig. 1**

The empty in the *j*th row and *k*th column represent the element $a_j*a_k$.

**ILLUSTRATIVE EXAMPLES**

**Example 1.** *Consider the set A = {1, 2, 3} and a binary operation * on the set A defined by*

$$a * b = 2a + 2b.$$

*Represent operation * as a table on A.*

**Sol.** The table of the operation is shown in Fig. 2.

| * | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 4 | 6 | 8 |
| 2 | 6 | 8 | 10 |
| 3 | 8 | 10 | 12 |

**Fig. 2**

**Properties of Binary Operations**

There are many properties of the binary operations which are as follows :

**1. Closure Property.** Consider a non-empty set A and a binary operation * on A. Then A is closed under the operation *, if $a * b \in$ A, where $a$ and $b$ are elements of A.

*For example,* the operation of addition on the set of integers is a closed operation. *i.e.*, if $a, b \in$ Z, then $a + b \in$ Z $\forall\, a, b \in$ Z.

**Example 2.** *Consider the set A = {1, 3, 5, 7, 9, ...}, the set of odd +ve integers. Determine whether A is closed under (i) addition (ii) multiplication.*

**Sol.** (*i*) The set A is not closed under addition because the addition of two odd numbers produces an even number which does not belong to A.

(*ii*) The set A is closed under the operation multiplication because the multiplication of two odd numbers produces an odd number. So, for every $a, b \in A$, we have $a * b \in A$.

NOTES

**2. Associative Property.** Consider a non-empty set A and a binary operation * on A. Then the operation * on A is associative, if for every $a, b, c, \in A$, we have $(a * b) * c = a * (b * c)$.

**Example 3.** *Consider the binary operation * on Q, the set of rational numbers, defined by*

$$a * b = a + b - ab \ \forall \ a, b \in Q.$$

*Determine whether * is associative.*

**Sol.** Let us assume some elements $a, b, c \in Q$, then by definition

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c$$
$$= a + b - ab + c - ca - bc + abc = a + b + c - ab - ac - bc + abc.$$

Similarly, we have

$$a * (b * c) = a + b + c - ab - ac - bc + abc$$

Therefore, $(a * b) * c = a * (b * c)$.

Hence * is associative.

**3. Commutative Property.** Consider a non-empty set A and a binary operation * on A. Then the operation * on A is commutative, if for every $a, b \in A$, we have $a * b = b * a$.

**Example 4.** *Consider the binary operation * on Q, the set of rational numbers, defined by*

$$a * b = a^2 + b^2 \ \forall \ a, b \in Q.$$

*Determine whether * is commutative.*

**Sol.** Let us assume some elements $a, b \in Q$, then by definition

$$a * b = a^2 + b^2 = b^2 + a^2 = b * a$$

Hence * is commutative.

**Example 5.** *Consider the binary operation * and Q, the set of rational numbers defined by*

$$a * b = \frac{ab}{2} \quad \forall \ a, b \in Q.$$

*Determine whether * is (i) associative (ii) commutative.*

**Sol.** (*i*) Let $a, b \in Q$, then we have

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

Hence * is commutative.

(*ii*) Let $a, b, c \in Q$, then by definition we have

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\frac{ab}{2} . c}{2} = \frac{abc}{4}$$

Similarly, $$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{\frac{abc}{2}}{2} = \frac{abc}{4}$$

Therefore, $a * (b * c) = a * (b * c)$

Hence, * is associative.

**4. Identity.** Consider a non-empty set A and a binary operation * on A. Then the operation * has an identity property if there exists an element, $e$, in A such that

$$a * e \text{ (right identity)} = e * a \text{(left identity)} = a \ \forall \ a \in A.$$

**Theorem 1.** *Prove that $e_1' = e_1''$ where $e_1'$ is a right identity and $e_1''$ is a left identity of a binary operation.*

**Proof.** We know that $e_1''$ is a right identity.

Hence, $e_1'' * e_1' = e_1''$ ...(1)

Also, we know that $e_1''$ is a left identity.

Hence, $e_1'' * e_1' = e_1'$ ...(2)

From (1) and (2), we have $e_1' = e_1''$.

Thus, we can say that if $e$ is a right identity of a binary operation, then $e$ is also a left identity.

## 1.5. SEMI-GROUP

Let us consider, an algebraic system (A, *), where * is a binary operation on A. Then, the system (A, *) is said to be a semi-group if it satisfies the following properties :

1. The operation * is a closed operation on set A.
2. The operation * is an associative operation.

**Example 6.** *Consider an algebraic system (A, *), where A = {1, 3, 5, 7, 9, ...}, the set of all positive odd integers and * is a binary operation means multiplication. Determine whether (A, *) is a semi-group.*

**Sol. Closure property.** The operation * is a closed operation because multiplication of two +ve odd integers is a +ve odd number.

**Associative property.** The operation * is an associative operation on set A. Since for every $a, b, c \in$ A, we have

$$(a * b) * c = a * (b * c)$$

Hence, the algebraic system (A, *) is a semi-group.

**Example 7.** *Let (A, *) be semi-group. Show that for a, b, c in A, if $a * c = c * a$ and $b * c = c * b$, then $(a * b) * c = c * (a * b)$.*

**Sol.** Take L.H.S., we have

$$\begin{aligned}(a * b) * c &= a * (b * c) && [\because \ * \text{ is associative}]\\ &= a * (c * b) && [\because \ b * c = c * b]\\ &= (a * c) * b && [\because \ * \text{ is associative}]\\ &= (c * a) * b && [\because \ a * c = c * a]\\ &= c * (a * b) && [\because \ * \text{ is associative}]\end{aligned}$$

Hence, $(a * b) * c = c * (a * b)$.

NOTES

## EXERCISE 1

1. Let $*$ be the operation on the set R of real numbers defined by $a * b = a + b + 2ab$
   (*a*) Find $2 * 3$, $3 * (-5)$, $7 * (1/2)$
   (*b*) Is (R, $*$) a semi-group ? Is it commutative ?
   (*c*) Find the identity element
   (*d*) Which elements have inverses and what are they ?
2. Let S be a semi-group with identity $e$ and let $b$ and $b'$ be inverses of $a$. Show that $b = b'$ *i.e.*, inverses are uniques, if they exist.
3. Let S = Q × Q, the set of ordered pairs of rational numbers, with the operation $*$ defined by
   $(a, b) * (x, y) = (ax, ay + b)$
   (*a*) Find $(3, 4) * (1, 2)$ and $(-1, 3) * (5, 2)$
   (*b*) Is S a semi-group ? Is it commutative ?
   (*c*) Find the identity element of S
   (*d*) Which elements, if any, have inverses and what are they ?
4. Let A be a non-empty set with the operation $*$ defined by $a * b = a$ and assume A has more than one element. Then
   (*a*) Is A a semi-groups ?
   (*b*) Is A commutative ?
   (*c*) Does A have an identity element ?
   (*d*) Which elements, if any have inverses and what are they ?

## 1.6. GROUP

Let us consider an algebraic system (G, $*$), where $*$ is a binary operation on G. Then the system (G, $*$) is said to be a group if it satisfies following properties.

(*i*) The operation $*$ is a closed operation.

(*ii*) The operation $*$ is an associative operation.

(*iii*) There exists an identity element w.r.t. the operation $*$.

(*iv*) For every $a \in$ G, there exists an element $a^{-1} \in$ G such that $a^{-1} * a = a * a^{-1} = e$

*For example*, the algebraic system (I, +), where I is the set of all integers and + is an addition operation, is a group. The element 0 is the identity element w.r.t. the operation +. The inverse of every element $a \in$ I is $-a \in$ I.

**Example 8.** *Prove that G = {1, 2, 3, 4, 5, 6} is a finite abelian group of order 6 under multiplication modulo 7.*

**Sol.** G = {1, 2, 3, 4, 5, 6, $\times_7$}

Consider the multiplication modulo 7 table as shown below. Recall that $a \times_7 b$ = The remainder when $ab$ is divided by 7

| $\times_7$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

From the table, we observe that each element inside the table is also an element of G. It means that G is closed under multiplication modulo 7.

Also for each $a, b, c \in G$

$$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c \quad \text{i.e., associative law hold.}$$

From the table, we observe that the first row inside the table is identical with the top-row of the table. Therefore, 1 is the identity (multiplicative) of G.

Also, $2 \times_7 4 = 1$ ; $3 \times_7 5 = 1$, $4 \times_7 2 = 1$, $5 \times_7 3 = 1$, $6 \times_7 6 = 1$

Hence, each element G has an inverse, *i.e.*,

Inverse of 2 is 4 and of 4 is 2

Inverse of 3 is 5 and of 5 is 3

Inverse of 6 is 6

Hence, G is a group under the multiplication modulo 7.

**Example 9.** *Consider an algebraic system (Q, *),where Q is the set of rational numbers and * is a binary operation defined by*

$$a * b = a + b - ab \ \forall \ a, b \in Q.$$

*Determine whether (Q, *) is a group.*

**Sol. Closure property.** Since the element $a * b \in Q$ for every $a, b \in Q$, hence, the set Q is closed under the operation *.

**Associative property.** Let us assume $a, b, c \in Q$, then we have

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + b + c - ab - ac - bc + abc.\end{aligned}$$

Similarly, $a * (b * c) = a + b + c - ab - ac - bc + abc.$

Therefore, $(a * b) * c = a * (b * c)$

$\therefore$ * is associative.

**Identity.** Let $e$ is an identity element. Then we have $a * e = a \ \forall \ a \in Q$

$\therefore \quad a + e - ae = a \quad$ or $\quad e - ae = 0$

or $\quad e(1 - a) = 0 \quad$ or $\quad e = 0$, if $1 - a \neq 0$

Similarly, for $e * a = a \ \forall \ a \in Q$, we have $e = 0$

Therefore, for $e = 0$, we have $a * e = e * a = a$

Thus, 0 is the identity element.

**Inverse.** Let us assume an element $a \in Q$. Let $a^{-1}$ is an inverse of $a$. Then we have

$$a * a^{-1} = 0 \qquad \text{[Identity]}$$

$\therefore \quad a + a^{-1} - aa^{-1} = 0$

or $\quad a^{-1}(1 - a) = -a \quad$ or $\quad a^{-1} = \dfrac{a}{a-1}, a \neq 1$

Now, $\dfrac{a}{a-1} \in Q$, if $a \neq 1$

Therefore, every element has inverse such that $a \neq 1$.

Since, the algebraic system (Q, *) satisfy all the properties of a group. Hence, (Q, *) is a group.

NOTES

**Theorem 2.** *Show that the identity element in a group is unique.*

**Proof.** Let us assume that there exists two identity elements *i.e.,* $e$ and $e'$ of G.

Since, $e \in$ G and $e'$ is an identity. We have $e'e = ee' = e$

Also, $e' \in$ G and $e$ is an identity. We have $e'e = ee' = e'$

$\therefore \qquad e = e'$

Hence, identity in a group is unique.

**Theorem 3.** *Show that inverse of an element $a$ in a group G is unique.*

**Proof.** Let us assume that $a \in$ G be an element. Also, assume that $a_1^{-1}$ and $a_2^{-1}$ be two inverse elements of $a$. Then we have,

$$a_1^{-1} a = aa_1^{-1} = e \quad \text{and} \quad a_2^{-1} a = aa_2^{-1} = e$$

Now, $\qquad a_1^{-1} = a_1^{-1} e = a_1^{-1}(aa_2^{-1}) = (a_1^{-1} a)a_2^{-1} = ea_2^{-1} = a_2^{-1}$

Thus, the inverse of an element is unique.

**Theorem 4.** *Show that $(a^{-1})^{-1} = a$ for all $a \in G$, where G is a group and $a^{-1}$ is an inverse of $a$.*

**Proof.** Given that $a^{-1}$ is an inverse of $a$. Then, we have

$$aa^{-1} = a^{-1} a = e$$

This implies that $a$ is also an inverse of $a^{-1}$. Therefore $(a^{-1})^{-1} = a$.

**Theorem 5.** *Show that $(ab)^{-1} = b^{-1} a^{-1}$ for all $a, b \in G$.*

**Proof.** We have to prove that $ab$ is inverse of $b^{-1} a^{-1}$. We prove

$$(ab)(b^{-1} a^{-1}) = (b^{-1} a^{-1})(ab) = e$$

Consider $\quad (ab)(b^{-1} a^{-1}) = [(ab)\, b^{-1}]a^{-1} = [a(bb^{-1})]\, a^{-1}$

$\qquad\qquad = (ae)\, a^{-1} = aa^{-1} = e \qquad$ ...(1)

Similarly, $\quad (b^{-1} a^{-1})(ab) = e \qquad$ ...(2)

$\therefore$ From (1) and (2), we have

$(ab)\,(b^{-1} a^{-1}) = e = (b^{-1} a^{-1})\, ab \qquad$ Hence proved.

**Theorem 6.** *Prove the left cancellation law in a group G holds i.e., $ab = ac \Rightarrow b = c \; \forall \; a, b, c \in G$.*

**Proof.** Consider $\quad ab = ac.$

Then, we have $\quad b = eb = (a^{-1} a)b = a^{-1}(ab) = a^{-1}(ac) \qquad [\because ab = ac]$

$\qquad = (a^{-1} a)c = ec = c \qquad$ | Associativity

Hence, $\quad ab = ac \;\Rightarrow\; b = c.$

**Theorem 7.** *Prove the right cancellation law in a group G holds i.e., $ba = ca \Rightarrow b = c \; \forall \; a, b, c \in G$.*

**Proof.** Consider $ba = ca$.

Then, we have $\quad b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1} \qquad [\because ba = ca]$

$\qquad = c(aa^{-1}) = ce = c \qquad$ | Associativity

Hence, $\quad ba = ca \;\Rightarrow\; b = c.$

**Theroem 8.** *Let G be a group and $a, b \in G$. Then the equation $a * x = b$ has a unique solution given by $x = a^{-1} * b$.*

**Proof.** Given $a, b \in G$ and G is a group under $*$, therefore, $a^{-1}$ exists in G

Hence $a^{-1} * b \in G$. | G is closed

Consider $a * x = b$

$= (a * a^{-1}) * b$ | $a * a^{-1} = e$

$= a * (a^{-1} * b)$ | Associativity

$\Rightarrow$ $x = a^{-1} * b$ | Left cancellation law

**Uniqueness.** Let the equation $a * x = b$ has two solutions, say, $x_1$ and $x_2$, then we have

$$a * x_1 = b \quad ...(1)$$

$$a * x_2 = b \quad ...(2)$$

(1) and (2) gives $a * x_1 = a * x_2$

$\Rightarrow$ $x_1 = x_2$ | Left cancellation law

## $Z_m$, The Integers Modulo $m$

The integers modulo $m$, denoted by $Z_m$, is the set given by

$Z_m = \{0, 1, 2, ... m-1; +_m, \times_m\}$ where the operations $+_m$ (read as addition modulo $m$) and $\times_m$ (read as multiplication modulo $m$) are defined as

$$a +_m b = \text{remainder after } a + b \text{ is divided by } m$$

$$a \times_m b = \text{remainder after } a \times b \text{ is divided by } m.$$

## Finite and Infinite Group

A group (G, $*$) is called a finite group if G is a finite set.

A group (G, $*$) is called an infinite group if G is an infinite set.

**For example**

**1.** The group (I, +) is an infinite group as the set I of integers is an infinite set.

**2.** The group G = {1, 2, 3, 4, 5, 6, 7} under multiplication modulo 8 is a finite group as the set G is a finite set.

## Order of Group

The order of the group G is the number of elements in the group G. It is denoted by $|G|$. A group of order 1 has only the identity element *i.e.*, ({e}).

A group of order 2 has two elements *i.e.*, one identity element and one some other element.

**Example 10.** *Consider an algebraic system ({0, 1}, +) where the operation + is defined as shown in (Fig. 3).*

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

**Fig. 3**

The system ({0, 1}, +) is a group. In this 0 is identity element and every element is its own inverse.

**Theorem 9.** *If G is a finite group of order n and $a \in G$, then there exists a positive integer m such that $a^m = e$ and $m \le n$.*

NOTES

**Proof.** Consider the elements of the group G as $a, a^2, a^3, \ldots, a^{n+1}$. These are $n + 1$ elements. Since $|G| = n$. Therefore two of its elements, say, $a^p, a^q$ must be equal, *i.e.*, $a^p = a^q$, $p < q$. Take $m = q - p$

$$\therefore \quad a^m = a^{q-p} = a^p \cdot a^{-p}$$
$$= a^q \cdot (a^p)^{-1} = a^q \cdot (a^q)^{-1} \qquad | \; a^p = a^q$$
$$= e$$

Further, since $p, q$ are among $n + 1$,

$$\therefore \quad 1 \le p < q \le n + 1 \;\Rightarrow\; q - p = m \le n.$$

## Subgroup

Let us consider a group (G, ∗). Also, let S ⊆ G ; then (S, ∗) is called a subgroup iff it satisfies following conditions :

(*i*) The operation ∗ is closed operation on S.

(*ii*) The operation ∗ is an associative operation.

(*iii*) As *e* is an identity element belonged to G. It must belong to the set S *i.e.*, the identity element of (G, ∗) must belongs to (S, ∗).

(*iv*) For every element $a \in S$, $a^{-1}$ also belongs to S.

*For example,* let (G, +) be a group, where G is a set of all integers and (+) is an addition operation. Then (H, +) is a subgroup of the group G, where H = {2*m* : *m* ∈ G}, the set of all even integer.

*For example,* let G be a group. Then the two subgroups of G are G and $G_1 = \{e\}$, *e* is the indentity element.

**Theorem 10.** *A subset H of a group G is a subgroup of G iff*

(*i*) *The identity element e ∈ H*

(*ii*) *H is closed under the same operation as in G*

(*iii*) *H is closed under inverses i.e., if a ∈ H, then* $a^{-1} \in H$.

**Proof.** Given G is a group and H is a subset of G. Let H is a subgroup of G, then, by definition, (*i*), (*ii*), (*iii*) are true.

**Converse.** Let (*i*), (*ii*), (*iii*) hold. We show H is a subgroup of G. We show the associativity of elements of H.

Let *a*, *b*, *c* ∈ G and since H ⊆ G ∴ *a*, *b c* ∈ H

Since elements of G are also elements of H

∴ associativity holds for H. Hence the **Theorem.**

**Another statement :** A subset H of a group G is a subgroup of G iff $a * b^{-1} \in H$.

**Theorem 11.** *Let $H_1$ and $H_2$ be subgroup of group G, neither of which contains the other. Show that there exist an element of G belonging neither to $H_1$ nor $H_2$.*

**Proof.** Given $H_1$ and $H_2$ are subgroups of G. Also $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$. We show that there exists an element belonging neither to $H_1$ nor $H_2$. Let, if possible, there is an element a belonging to $H_1$ and $H_2$ *i.e.*, $a \in H_1 \cap H_2$.

Now $a \in H_1$ and since $H_1$ is a subgroup of G $\;\therefore\; a^{-1} \in H_1$ ...(1)

But $a \in H_2$ and since $H_2$ is a subgroup of G $\;\therefore\; a^{-1} \in H_2$ ...(2)

(1) and (2) gives $H_1 \subseteq H_2$, a contradiction.

Hence the theorem.

**Theorem 12.** *If H and K are two subgroups of G, then H ∩ K is also a subgroup of G.*

**Proof.** We know that a subset H of a group G is a subgroup of G iff $ab^{-1} \in H \; \forall \; a, b \in H$.

Let $a, b \in H \cap K$. We show $ab^{-1} \in H \cap K$.

Now $\quad a \in H \cap K \Rightarrow a \in H$ and $a \in K$

Also $\quad b \in H \cap K \Rightarrow b \in H$ and $b \in K$

Since H is a subgroup of G and $a, b \in H$

$\Rightarrow \quad ab^{-1} \in H$ (Using theorem X) ...(1)

Also K is a subgroup of G and $a, b \in K$

$\Rightarrow \quad ab^{-1} \in K$ ...(2)

From (1) and (2), $ab^{-1} \in H \cap K$. Hence $H \cap K$ is a subgroup of G.

**Cor.** If H and K are two subgroups of a group G, then give an example to show that $H \cup K$ may not be a subgroup of G

Consider G = The group of integers under +

$H_1 = \{... -6, -4, -2, 0, 2, 4, 6 ...\}$

$H_2 = \{... -12, -9, -6, -3, 0, 3, 6, 9, 12, ...\}$ are subgroups of G under +.

But $H_1 \cup H_2 = \{... -4, -3, -2, 0, 2, 3, 4, 6, ...\}$

Since $2 \in H_1 \cup H_2$, $3 \in H_1 \cup H_2 \Rightarrow 2 + 3 = 5 \notin H_1 \cup H_2$ *i.e.*, $H_1 \cup H_2$ is not closed under +. Hence $H_1 \cup H_2$ is not a subgroup of G under +.

**Theorem 13.** *If H is a non-empty finite subset of a group G and H is closed under multiplication. Then H is a subgroup of G.*

**Proof.** We know that a non-empty subset H of a group G is a subgroups of G iff

(*i*) $a \in H, b \in H \Rightarrow ab \in H$

(*ii*) $a \in H \Rightarrow a^{-1} \in H$

The condition (*i*) is true since it is given that H is closed under multiplication.

To show (*ii*), Let $a \in H, a \in H \Rightarrow a^2 \in H$

| H is closed under multiplication

Again $\quad a \in H, a^2 \in H \Rightarrow a^3 \in H$ and so on.

Thus the infinite collection of all the elements $a, a^2, a^3, ... a^m, ...,$ belongs to H. But H is finite. $\therefore$ there must be repeation. Let $a^r = a^s \quad r > s > 0$

$\Rightarrow \quad a^r . a^{-s} = e$

$\Rightarrow \quad a^{r-s} = e \in H$

Take $y = a^{r-s-1}$ and consider

$$ya = a^{r-s-1} . a = a^{r-s} = e$$

Similarly, $\quad ay = e$

Hence $\quad ya = e = ay$

$\Rightarrow$ $y$ is the inverse of $a$. Hence the theorem.

**Theorem 14.** Let H be a subgroup of G. Then

(*a*) $H = Ha \quad \Leftrightarrow \quad a \in H$

(*b*) $Ha = Hb \quad \Leftrightarrow \quad a b^{-1} \in H$

(*c*) $aH = bH \quad \Leftrightarrow \quad a^{-1} b \in H$

(*d*) $HH = H$.

**Proof.** (*a*) Let $\quad Ha = H$. If $e \in H \Rightarrow e\, a \in Ha = H$

$\Rightarrow \quad a \in H$ | $ea = a$

Conversly, Let $a \in H$. As H is a subgroup and $h \in H$, $a \in H$

$\Rightarrow \quad h\, a \in H$ | H is closed under multiplication.

$\Rightarrow \quad H\, a \subseteq H$ ...(1)

Again, if $h \in H$, $a \in H$ and since H is a subgroup of G,

$\therefore \quad h\, a^{-1} \in H$ (Theorem X)

$\Rightarrow \quad (ha^{-1})\, a \in H\, a$

$\Rightarrow \quad h(a^{-1}a) \in Ha \Rightarrow h\, e \in Ha$

$\Rightarrow \quad h \in H\, a$

$\Rightarrow \quad H \subseteq H\, a$ ...(2)

**NOTES**

From (1) and (2) $Ha = H$

(*b*) Let $Ha = Hb$ and we show $ab^{-1} \in H$

Now $a = e\,a \in Ha$

$\Rightarrow \quad a \in Ha = Hb$

$\Rightarrow \quad a \in Hb \Rightarrow \quad a = hb, h \in H$

$\Rightarrow ab^{-1} = (hb)b^{-1} = h(bb^{-1}) = he = h \in H$

$\Rightarrow ab^{-1} \in H$

Conversely, Let $ab^{-1} \in H \Rightarrow ab^{-1} = h, h \in H$

$\Rightarrow \quad a = hb$

$\Rightarrow \quad Ha = Hhb = Hb$ | For $h \in H, Hh = H$

(*c*) Proceed yourself as in Part (*b*).

(*d*) Let $h \in H$. Then,

$H = Hh \quad \forall h \in H$ | Using part (*a*)

$\Leftrightarrow \quad H \subseteq HH \subseteq H$

$\therefore \quad HH = H.$

## Abelian Group

Let us consider, an algebraic system (G, *), where * is a binary operation on G. Then the system (G, *)is said to be an abelian group if it satisfies all the properties of the group plus an additional following property :

(*i*) The operation * is commutative *i.e.*,

$$a * b = b * a \ \forall \ a, b \in G$$

*For example,* consider an algebraic system (I, +), where I is the set of all integers and + is an addition operation. The system (I, +) is an abelian group because it satisfies all the properties of a group. Also the operation + is commutative for every *a*, $b \in I$.

## ILLUSTRATIVE EXAMPLE

**Example 1.** *Consider an algebraic system (G, *), where G is the set of all non-zero real numbers and * is a binary operation defined by* $a * b = \frac{ab}{4}$. *Show that (G, *) is an abelian group.*

**Sol. Closure property.** The set G is closed under the operation * . Since, $a * b = \frac{ab}{2}$ is a real number. Hence, belongs to G.

**Associative property.** The operation * is associative. Let *a, b, c* ∈ G, then we have

$$(a * b) * c = \left(\frac{ab}{4}\right) * c = \frac{(ab)c}{16} = \frac{abc}{16}.$$

Similarly, $$a * (b * c) = a * \left(\frac{bc}{4}\right) = \frac{a(bc)}{16} = \frac{abc}{16}.$$

**Identity.** To find the identity element, let us assume that *e* is a positive real number. Then for $a \in G$,

$$e * a = a \Rightarrow \frac{ea}{4} = a \quad \text{or} \quad e = 4$$

Similarly, $a * e = a$

$$\Rightarrow \frac{ae}{4} = a \quad \text{or} \quad e = 4.$$

NOTES

Thus, the identity an element in G is 4.

**Inverse.** Let us assume that $a \in$ G. If $a^{-1} \in$ Q is an inverse of $a$, then $a * a^{-1} = 4$

$$\Rightarrow \frac{aa^{-1}}{4} = 4 \quad \text{or} \quad a^{-1} = \frac{16}{a}$$

Similarly, $a^{-1} * a = 4$ gives

$$\Rightarrow \frac{a^{-1}a}{4} = 4 \quad \text{or} \quad a^{-1} = \frac{16}{a}.$$

Thus, the inverse of an element $a$ in G is $\frac{16}{a}$.

**Commutative.** The operation $*$ on G is commutative.

Since, $a * b = \frac{ab}{4} = \frac{ba}{4} = b * a.$

Thus, the algebraic system (G, $*$) is closed, associative, has identity element, has inverse and commutative. Hence, the system (G, $*$) is an abelian group.

## EXERCISE 2

1. If $a, b, c$ are elements of a group G and $a * b = c * a$. Then $b = c$ ? Explain your answer.
2. Which of the following are groups ?
   (*i*) $M_{2\times3}(R)$ with matrix addition
   (*ii*) $M_{2\times2}(R)$ with matrix multiplication
   (*iii*) The positive real numbers with multiplication
   (*iv*) The non-zero real numbers with multiplication
   (*v*) The set [– 1, 1] with multiplication.
3. Give an example of (*i*) a finite abelian group (*ii*) an infinite non-abelian group.
4. Let V = {$e, a, b, c$}. Let $*$ be defined by $x * x = e$ for all $x \in$ V. Write a complete table for $*$ so that (V, $*$) is a group.
5. Which of the following subsets of the real numbers is a subgroup of [R, +] ?
   (*a*) The rational numbers
   (*b*) The positive real numbers
   (*c*) $H = \left\{\frac{K}{2} : K \text{ is an integer}\right\}$
   (*d*) $H = \{2^K : K \text{ is an integer}\}$
   (*e*) $H = \{x : -100 \le x \le 100\}$
6. Let G be a group of order $p$, $p$ is prime. Find all subgroups of G.

## Normal Subgroup

A subgroup H of a group G is called normal subgroup of G if for every $g \in$ G, $h \in$ H, $\Rightarrow$ $ghg^{-1} \in$ H.

*or*

A subgroup H of a group G is called a normal subgroup of G iff for $g \in$ G, we have

$$gHg^{-1} = H \; \forall \, g \in G$$

**Example 2.** *Every subgroup of an abelian group is normal.*

**Sol.** Let H be a subgroup of a normal group G. We show H is normal. Let $h \in H$ and $g \in G$. Consider

NOTES

$$ghg^{-1} = gg^{-1}h$$
$$= eh$$
$$= h \in H$$

$\Rightarrow$ $ghg^{-1} \in H$.

| $h \in H \subseteq G \;\Rightarrow\; h \in G$ Also $h, g^{-1} \in G$ and since G is abelian $\therefore\; hg^{-1} = g^{-1}h$ |

Hence, H is a normal subgroup of G.

## Cyclic Group

A group G is called cyclic if for some $a \in G$, every element $x \in G$ is of the form $a^n$ for some $n \in Z$. The element $a$ is called the generator of G.

If G is cyclic, we write $G = < a >$

For *e.g.*, If $G = \{1, -1, i, -i\}$, then G is a cyclic group generated by $i$.

Since $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$

*i.e.*, every element of G is of the form $i^n$ for some $n \in Z$. Hence $i$ is a generator for the cyclic group.

**Remark.** The order of a generator of the cyclic group is equal to the order of the group.

*e.g.*, $Z_{12} = [Z_{12} ; +_{12}]$ is a cyclic group.

**Sol.** $Z_{12} = \{0, 1, 2, \ldots 11, +_{12}\}$.

Consider $5 = 5$

$$5 +_{12} 5 = 10$$
$$5 +_{12} 5 +_{12} 5 = 3$$
$$5 +_{12} 5 +_{12} 5 +_{12} 5 = 8$$
$$5 +_{12} 5 +_{12} 5 +_{12} 5 +_{12} 5 = 25 = 1 \text{ etc.}$$

Thus we see that every element of $Z_{12}$ is of the form $5n$ for some $n \in Z$. Thus 5 is a generator of $Z_{12}$.

Hence $[Z_{12}, +_{12}]$ is a cyclic group with 5 as generator. Since inverse of 5 is 7 ($5 +_{12} 7 = 0$), therefore, 7 is also a generator. (theorem X below)

**Theorem 15.** *If a is a generator of a cyclic group G, show that inverse of a is also a generator.*

**Proof.** Let $G = <a>$ *i.e.*, G is a cyclic group and $a$ is its generator. Let $g \in G$, then

$$g = a^r \text{ for some } r \in Z$$

Take $r = -s, s \in Z$, we have

$$g = a^{-s} = (a^{-1})^s \text{ for some } s \in Z$$

Thus every element $g \in G$ is of the form $(a^{-1})^s$. Hence $a^{-1}$ is a generator.

**Theorem 16.** *Every cyclic group is abelian.*

**Proof.** Let G be a cyclic group with $a$ as its generator. *i.e.*, let $G = <a>$ and $g_1 \in G$.

Then $g_1 = a^r$ for some $r \in Z$

Let $g_2 \in$ G, then $g_2 = a^s$ for some $s \in$ Z

Consider $g_1 \cdot g_2 = a^r \cdot a^s = a^{r+s}$

$= a^{s+r}$ | $r + s = s + r$ as Z is abelian

$= a^s \cdot a^r = g_2 \cdot g_1$

$\Rightarrow$ G is abelian.

**Theorem 17.** *Every subgroup of a cyclic group is cyclic.*

**Proof.** Let G = <a> *i.e.,* G is a cyclic group with $a$ as its generator. Let H be a subgroup of G.

**Case I.** If H = {$e$}, then H = <e> *i.e.,* H is a cyclic group with $e$ as a generator.

**Case II.** If H ≠ {$e$}, then $o$(H) ≥ 2 *i.e.,* there exists $e \neq a \in$ H.

Since H is a subgroup, it must be closed under inverses and so contains positive powers of $a$. Let $m$ is the smallest power of a such that $a^m \in$ H. We claim $b = a^m$ is a generator of H. Let $x \in$ H. But H ⊆ G ∴ $x \in$ G.

Since G is a cyclic group G with $a$ as its generator. ∴ $x = a^n$ for some $n \in$ Z.

Dividing $n$ by $m$, we get a quotient $q$ and remainder $r$. *i.e.,*

$$n = mq + r,\ 0 \le r < m$$

Now $a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r$

$\Rightarrow$ $a^r = b^{-q} \cdot a^n$

Here $a^n$, $b \in$ H and since H is a subgroup ∴ $b^{-q}\, a^n \in$ H which means $a^r \in$ H.

But $m$ was the least positive integer of a such that $a^m . \in$ H and $r < m$.

∴ We must have $r = 0$

Hence $a^n = b^q$ for some $q \in$ Z

$\Rightarrow$ $x = a^n = b^q$ *i.e.,* every element $x \in$ H is of the form $b^q$ for some $q \in$ Z

∴ H is cyclic.

**Theorem 18.** *Every group of prime order is cyclic.*

**Proof.** Let G be a group of order $p$, $p$ is prime. It means G must contain at least two elements. Since 2 is the least positive integer which is prime *i.e.,* if $a \in$ G, then $o(a) \ge 2$.

Let $o(a) = m$ and H be a cyclic subgroup of G generated by $a$, then

$o(\text{H}) = o(a) = m$

| The order of a cyclic group is equal to the order of its generator

Also By Lagrange's theorem,

$$o(\text{H})\ |\ o(\text{G}) \Rightarrow m\ |\ p$$

$\Rightarrow$ $p = 1$ or $p = m$

But $p \neq 1$ ∴ $p = m$

$\Rightarrow$ $o(\text{H}) = o(\text{G}) \Rightarrow \text{H} = \text{G}.$

Hence G is cyclic since H is cyclic.

**Theorem 19.** *Let G is a cyclic group of order p (p is prime). Show that G has no proper subgroups except G and {e}.*

**Proof.** Let G is a cyclic group of order $p$.

Let H be any subgroup of G and $o$(H) = $m$.

By Lagrange theorem, $o(\text{H})\ |\ o(\text{G}) \Rightarrow m\ |\ p$

$\Rightarrow$ $p = 1$ or $p = m$

But $p \neq 1 \quad \therefore \quad p = m$

*i.e.*, $o(H) = m = p \Rightarrow$ H is a group of prime order and hence cyclic. Also $o(G) = m$

$\therefore$ G = H *i.e.* G has no proper subgroups.

**Cyclic group generated by $a$.** Let G be any group and $a \in G$. Define $a^0 = e$ ; the *cyclic group generated by a*, denoted by $<a>$, where $< a >$ denotes the set of all powers of $a$, is defined by $<a> = \{......, a^{-2}, a^{-1}, e, a, a^2, a^3, .....\}$

$<a>$ contains the identity element $e$, closed under group operation, contains *inverses*.

$\therefore$ $<a>$ is a subgroup of G and is called the *cyclic group generated* by $a$.

## 1.7. GROUP HOMOMORPHISM

A mapping from a group (G,.) into a group $(\overline{G}, *)$ is said to be a group *homomorphism* if

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

### Group Isomorphism

A homomorphism $\phi$ which is one-one and onto is called **isomorphism** and the groups G and G′ are called **isomorphic**, written as $G \cong G'$.

A homomorphism which is onto is called **epimorphism**

A homomorphism which is one-one is called **monomorphism.**

### KERNEL f

If $f$ is a homomorphism of G to $\overline{G}$, then kernel $f$ is the set defined by

$$\text{Ker} f = [x \in G : f(x) = \bar{e}, \bar{e} \in \overline{G}]$$

### IMAGE f

The image $f$ is the set of the images of the elements under $f$ *i.e.*,

$\text{Im}(f) = \{b \in G' : f(a) = b \text{ for } a \in G\}$ where $f$ is a homomorphism of G to G′.

The term 'range $f$' is also used for 'image $f$'.

**Example 3.** *Let G be a group of real numbers under addition and let G′ be the group of positive real numbers under multiplication. Define $f : G \to G'$ by $f(a) = 2^a$.*

*Show that f is a homomorphism. Also show that G and G′ are isomorphic.*

**Sol.** Given $f$ is a mapping from (G, +) to (G′, .) defined by $f(a) = 2^a$

Let $a, b \in G$ and consider

$$f(a + b) = 2^{a+b} = 2^a \,.\, 2^b = f(a) \,.\, f(b)$$

Hence $f : G \to G'$ is homomorphism.

**To check $f$ is one-one.** Let $f(a) = f(b)$

$\Rightarrow \quad 2^a = 2^b \Rightarrow a = b$

$\therefore$ $f$ is one-one.

**To check $f$ is onto :** For each $a \in \mathbb{R}$, we have $2^a$ is a positive real number. Thus $f(a) = 2^a$ is onto.

Hence $f : G \to G'$ is an isomorphism and the groups G and G′ are isomorphic *i.e.,* $G \cong G'$.

**Theorem 20.** *Let $f : G \to G'$ is a group homomorphism. Then*

*(a) $f(e) = e'$, $e \in G$, $e' \in G'$*

*(b) $f(a^{-1}) = (f(a))^{-1}\ \forall\ a \in G$.*

**Proof.** (*a*) Given $f : G \to G'$ is a homomorphism from G to G′. For $x \in G$, consider

$$f(x)\, e' = f(x) \qquad | e' \text{ is identity of } G'$$
$$= f(xe) = f(x)\, f(e) \qquad | f \text{ is homomorphism}$$
$$\Rightarrow \quad e' = f(e) \qquad |\text{Left cancellation law}$$
$$\Rightarrow \quad f(e) = e'$$

(*b*) From Part (*a*), $e' = f(e) = f(aa^{-1})$

$$= f(a)\, f(a^{-1}) \qquad | f \text{ is homomorphism}$$
$$\Rightarrow \quad f(a)\, f(a^{-1}) = e'$$
$$\Rightarrow \quad (f(a))^{-1} f(a)\, f(a^{-1}) = (f(a))^{-1} e'$$
$$\Rightarrow \quad f(a^{-1}) = (f(a))^{-1}$$

**Theorem 21.** *If $f$ is a homomorphism of G to $\overline{G}$ with Ker $f$ = K. Show that K is a normal subgroup of G.*

**Proof.** By definition,

$$\text{Ker} f = \{x \in G : f(x) = e',\ e' \in \overline{G}\} = K$$

We first show that Ker $f$ is a subgroup of G

Let $\quad x, y \in \text{Ker} f \;\Rightarrow\; f(x) = e', f(y) = e'$

Consider $\quad f(xy^{-1}) = f(x)\, f(y^{-1}) \qquad |$ homomorphism

$$= f(x)\, (f(y))^{-1} = e'\, (e')^{-1} = e'$$
$$\Rightarrow \quad xy^{-1} \in \text{Ker} f \;\Rightarrow\; \text{Ker} f \text{ is a subgroup of G.}$$

Let $g \in G$ and $x \in \text{Ker} f$, consider

$$f(gxg^{-1}) = f(g)\, f(xg^{-1}) \qquad | f \text{ is homomorphism}$$
$$= f(g)\, f(x)\, f(g^{-1}) = f(g)\, f(x)\, (f(g))^{-1}$$
$$= f(g)\, e'\, (f(g))^{-1} = f(g)\, (f(g))^{-1} = e'$$
$$\Rightarrow \quad gxg^{-1} \in \text{Ker} f \;\Rightarrow\; \text{Ker} f \text{ is a normal subgroup of G.}$$

**Theorem 22.** *Let $f$ be a homomorphism of a group G to a group G′. Let Im($f$) be the homomorphism image of G in G′. Then Im($f$) is a subgroup of G′.*

**Proof.** By definition, $\text{Im}(f) = \{f(x) : x \in G\}$

Take $\quad e \in G \;\Rightarrow\; e' = f(e) \in \text{Im}(f)$

*i.e.* $\text{Im}(f) \neq \phi$, we first show that Im($f$) is a subgroup of G′. Let $x', y' \in \text{Im}(f)$

$\Rightarrow$ There exists $x, y \in G$ such that $f(x) = x'$, $f(y) = y'$

Consider $\quad x'y'^{-1} = f(x)\, (f(y))^{-1}$

$$= f(x)\, f(y^{-1}) \qquad | f \text{ is a homomorphism}$$
$$= f(xy^{-1}) \in \text{Im}(f) \;|\; x, y \in G \text{ and G is a group} \;\therefore\; xy^{-1} \in G$$

NOTES

$\Rightarrow \quad x' y'^{-1} \in \text{Im}(f)$

$\Rightarrow$ Im($f$) is a subgroup of G′.

**Theorem 23.** *Fundamental Theorem of Group Homomorphism*

**Statement.** Let $f : G \to G'$ is a homomorphism. Then $G/K \cong G'$, where K = Ker $f$

**Proof.** Given $f$ is a homomorphism of G to G′. Also Ker $f$ is a normal subgroup of G. ∴ G/Ker $f$ is defined.

Define $\theta : G/K \to G'$ by $\theta(Kx) = f(x)$, K = Ker $f$

We show θ is well-defined, one-one and homomorphism.

**θ is well-defined :** Consider $Kx = Ky$

$\Rightarrow \quad xy^{-1} \in K = \text{Ker } f$ | $Ha = Hb \Leftrightarrow ab^{-1} \in H$

$\Rightarrow \quad f(xy^{-1}) = \bar{e}, \bar{e} \in G'$

$\Rightarrow \quad f(x) f(y^{-1}) = \bar{e}$ | Homomorphism

$\Rightarrow \quad f(x) (f(y))^{-1} = \bar{e}$

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

$\Rightarrow \quad \theta(Kx) = \theta(Ky)$

$\Rightarrow$ θ is well-defined.

**θ is one-one :** Let $\theta(Kx) = \theta(Ky)$

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

$\Rightarrow \quad f(x) (f(y))^{-1} = \bar{e}$

$\Rightarrow \quad f(x) f(y^{-1}) = \bar{e}$

$\Rightarrow \quad f(xy^{-1}) = \bar{e}$

$\Rightarrow \quad xy^{-1} \in K = \text{Ker } f$

$\Rightarrow \quad Kx = Ky$ | $Ha = Hb \Leftrightarrow ab^{-1} \in H$

$\Rightarrow$ θ is one-one.

**θ is homomorphism.** Consider

$$\theta(KxKy) = \theta(K\,xy) = f(xy) \quad | \; HaHb = Hab$$
$$= f(x) f(y) = \theta(Kx)\, \theta(Ky)$$

$\Rightarrow$ θ is a homomorphism.

We lastly show that θ is onto. Let $y \in G'$. Since G′ is the Image of G under $f$, there exists $x \in G$ such that $f(x) = y \Rightarrow \theta(Kx) = y$ *i.e.,* θ is onto. Therefore, we have proved that θ is homomorphism, one-one and onto

$$\therefore \quad G \,|\, K \cong G'.$$

**Theorem 24.** *Any finite cyclic group of order n is isomorphic to $Z_n$.*

**Proof.** Let G = <$a$> be a finite cyclic group, with $a$ as its generator and let $o(G) = n$

Define $f : Z \to G$ by $f(m) = a^m$

Let $m, r \in Z$ such that $f(m) = a^m$, $f(r) = a^r$

Consider $\quad f(m + r) = a^{m+r} = a^m \,.\, a^r = f(m) f(r)$

Thus $f$ is a homomorphism of Z to G.

∴ By **fundamental theorem of group homomorphism.** Z | Ker $f \cong G$

But if $s \in$ Ker $f$, then by definition,

$$f(s) = e, e \in G$$

$\Leftrightarrow$ $a^s = e$

$\Leftrightarrow$ $o(a)/s$

$\Leftrightarrow$ $n/s$

$\Leftrightarrow$ $s = nk$, for some $k$

$\Leftrightarrow$ $s \in \langle n \rangle$

$\Leftrightarrow$ $\text{Ker } f = \langle n \rangle$

Hence $Z \mid \langle n \rangle \cong G$ or $G \cong Z_n$, where $Z_n = Z/\langle n \rangle$.

**EXERCISE 3**

1. Let H be a subgroup of a group G and $a, b \in G$. Then $a \in b * H$ iff $b^{-1} * a \in H$.
2. If H is a finite subgroup of a group G. Show that H and any coset H$a$ have the same number of elements.
3. Let $f : G \to G'$ be a homomorphism with kernel K. Then K is a normal subgroup of G.
4. Show that any infinite cyclic group is isomorphic to additive group of integers.

## 1.8. RING

Let R be a non-empty set with two binary compositions, addition (+) and multiplication (.). Then R is called a ring iff it satisfies the following:

**I.** R is an abelian group under + *i.e.*,

(*i*) For $a, b \in R \Rightarrow a + b \in R$ *i.e.*,
R is closed under addition

(*ii*) For $a, b, c \in R$, $a + (b + c) = (a + b) + c$ *i.e.*,
Associativity under addition holds in R.

(*iii*) For each $a \in R$, $\exists\, 0 \in R$ such that $a + 0 = a = 0 + a$ *i.e.*,
R has additive identity.

(*iv*) For each $a \in R$, $\exists\, -a \in R$ such that $a + (-a) = 0$ *i.e.*,
R has an additive inverse.

(*v*) For each $a, b \in R$, $a + b = b + a$ *i.e.*,
R is additive.

**II.** For each $a, b \in R$, $a.\, b \in R$ *i.e.*,
R is closed under multiplication.

**III.** For $a, b, c \in R$, $a.\,(b\,.\,c) = (a.\,b)\,.\,c$ *i.e.*,
Associativity under multiplication holds in R.

**IV.** For $a, b, c \in R$,

(*i*) $a\,.\,(b + c) = a.\, b + a.\, c$ (Left distributive law)

(*ii*) $(a + b)\,.\,c = a.\, c + b\,.\,c$ (Right distributive law).

**Remark:** The additive identity 0 of R is unique. We call it 'zero' of the ring. The additive inverse is also unique.

NOTES

### Commutative Ring

A ring R is called a commutative ring if $a \cdot b = b \cdot a \quad \forall\, a, b \in R$.

### Ring with Unity

A ring R is called ring with unity if for each $x \in R, \exists\, 1 \in R$ such that $1 \cdot x = x = x \cdot 1$. The element '1' is called multiplicative identity of R.

### Finite and Infinite Ring

A ring R with finite number of elements, is known as finite ring, otherwise it is known as infinite ring.

### Ring with Zero Divisors

Let R be a ring and $0 \neq a, b \in R$. Then R is called *ring with zero divisors* if $a \cdot b = 0$. *i.e.,*

If product of two non-zero elements in a ring R is zero, then R is called ring with zero divisors. Also we say that the element $a$ is a zero divisor of $b$ or $b$ is a zero divisor of $a$.

### Ring without Zero Divisors

A ring R is called ring without zero divisors if whenever

$$a \cdot b = 0 \;\Rightarrow\; a = 0 \;\text{ or }\; b = 0 \;\forall\, a, b \in R.$$

## ILLUSTRATIVE EXAMPLES

**Example 1.** *Let Z be the set of integers, then (Z, +, .) is a ring. Also Z is a commutative ring with unity.*

**Sol.** We know that Z is an additive group under +. (See Chapter on 'Groups').

Also for $a, b \in Z \;\Rightarrow\; a \cdot b \in Z \quad \forall\, a, b \in Z$ *i.e.,*

Z is closed under multiplication.

For $a, b, c \in Z$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall\, a, b, c \in Z$ *i.e.,*

Associativity under multiplication holds in Z.

For $a, b, c \in Z$, $\quad a \cdot (b + c) = a \cdot b + a \cdot c$

$$(a + b) \cdot c = a \cdot c + b \cdot c \;\forall\, a, b, c \in Z$$

Hence we can say that Z is a ring.

Further, for $a, b \in Z$, $\quad a \cdot b = b \cdot a \quad \forall\, a, b \in Z$

$\therefore$ Z is commutative also.

Also for $a \in Z, \exists\, 1 \in Z$ such that

$$1 \cdot a = a = a \cdot 1 \quad \forall\, a \in Z.$$

$\therefore$ Z is a ring with unity (multiplicative identity).

## 1.9. RING ISOMORPHISM

NOTES

Let (R, +, ·) and [R′, +′, ·′] be two rings. The ring R is isomorphic to the ring R′ iff there exists a mapping $f : R \to R'$ such that

(*i*) $f$ is one-one and onto

(*ii*) $f(a + b) = f(a) +' f(b) \quad \forall\ a, b \in R$

(*iii*) $f(a \,.\, b) = f(a) \cdot' f(b) \quad \forall\ a, b \in R$.

The mapping $f : R \to R'$ satisfying the conditions (*i*), (*ii*) and (*iii*) is called ring isomorphism.

**Remarks :** To check whether the two *rings are isomorphic*, we should check the following :

(*a*) Both rings should have same cardinality.

(*b*) Both rings should be commutative.

(*c*) Both rings should have unity.

(*d*) If there exists an equation which is solvable in one ring, but not solvable in another ring, then two rings cannot be isomorphic.

**Example 2.** *Consider the rings* [Z, + , ·] *and* [2Z, + , ·] *and define*

$$f : Z \to 2Z \text{ by } f(n) = 2n \quad \forall\ n \in Z$$

*Is f a group homomorphism ? Is f a ring isomorphism ?*

**Sol.** Z and 2Z are groups under addition.

Consider $f : Z \to 2Z$ defined by $f(n) = 2n\ \forall\ n \in Z$

For $m, n \in Z$, consider

$$f(m + n) = 2(m + n)$$
$$= 2m + 2n = f(m) + f(n)\ \forall\ m, n \in Z$$

Hence $f : Z \to 2Z$ is a group homomorphism.

**To check whether f is a ring homomorphism.**

For $m, n \in Z$, consider $f(mn) = 2\,mn$

and $f(m) f(n) = 2m \,.\, 2n = 4\,mn.$

$\therefore$ $f(mn) \neq f(m) f(n)\ \forall\ m, n \in Z$

$\therefore$ $f : Z \to 2Z$ cannot be a ring isomorphism.

## 1.10. SUBRING

Let [R, + , ·] be a ring and S be a subset of R. Then S is called a subring of R iff S is itself a ring under the operations of R.

**Theorem 25.** *A non-empty subset of a ring R is a subring of R iff*

(*i*) $a, b \in S \Rightarrow a - b \in S\ \forall\ a, b \in S$

(*ii*) $a, b \in S \Rightarrow ab \in S\ \forall\ a, b \in S$.

**Proof.** Let S be a subring of R. We prove (*i*) and (*ii*).

As S is a subring of R, S is itself a ring under the operations of R.

Hence S is additive group under +. that is, S is closed under addition. *i.e.*,

For $a, b \in S, a + b \in S\ \forall\ a, b \in S$

Also for each $b \in S$, there exists $-b \in S$ such that $-b$ is the additive inverse of $b$.

Now $a \in S, -b \in S \Rightarrow a + (-b) \in S$

$\Rightarrow$ $a - b \in S$, which proves (*i*)

NOTES

Further, as S is a subring of R, it must be a ring under the operations of R. Thus, S is closed under multiplication *i.e.*;

For $a, b \in S \Rightarrow a \,.\, b \in S \;\forall\; a, b \in S$, which proves (*ii*)

**Converse.** Let (*i*) and (*ii*) hold. We show S is a subring of R under the operations of R.

For $a, a \in S \Rightarrow a - a \in S \Rightarrow 0 \in S$ | Using (*i*)

*i.e.*, S has additive identity.

Again $0 \in S, a \in S \Rightarrow 0 - a \in S \Rightarrow -a \in S$ | Using (*i*)

*i.e.*, S has additive inverse.

For $a \in S, b \in S \Rightarrow -b \in S$ (Proved above)

From (*i*), $a - (-b) \in S$

$\Rightarrow a + b \in S \;\forall\; a, b \in S$

*i.e.*, S is closed under addition.

Since $S \subseteq R$, elements of S are also in R

$\therefore$ Associativity under addition holds in S

For $a, b \in S \subseteq R \Rightarrow a, b \in R$

$\therefore a + b = b + a$ | R is additive group

Hence we can say that S is an additive group.

From (*ii*), $a, b \in S \Rightarrow a. b \in S \;\forall\; a, b \in S$

*i.e.*, S is closed under multiplication.

Finally, $a, b, c \in S \subseteq R \Rightarrow a, b, c \in R$

$\therefore a. (b + c) = a \,.\, b + a \,.\, c$

$(a + b) \,.\, c = a \,.\, c + b \,.\, c$ | Distributive laws hold In R

*i.e.*, left distributive law and right distributive law holds in S.

Hence S is a ring under the operations of R.

**Example 3.** *The set of integers Z is subring of Q.*

**Sol.** We know that "*A non-empty subset S of a ring R is a subring of R*

iff (*i*) $a, b \in S \Rightarrow a - b \in S \;\forall\; a, b \in S$

(*ii*) $a, b \in S \Rightarrow a \,.\, b \in S \;\forall\; a, b \in S$.

Since $Z \subseteq Q$ *i.e.*, Z is a subset of Q.

For $a, b \in Z \Rightarrow a - b \in Z \;\forall\; a, b \in Z$ is true.

Also for $a, b \in Z \Rightarrow a \,.\, b \in Z \;\forall\; a, b \in Z$. | Theorem II

Hence Z is a subring of Q.

## EXERCISE 4

1. Consider the following sets. The operations involved are the usual operations defined on the sets.

(*a*) $[Z, +, \cdot]$ (*b*) $[Q, +, \cdot]$ (*c*) $[C, +, \cdot]$

(*d*) $[M_{2+2}(R), +, \cdot]$ (*e*) $[Z_2, +_2, \times_2]$ (*f*) $[Z_6, +_6, \times_6]$

(*g*) $[Z_8, +_8, \times_8]$ (*h*) $[Z_5, +_5, \times_5]$ (*i*) $[Z \times Z, +, \cdot]$

(*j*) $[Z_2^3, +, \cdot]$

(*i*) Which of the above sets are rings ?

(*ii*) Which of the above rings are commutative ? Are they rings with unity? Determine the unity of the above rings.

**2.** Perform the indicated operations on the $[Z_8; +_8, \times_8]$:

(*i*) $2\times_8(-4)$ (*ii*) $(-3)\times_8 5$

(*iii*) $(-2)\times_8(-4)$ (*iv*) $(-3)\times_8 5 +_8 (-3)\times_8(-5)$

**3.** For any ring $[R; +, \cdot]$, simplify

(*i*) $(a + b)(c + d)$ for $a, b, c, d \in R$

(*ii*) If R is commutative, show that $(a + b)^2 = a^2 + 2ab + b^2 \; \forall \; a, b \in R$

(*iii*) Simplify $(a + b)^5$ in $Z_5$.

**4.** Suppose $a^2 = a$ for every $a \in R$ (such a ring is called a *Boolean ring.*) Prove that R is commutative given that $x + y = 0 \;\Rightarrow\; x = y$ for all $x, y \in R$.

**5.** Let G be any additive group. Define a multiplication in G by $a.b = 0$ for every $a, b \in G$. Show that this makes G into a ring.

**6.** Let R be a ring with a unity element. Show that R*, the set of units in R is a group under multiplication.

## 1.11. FIELD

A commutative ring F with unity such that each non-zero element has a multiplicative inverse *i.e.*, E $a^{-1} \in F$ such that $aa^{-1} = 1 = a^{-1}a$, is called field. It is denoted by F. Alternatively, F is a field if its non-zero elements form a group under multiplication.

### ILLUSTRATIVE EXAMPLES

**Example 1.** *Consider the set M of all 2 × 2 matrices of the type* $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ *where* $\bar{a}, \bar{b}$ *are the conjugates of a and b. Is M a field ? Justify your answer.*

**Sol.** Consider A, B ∈ M where $A = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

Then $$AB = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 5 \\ 1 & 5 \end{pmatrix}$$

Also $$BA = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 5 \\ 1 & -1 \end{pmatrix} \neq AB$$

Hence M is not commutative and therefore cannot be field.

**Example 2.** *Consider* $Z_7 = [0, 1, 2, 3, \ldots\ldots 6, +_7, \times_7]$*. Show that* $Z_7$ *is a field.*

NOTES

**Sol.** Consider the addition modulo 7 table as shown in Table I.

**Table I**

| $+_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

We first show that $Z_7$ is a ring under addition modulo 7 and multiplication modulo 7.

From Table I, we observe that each element inside the table is also in $Z_7$. It means that Z is closed under $+_7$.

Addition modulo is always associative

The first row inside the table coincides with the top most row of Table I. It means 0 is the additive identity.

Each element of $Z_7$ has additive inverse.

For example, Inverse of 1 is 6. Inverse of 2 is 5 etc. | $1 +_7 6 = 7 = 0$

| $2 +_7 5 = 7 = 0$

Also Table I is symmetrical w.r.t. $+_7$. It means $Z_7$ is additive w.r.t. $+_7$ *i.e.*,

For $a, b \in Z_7, a +_7 b = b +_7 a \ \forall \ a, b \in Z_7$.

$\therefore$ $Z_7$ is an additive group w.r.t $+_7$.

Now consider the multiplication modulo 7 table as shown in Table II.

**Table II**

| $\times_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

From Table II, we observe that each element inside the table is also in $Z_7$. It means $Z_7$ is closed w.r.t. $\times_7$. *i.e.*, for $a, b \in Z_7 \Rightarrow a \times_7 b \in Z_7 \ \forall \ a, b \in Z_7$

Finally, For $a, b, c \in Z_7$,

$$a \times_7 (b +_7 c) = a \times_7 b +_7 a \times_7 c$$

$$(a +_7 b) \times_7 c = a \times_7 c +_7 6 \times_7 c \text{ is true for all } a, b, c \in Z_7.$$

Hence $Z_7$ is a ring w.r.t. addition modulo 7 and multiplication modulo 7.

Also the Table II is symmetrical w.r.t. $\times_7$. It means that $Z_7$ is commutative *i.e.*,

$$a \times_7 b = b \times_7 a \ \forall \ a, b \in Z_7$$

Further, the second row inside the table coincides with the topmost row of Table II. It means 1 is the multiplicative identity of $Z_7$.

Hence, we have shown that $Z_7$ is a commutative ring with unity. To show $Z_7$ is a field, we show each non-zero element of $Z_7$ has multiplicative inverse.

The units of $Z_7$ are those elements which are relative primes to 7. (See Topic on 'units')

The elements which are prime to 7 are 1, 2, 3, 4, 5, 6. Hence the units of $Z_7$ are 1, 2, 3, 4, 5, 6. We can also check the elements which are units as below.

$$1 \times_7 1 = 1 \; ; \; 2 \times_7 4 = 1 \; ; \; 3 \times_7 5 = 1 \; ;$$
$$4 \times_7 2 = 1 \; ; \; 5 \times_7 3 = 1 \; ; \; 6 \times_7 6 = 1.$$

Hence, each non-zero element of $Z_7$ has multiplicative inverse. Therefore $Z_7$ is a field.

## 1.12. 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.

### 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 **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* $a, b \in F$.

NOTES

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.

## 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 $(a_1, a_2), (b_1, b_2) \in V_2$.

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.**

## 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.

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.

## ILLUSTRATIVE EXAMPLES

NOTES

**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. usual 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 $i$th coordinate or component of X. $0 = (0, 0, ....., 0)$ 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 $\lambda$ is a real number, we define $\lambda X = (\lambda x_1, \lambda x_2, ......, \lambda x_n)$ and *is called (coordinate wise) scalar multiplication* ($\lambda$ 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 $0 = (0, 0, ......, 0)$ called the zero vector such that

$$X + 0 = X = 0 + X, \forall X \in R^n.$$

(*iv*) For each X in $R^n$, there exists a unique Y in $R^n$ such that

$$X + Y = 0 = Y + X$$

Y is denoted by – X and is the vector

$$-X = (-x_1, -x_2, ..., -x_n) \text{ if } X = (x_1, x_2, ......., x_n).$$

**(2) The scalar multiplication satisfies the following properties :**

(*i*) $1.X = X, \quad \forall X \in R^n$

(*ii*) $a(X + Y) = aX + aY, \quad \forall X, Y \in R^n$ and $a \in R$

(*iii*) $(a + b)X = aX + bX, \quad \forall X \in R^n$ and $a, b \in R$

(*iv*) $(ab)X = a(bX), \quad \forall X \in R^n$ 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 $\lambda$ is a complex number, then $\lambda X = (\lambda x_1, \lambda x_2, ......, \lambda x_n)$ is not in $R^n$ because the numbers $\lambda x_i$ are 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 any field forms a vector space over itself.*

**Sol.** Let F be any field.

Let V = F.

NOTES

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 (1), (V, +) is an abelian group ($\because$ V = F is a field).

(II) From the field properties of F, it follows that scalar multiplication 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 $a, b \in F$.

Hence, V is a vector space over F.

## 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*) $a\mathbf{0} = \mathbf{0}, \quad \forall a \in F$

(*ii*) $0u = \mathbf{0}, \quad \forall u \in V$

(*iii*) $(-1) u = -u, \quad \forall u \in V$

(*iv*) $a(-u) = -(au) = (-a) u, \quad \forall a \in F, u \in V$

(*v*) $a(u - v) = au - av, \quad \forall a \in F, u, v \in V$

(*vi*) If $a u = \mathbf{0}$, then $a = 0$ or $u = \mathbf{0}$.

**Proof.** (*i*) Let $u \in V$.

Then $au = a(u + \mathbf{0}) = au + a\mathbf{0}$

$\Rightarrow a\mathbf{0} = \mathbf{0}$

(*ii*) $0 + 0 = 0, 0 \in F$

$\Rightarrow (0 + 0) = u = 0u, \forall u \in V$

$\Rightarrow 0u + 0u = 0u$

$\Rightarrow 0u = \mathbf{0}$

(*iii*) $(-1) u + u = (-1) u + 1. u = (-1 + 1) u = 0u = \mathbf{0}$

$\Rightarrow (-1) u = -u$.

Proofs of others are left to the reader as an exercise.

## EXERCISE 5

1. 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.
2. 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.

3. Which of the following sets form vector spaces over reals ? Explain
   (*i*) All polynomials over R with constant term zero.
   (*ii*) All polynomials over R with constant term 1.
   (*iii*) Set of all ordered pairs $(a, b)$ of integers.
   (*iv*) All polynomials with positive coefficients.

4. 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 $\alpha$ are all rational numbers.

## 1.13. LINEAR COMBINATION OF VECTORS

For a vector space V(F), if $u, v \in V$ and $a, b \in F$, then

$$au + bv \in V.$$

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 :

**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 $v = a_1v_1 + a_2v_2 + \ldots\ldots + a_nv_n$.*

*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 $(1, 0, 0, \ldots\ldots, 0), (0, 1, 0, \ldots\ldots, 0), \ldots\ldots, (0, 0, \ldots\ldots, 0, 1)$ 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 3.** *Write the vector* $v = \begin{bmatrix} 3 & -1 \\ 1 & -2 \end{bmatrix}$ *in the vector space of $2 \times 2$ 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 $$v = a_1v_1 + a_2v_2 + a_3v_3 \,;\, a_1, a_2, a_3 \in R \quad \ldots(1)$$

NOTES

$$\Rightarrow \quad \begin{bmatrix} 3 & -1 \\ 1 & -2 \end{bmatrix} = a_1 \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} + a_2 \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} + a_3 \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + a_2 + a_3 & a_1 + a_2 - a_3 \\ -a_2 & -a_1 \end{bmatrix}$$

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),

$$v = 2v_1 - v_2 + 2v_3.$$

## 1.14. INTERSECTION AND SUM OF VECTOR SPACES

**Theorem 26.** *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 a subspace]

and $u, v \in W_2 ; a \in F \Rightarrow au + v \in W_2$ [$\because$ $W_2$ is a 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 $W_1, W_2, ......, W_n$ are $n$-subspaces of V, then their intersection $W_1 \cap W_2 \cap ...... \cap W_n$ is also a subspace of V.

### 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. usual vector addition and scalar multiplication defined in matrices.

Let $$W_1 = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \middle| a, c, d \in R \right\},$$

$$W_2 = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| a, b \in R \right\}.$$

Then, one can easily see that $W_1$, $W_2$ are two subspaces of V.

$$\therefore \quad W_1 + W_2 = \left\{ \begin{pmatrix} 2a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$$

Obviously, $W_1 \subseteq W_1 + W_2$

$(\because \; u \in W_1, 0 \in W_2 \Rightarrow u + 0 = u \in W_1 + W_2, \forall u \in W_1)$

Similarly, $W_2 \subseteq W_1 + W_2$.

Hence, $W_1 \cup W_2 \subseteq W_1 + W_2$.

**Theorem 27.** *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 $au_1 + v_1 \in W_1$ 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 28.** *If $W_1$ and $W_2$ are two subspaces of a vector space V(F), then*

$$W_1 + W_2 = \langle W_1 \cup W_2 \rangle$$

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, $W_1 \subseteq W_1 + W_2$ and $W_2 \subseteq W_1 + W_2$

$$\therefore \quad W_1 \cup W_2 \subseteq W_1 + W_2$$

Since $\langle W_1 \cup W_2 \rangle$ is the smallest subspace containing $W_1 \cup W_2$, therefore,

$$\langle W_1 \cup W_2 \rangle \subseteq W_1 + W_2 \qquad \ldots(1)$$

Conversely, let $u + v \in W_1 + W_2$ where $u \in W_1, v \in W_2$.

$$\therefore \quad 1.u + 1.v = u + v \in \langle W_1 \cup W_2 \rangle$$

$$\therefore \quad W_1 + W_2 \subseteq \langle W_1 \cup W_2 \rangle \qquad \ldots(2)$$

$\therefore$ From (1) and (2),

$$W_1 + W_2 = \langle W_1 \cup W_2 \rangle.$$

**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 $W_1, W_2, \ldots, W_n$ are subspaces of V then $W_1 + W_2 + \ldots + W_n$ 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 $W_n$).*

## Direct Sum of Subspace

NOTES

Let V be a vector space over a field F. Let $W_1, W_2, ...., W_n$ be subspaces of V. Then, each vector in the sum $W_1 + W_2 + ...... + W_n$ 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 $W_1 + W_2 + ...... + W_n$ in more than one way. In case we can express **each vector** in $W_1 + W_2 + ...... + W_n$ 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 $W_1 + W_2 + ..... + W_n$ of subspaces $W_1, W_2, ......, W_n$ as the **direct sum** of subspaces $W_1, W_2, ....., W_n$ and we write it as $W_1 \oplus W_2 \oplus ..... \oplus W_n$.

**Theorem 29.** *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 $w_i = \mathbf{0}$.* 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 $v_i \in W_i$.

The two expressions for $w$ are identical.

From (1), $(u_1 - v_1) + (u_2 - v_2) + ...... + (u_n - v_n) = \mathbf{0}$

$\Rightarrow$ $u_1 - v_1 = \mathbf{0},\ u_2 - v_2 = \mathbf{0},\ ......,\ u_n - v_n = \mathbf{0}$

(by given hypothesis)

$\Rightarrow$ $u_i = v_i$, for $i = 1, 2, ....., n$.

$\Rightarrow$ 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 subspaces only *to be the direct sum.*

# 1.15. LINEAR INDEPENDENCE OF VECTORS

**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

$$a_1v_1 + a_2v_2 + ...... + a_nv_n = \mathbf{0},\ a_i \in F$$

implies $a_1 = a_2 = ...... = a_n = 0.$

*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.*

**Example 4.** *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 $a_1, a_2, ......, a_r$.

$$\Rightarrow \quad A(a_1X_1) + A(a_2X_2) + ...... + A(a_rX_r) = O$$

$$\Rightarrow \quad A(a_1X_1 + a_2X_2 + ...... + a_rX_r) = O \quad ...(1)$$

Since A is non-singular, $A^{-1}$ exists.

Pre-multiplying both sides of (1) by $A^{-1}$, we have

$$A^{-1}A(a_1X_1 + a_2X_2 + ..... + a_rX_r) = A^{-1}O$$

$$\Rightarrow \quad (A^{-1}A)(a_1X_1 + a_2X_2 ...... + a_rX_r) = O$$

$$\Rightarrow \quad a_1X_1 + a_2X_2 + ...... + a_rX_r = O \quad (\because \; AA^{-1} = I)$$

$\Rightarrow \quad a_1 = a_2 = ...... = a_r = 0$, since $X_1, X_2, ......, X_r$ are linearly independent.

Hence, $AX_1, AX_2, ......, AX_r$ are linearly independent.

**Theorem 30.** *Any set which contains the null vector* **0** *is linearly dependent.*

**Proof.** Let $\{v_1, v_2, ....., v_r\}$ be a set of vector 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 31.** *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.

## EXERCISE 6

1. Examine for linear independence or dependence of the following sets of vectors in $V_3(R)$
   (*i*) {(1, 2, 3), (2, – 2, 0)} (*ii*) {(1, 2, 3), (3, – 2, 1), (1, – 6, – 5)}
   (*iii*) {(1, 3, 2), (5, – 2, 1), (– 7, 13, 4)} (*iv*) {(1, 1, 1), (1, 2, 3), (2, 3, 8)}.
   (*v*) {(3, 0, – 3), (– 1, 1, 2), (4, 2, – 2), (2, 1, 1)}.
2. 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*) $1 + x, x + x^2, x^2 + x^3, x^3 + x^4, x^4 - 1$.
3. A set of vectors is linearly dependent. Show that at least one member of the set is a linear combination of the remaining ones.

NOTES

4. If $u, v, w$ are L.I. in V(F) where F is any subfield of C, then show that the vectors

(i) $u + v, v + w, w + u$

(ii) $u + v, v - w, u - 2v + w$ are L.I.

[**Hint.** (i) For scalars $a, b, c$

$a(u + v) + b(v + w) + c(w + u) = 0$

$\Rightarrow \quad (a + c)u + (a + b)v + (b + c)w = \mathbf{0}$

Since $u, v, w$ are L.I.

$a + c = 0, a + b = 0, b + c = 0$

$\Rightarrow \quad a = b = c = 0$ is the **only** solution.

$\Rightarrow \quad u + v, v + w + u$ are L.I.

5. 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.

## 1.16. BASIS AND DIMENSION OF A VECTOR SPACE

### 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 $v_1, v_2, \ldots, v_n$ 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 $V_0 = \{0\}$ is zero dimensional.

### 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, $\mathbf{R^2}$ and $\mathbf{R^n}$ 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 $\le n$ 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 32. (*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 $B_1 \supsetneq B$, and B 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 $B_2$.

$\therefore$ $$B_2 = \{v_1, v_2, ......, v_m, u_1, u_2, ......, u_{k-1}, u_{k+1}, ....., u_n\}$$

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.

## 1.17. LINEAR TRANSFORMATION

**Definition.** *Let U and V be any two vector spaces over the same field F. Then, a function (map or mapping) $T : U \to V$ is called a linear transformation (written as L.T.) if*

(*i*) $T(u_1 + u_2) = T(u_1) + T(u_2)$, $\quad \forall\ u_1, u_2 \in U$

*and* (*ii*) $T(au) = aT(u)$, $\quad \forall\ u \in U$ *and* $a \in F$.

Here, plus in $u_1 + u_2$ denotes addition in U and plus in $T(u_1) + T(u_2)$ denotes addition in V. Similar is the case for scalar multiplications in (*ii*).

Thus, a linear transformation is a function from U to V which preserves vector addition and scalar multiplication.

Its domain and range are vector spaces, *i.e.*, the variables as well as the values are vectors.

If $T : U \to V$ such that $T(u) = v$, then U and V are taken as vector spaces over the same field. *The vector space U is called the* **domain** *of the linear transformation T and*

*V is called the* **codomain** *of T. $v \in V$, is called the* **image** *of u under T and u is called the pre-image of v under T.*

*The set $T(U) = \{T(u) \mid u \in U\}$ of images of elements of U is called the range of T and is a subset of V. It is denoted by R(T). Linear transformation is also called* **vector space homomorphism.**

NOTES

**Theorem 33.** *If U and V are two vector spaces over the same field F, then a function $T : U \to V$ is a linear transformation if and only if*

$$T(au + bv) = aT(u) + bT(v), \quad \forall\, a, b \in F \quad \text{and} \quad u, v \in U.$$

**Proof.** (*i*) Let T be a L.T. from U to V.

Then, $$T(u + v) = T(u) + T(v) \quad \forall\, u, v \in U \qquad ...(1)$$

and $$T(au) = aT(u), \quad \forall\, u \in U, a \in F \qquad ...(2)$$

Now, $$T(au + bv) = T(au) + T(bv) \qquad \text{[By (1)]}$$
$$= aT(u) + bT(v) \qquad \text{[By (2)]}$$

(*ii*) Conversely, let

$$T(au + bv) = aT(u) + bT(v), \quad \forall\, u, v \in U \,;\, a, b \in F \qquad ...(3)$$

To show that T is a L.T., take $a = 1, b = 1$ in (3), we have

$$T(u + v) = T(u) + T(v), \forall\, u, v \in U.$$

Again, take $b = 0$ in (3), we have

$$T(au) = aT(u),$$

Hence, T is a L.T.

**Note.** The result of above theorem can be used as an alternative def. of **linear** transformation.

**Def.** *A linear transformation $T : U \to U$ is also called a* **linear operator.** *i.e. a L.T. from a vector space U into itself is called a* **linear operator**.

**Def.** *We know that a field F can be regarded as a vector space over itself. A L.T. T from a vector space F(F) to F(F) is called a* ***linear functional.***

## ILLUSTRATIVE EXAMPLES

**Example 1.** *Show that the function $T : R^3 \to R^3$ defined by*

$$T(x_1, x_2, x_3) = (x_1, x_2, 0)$$

*is a linear transformation.*

*(This function is also called the projection of $R^3$ on $x_1 x_2$-plane).*

**Sol.** To show that T is a L.T., we have to show that

$$T(X + Y) = T(X) + T(Y) \text{ and } T(aX) = aT(X)$$

for all X, Y $\in R^3$ and all scalars $a$.

Let $$X = (x_1, x_2, x_3) \quad \text{and} \quad Y = (y_1, y_2, y_3)$$

Now, $$X + Y = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$$

and $$aX = (ax_1, ax_2, ax_3).$$

By definition of T,

$$T(X + Y) = T(x_1 + y_1, x_2 + y_2, x_3 + y_3)$$
$$= (x_1 + y_1, x_2 + y_2, 0) \qquad \textit{(By rule of given mapping)}$$

$$= (x_1, x_2, 0) + (y_1, y_2, 0)$$

$$= T(X) + T(Y). \qquad \textit{(By rule of given mapping)}$$

and $\quad T(aX) = T(ax_1, ax_2, ax_3)$

$$= (ax_1, ax_2, 0) \qquad \text{(By rule of given mapping)}$$

$$= a(x_1, x_2, 0) = aT(X).$$

Hence, T is a L.T.

## 1.18. EQUALITY OF TWO LINEAR TRANSFORMATIONS

*Two linear transformations T and S from $U \to V$ are said to be equal iff $T(u) = S(u)$ for all $u \in U$.*

**Theorem 34.** *If $B = \{u_1, u_2, ..., u_n\}$ is a basis for U and $v_1, v_2, ..., v_n$ be any n vectors (not necessarily different) in V, then there exists a unique linear transformation $T : U \to V$ such that*

$$T(u_i) = v_i, \text{ for } i = 1, 2, ..., n. \qquad ...(1)$$

**Proof.** Let $u$ be any element of U.

Then, $u$ can be uniquely expressed as

$$u = a_1u_1 + a_2u_2 + ... + a_nu_n$$

for some scalars $a_1, a_2, ..., a_n$.

Define $\quad T(u) = a_1v_1 + a_2v_2 + ... + a_nv_n \qquad ...(2)$

We shall show that T is the required linear transformation. *i.e.*, we shall show that

(*i*) T is a L.T. (*ii*) T satisfies (1) and (*iii*) T is unique.

**To prove** (*i*), let $u$, $v$ be any two vectors of U and $a$, $b$ be any scalars.

Then, $\quad u = a_1u_1 + a_2u_2 + ... + a_nu_n$

and $\quad v = b_1u_1 + b_2u_2 + ... + b_nu_n.$

$\Rightarrow \quad au + bv = (aa_1 + bb_1)u_1 + (aa_1 + bb_2)u_2 + ... + (aa_n + bb_n)v_n$

$\therefore \quad T(au + bv) = T((aa_1 + bb_1) u_1 + (aa_2 + bb_2) u_2 + ... + (aa_n + bb_n)) v_n$

$$= (aa_1 + bb_1)v_1 + (aa_2 + bb_2)v_2 + ... + (aa_n + bb_n)v_n \qquad \text{[By (2)]}$$

$$= a(a_1v_1 + a_2v_2 + ... + a_nv_n) + b(b_1v_1 + b_2v_2 + ... + b_nv_n)$$

$$= a\,T(u) + b\,T(v)$$

$\therefore$ T is a L.T.

**To prove** (*ii*), $\quad u_i = 0u_1 + ... + 0u_{i-1} + 1u_i + ... + 0u_n$

and therefore, $\quad T(u_i) = 0v_1 + 0v_2 + ...... + 1v_i + ...... + 0v_n$

$\Rightarrow \quad T(u_i) = 1v_i = v_i, \forall i$

**To prove** (*iii*), let $S : U \to V$ be another L.T. such that.

$$S(u_i) = v_i \text{ for } i = 1, 2, ......, n$$

Then, $\quad S(u) = S(a_1u_1 + a_2u_2 + ... + a_nu_n)$

$$= a_1\,S(u_1) + a_2\,S(u_2) + ... + a_n\,S(u_n)$$

$$= a_1v_1 + a_2v_2 + ... + a_nv_n = T(u), \forall u \in U.$$

Hence $\quad S = T.$

**Remark.** The above theorem can be used to define a L.T. T on a basis $\{u_1, u_2, ..., u_n\}$ of a vector space U and then the value of T on a general $u$ is obtained as follows :

If $$u = a_1u_1 + a_2u_2 + ... + a_nu_n, \text{ then}$$
$$T(u) = a_1\, T(u_1) + a_2\, T(u_2) + ... + a_n\, T(u_n).$$

**NOTES**

The following example illustrates how to define a L.T. T by specifying its values on a basis.

## EXERCISE 7

1. Which of the following functions are linear transformations ?
   (*i*) $T : R^2 \to R^2$ defined by
   (*a*) $T(x, y) = (x, x + y)$ (*b*) $T(x, y) = (1 + x, y)$
   (*c*) $T(x, y) = (y, x)$ (*d*) $T(x, y) = (x^2, y)$.
   (*ii*) $T : R^2 \to R^3$ defined by
   (*a*) $T(x, y) = (x + 2y, 3x - 5y, y)$ (*b*) $T(x, y) = (2x - y, x - y, -2x)$.
   (*iii*) $T : R^3 \to R$ defined by
   $T(x, y, z) = x + 2y - 5z$.
   (*iv*) $T : R^3 \to R^2$ defined by
   (*a*) $T(x, y, z) = (|\, x \,|, 0)$ (*b*) $T(x, y, z) = (2x - 3y, 7y + 2z)$
   (*c*) $T(x, y, z) = (x - z, y)$ (*d*) $T(x, y, z) = (x, y)$
   (*e*) $T(x, y, z) = (x + y + z, 0)$.
   (*v*) $T : R^3 \to R^3$ defined by
   $T(x, y, z) = (y, -x, -z)$.
2. Find *a* L.T. in the following cases :
   (*i*) $T : R^2 \to R^2$ such that $T(1, 2) = (3, 0)$ and $T(2, 1) = (1, 2)$
   (*ii*) $T : R^2 \to R^2$ such that
   $$T(0, 1) = (3, 4),\ T(3, 1) = (2, 2) \quad \text{and} \quad T(3, 2) = (5, 7)$$
   (*iii*) $T : \int_3(x) \to \int_3(x)$ such that $T(1 + x) = 1 + x$,
   $$T(2 + x) = x + 3x^2 \quad \text{and} \quad T(x^2) = 0.$$
3. Show that
   $T : R^2 \to R^2$ such that
   $$T\,(0, 1) = (3, 4),\ T(3, 1) = (2, 2)$$
   and $T(3, 2) = (5, 7)$ is not a L.T.
4. Find a L.T. T in each of the following cases, which transforms
   (*i*) the vectors, (1, 1, 1), (1, 1, 0), (1, 0, 0) in $R^3$ to (2, 1), (2, 1), (2, 1) in $R^2$.
   (*ii*) (2, 3), (3, 2) in $R^2$ to (1, 2), (2, 3) in $R^2$.
   (*iii*) (3, – 1, – 2), (1, 1, 0), (– 2, 0, 2) in $R^3$ to twice the elementary vectors $2e_1, 2e_2, 2e_3$ in $R^3$.
   (*iv*) (1, 1, 1), (– 1, 1, – 1), (1, 1, 2) in $R^3$ to (1, 1), (1, 1), (1, 0) in $R^2$.

## 1.19. ONE-TO-ONE AND ONTO TRANSFORMATION

*A linear transformation $T : U \to V$ is said to be one to one (or just one-one) if different elements of U have different images i.e., if $u_1, u_2 \in U$ and $u_1 \neq u_2$, then $T(u_1) \neq T(u_2)$.*

*A linear transformation $T : U \to V$ is said to be onto if for each $v \in V$, there exists at least one $u \in U$ such that $T(u) = v$.*

A linear transformation T which is onto is also called *surjective,* a one-to-one transformation is called *injective* and the one which is both one to one and onto is called *bijective. A bijective linear transformation is also called an isomorphism.*

**Example 2.** *Show that the function $T : R^2 \to R^2$ defined by $T(x_1, x_2) = (x_1 - x_2, x_1 + x_2)$, for $(x_1, x_2) \in R^2$ is bijective (i.e., an isomorphism).*

**Sol.** $T : R^2 \to R^2$ defined by $T(x_1, x_2) = (x_1 - x_2, x_1 + x_2)$ for $(x_1, x_2) \in R^2$ is a L.T. (Prove it !)

**T is one-to-one**

Let $u_1 = (x_1, x_2)$ and $u_2 = (y_1, y_2)$ be any two elements of $R^2 (= U)$.

Then, $\quad T(u_1) = T(u_2)$

$\Rightarrow \quad (x_1 - x_2, x_1 + x_2) = (y_1 - y_2, y_1 + y_2)$

$\Rightarrow \quad x_1 - x_2 = y_1 - y_2, x_1 + x_2 = y_1 + y_2$

$\Rightarrow \quad x_1 = y_1, x_2 = y_2$

$\Rightarrow \quad u_1 = u_2$

$\therefore$ T is one-to-one.

**To show T is onto.**

Let $(y_1, y_2) \in R^2 (= V)$ be any element.

T is onto if there exists $(x_1, x_2) \in R^2 = U$ such that

$$T(x_1, x_2) = (y_1, y_2)$$

*i.e.,* if $\quad (x_1 - x_2, x_1 + x_2) = (y_1, y_2)$

*i.e.,* if $\quad x_1 - x_2 = y_1, x_1 + x_2 = y_2$

*i.e.,* if $\quad x_1 = \frac{1}{2}(y_1 + y_2), x_2 = \frac{1}{2}(y_2 - y_1)$

Thus, $(y_1, y_2)$ is the image of $(\frac{1}{2}(y_1 + y_2), \frac{1}{2}(y_1 - y_2))$.

$\therefore$ T is onto.

$\therefore$ T is bijective.

## 1.20. NULL SPACE OR KERNEL OF A LINEAR TRANSFORMATION

*The null space (or Kernel) of L.T. $T : U(F) \to V(F)$ is the set of those elements of U whose image under T is the zero element of V,* and is denoted by N(T).

*i.e.,* $\quad N(T) = \{u \mid u \in U \text{ and } T(u) = 0\}$.

Let us find R(T) and N(T) of some linear transformations.

**1.** Consider $T : R^3 \to R^3$ defined by

$$T(x_1, x_2, x_3) = (x_1, x_2, 0).$$

Here, $R(T) = \{(x_1, x_2, 0) \mid x_1, x_2 \in R\}$ which is nothing but the $x_1x_2$-plane in $R^3$.

To find N(T), we want those vectors $(x_1, x_2, x_3)$ for which

$$T(x_1, x_2, x_3) = 0.$$

$\Rightarrow \quad (x_1, x_2, 0) = (0, 0, 0) \quad \Rightarrow \quad x_1 = 0, x_2 = 0.$

Thus, every element of the form $(0, 0, x_3)$ will be mapped by T into (0, 0, 0) and no other element is so mapped. Hence.

$$N(T) = \{(0, 0, x_3) \mid x_3 \in R\}$$

and is nothing but $x_3$-axis of $R^3$.

**2.** Consider $T : R^3 \to R^2$ defined by

$$T(x_1, x_2, x_3) = (x_1 - x_2, x_1 + x_3)$$

NOTES

Here $R(T) = \{(x_1 - x_2, x_1 + x_3) \mid x_1, x_2, x_3 \in R\}$

We are to find vectors $(a, b) \in R^2$ such that

$$a = x_1 - x_2, b = x_1 + x_3$$

$\Rightarrow$ $x_2 = x_1 - a, x_3 = b - x_1$

Hence, $T(x_1, x_1 - a, b - x_1) = (a, b)$.

Thus, every vector $(a, b)$ of $R^2$ is in R(T)

*i.e.,* $R(T) = R^2$. T is infact, onto.

To find N(T), we want those vectors $(x_1, x_2, x_3) \in R^3$ for which

$$T(x_1, x_2, x_3) = \mathbf{0}.$$

$\Rightarrow$ $(x_1 - x_2, x_1 + x_3) = (0, 0)$

$\Rightarrow$ $x_1 - x_2 = 0$ and $x_1 + x_3 = 0$

$\Rightarrow$ $x_1 = x_2 = -x_3$

Thus $N(T) = \{(x_1, x_1, -x_1) \mid x_1 \in R\}$.

*i.e.,* N(T) is the subspace of $R^3$ generated by $< (1, 1, -1) >$.

**3.** Consider the zero map $T : U \to V$ defined by

$$T(u) = \mathbf{0}, \forall u \in U.$$

Here, $R(T) = \{\mathbf{0}\}$ and $N(T) = U$.

T is not onto.

**4.** Consider the identity map $T : U \to U$ defined by

$$T(u) = u, \forall u \in U.$$

Here, $R(T) = U$ and $N(T) = \{\mathbf{0}\}$

T is onto.

**5.** Consider the L.T. $T : R^2 \to R^2$ defined by

$$T(x_1, x_2) = (x_1, -x_2).$$

Here, $R(T) = R^2$ and $N(T) = \{(0, 0)\}$.

Here, T is onto.

**Theorem 35.** *Let $T : V \to W$ be a linear transformation. Then, T is onto iff $\rho(T) = \dim W$*

**Proof.** (*i*) Let $\rho(T) = \dim W$

$\Rightarrow$ $\dim R(T) = \dim W$

$\Rightarrow$ $R(T) = W \Rightarrow$ T is onto

(*ii*) Conversely, let T be onto

$\therefore$ $R(T) = W \Rightarrow \rho(T) = \dim W$.

**Theorem 36.** *Let T be a L.T. of the finite dimensional vector space V to itself. Then if we know that either T is one-one or that T is onto, then we can always conclude that T is both one-one and onto (i.e. bijective).*

**Proof.** It will suffice to show that each of the statements ' T is one-one' and ' T is onto' implies the other.

Now, T is one-one iff $\mu(T) = 0$

*i.e.,* iff $\rho(T) = \dim V$

*i.e.,* iff T is onto.

## EXERCISE 8

1. Which of the following L.T.'s are one-to-one, onto or both one-to-one and onto ?
   (*i*) $T(x_1, x_2, x_3) = (x_1 - x_2, x_2 - x_3, x_3 - x_1)$
   (*ii*) $T(x_1, x_2, x_3) = (x_1 - x_2, x_2 - x_3)$ (*iii*) $T(x_1, x_2, x_3) = (x_1 - x_2, x_2)$.
2. Find R(T) and N(T) of the following linear transformations :
   (*i*) $T : R^2 \to R^2$ defined by $T(x_1, x_2) = (x_1 + x_2, x_1)$
   (*ii*) $T : R^2 \to R^3$ defined by $T(x_1, x_2) = (x_1, x_1 + x_2, x_2)$
   (*iii*) $T : R^3 \to R^3$ defined by $T(x_1, x_2, x_3) = (x_1, x_2, x_3)$
   (*iv*) $T : \int \to \int$ defined by $T(p(x)) = x\,p(x)$.

The images of a linearly independent set of vectors by a linear transformation may not form a linearly independent set. However, the following theorem says that a one-to-one linear transformation preserves linear independence and under any linear transformation, the set of pre-images of a linearly independent set of vectors is linearly independent.

## 1.21. RANK AND NULLITY

*If T is a linear transformation from a vector space U to a vector space V, then the dimension of range space R(T) of T is called the rank of T and is denoted by ρ(T). The dimension of null space N(T) of T is called the nullity of T and is denoted by μ(T).*

**Theorem 37 *(Sylvestor's Law).*** *If T : U(F) → V(F) is a linear transformation on an n-dimensional vector space U, then*

$$\text{Rank } (T) + \text{Nullity } (T) = \text{Dimension } U.$$

**Proof.** Since null space N(T) is a subspace of finite dimensional vector space U, let the set

$$A = \{u_1, u_2, \ldots\ldots, u_k\}, \ (k \le n)$$

be a basis set of N(T).

$\therefore$ Nullity of $T = \mu(T) = k$ ...(1)

Now, extend the set A to a basis of U(F).

Let $B = \{u_1, u_2, \ldots\ldots, u_k, u_{k+1}, \ldots, u_n\}$ be a basis of U

($\because$ U is $n$th dimensional vector space).

**We claim.** The set $C = \{T(u_{k+1}), T(u_{k+2}), \ldots\ldots, T(u_n)\}$ is a basis of R(T).

**Firstly, we show that the set C is L.I.**

Let $a_{k+1}\, T(u_{k+1}) + a_{k+2}\, T(u_{k+2}) + \ldots + a_n\, T(u_n) = \mathbf{0}$ ...(2)

$\Rightarrow \quad T(a_{k+1}u_{k+1} + u_{k+2}u_{k+2} + \ldots + a_n u_n) = \mathbf{0}$

$\Rightarrow \quad a_{k+1}u_{k+1} + a_{k+2}u_{k+2} + \ldots + a_n u_n \in N(T).$

Since A is a basis set of N(T),

$$a_{k+1}u_{k+1} + a_{k+2}u_{k+2} + \ldots + a_n u_n$$

can be expressed as a linear combination of elements of A.

NOTES

Let $a_{k+1}u_{k+1} + a_{k+2}u_{k+2} + ... + a_n u_n = b_1 u_1 + b_2 u_2 + .... + b_k u_k$

$\Rightarrow \quad b_1 u_1 + b_2 u_2 + ... + b_k u_k - a_{k+1}u_{k+1} - ... - a_n u_n = \mathbf{0}$

$\Rightarrow \quad b_1 = b_2 = ... = b_k = 0$ and $a_{k+1} = ... = a_n = 0$

($\because$ B is a basis of U)

$\therefore$ From (2), C is L.I.

**Secondly, we show that C spans R(T).**

Let $v$ be any element of R(T).

$\therefore$ There exists an element $u \in$ U such that

$$T(u) = v \quad ...(3)$$

Since B is a basis of U, therefore $u$ can be expressed as a linear combination of elements of B.

Let $\quad u = a_1 u_1 + a_2 u_2 + ... + a_k u_k + ... + a_n u_n.$

$\Rightarrow \quad T(u) = T(a_1 u_1 + a_2 u_2 + ... + a_k u_k + ... + a_n u_n)$

$\quad = a_1 T(u_1) + a_2 T(u_2) + ... + a_k T(u_k) + ... + a_n T(u_n) \quad ...(4)$

Since $u_1, u_2, ......, u_k \in$ N(T), we have

$\therefore \quad T(u_i) = \mathbf{0}$ for $i = 1, 2, 3, ....., k$

$\therefore$ From (4), $\quad v = a_{k+1} T(u_{k+1}) + ..... + a_n T(u_n)$

$\Rightarrow$ The set C spans R(T).

Hence, the set C is a basis of R(T).

$\therefore$ Dimension of R(T) = number of elements in a basis set C.

$\quad = n - k$

$\Rightarrow \quad \rho(T) = n - k$

$\Rightarrow \quad \rho(T) + \mu(T) = n. \quad (\because \mu(T) = k)$

**Example 3.** *If $T : R^2 \to R^3$ is a L.T. defined by $T(x_1, x_2) = (x_1 - x_2, x_2 - x_1, - x_1)$, then find a basis and dimension for its R(T) and N(T).*

*Also verify that $\rho(T) + \mu(T) = 2$(= dimension of $R^2$).*

**Sol.** We know that

$$N(T) = \{(x_1, x_2) \mid T(x_1, x_2) = \mathbf{0} \in R^3\}.$$

Let $(x_1, x_2)$ be any element of N(T).

$\Rightarrow \quad T(x_1, x_2) = \mathbf{0}$

$\Rightarrow \quad (x_1 - x_2, x_2 - x_1, - x_1) = (0, 0, 0)$

$\Rightarrow \quad x_1 - x_2 = 0, x_2 - x_1 = 0, - x_1 = 0$

Solving, we have $\quad x_1 = x_2 = 0.$

$\therefore$ (0, 0) is the only member of N(T). *i.e.*, N(T) = {0}.

$\therefore$ Nullity of T = dimension of N(T) = 0.

**To find R(T) and its dimension**

Since $\quad T(x_1, x_2) = (x_1, x_2, x_2 - x_1, - x_1)$

$\therefore \quad R(T) = \{(x_1 - x_2, x_2 - x_1, - x_1) \mid (x_1, x_2) \in R^2\}. \quad ...(1)$

Let $v$ be any element of R(T).

$\therefore$ There exists $(x_1, x_2) \in R^2$ such that

$$T(x_1, x_2) = v.$$

Now, $\quad (x_1, x_2) = x_1(1, 0) + x_2 (0, 1) = x_1 e_1 + x_2 e_2$

$\Rightarrow \quad v = T(x_1, x_2) = T(x_1 e_1 + x_2 e_2) = x_1 T(e_1) + x_2 T(e_2) \quad ...(2)$

But $\left.\begin{array}{l} T(e_1) = T(1,0) = (1-0, 0-1, -1) = (1,-1,-1) \\ T(e_2) = T(0,1) = (0-1, 1-0, 0) = (-1,1,0) \end{array}\right\}$ [By (1)]

NOTES

Substituting values of $T(e_1)$ and $T(e_2)$ in (2), we have

$$v = T(x_1, x_2) = x_1 (1, -1, -1) + x_2(-1, 1, 0)$$

Therefore every vector $v$ of R(T) is a linear combination of vectors $(1, -1, -1)$ and $(-1, 1, 0)$.

Moreover, $(1, -1, -1)$ and $(-1, 1, 0)$ are L.I. because neither vector is a multiple of the other.

Hence, $\{(1, -1, -1), (-1, 1, 0)\}$ is a basis of R(T)

$\therefore$ Dimension of R(T) = 2.

Since dimension of $R^2$ is 2.

$\therefore$ Rank T + Nullity T = Dimension of $R^2$.

## 1.22. OPERATIONS ON A LINEAR TRANSFORMATION

### Addition of Linear Transformations

Let $L(R^n, R^m)$ be the set of all linear transformations from $R^n$ to $R^m$. If $T, S \in L(R^n, R^m)$, we denote the sum of T and S by T + S and is defined by $(T + S)(X) = T(X) + S(X)$.

Now, $\quad T + S \in L(R^n, R^m)$

For, 
$$\begin{aligned}(T + S)(X + Y) &= T(X + Y) + S(X + Y)\\ &= (T(X) + T(Y)) + (S(X) + S(Y))\\ &= (T(X) + S(X)) + (T(Y) + S(Y))\\ &= (T + S)(X) + (T + S)(Y)\end{aligned}$$

and 
$$\begin{aligned}(T + S)(\lambda.X) &= T(\lambda.X) + S(\lambda.X) = \lambda.T(X) + \lambda.S(X)\\ &= \lambda(T(X) + S(X)) = \lambda((T + S)(X))\end{aligned}$$

If $A = [a_{ij}]$, $B = [b_{ij}]$, $C = [c_{ij}]$ are the matrices associated with the linear transformations T, S and T + S, then the natural question is : What is the relationship between A, B and C ?

If $X = (x_1, x_2, \ldots\ldots, x_n)$, $Y = (y_1, y_2, \ldots\ldots, y_m)$ and $Z = (z_1, z_2, \ldots\ldots, z_m)$ are such that T(X) = Y and S(X) = Z, then we have

$$\left.\begin{array}{l} y_i = \sum_{j=1}^{n} a_{ij} x_j,\ i = 1, 2, \ldots\ldots, m \\ \text{and} \quad z_i = \sum_{j=1}^{n} b_{ij} x_j,\ i = 1, 2, \ldots\ldots m \end{array}\right\} \quad \ldots(1)$$

Now, 
$$\begin{aligned}(T + S)(X) &= T(X) + S(X) = (y_1, y_2, \ldots\ldots, y_m) + (z_1, z_2, \ldots\ldots, z_m)\\ &= (y_1 + z_1, y_2 + z_2, \ldots\ldots, y_m + z_m) \quad \ldots(2)\end{aligned}$$

$\therefore$ From (1) and (2),

$$y_i + z_i = \sum_{j=1}^{n} (a_{ij} + b_{ij}) x_j,\ i = 1, 2, \ldots\ldots, m$$

Thus, *the matrix associated to* $T + S$ *is* $C = [a_{ij} + b_{ij}]$, $1 \le i \le m$, $1 \le j \le n$ *which is the sum of the matrices A and B.*

### Scalar Multiplication

NOTES

For a transformation $T \in L(R^n, R^m)$ and $\lambda \in R$, we define the function $\lambda T : R^n \to R^m$ by $(\lambda T)(X) = \lambda T(X) = (\lambda y_1, \lambda y_2, ......, \lambda y_m)$

if $$T(X) = (y_1, y_2, ......., y_m)$$

One can verify that $\lambda T \in L(R^n, R^m)$

If $A = [a_{ij}]$ is the matrix associated with T, then

$$y_i = a_{i1}x_1 + a_{i2}x_2 + ...... + a_{in}x_n, \; i = 1, 2, ....., m$$

so that $$\lambda y_i = \lambda a_{i1}x_1 + \lambda a_{i2}x_2 + ...... + \lambda a_{in}x_n, \; i = 1, 2, ......., m$$

Thus, *the matrix associated to* $\lambda T$ is $[\lambda a_{ij}]$.

---

## EXERCISE 9

1. For each of the following linear transformations, find a basis and the dimension of:

   (*i*) its range space (*ii*) its null space.

   Also verify that rank (T) + Nullity (T) = dim. U

   (*a*) $T : R^2 \to R^3$ such that $T(x_1, x_2) = (x_1 + x_2, x_1 - x_2, x_2)$

   (*b*) $T : R^3 \to R^2$ such that $T(x, y, z) = (x + y, y + z)$.

2. Find a linear transformation $T : R^3 \to R^4$ whose range is spanned by the vectors $(1, 2, 0, -4)$ and $(2, 0, -1, -3)$.

3. Let $T_1$ and $T_2$ be two linear operators defined on $R^2$ as

   $$T_1(x, y) = (x + y, 0) \quad \text{and} \quad T_2(x, y) = (-y, x).$$

   Find a formulae defining the operators

   (*i*) $T_1 o T_2$ (*ii*) $T_2 o T_1$ (*iii*) $T_1^2 (= T_1 o T_1)$.

## 1.23. ISOMORPHISM

*Two vector spaces U(F) and V(F) are said to be isomorphic vector spaces if there exists a one-one and onto linear transformation T from U(F) to V(F) and we write U(F) ≅ V(F). The one-one and onto linear transformation T is called an isomorphism of U onto V.*

**Theorem 38.** *Every n-dimensional vector space U(F) is isomorphic to* $F^n$.

**Proof.** Let $\{u_1, u_2, ......, u_n\}$ be a basis of U.

Then, each $u \in U$, can be written as :

$$u = a_1u_1 + a_2u_2 + ...... + a_nu_n \text{ for scalars } a_1, a_2, ......., a_n.$$

Define a function $T : U \to F^n$ by

$$T(u) = (a_1, a_2, ......, a_n).$$

*We shall show that T is an isomorphism.*

(*i*) *To show T is one-one.*

Let $u, v \in U$.

$\Rightarrow \quad u = a_1u_1 + a_2u_2 + \ldots\ldots + a_nu_n$ for some scalars $a_1, a_2, \ldots\ldots, a_n$

and $\quad v = b_1u_1 + b_2u_2 + \ldots\ldots + b_nu_n$ for some scalars $b_1, b_2, \ldots\ldots, b_n$.

$\therefore \quad T(u) = (a_1, a_2, \ldots\ldots, a_n)$ and $T(v) = (b_1, b_2, \ldots\ldots, b_n)$

Now, $\quad T(u) = T(v)$

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

$\Rightarrow \quad a_1 - b_1 = 0, a_2 - b_2 = 0, \ldots\ldots, a_n - b_n = 0$

$(\because \; u_1, u_2, \ldots\ldots, u_n$ are L.I.)

$\Rightarrow \quad a_i = b_i$, for $i = 1, 2, \ldots\ldots, n$.

$\Rightarrow \quad u = v$.

Hence T is one one.

(*ii*) **To show :** *T is onto*

If $(a_1, a_2, \ldots\ldots, a_n)$ is any element of $F^n$, then $a_1u_1 + a_2u_2 + \ldots\ldots + a_nu_n \in U$ such that $T(a_1u_1 + a_2u_2 + \ldots\ldots + a_nu_n) = (a_1, a_2, \ldots\ldots, a_n)$

Hence, T is onto.

(*iii*) **To show :** *T is a L.T*

Let $u, v \in U$ and $a, b$ scalars.

Then, $u = a_1u_1 + a_2u_2 + \ldots\ldots + a_nu_n$ for some scalars $a_1, a_2, \ldots\ldots, a_n$

and $\quad v = b_1u_1 + b_2u_2 + \ldots\ldots + b_nu_n$ for some scalars $b_1, b_2, \ldots\ldots, b_n$.

$\therefore \quad au + bv = (aa_1 + bb_1)u_1 + \ldots\ldots + (aa_n + bb_n)u_n$

$\therefore \quad T(au + bv) = (aa_1 + bb_1, \ldots\ldots, aa_n + bb_n)$

Also, $\quad aT(u) + bT(v) = a(a_1, a_2, \ldots\ldots, a_n) + b(b_1, b_2, \ldots\ldots, b_n)$

$= (aa_1 + bb_1, aa_2 + bb_2, \ldots\ldots, aa_n + bb_n)$

$\therefore \quad T(au + bv) = aT(u) + bT(v)$.

$\therefore$ T is a L.T.

Hence, T is an isomorphism

or $\quad U \simeq F^n$.

## 1.24. EIGEN VALUES AND EIGEN VECTORS IN A LINEAR TRANSFORMATION

**Definition.** *Let $T : V \to V$ be a linear operator on an n-dimensional vector space over the field F. A scalar $\lambda \in F$ is called the* **eigen value** *of T if there exists a non-zero vector $v \in V$ such that $T(v) = \lambda v$ and any $v \neq \mathbf{0}$ of V such that $T(v) = \lambda v$ is called an eigen vector of T associated with the eigen value $\lambda$.*

**Note.** (*i*) Eigen value is also known as proper value, characteristic value, spectral value or latent value. Similarly, Eigen vector is also called proper vector, characteristic vector, spectral vector or latent vector.

(*ii*) If $v$ is an eigen vector of T corresponding to the eigen value $\lambda$, then every scalar multiple $kv$ $(k \neq 0)$ of $v$ is also an eigen vector corresponding to $\lambda$, because

$$T(kv) = kT(v) = k(\lambda v) = \lambda(kv)$$

(*iii*) The set of all eigen values of T is called the spectrum of T.

NOTES

(*iv*) If A is an $n$-square matrix associated with the linear operator $T : V \to V$ (dim $V = n$ say), then we can define eigen value as a root of $(A - \lambda I) X = O$ and the non-zero solution X as the eigen vector. This concept, the students have already studied in B.A./B.Sc. I.

**Theorem 39.** *Let $T : V \to V$ be a linear operator on a finite dimensional vector space V(F). If $v \in V$ is an eigen vector of T, then v cannot be associated with more than one eigen value of T.*

**Proof.** Let, if possible, $v$ corresponds to two different eigen values $\lambda_1, \lambda_2$ of T.

$$\therefore \quad T(v) = \lambda_1 v \quad \text{and} \quad T(v) = \lambda_2 v$$

$$\Rightarrow \quad \lambda_1 v = \lambda_2 v \quad \Rightarrow \quad (\lambda_1 - \lambda_2) v = \mathbf{0}$$

$$\Rightarrow \quad v = \mathbf{0} \qquad (\because \lambda_1 \neq \lambda_2)$$

which is not possible as $v$ being an eigen vector must be non-zero.

Hence, $v$ cannot be associated with more than one eigen value of T.

**Theorem 40.** *Let λ be an eigen value of a linear operator T on a vector space V(F). Then, the set $V_\lambda$ of all eigen vectors of T corresponding to eigen value λ, is a subspace of V(F).*

**Proof.** Here, $V_\lambda = \{v \in V \mid v \text{ is an eigen vector of T corresponding to } \lambda\}$

$$= \{v \in V \mid T(v) = \lambda v\}$$

Since λ is an eigen value of T, there exists a non-zero vector $v'$ such that

$$T(v') = \lambda v'.$$

$$\therefore \quad v' \in V_\lambda \quad \Rightarrow \quad V_\lambda \neq \phi.$$

Let $v_1, v_2 \in V_\lambda$ and $a, b \in F$.

$$v_1, v_2 \in V_\lambda \quad \Rightarrow \quad T(v_1) = \lambda v_1 \quad \text{and} \quad T(v_2) = \lambda v_2$$

Now, $\quad T(av_1 + bv_2) = T(av_1) + T(bv_2) \qquad (\because$ T is a L.T.)

$\qquad = aT(v_1) + bT(v_2) \qquad (\because$ T is a L.T.)

$\qquad = a(\lambda v_1) + b(\lambda v_2) = \lambda(av_1 + bv_2)$

$\Rightarrow \quad av_1 + bv_2$ is an eigen vector corresponding to λ.

$\Rightarrow \quad av_1 + bv_2 \in V_\lambda$.

Hence, $V_\lambda$ is a subspace of V.

**Note.** *This subspace $V_\lambda$ is called the eigen space or the characteristic space of the eigen value λ.*

---

## EXERCISE 10

1. Find all the eigen values and basis for eigen space if the linear operator $T : R^2 \to R^2$ is given by $T(x, y) = (x + 2y, 3x + 2y)$.
2. For each of the following operator $T : R^3 \to R^3$, find the eigen values and a basis for each eigen space.

   (*a*) $T(x, y, z) = (2x + y, y - 3, 2y + 4z)$

   (*b*) $T(x, y, z) = (x + y + z, 2y + z, 2y + 3z)$.
3. Find all the eigen values and basis for each eigen space of linear operator

   $T : R^3 \to R^3$ defined by

   $$T(x, y, z) = (3x + y + 4z, 2y + 6z, 5z).$$

## 1.25. BILINEAR FORMS

NOTES

***Bilinear Forms.*** *Let $V_m (= R^m)$ and $V_n (= R^n)$ be two vector spaces over the same field F. Let X and Y be any two arbitrary vectors of $V_m$ and $V_n$ respectively. Then, a bilinear form over F is a function f of two vector variables X, Y and satisfying the following properties.*

(*i*) $f(aX_1 + X_2, Y) = af(X_1, Y) + f(X_2, Y) \quad \forall X_1, X_2 \in V_m, Y \in V_n, a \in F$

and (*ii*) $f(X, aY_1 + Y_2) = af(X, Y_1) + f(X, Y_2), \quad \forall X \in U_m, Y_1, Y_2 \in V_n, a \in F.$

For a fixed $Y \in V_n$, $f(X, Y)$ defines a linear function from $V_m \to F$ and for a fixed X, $f(X, Y)$ defines a linear function from $V_n \to F$.

Because of this linear function properties w.r.t. two vector spaces $V_m$ and $V_n$ when considered separately, $f(X, Y)$ is called a bilinear form.

**For example,** (*i*) Consider a function $f : R^3 \times R^2 \to R$ defined by

$$f(X, Y) = x_1y_1 + 2x_1y_2 + x_2y_2 + 3x_3y_1,$$

where $$X = (x_1, x_2, x_3), Y = (y_1, y_2).$$

Then $f(X, Y)$ defines a bilinear form.

For, let $$X_1 = (x_{11}, x_{12}, x_{13}), X_2 = (x_{21}, x_{22}, x_{23})$$

and $$Y_1 = (y_{11}, y_{12}) \quad \text{and} \quad Y_2 = (y_{21}, y_{22})$$

(We are using double suffix notation to denote elements of vectors where the first suffix indicates the vector and second suffix indicates its element).

Let $(X_1, Y_1), (X_2, Y_2) \in R^3 \times R^2$ such that $(X_1, Y_1) = (X_2, Y_2)$

$$\Rightarrow \quad x_{11} = x_{21}, x_{12} = x_{22}, x_{13} = x_{23} \quad \text{and} \quad y_{11} = y_{21}, y_{12} = y_{22} \qquad ...(1)$$

Now, $$f(X_1, Y_1) = x_{11}y_{11} + 2x_{11}y_{12} + x_{12}y_{12} + 3x_{13}y_{11}$$
$$= x_{21}y_{21} + 2x_{21}y_{22} + x_{22}y_{22} + 3x_{23}y_{21} = f(X_2, Y_2).$$

$\Rightarrow$ image under $f$ is unique.

*To show that f satisfies the linearity conditions (i) and (ii) of the definition.*

$$f(aX_1 + X_2, Y_1) = (ax_{11} + x_{21})y_{11} + 2(ax_{11} + x_{21})y_{12} + (ax_{12} + x_{22})y_{12} + 3(ax_{13} + x_{23})y_{11}$$
$$= a(x_{11}y_{11} + 2x_{11}y_{12} + x_{12}y_{12} + 3x_{13}y_{11}) + (x_{21}y_{11} + 2x_{21}y_{12} + x_{22}y_{12} + 3x_{23}y_{11})$$
$$= a\,f(X_1, Y_1) + f(X_2, Y_1), \quad \forall a \in R$$

Similarly, we can show that

$$f(X_1, aY_1 + Y_2) = a\,f(X_1, Y_1) + f(X_2, Y_1), \quad \forall a \in R.$$

Hence, $f$ is a bilinear form.

(*ii*) Consider a function $f : R^2 \times R^2 \to R$ defined by

$$f(X, Y) = x_1y_1 + x_2y_2 + 1$$

where $$X = (x_1, x_2) \quad \text{and} \quad Y = (y_1, y_2).$$

Then, $f$ is not a bilinear form

Infact $f$ does not satisfy the linearity property as shown below.

Let $$X_1 = (x_{11}, x_{12}), X_2 = (x_{21}, x_{22}) \quad \text{and} \quad Y = (y_1, y_2)$$

Then, $$aX_1 + X_2 = a(x_{11}, x_{12}) = (x_{21}, x_{22})$$
$$= (ax_{11} + x_{21}, ax_{12} + x_{22}), \quad \forall a \in R$$

NOTES

Now, $f(aX_1 + X_2, Y) = (ax_{11} + x_{21})y_1 + (ax_{12} + x_{22})y_2 + 1$

and $af(X_1, Y) + f(X_2, Y) = a(x_{11}y_1 + x_{12}y_2 + 1) + (x_{21}y_1 + x_{22}y_2 + 1)$

$\therefore$ $f(aX_1 + X_2, Y) \neq af(X_1, Y) + f(X_2, Y)$

Hence $f$ is not a bilinear form.

## Effect of Linear Transformations on a Bilinear Form

Let the $m$ $x$'s of the bilinear form $X'AY = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}\, x_i y_j$ be changed to new variables $u$'s using the linear transformation

$$x_i = \sum_{j=1}^{n} b_{ij}\, u_j, \ (i = 1, 2, ..., m) \text{ or } X = BU$$

and the $n$ $y$'s be replaced by new variables $v$'s using the linear transformation

$$y_i = \sum_{j=1}^{n} c_{ij}\, v_j, \ (i = 1, 2, ...., n) \text{ or } Y = CV.$$

Then, $X'AY = (BU)'\, A(CV) = U'(B'AC)V = U'DV$ where

$$D = B'AC.$$

*Thus, a bilinear form remains a bilinear form when subjected to linear transformations.*

Applying the linear transformations U = IX and V = IY, we obtain a new bilinear form $(IX)'(B'AC)\,(IY) = X'(B'AC)Y = X'DY$ in the original variables.

## EXERCISE 11

1.* Express the following bilinear forms in the matrix notation and find the matrix of the bilinear form :

(i) $x_1y_1 + 2x_1y_2 - x_1y_3 + 7x_2y_1 - x_2y_2 + 3x_2y_3 + x_3y_1 - 5x_3y_2$

(ii) $2x_1y_1 + x_1y_3 - 2x_2y_1 + 7x_2y_2 - 2x_2y_3$

(iii) $2x_1y_1 - x_1y_2 + x_2y_2 - x_3y_2$

(iv) $-2x_1y_1 - x_1y_2 + 2x_2y - x_3y_1 + 3x_3y_2$

(v) $3x_1y_1 + x_1y_2 + x_2y_1 - 2x_2y_2 - 4x_2y_3 - 4x_3y_3 + 3x_3y_3$

which of the above forms are symmetric ?

2. Write the bilinear forms corresponding to the matrix A in the variables X and Y when

(i) $A = \begin{bmatrix} 2 & 3 & 5 \\ -2 & 1 & 7 \end{bmatrix}$, $X = (x_1, x_2)$, $Y = (y_1, y_2, y_3)$

(ii) $A = \begin{bmatrix} 0 & 5 & -1 \\ 7 & 0 & 9 \\ 1 & 3 & 1 \end{bmatrix}$, $X = (x_1, x_2, x_3)$, $Y = (y_1, y_2, y_3)$

(iii) $A = \begin{bmatrix} 1 & 5 \\ -2 & 1 \\ 3 & 5 \end{bmatrix}$, $X = (x_1, x_2, x_3)$, $Y = (y_1, y_2)$.

## SUMMARY


- An algebraic system (G, *) is said to be a group if it satisfies the following properties.
  (*i*) The operation * is a closed operation.
  (*ii*) The operation * is an associative operation.
  (*iii*) There exists an identity element w.r.t. the operation *.
  (*iv*) For every $a \in G$, there exist an element $a^{-1} \in G$ such that $a^{-1} * a = a * a^{-1} = e$
- A group (G, *) is called a finite group if G is a finite set.
- The order of the group G is the number of elements in the group G.
- A homomorphism $\phi$ which is one-one and onto is called isomorphism and the groups G and G' are called isomorphic.
- A ring R with finite number of elements is known as finite ring, otherwise it is known as infinite ring.
- A commutative ring F with unity such that each non-zero element has a multiplicative inverse *i.e.*, $Ea^{-1} \in F$ such that $aa^{-1} = 1 = a^{-1}a$ is called field.
- Vector space is also called the linear space.
- 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 $V_2$ 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.
- Let U and V be any two vector spaces over the same field F. Then a function (map or mapping) $T : U \to V$ is called a linear transformation (Written as L.T.) if
  (*i*) $T(u_1 + u_2) = T(u_1) + T(u_2) \quad \forall \mu_1, \mu_2 \in U$
  and (*ii*) $T(au) = aT(u) \quad \forall \mu \in U$ and $a \in F$.
- A linear transformation T which is onto is called surjective.
- Eigen value is also known as proper value, characteristic value, spectral value or latent value.
- A bilinear form is a special type of function involving two different real or complex vector variables having the value of the function in a real or complex field F.


## TEST YOURSELF

1. Let S = N × N, the set of ordered pairs of positive integers with the operation * defined by
   $(a, b) * (c, d) = (ad + bc, bd)$
   (*a*) Find (3, 4) * (1, 5) and (2, 1) * (4, 7)
   (*b*) Is S a semi-group ? Is S commutative ?
2. Prove that if H, K are subgroups of a group G and $H \cup K = G$. Then either H = G or K = G.
3. Show that the intersection of any number of subgroups of G is a subgroup of G.
4. Let G be a group and $a, b \in G$. Then the equation $x * a = b$ has a unique solution given by $x = b * a^{-1}$.
5. Prove that if $x^2 = 1$ in an integral domain D, then $x = 0$ or $x = 1$.
6. If R is a ring with unity, then this unity is unique.
7. Prove that the ring $Z_2 \times Z_3$ is commutative and has unity.
8. If J and K are ideals in a ring R, then J + K and $J \cap K$ are also ideals in R.
9. (*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.

NOTES

10. 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 $a \in Q, u \in R$.

11. Show that the set $\{x^3 - x + 1, x^3 + 2x + 1, x + 1\}$ is L.I. in the vector space of all polynomials over the field of reals.

12. Prove that the vectors $(a_1, a_2)$ and $(b_1, b_2)$ in $V_2(F)$ are L.D. if $a_1 b_2 - a_2 b_1 = 0$.

13. Show that the L.T. $T : R^2 \to R^2$ defined by

$$T(x_1, x_2) = (x_1 \cos\theta + x_2 \sin\theta, -x_1 \sin\theta + x_2 \cos\theta)$$

is a bijective (*i.e.*, an isomorphism).

14. (*a*) Show that the L.T. $T : R^2 \to R$ defined by $T(x_1, x_2) = x_1$ is onto but not one to one.

(*b*) Show that the L.T. $T : R^3 \to R^3$ defined by

$$T(x, y, z) = (x, ay, z)$$

where $a$ is a fixed real number is an isomorphism.

15. Given the linear transformation $Y = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 3 & 1 \\ -2 & 3 & 5 \end{bmatrix} X$, show that (*i*) it is singular (*ii*) the images of the linearly independent vectors $X_1 = (1, 1, 1)$, $X_2 = (2, 1, 2)$ and $X_3 = (1, 2, 3)$ are linearly dependent.

16. Show that $T : R^3 \to R^3$ defined by $T(x, y, z) = (x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta, z)$ is non-singular for all values of θ.

17. Let P and Q be two $n \times n$ matrices over a field F and X an eigen vector of both the matrices P and Q. Show that X is also an eigen vector of the matrix $\alpha P + \beta Q$ where $\alpha, \beta \in F$.

18. Obtain the linear transformation which reduce each of the following bilinear forms to the canonical form :

(*i*) $x_1y_1 + 2x_1y_2 - x_1y_3 + 2x_2y_1 + 3x_2y_3 - x_3y_1 + 3x_3y_2 + x_3y_3$

(*ii*) $X' \begin{bmatrix} 3 & 2 & -1 \\ 3 & 2 & 3 \\ -1 & 3 & 1 \end{bmatrix} Y$ (*iii*) $X' \begin{bmatrix} 1 & -5 & 1 & 0 \\ 4 & 1 & 1 & 5 \\ -5 & 2 & 3 & 0 \end{bmatrix} Y$ (*iv*) $X' \begin{bmatrix} 1 & 2 & 3 \\ -2 & 1 & 3 \\ 1 & 1 & -2 \\ 3 & 7 & 0 \end{bmatrix}$

NOTES

# Block–2
# Graph Theory

## UNIT 1

# FUNDAMENTAL CONCEPTS, ALGORITHMS AND APPLICATIONS

### STRUCTURE

NOTES

## 1.1. OBJECTIVES

After going through this unit, you will be able to discuss about graphs, multigraphs, weighted graphs, planar graphs, directed and undirected graphs, graph colouring and covering, trees and rooted trees and various algorithms related to graphs and trees.

## 1.2. INTRODUCTION

In many problems dealing discrete objects and binary relations, a graphical representation of the objects and the binary relations on them is a very convenient form of representation. This leads us naturally to a study of the theory of graphs.

Also, we will discuss about special class of graphs, called trees. It is essential to know the various common types of trees, their basic properties and applications.

## 1.3. GRAPH TERMINOLOGY

The graphs consist of points or nodes called vertices which are connected to each other by way of lines called edges. These lines may be directed or undirected.

## 1.4. ENUMERATION OF GRAPHS

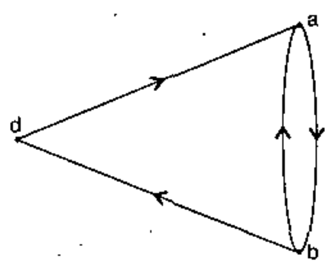
**Directed Graph**

A directed graph is defined as an ordered pair (V, E) where V is a set and E is a binary relation on V. A directed graph can be represented geometrically as a set of marked points V with a set of arrows E between pairs of points. Also,

The elements in V are called **vertices.**

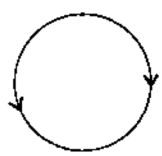
The ordered pairs in E are called **edges.**

For *e.g.*, consider the Fig. 1 given below. It is a directed graph.




Directed graph

**Fig. 1**



Loop

**Fig. 2**

Here, the vertices are $a$, $b$, $d$ and the edges are $(a; b)$, $(b, a)$, $(b, d)$, $(d, a)$.

An edge is said to be ***incident*** with the vertices it joins. For example, the edge $(a, b)$ is *incident* with the vertices $a$ and $b$. Also, we say that the edge $(a, b)$ is *incident* from vertex $a$ and incident into vertex $b$.

The vertex $a$ is called the **initial vertex** and the vertex $b$ is called the **terminal vertex** of the edge $(a, b)$.

An edge that is incident from and into the same vertex is called a **loop** or **self-loop.** (Fig. 2).

Degree of a self-loop is two as it is twice incident on a vertex.

Corresponding to an edge $(a, b)$, the vertex $a$ is said to be **adjacent** to the vertex $b$ and the vertex $b$ is said to be adjacent from the vertex $a$.

A vertex is said to be an **isolated** vertex if there is no edge incident with it.

*For example*, consider the following graph (Fig. 3)

The vertex '$a$' has a **self-loop**. $\therefore$ deg $a = 4$

The vertex '$b$' is a **Pendent** vertex since only one edge is incident on it.

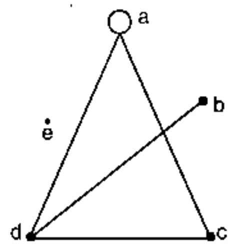



**Fig. 3**

The vertex '$e$' is an **isolated** vertex as it has no edge incident on it. Also deg $e = 0$.

**Undirected Graph**

An undirected graph G consists of a set of vertices, V and a set of edges E. The edge set contains the unordered pair of vertices. If $(u, v) \in$ E then we say $u$ and $v$ are connected by an edge where $u$ and $v$ are vertices in the set V.

*For example, let* $V = \{1, 2, 3, 4\}$ *and* $E = \{(1, 2), (1, 4), (3, 4), (2, 3)\}$. *Draw the graph.*

The graph can be drawn in several ways.

Two of which are as follows (Fig. 4 and Fig. 5). These are directed graphs.

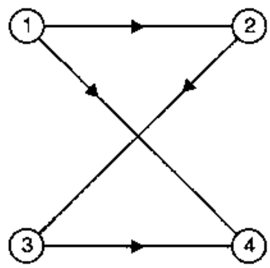



**Fig. 4**

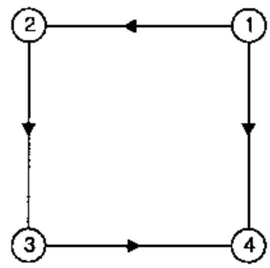



**Fig. 5**

*Consider the graph shown in Fig. 6. Determine the edge set and the vertex set of this undirected graph.*

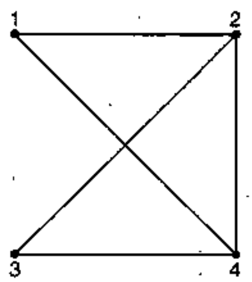



**Fig. 6**

The edge set is E = {(1, 2), (1, 4), (2, 3), (2, 4), (3, 4)}
The vertex set is V = {1, 2, 3, 4}.

NOTES

### Mixed Graph

A graph G = [V, E] in which some edges are directed and some are undirected is called a mixed graph. The graph shown in Fig. 7 is a mixed graph.

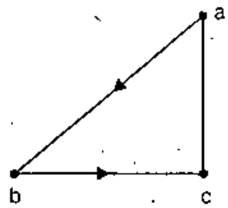



**Fig. 7**

### Finite graph

A graph G = [V, E] is said to be finite if V and E are finite sets.

### Linear graph

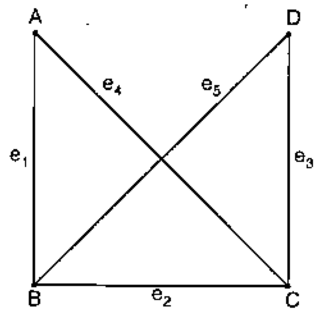
A graph G = (V, E) is said to be a linear graph if its edges joining vertices lie along a line. *For example,*  is a linear graph.

### Discrete or null graph

A graph containing only vertices and no edge is called a **discrete** or **null graph**. The set E of edges in a graph G = [V, E] is empty in a discrete graph. Also each vertex in a discrete graph is an isolated vertex.

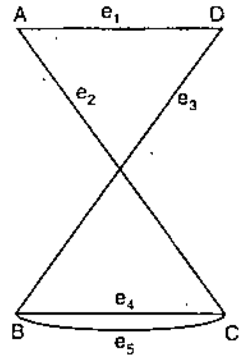
### Simple Graph

A simple graph is one for which there is no more one edge directed from any one vertex to any other vertex. All other graphs are called **multigraphs.** (see Figs. 8, 9)




Simple graph

**Fig. 8**




Multigraph

**Fig. 9**

In Fig. 9, the edges $e_4$ and $e_5$ are called **multi edges.**

### Complement Graph

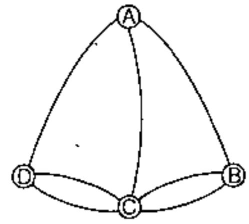
The complement of a graph is defined to be a graph which has the same number of vertices as in graph G and has two vertices connected iff they are not connected in the graph G.

### Degree

Let $v$ be a vertex of an *undirected graph.* The degree of $v$, denoted by $d(v)$, is the number of edges that connect $v$ to the other vertices in the graph. The degree of a graph cannot be negative.

### InDegree and OutDegree

If $v$ is a vertex of a *directed graph,* then the *outdegree* of $v$, denoted by outless ($v$), is the number of edges of the graph that initiate $v$. The *indegree* of $v$, denoted by indeg($v$), is the number of edges that terminate at $v$. For *e.g.,* consider the graph shown in Fig. 10. The degrees of A, B, C, D are 3, 3, 5, and 3 respectively.



Multigraph

**Fig. 10**

### Source and Sink

A vertex with indegree 0 is called a *source* and a vertex with outdegree 0 is called a **sink.**

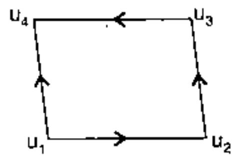


**Fig. 11**

*For example,* consider the graph shown in Fig. 11. Here $u_4$ is a sink.

*For example*, consider the graph shown below (Fig. 12)

The graph shown in Fig. 12 has 7 edges.

Indegree of '$a$' = 3, Indegree of '$b$' = 2;

Indegree of '$c$' = 1, Indegree of '$d$' = 1

Also, outdegree of '$a$' = 1, outdegree of '$b$' = 3

outdegree of '$c$' = 0, $\therefore$ $c$ is a **sink.**

outdegree of '$d$' = 3.

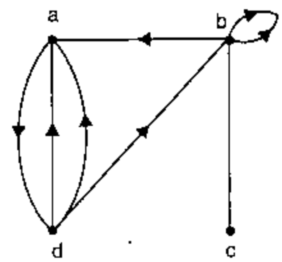


**Fig. 12**

### Even and Odd Vertex

A vertex is said to be **even vertex** if its degree is an even number.

A vertex is said to be an **odd vertex** if its degree is an odd number.

*For example,* consider the graph, as shown in Fig. 13.

The vertices A and D are even vertices since deg(A) = 2, deg(D) = 2

The vertices B and C are odd vertices since deg(B) = 3, deg(C) = 3

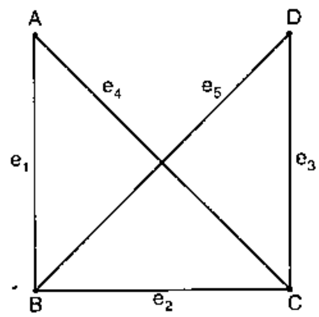


**Fig. 13**

A vertex of degree zero is called ***isolated vertex.***

A vertex with degree one is called a **pendent vertex**. The only edge which is incident with a pendent vertex is called the **pendent edge.**

### Adjacent Vertices

Two vertices are called adjacent if they are connected by an edge. If there is an edge ($e_1$, $e_2$), then we say that vertex $e_1$ is adjacent to vertex $e_2$ and vertex $e_2$ is adjacent to vertex $e_1$.

**Theorem 1.** *Show that the sum of degree of all the vertices in a graph G, is even.*

**Proof.** Each edge contribute two degrees in a graph. Also, each edge contributes one degree to each of the vertices on which it is incident.

NOTES

Hence, if there are N edges in G, then we have

$$2N = d(v_1) + d(v_2) + ......+ d(v_N)$$

Thus, 2N is always even.

**Another statement.** The sum of the degrees of the vertices of a graph G is equal to twice the number of edges in G.

**Theorem 2.** *Prove that in any graph, there are an even number of vertices of odd degree.*

**Proof.** Consider a graph having vertices of degree even and odd. Now, make two groups of vertices. One with even degree of vertices $v_1, v_2, ..., v_k$ and other with odd degree of vertices $u_1, u_2, ..., u_n$.

Suppose,

$$V = d(v_1) + d(v_2) + ... + d(v_k)$$

$$U = d(u_1) + d(u_2) + ... + d(u_n).$$

Now, we know that sum of degree of all the vertices is even (Theorem I). So, V + U is even.

Since, V is the sum of K even numbers. Hence, it is even. But U is the sum of $n$ odd numbers. So, to be U an even number, $n$ must be even. Hence proved.

## ILLUSTRATIVE EXAMPLES

**Example 1.** *Verify that the sum of the degree of all the vertices is even for the graph shown in Fig. 14.*

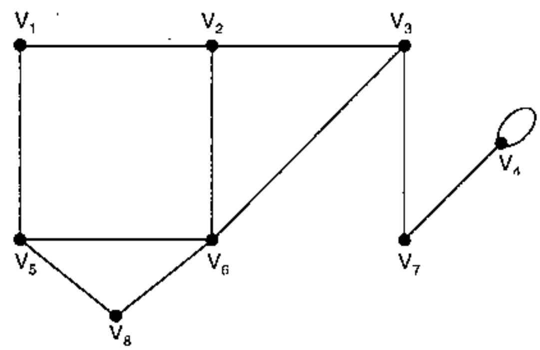



**Fig. 14**

**Sol.** The sum of degree of all the vertices is

$$= d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) + d(v_6) + d(v_7) + d(v_8)$$

$$= 2 + 3 + 3 + 3 + 3 + 4 + 2 + 2 = 22, \text{ which is even.}$$

**Example 2.** *Verify that there are an even number of vertices of odd degree in the graph shown in Fig. 15.*

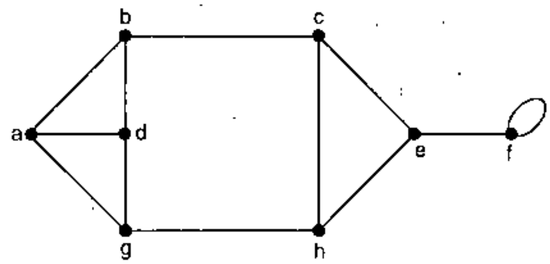



**Fig. 15**

**Sol.** The number of vertices of degree odd are 8 and each have degree three in the above graph. Hence, we have even number of vertices of odd degree.

## 1.5. PATHS AND CIRCUIT

A path of length $n$ is a sequence of $n + 1$ vertices of a graph in which each pair of vertices is an edge of the graph.

1. **A Simple Path.** The path is called simple one if no edge is repeated in the path *i.e.*, all the vertices are distinct except that first vertex equal to last vertex.

2. **An Elementary Path.** The path is called elementary one if no vertex is repeated in the path *i.e.*, all the vertices are distinct.

3. **Circuit or Closed Path.** The circuit or closed path is a path which starts and ends at the same vertex *i.e.*, $v_0 = v_n$.

4. **Simple Circuit Path.** The simple circuit is a simple path which is a circuit.

**Theorem 3 (*a*).** *Suppose a graph G contains two distinct paths from a vertex u to a vertex v. Show that G has a cycle.*

**Proof.** Consider two distinct paths from $u$ to $v$ be $P_1 = (e_1, e_2, e_3, \ldots\ldots, e_n)$ and $P_2 = (e_1', e_2', e_3', \ldots\ldots, e_n')$.

Now delete from the paths $P_1$ and $P_2$ all the initial edges which are identical *i.e.*, of we have $e_1 = e_1', e_2 = e_2', e_3 = e_3', \ldots\ldots, e_k = e_k'$ but $e_{k+1} \neq e'_{k+1}$. We will delete all the first $k$ edges of both the paths $P_1$ and $P_2$.

Now, after deleting the $k$ edges both the paths start from the same vertex, (let $u_1$) and end at $v$.

Now, to construct a cycle, start from vertex $u$, and follow the left over path of $P_1$ until we first meet any vertex of the left over path of $P_2$.

If this vertex is $u_2$, then the remaining cycle is computed by following the left over path of $P_2$ which starts from $u_2$ and ends at $v$.

**Theorem 3 (*b*).** *If a graph has n vertices and vertex v is connected to vertex w, then there exists a path from v to w of length no more than n.*

**Proof.** We prove this theorem by method of contradiction. Let us assume that $v$ is connected to $w$, and the shortest path from $v$ to $w$ has length $m$, where $m$ is greater than $n$.

We know that, a vertex list for a path of length $m$ will have $m + 1$ vertices. This path can be represented as $v_0, v_1, v_2 \ldots v_m$, where $v_0 = v$ and $v_m = w$.

Now since there are only $n$ distinct vertices and $m$ vertices are listed in the path after $v_0$, thus there must be same duplicated vertices in the last $m$ vertices of the vertex list, that represents a circuit in the path. Thus our assumption is not true and the minimum path length can be reduced, which is a contradiction.

NOTES

**Example 3.** *Consider the graph shown in Fig. 16. Give an example of the following :*

(*i*) *A simple path from* $V_1$ *to* $V_6$.

(*ii*) *An elementary path from* $V_1$ *to* $V_6$.

(*iii*) *A simple path which is not elementary from* $V_1$ *to* $V_6$.

(*iv*) *A path which is not simple and starting from* $V_2$.

(*v*) *A simple circuit starting from* $V_1$.

(*vi*) *A circuit which is not simple and starting from* $V_2$.

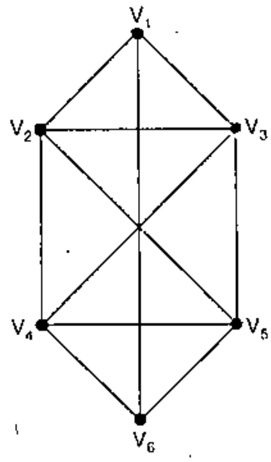


**Fig. 16**

**Sol.** (*i*) A simple path from $V_1$ to $V_6$ is

$V_1, V_2, V_3, V_4, V_5, V_6$.

(*ii*) An elementary path from $V_1$ to $V_6$ is

$V_1, V_2, V_3, V_5, V_4, V_6$.

(*iii*) A simple path which is not elementary from $V_1$ to $V_6$ is

$V_1, V_2, V_3, V_5, V_2, V_4, V_6$.

(*iv*) A path which is not simple and starting from $V_2$ is

$V_2, V_3, V_4, V_5, V_3, V_4, V_6$.

(*v*) A simple circuit starting from $V_1$ is

$V_1, V_2, V_4, V_6, V_5, V_3, V_1$.

(*vi*) A circuit which is not simple and starting from $V_2$ is

$V_2, V_3, V_1, V_2, V_5, V_4, V_2$.

**Undirected Complete Graph**

An undirected complete graph G = (V, E) of $n$ vertices is a graph in which each vertex is connected to every other vertex *i.e.*, and edge exists between every pair of distinct vertices. It is denoted by $K_n$. A complete graph with $n$ vertices will have $n(n-1)/2$ edges.

The complete graph $k_n$ for $n$ = 1, 2, 3, 4, 5, 6 are shown below:

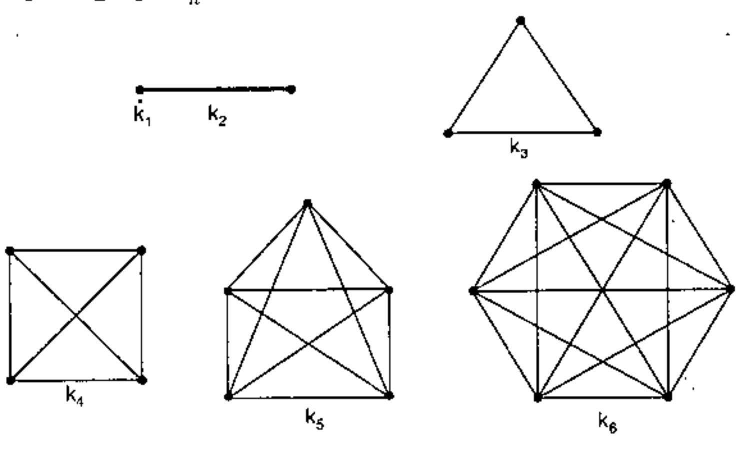


**Fig. 17**

**Example 4.** *Draw undirected complete graphs $K_4$ and $K_6$.*

**Sol.** The undirected complete graph of $K_4$ is shown in Fig. 17(*a*) and that of $K_6$ is shown in Fig. 18.

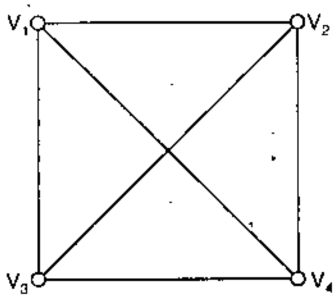



**Fig. 17.(*a*)** $K_4$

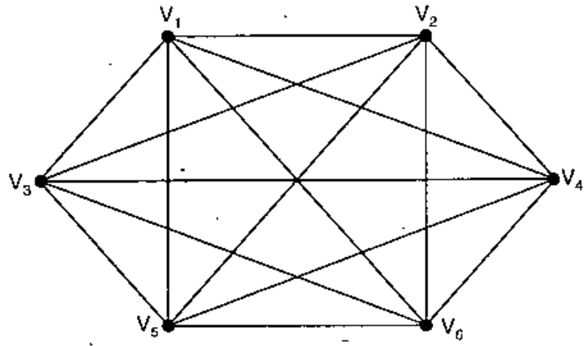



**Fig. 18.** $K_6$

**Connected Graph**

A graph is called connected if there is a path from any vertex $u$ to $v$ or vice-versa.

**Disconnected Graph**

A graph is called disconnected if there is no path between any two of its vertices.

**Connected Component**

A subgraph of graph G is called the connected component of G, if it is not contained in any bigger subgraph of G, which is connected. It is defined by listing its vertices.

**Example 5.** *Consider the graph shown in Fig. 19. Determine its connected components.*

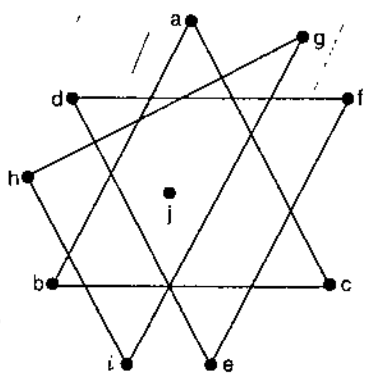



**Fig. 19**

**Sol.** The connected components of this graph is {*a*, *b*, *c*}, {*d*, *e*, *f*}, {*g*, *h*, *i*} and {*j*}.

**Theorem 4.** *Let G be a connected graph with at least two vertices. If the number of edges in G is less than the number of vertices, then prove that G has a vertex of degree 1.*

NOTES

**Proof.** Let G be a connected graph with $n \geq 2$ vertices. Because graph G is connected, G has no isolated vertices. Suppose G has no vertex of degree 1. Then the degree of each vertex is at least 2. This implies that the sum of the degrees of vertices of G is at least $2n$. Hence, it follows that the number of edges is at least $n$ ($\because$ the sum of the degrees of vertices in any graph is twice the number of edges), which is a contradiction. This implies that G contains at least one vertex of degree 1.

## 1.6. SUBGRAPH

A subgraph of a graph G = (V, E) is a graph G′ = (V′, E′) in which $V' \subseteq V$ and $E' \subseteq E$ and each edge of G′ has the same end vertices in G′ as in graph G.

**Note.** A single vertex is a subgraph.

**Example 6.** *Consider the graph G shown in Fig. 20. Show the different subgraphs of this graph.*

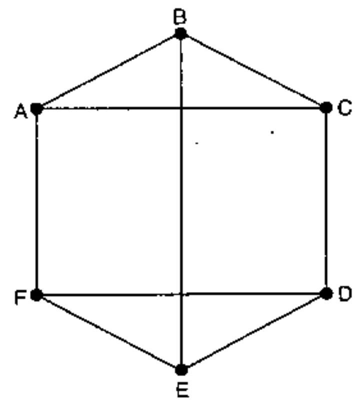



**Fig. 20**

**Sol.** The following are all subgraphs of the above graph (shown in Figs. 21, 22, 23, 24). There may be another subgraphs of this graph.

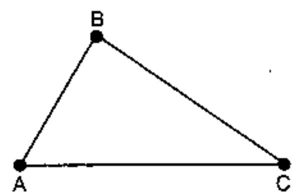



**Fig. 21**

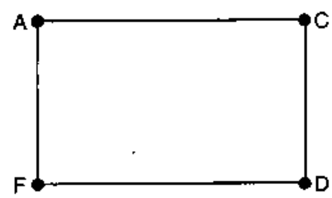



**Fig. 22**

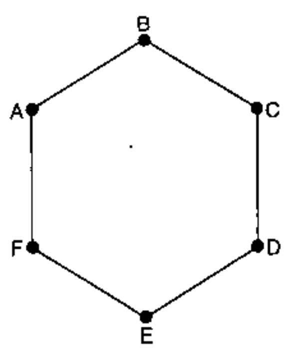



**Fig. 23**

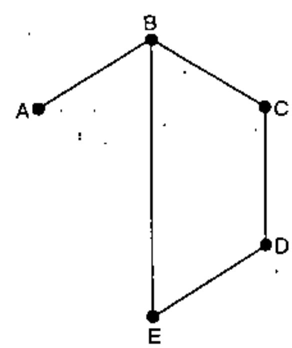



**Fig. 24**

**Example 7.** *Consider the multigraph shown in Fig. 25. Show two different subgraphs of this multigraph which are itself multigraphs.*

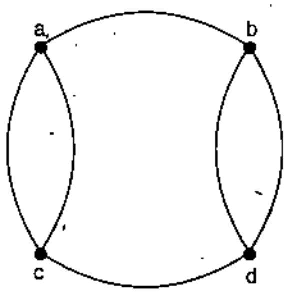



**Fig. 25**

**Sol.** The two different subgraphs of this multigraph which are itself multigraphs are shown in Figs. 26 and 27. There may be another subgraphs of this multigraph.

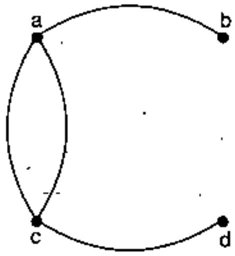



**Fig. 26**

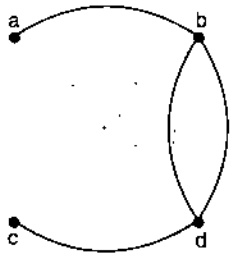



**Fig. 27**

## Spanning Subgraph

A graph $G_1 = (V_1, E_1)$ is called a spanning subgraph of $G = (V, E)$ if $G_1$ contains all the vertices of G and $E \neq E_1$.

**For example :** The Fig. 28 is the spanning subgraph of the graph shown in Fig. 29.

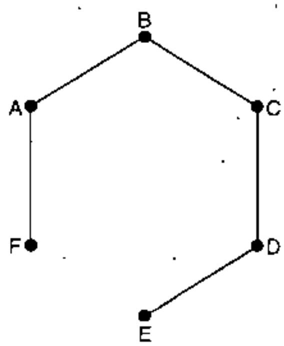



**Fig. 28.** Spanning Subgraph.

## Complement of a graph

Let $G = (V, E)$ be a given graph. A graph $\overline{G} = (\overline{V}, \overline{E})$ is said to be complement of $G = (V, E)$ If $\overline{V} = V$ and $\overline{E}$ does not contain edges of E. *i.e.*, edges in $\overline{E}$ are join of those pairs of vertices which are not joined in G.

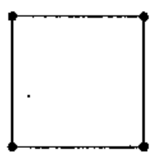


**Fig. 29**

NOTES

Consider the graph shown in Fig. 29.

The complement graph is shown in Fig. 30.

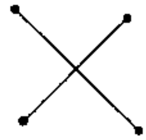


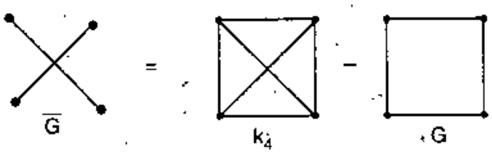
**Fig. 30**

Note that a graph and its complement graph have same vertices.

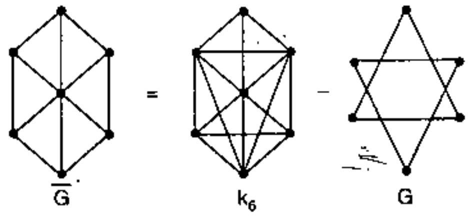
If a graph G has $n$ vertices and $K_n$ is a complete graph with $n$ vertices, then

$$\overline{G} = K_n - G$$

Consider $K_4$. Then



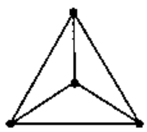
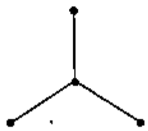

Consider $K_6$. Then

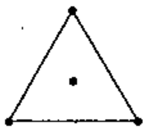



**Complement of a Graph**

Let G = (V, E) be a graph and S be a subgraph of G. If edges of S be deleted from the graph G, the graph so obtained is complement of subgraph S. It is denoted by $\overline{S}$.

$\therefore \quad \overline{S} = G - S$

Consider the graph  and its subgraph  Then the complement of subgraph S is

$\overline{S} =$ 

Note that in a complement of a subgraph, the number of vertices do not change.

## 1.7. CUT SET

Consider a connected graph G = (V, E). A cut set for G is a smallest set of edges such that removal of the set, disconnects the graph whereas the removal of any proper subset of this set, left a connected subgraph.

*For example, consider the graph shown in Fig. 31. We determine the cut set for this graph.*

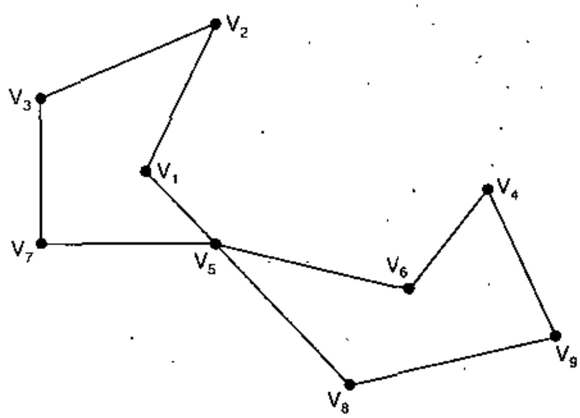



Fig. 31

For this graph, the edge set $\{(V_1, V_5), (V_7, V_5)\}$ is a cut set. After the removal of this set, we have left with a disconnected subgraph. While after the removal of any of its proper subset, we have left with a connected subgraph.

### Cut Points or Cut Vertices

Consider a graph G = (V, E). A cut point for a graph G, is a vertex $v$ such that $G-v$ has more connected components than G or disconnected.

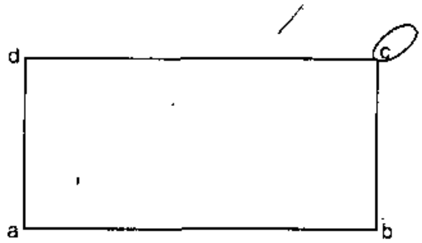
The subgraph $G-v$ is obtained by deleting the vertex $v$ from the graph G and also deleting all the edges incident on $v$.

## EXERCISE 1

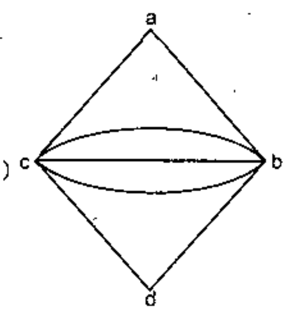
1. (*a*) If V = {1, 2, 3, 4, 5} and E = {(1, 2), (2, 3), (3, 3), (3, 4), (4, 5)}. Find the number of edges and size of graph G = (V, E)

   (*b*) Find the order and size of the graph G shown in the figure below :

(*i*)




(*ii*)




2. (*a*) A graph G has 16 edges and all vertices of G are of degree 2. Find the number of vertices.

   (*b*) A graph G has 21 edges, 3 vertices of degree 4 and other vertices are of degree 3. Find the number of vertices in G.

   (*c*) A graph G has 5 vertices, 2 of degree 3 and 3 of degree 2. Find the number of edges.

3. (*a*) How many nodes (vertices) are required to construct a graph with exactly 6 edges in which each node is of degree 2.

   (*b*) Show that there does not exist a graph with 5 vertices with degrees 1, 3, 4, 2, 3 respectively.

(c) Can there be a graph with 8 vertices and 29 edges?

(d) How many vertices are there is a graph with 10 edges if each vertex has degree 2?

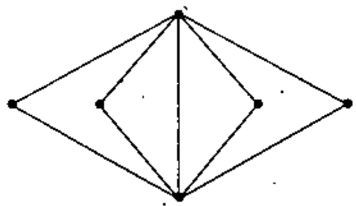
(e) Does there exist a graph with two vertices each of degree 4? If so, draw it.

NOTES

4. (a) Draw a simple graph with 3 vertices

(b) Draw a simple graph with 4 vertices

5. Consider the graph G shown below:



(a) Is G simple?

(b) What is order and size of incidence matrix for G.

(c) Find minimum and maximum degree for G.

## 1.8. WEIGHTED GRAPHS

A graph G = (V, E) is called a weighted graph if each edge of graph G is assigned a positive number $w$ called the weight of the edge $e$. For example,

The graph shown in Figs. 32 and 33 is a weighted graph.

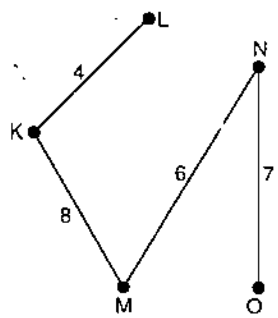



**Fig. 32**

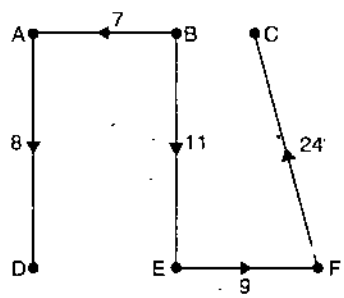



**Fig. 33**

### Multiple Edges

Two edges $e_1$ and $e_1'$ which are distinct are said to be multiple edges if they connect the end points *i.e.*, if $e_1 = (u, v)$ and $e_1' = (u, v)$ then $e_1$ and $e_1'$ are multiple edges.

## 1.9. MULTIGRAPH

A multigraph G = (V, E) consists of a set of vertices V and a set of edges E such that edge set E may contain multiple edges and self loops. For *e.g.*, Consider the following graph shown in Fig. 34.

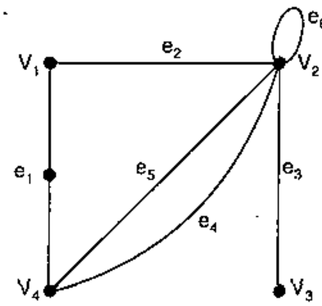



**Fig. 34.** Undirected Multigraph.

In the above Fig. 35, $e_4$ and $e_5$ are multiple edges, $e_6$ is a self-loop.

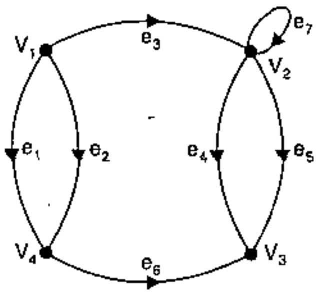



**Fig. 35.** Directed Multigraph.

In the graph shown in Fig. 35, the edges $e_1$, $e_2$ and $e_4$, $e_5$ are multiple edges $e_7$ is a loop.

## 1.10. REPRESENTATION OF GRAPHS

There are two important ways to represent a graph G with the matrices *i.e.,*

I. Adjacency matrix representation.

II. Incidence matrix representation.

### (*a*) Representation of Undirected Graph

(*i*) **Adjacency matrix representation.** If an undirected graph G consists of $n$ vertices, then the adjacency matrix of graph is an $n \times n$ matrix $A = [a_{ij}]$ and defined by

$$a_{ij} = \begin{cases} 1, \text{ if } \{v_i, v_j\} \text{ is an edge } i.e., v_i \text{ is adjacent to } v_j \\ 0, \text{ if there is no edge between } v_i \text{ and } v_j \end{cases}$$

If there exists an edge between vertex $v_i$ and $v_j$, where $i$ is a row and $j$ is a column then value of $a_{ij} = 1$.

If there is no edge between vertex $v_i$ and $v_j$, then value of $a_{ij} = 0$.

Note that adjacency matrix of G is a symmetric matrix. Since simple graph does not contain any self loop, so diagonal entries of adjacency matrix are all zero. Further, as adjacency matrix contains 0 or 1, so it is also known as Boolean matrix.

**Note.** *Degree of a vertex $v_i$ in G is equal to sum of entries in the ith row or ith column of the adjacency matrix.*

For example, *we find the adjacency matrix $M_A$ of graph G shown in Fig.36.*

NOTES

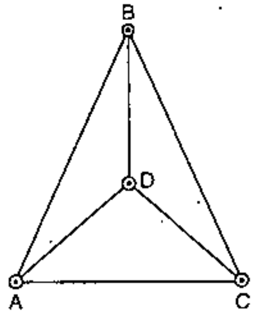



**Fig. 36**

Since the graph G consists of four vertices. Therefore, the adjacency matrix will be a 4 × 4 matrix. The adjacency matrix is as follows in Fig. 37.

$$M_A = \begin{array}{c} \\ A \\ B \\ C \\ D \end{array}\begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

degree of vertex '*c*' is 3 which is equal to sum of entries in third row 6/4 mm of adjacency matrix.

**Fig. 37**

**Adjacency List.** In a adjacency list of a graph, we list each vertex followed by the vertices adjacent to it. First write vertices of graph in a vertical column, then after each vertex, write the vertices adjacent to it.

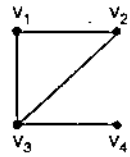



**Fig. 38**

Consider the graph shown in Fig. 38 the adjacency list is given below :

$v_1$; $v_2$, $v_3$

$v_2$; $v_1$, $v_3$

$v_3$; $v_1$, $v_2$, $v_4$

$v_4$; $v_3$

(*ii*) **Incidence matrix or Binary matrix representation.** If an undirected graph consists of $n$ vertices and $m$ edges, then the incidence matrix is an $n \times m$ matrix $C = [c_{ij}]$ defined by

$$c_{ij} = \begin{cases} 1, \text{ if the vertex } v_i \text{ incident by edge } e_j \\ 0, \text{ otherwise} \end{cases}$$

There is a row for every vertex and a column for every edge in the incidence matrix.

Note that incidence matrix of a graph need not be a square matrix. Entries in a row are added to give degree of corresponding vertex.

For example ;

Consider the graph $G = [V, E.]$

where $V = [v_1, v_2, v_3, v_4]$, $E = [e_1, e_2, e_3]$ as

shown in Fig. 39.

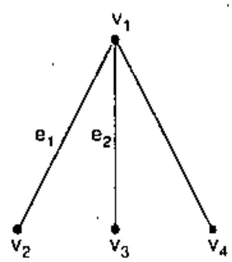



**Fig. 39**

The incidence matrix $M_1$ for G is shown below :

$$M_1 = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccc} e_1 & e_2 & e_3 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

Since each edge in the graph is incident on $v_1$,

$\therefore$ first row for $v_1$ has all entries 1.

$\therefore$ degree $v_1 = 1 + 1 + 1 = 3$

Also $v_2$, $v_3$, $v_4$ are pendant vertices.

In incidence matrix of a graph, sum of entries in column is not degree of vertex. As an edge is incident on two vertices in a graph, therefore, each column of incidence matrix will have two 1's.

The number of one's in an incidence matrix of undirected graph (without loops) is equal to the sum of degrees of all the vertices of the graph.

**For example :** *Consider the undirected graph G as shown in Fig. 40. We find its incidence matrix $M_I$.*

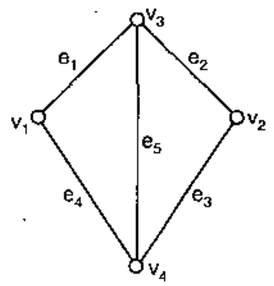



**Fig. 40**

**Sol.** The undirected graph consists of four vertices and five edges. Therefore, the incidence matrix is a 4 × 5 matrix, which is shown below :

$$M_1 = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \end{array}$$

**Fig. 40(a)**

### (*b*) Representation of Directed Graph

(*i*) **Adjacency matrix representation.** If a directed graph G consists of $n$ vertices, then the adjacency matrix of graph is an $n \times n$ matrix $A = [a_{ij}]$ defined by

$$a_{ij} = \begin{cases} 1, \text{ if } v_i, v_j \text{ is an edge } i.e., \text{ if } v_i \text{ is initial vertex and } v_j \text{ is final vertex} \\ 0, \text{ if there is no edge between } v_i \text{ and } v_j \end{cases}$$

If there exists an edge between vertex $v_i$ and $v_j$ with $v_i$ as initial vertex and $v_j$ as final vertex, then value of $a_{ij} = 1$.

If there is no edge between vertex $v_i$ and $v_j$ then value of $a_{ij} = 0$.

The number of one's in the adjacency matrix of a directed graph is equal to the number of edges.

NOTES

**For example :** *Consider the directed graph shown in Fig. 41. We determine its adjacency matrix* $M_A$.

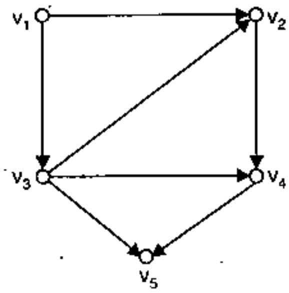



**Fig. 41**

**Sol.** Since the directed graph G consists of five vertices. Therefore, the adjacency matrix will be a 5 × 5 matrix. The adjacency matrix of the directed graph is as follows in Fig. 42.

$$M_A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

**Fig. 42**

(*ii*) **Incidence matrix representation.** If a directed graph consists of $n$ vertices and $m$ edges then the incidence matrix is an $n \times m$ matrix $C = [c_{ij}]$, defined by

$$c_{ij} = \begin{cases} 1, & \text{if } v_i \text{ is initial vertex of edge } e_j \\ -1, & \text{if } v_i \text{ is final vertex of edge } e_j \\ 0, & \text{if } v_i \text{ is not incident on edge } e_j \end{cases}$$

The number of one's in the incidence matrix is equal to the number of edges in the graph.

*For example, Consider the directed graph G shown in Fig. 43. Find its incidence matrix* $M_I$.

**Sol.** The directed graph consists of four vertices and five edges. Therefore, the incidence matrix is a 4 × 5 matrix which is shown in Fig. 43.

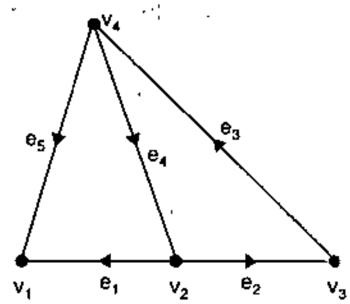



**Fig. 43**

$$M_I = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} -1 & 0 & 0 & 0 & -1 \\ 1 & 1 & 0 & -1 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 1 \end{bmatrix} \end{array}$$

**Fig. 44**

**(c) Representation of Multigraph**

Represented only by adjacency matrix representation.

(*i*) **Adjacency matrix representation of multigraph.** If a multigraph G consists of $n$ vertices, then the adjacency matrix of graph is an $n \times n$ matrix $A = [a_{ij}]$ and is defined by

$$a_{ij} = \begin{cases} N, \text{ If there are one or more than one edges between vertex } v_i \text{ and } v_j, \text{ where N is the number of edges.} \\ 0, \text{ otherwise.} \end{cases}$$

If there exists one or more than one edges between vertex $v_i$ and $v_j$ then $a_{ij} = N$, where N is the number of edges between $v_i$ and $v_j$.

If there is no edge between vertex $v_i$ and $v_j$ then value of $a_{ij} = 0$. For *e.g.*,

**For example :** *Consider the multigraph shown in Fig. 45. We determine its adjacency matrix.*

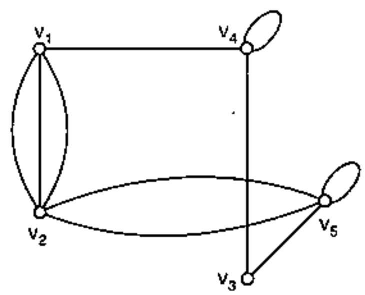



**Fig. 45**

**Sol.** Since the multigraph consists of five vertices. Therefore, the adjacency matrix will be an 5 × 5 matrix. The adjacency matrix of the multigraph is as follows in Fig. 46.

$$M_A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 0 & 3 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

**Fig. 46**

## ILLUSTRATIVE EXAMPLES

**Example 1.** *Draw the undirected graph represented by adjacency matrix $M_A$ shown in Fig. 47.*

$$M_A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

**Fig. 47**

NOTES

**Sol.** The graph represented by adjacency matrix $M_A$ is shown in Fig. 48.

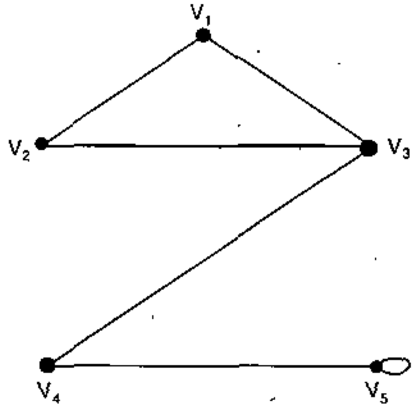



**Fig. 48**

**Example 2.** *Draw the directed graph G whose incidence matrix $M_I$ is shown in Fig. 49.*

$$M_I = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 \end{array} \\ \begin{bmatrix} -1 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & +1 & -1 & 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & -1 \end{bmatrix} \end{array}$$

**Fig. 49**

**Sol.** The directed graph corresponding to the incidence matrix $M_I$ is shown in Fig. 50.

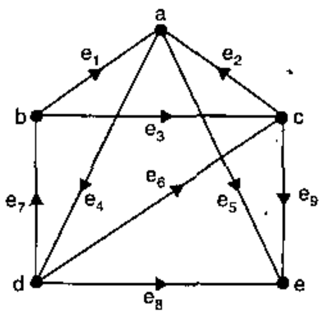
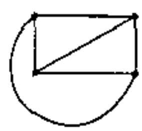



**Fig. 50**

## 1.11. PLANAR GRAPH

A graph is said to be planar if it can be drawn in a plane so that no edges cross.

For *e.g.*, the graph  is a planar graph. Also $K_4$ =  is a planar graph because it can be re-drawn as  in which edges do not cross each other.

*For example*: The graphs shown in Fig. 51 and Fig. 52 are planar graphs.

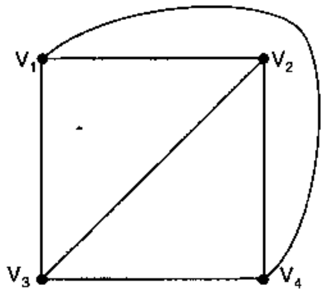



**Fig. 51**

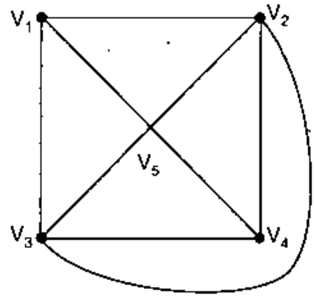



**Fig. 52**

**Theorem 5.** *A planar and connected graph has a vertex of degree less than or equal to 5.*

**Proof.** Let G be connected and planar and suppose, if possible, degree of each vertex $x \in$ G is greater than 5.

*i.e.*, $\deg x > 5 \Rightarrow \deg x \geq 6$ *i.e.*, sum of degree of all vertices $\geq 6v$

$\Rightarrow$ $2e \geq 6v$, where $e$ and $v$ are the number of edges and vertices respectively.

$\Rightarrow$ $e \geq 3v$, which contradicts $e \leq 3u - 6 < 3v$.

Hence $\deg x \leq 5$.

## Region of a Graph

Consider a planar graph G = (V, E). A region is defined to be an area of the plane that is bounded by edges and cannot be further subdivided. A planar graph divides the plane into one or more regions. One of these regions will be infinite.

(*a*) **Finite Region.** If the area of the region is finite, then that region is called finite region.

(*b*) **Infinite Region.** If the area of the region is infinite, that region is called infinite region. A planar graph has only one infinite region.

**Example 3.** *Consider the graph shown in Fig. 53. Determine the number of regions, finite regions and an infinite region.*

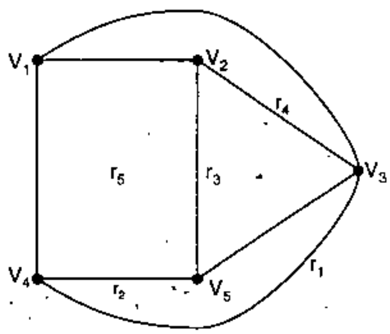



**Fig. 53**

**Sol.** There are five regions in the above graph *i.e.*, $r_1$, $r_2$, $r_3$, $r_4$ and $r_5$.

There are four finite regions in the graph *i.e.*, $r_2$, $r_3$, $r_4$ and $r_5$.

There is only one infinite region *i.e.*, $r_1$.

## Properties of Planar Graphs

NOTES

**Theorem I.** *If a connected planar graph G has e edges and r regions, then* $r \leq \frac{2}{3}e$.

**Theorem II.** *If a connected planar graph G has e edges and v vertices, then* $3v - e \geq 6$.

**Theorem III.** *A complete graph* $K_n$ *is planar if and only if* $n < 5$.

**I. Proof.** In a connected planar graph, each region is bounded by at least 3 regions

$\therefore$ $r$ regions are bounded by minimum $3r$ edges

$\Rightarrow$ Number of edges in graph $\geq 3r$

But number of edge in the graph = $2e$ (as each edge belongs to two regions)

$$\therefore \quad 2e \geq 3r$$

$$\Rightarrow \quad r \leq \frac{2e}{3}$$

**II.** Let $r$ be the no. of regions in a planar representation of G. $\therefore$ By Euler formula

$$v + r - e = 2 \qquad ...(1)$$

Now sum of degrees of the regions = $2e$. But each region has degree 3 or more.

$$\therefore \quad 2e \geq 3r \quad \Rightarrow \quad r \leq \frac{2e}{3}.$$

From (1) we get $\quad 2 = v + r - e \leq v + \frac{2e}{3} - e = v - \frac{e}{3}$

$$6 \leq 3v - e$$

$\Rightarrow \quad e \leq 3v - 6$ Hence proved.

**III.** If G has one or two vertices, then the result is true. If G has at least 3 vertices then

$$e \leq 3v - 6 \quad \text{or} \quad 2e \leq 6v - 12 \qquad ...(1)$$

If degree of every vertex were at least 6, then using $2e = \sum_{v \in V} \deg v$, we would have $2e \geq 6v$, which contradicts the inequality (1), Hence there must be a vertex with degree not greater than 5.

**Example 4.** *Prove that complete graph* $K_4$ *is planar.*

**Sol.** The complete graph $K_4$ contains 4 vertices and 6 edges.

We know that for a connected planar graph $3v - e \geq 6$. Hence for $K_4$, we have

$$3 \times 4 - 6 = 6 \text{ which satisfies the property (3).}$$

Thus $K_4$ is a planar graph. Hence proved.

## State and Prove Euler's Theorem

**Statement.** *Consider any connected planar graph G = (V, E) having R regions, V vertices and E edges. Then*

$$V + R - E = 2.$$

**Proof.** Use induction on the number of edges to prove this theorem.

Assume that the edges $e = 1$. Then we have two cases, graphs of which are shown in Figs. 54 and 55.

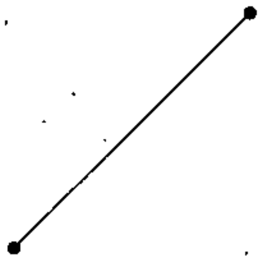


**Fig. 54**

**Fig. 55**

In Fig. 54 we have V = 2 and R = 1. Thus 2 + 1 – 1 = 2

In Fig. 55 we have V = 1 and R = 2. Thus 1 + 2 – 1 = 2. Hence, the result holds for $e = 1$.

Let us assume that the formula holds for connected planar graphs with K edges.

Let G be a graph with K + 1 edges.

Firstly, we suppose that G contains no circuits. Now, take a vertex $v$ and find a path starting at $v$. Since G is circuit free, whenever we find an edge, we have a new vertex. At last we will reach a vertex $v$ with degree 1. So we cannot move further as shown in Fig. 56.

Now remove vertex $v$ and the corresponding edge incident on $v$. So, we are left with a graph G* having K edges as shown in Fig. 57.

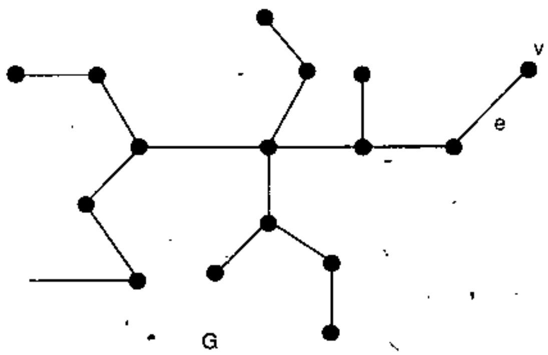



**Fig. 56. G.**

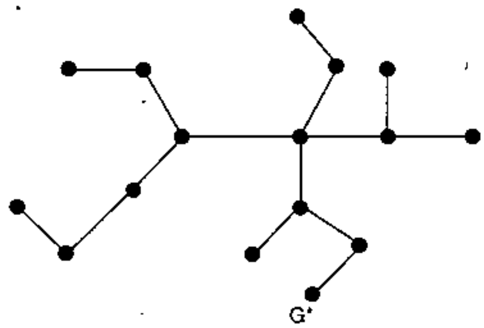



**Fig. 57. G*.**

Hence, by inductive assumption, Euler's formula holds for G*.

Now, since G has one more edge than G*, one more vertex than G* with same number of regions as in G*. Hence, the formula also holds for G.

Secondly, we assume that G contains a circuit and $e$ is an edge in the circuit shown in Fig. 58.

NOTES

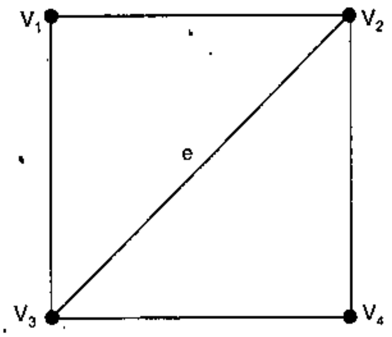



**Fig. 58**

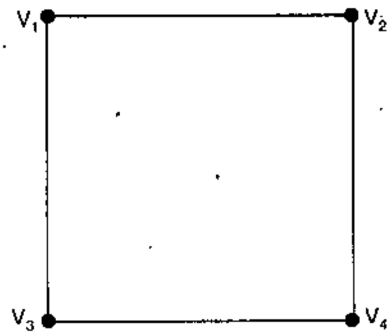



**Fig. 59**

Now, as $e$ is the part of a boundary for two regions. So, we only remove the edge and we are left with graph G* having K edges (Fig. 59).

Hence, by inductive assumption, Euler's formula holds for G*.

Now, since G has one more edge than G*, one more region than G* with same number of vertices as G*. Hence the formula also holds for G which, verifies the inductive step and hence proves the theorem.

**Example 5.** *Show that* $V - E + R = 2$ *for the connected planar graphs shown in Figs. 60 and 61.*

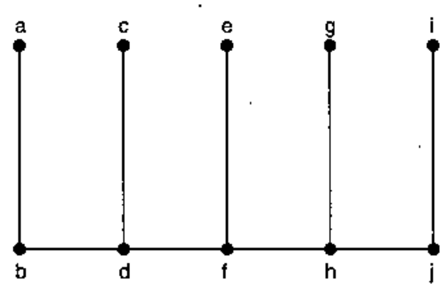



**Fig. 60**

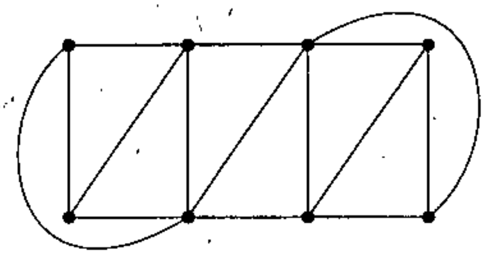


**Fig. 61**

**Sol.** (*i*) The graph shown in Fig. 60 contains vertices V = 10, edges E = 9 and regions R = 1. Putting the values, we have 10 – 9 + 1 = 2. Hence proved.

(*ii*) The graph shown in Fig. 61 contains vertices V = 8, edges E = 15 and regions R = 9. Putting the values, we have 8 – 15 + 9 = 2. Hence proved.

## 1.12. NON PLANAR GRAPHS

A graph is said to be non planar if it cannot be drawn in a plane so that no edges cross.

**For example :** The graphs shown in Figs. 62 and 63 are non planar graphs.

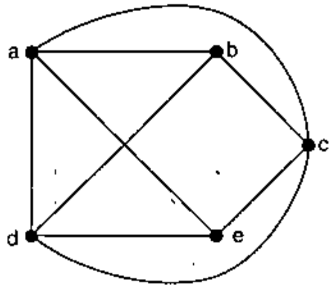



**Fig. 62**

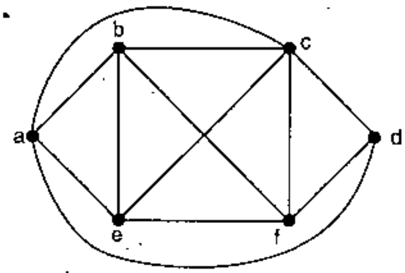



**Fig. 63**

These graphs cannot be drawn in a plane so that no edges cross hence they are non planar graphs.

**Properties of Non Planar Graphs**

A graph is non-planar if and only if it contains a subgraph homeomorphic to $K_5$ or $K_{3,3}$ [KURATOWSKI'S THEOREM].

**Example 6.** *Show that $K_5$ is non-planar. Fig. 64.*

**Sol.** Clearly $K_5$ is a connected. Also we show $K_5$ is non planar. For,

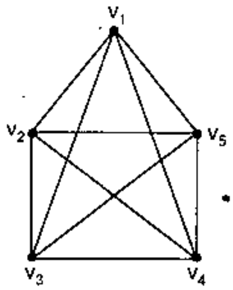



**Fig. 64**

$$v = 5, e = 10$$

If, $K_5$ is planar then, $e \leq 3v - 6$

$\Rightarrow$ $10 \leq 3(5) - 6$

$\Rightarrow$ $10 \leq 15 - 6$

$\Rightarrow$ $10 \leq 9$, a contradiction

$\therefore$ The graph $K_5$ is non planar.

**Remark.** If $e \leq 3v - 6$ does not hold, then G is always non planar. But if this condition holds, then we cannot conclude that G is planar.

**Theorem 6.** *Prove that every planar graph has at least one vertex of degree 5 or less than 5.*

**Proof.** Consider a graph G, whose all vertices are of degree 6 or more, then the sum of the degrees of all the vertices would be greater than or equal to $6v$. We know that the sum of the degrees of the vertices is twice the number of edges. Therefore, we have

$$6v \leq 2e$$

or $$v \leq \frac{e}{3} \quad ...(1)$$

But, any planar graph have the property,

$$r \leq \frac{2e}{3} \quad ...(2)$$

Also, from Euler's formula, we have

$$2 = v - e + r \quad ...(3)$$

NOTES

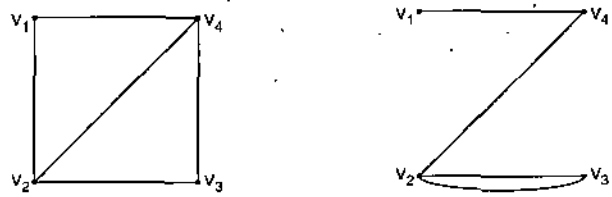
Now, putting the value of $v$ and $r$ from (1) and (2) in (3), we have

$$2 \leq \frac{e}{3} - e + \frac{2e}{3} = 0$$

Since, the statement $2 \leq 0$ is not true, hence we conclude that there must exist some vertex in G with degree 5 or less than 5.

## EXERCISE 2

**1.** Find the adjacency matrix $A = (a_{ij})$ of the graphs shown below :

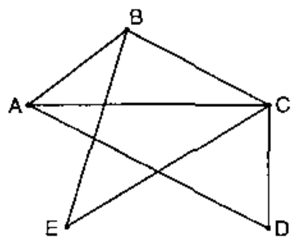



(*a*) (*b*)

**2.** Draw the graph G corresponding to each adjacency matrix.

(*a*) $A = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ (*b*) $A = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$

**3.** (*a*) Consider the graph (Fig. I) G show in the given figure. Verify Euler Theorem *i.e.*, V + R – E = 2.



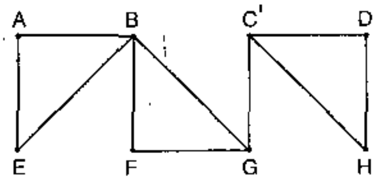
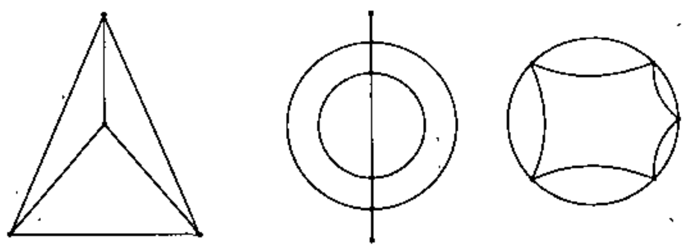




**Fig. I.** **Fig. II.**

(*b*) Verify Euler Theorem *i.e.*, V + R – E = 2 for the graph Fig. II.

**4.** (*a*) Verify Euler's formula for the following graphs :

(*b*) Show that if G is a bipartite simple graph with $u$ vertical and $e$ edges, then $e = \frac{u}{4}$.



(*a*) (*b*) (*c*)

**5.** Show that a connected graph G with $n$ vertices must have atleast $(n - 1)$ edges.

## 1.13. GRAPH COLOURING

Suppose that G = (V, E) is a graph with no multiple edges. A vertex colouring of G is an assignment of colours to the vertices of G such that adjacent vertices have different colours. A graph G is M-colourable if there exists a colouring of G which uses M-colours.

**Proper Colouring.** A colouring is proper if any two adjacent vertices $u$ and $v$ have different colours otherwise it is called improper colouring.

A graph can be coloured by assigning a different colour to each of its vertices. However, for most graphs a colouring can be found that uses fewer colours than the number of vertices in the graph.

### Chromatic number of G

The minimum number of colours needed to produce a proper colouring of a graph G is called the chromatic number of G and is denoted by $\chi(G)$.

The graph shown in Fig. 65 is minimum 3-colourable, hence $\chi(G) = 3$.

Similarly, for the complete graph $K_6$ we need six colours to colour $K_6$ since every vertex is adjacent to every other vertex and we need a different colour for each vertex. ∴ The chromatic number for $K_6$ is $\chi(K_6) = 6$. Similarly, the chromatic number of $K_{10}$ is $\chi(K_{10}) = 10$.

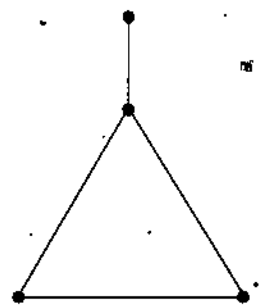


**Fig. 65**

### ILLUSTRATIVE EXAMPLES

**Example 1.** *The chromatic number of $K_n$ is n.*

**Sol.** A colouring of $K_n$ can be constructed using $n$ colours by assigning a different colour to each vertex. No two vertices can be assigned the same colour, since every two vertices of this graph are adjacent. Hence the chromatic number of $K_n = n$.

**Example 2.** *The chromatic number of complete bipartite graph $K_{m, n}$, where m and n are positive integers is two.*

**Sol.** The number of colours needed does not depend upon $m$ and $n$. However, only two colours are needed to colour the set of $m$ vertices with one colour and the set of $n$ vertices with a second colour. Since, edges connect only a vertex from the set of $m$ vertices and a vertex from the set of $n$ vertices, no two adjacent vertices have the same colour.

**Note 1.** Every connected bipartite simple graph has a chromatic number of 2 or 1.

**2.** Conversely, every graph with a chromatic number of 2 is bipartite.

**Example 3.** *The chromatic number of graph $c_n$, where $c_n$ is the cycle with n vertices is either 2 or 3.*

**Sol.** Two colours are needed to colour $c_n$, where $c_n$ is even. To construct such a colouring, simply pick a vertex and colour it black. Then move around the graph in clockwise direction colouring the second vertex white, the third vertex black, and so on. The $n$th vertex can be coloured white since the two vertices adjacent to it, namely the $(n - 1)$th and the first are both coloured black as shown in Fig. 66.

NOTES

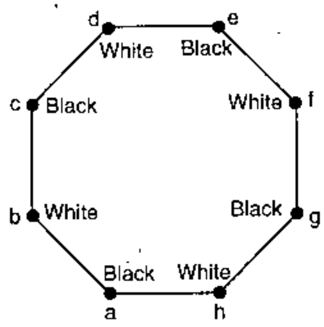



**Fig. 66**

When $n$ is odd and $n > 1$, the chromatic number of $c_n$ is 3. To construct such a colouring, pick an initial vertex. First use only two colours and alternate colours as the graph is traversed in a clockwise direction. However, the $n$th vertex reached is adjacent to two vertices of different colours, the first and $(n - 1)$th. Hence, a third colour is needed. (Fig. 67)

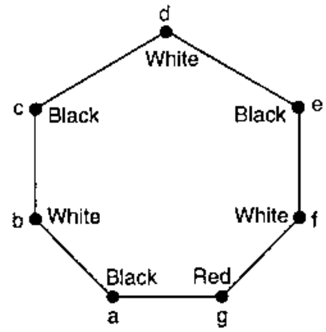



**Fig. 67**

**Example 4.** *Determine the chromatic number of the graphs shown in Fig. 68.*

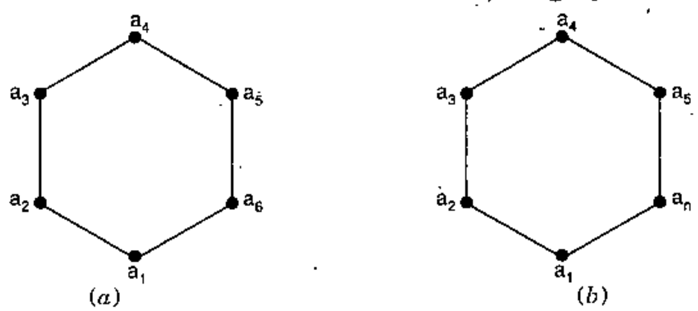



**Fig. 68**

**Sol.** The graphs shown in Fig. 68($a$), has the chromatic number $\chi(G) = 2$.

The graph shown in Fig. 68($b$) has the chromatic number $\chi(G) = 2$, when $n$ is an even number and $\chi(G) = 3$, where $n$ is odd.

**Theorem 7.** *If an undirected graph has a subgraph $K_3$, then its chromatic number is at least three.*

**Proof.** Let G be an undirected graph. As G contains a complete graph $K_3$, which is 3-colourable. ∴ G cannot be coloured with one or two colours

∴ $\psi(G) \geq 3$.

**Four Colour Theorem.** Every planar graph is four colourable.

**Five Colour Theorem.** Every planar graph has chromatic number ≤ 5.

**Theorem 8.** *The vertices of every planar graph can be properly coloured with five colours.*

**Proof.** We will prove this theorem by induction. All the graphs with 1, 2, 3, 4 or 5 vertices can be properly coloured with five colours. Now let us assume that every planar graph with $n - 1$ vertices can be properly coloured with five colours. Next, if we prove that any planar graph G with $n$ vertices will require no more than five colours, we have done.

Consider the planar graph G with $n$ vertices.

Since G is planar, it must have at least one vertex with degree five or less as shown in theorem V. Assume this vertex to be '$u$'.

Let $G_1$ be a graph of $n - 1$ vertices obtained from G by deleting vertex '$u$'. The $G_1$ graph requires no more than five colours (Induction hypothesis). Consider that the vertices in $G_1$ have been properly coloured and now add to it '$u$' and all the edges incident on $u$. If the degree of $u$ is 1, 2, 3, or 4, a proper colour to $u$ can be easily assigned.

Now, we have one case left, in which the degree of $u$ is 5, and all the 5 colours have been used in colouring the vertices adjacent to $u$, as shown in Fig. 69.

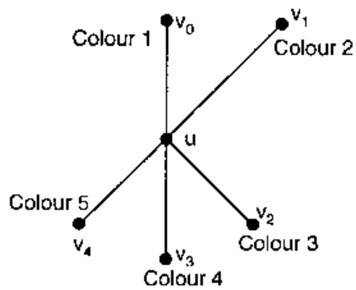



**Fig. 69**

Suppose that there is a path in $G_1$ between vertices $v_0$ and $v_3$ coloured alternately with colours 1 and 4 as shown in Fig. 70.

NOTES

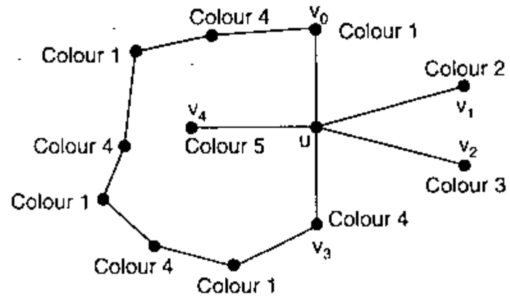



**Fig. 70**

Then a similar path between $v_4$ and $v_2$, coloured alternately with colours 5 and 3, cannot exist ; otherwise, these two paths will intersect and cause G to be non-planar.

Thus, if there is no path between $v_4$ and $v_2$ coloured alternately with colour 5 and 3 of all vertices connected to $v_2$ through vertices of alternating colours 5 and 3. This interchange will colour vertex $v_2$ with colour 5 and yet keep G, properly coloured. As vertex $v_4$ is still with colour 5, the colour 3 is left over with which to colour vertex $u$ which proves the theorem.

## 1.14. COVERING, INDEPENDENCE AND DOMINATION

**Definitions.** An edge $\{u, v\}$ in a graph is termed to cover its incident vertices $u$ and $v$.

A vertex in a graph is said to cover the edges with which it is incident.

If $G = (V, E)$ is a graph and $E' \subseteq E$, then $E'$ is said to be an edge cover of G and to cover G if for each vertex $v \in V$, there in the sense that it covers all the edges of the graph but no proper subset of it does so. However U does not correspond to the vertex covering number because $U_1 = \{v_5\}$ is the unique minimum vertex cover and thus $\alpha_0 = I_1$. Also $\alpha_1 = 4$ because the set of edges $\{e_1, e_2, e_3, e_4\}$ is the minimum edge cover.

In general, the edges (vertices) of any spanning tree, Hamiltonian path or unicursal path of any connected graph G, constitute an edge (vertex) cover of G.

Let G be a graph with vertex set V. We can make some remarks about edge coverings in G.

C(1) An edge covering of G can always be found so long as G does not contain an isolated vertex.

C(2) If $| V | = n$, where $(n > 1)$, then any edge covering of G will contain at least $n/2$ edges. If $G = K_n$, then $\alpha_1 = [(n + 1)/2]$.

C(3) Every edge covering includes every pendant edge.

C(4) It is possible to remove a subset of edges (possibly empty) from any edge covering of G in order to create a minimal (but not necessarily minimum) edge covering of G.

C(5) Minimal edge coverings are acyclic.

The similar remarks are about vertex coverings.

C(6) A vertex covering exists for any graph G.

C(7) If $G = K_n$, then $\alpha_0 = n - 1$.

A vertex covering may have only a single element. This is true for any star. A graph which possesses a unique vertex called the centre with which every edge is incident. Figure 71(*a*) depicts a star with centre $v_5$.

C(8) It is possible to remove a subset of vertices (possibly empty) from any vertex covering in order to create a minimal (but not necessarily minimum) vertex covering.

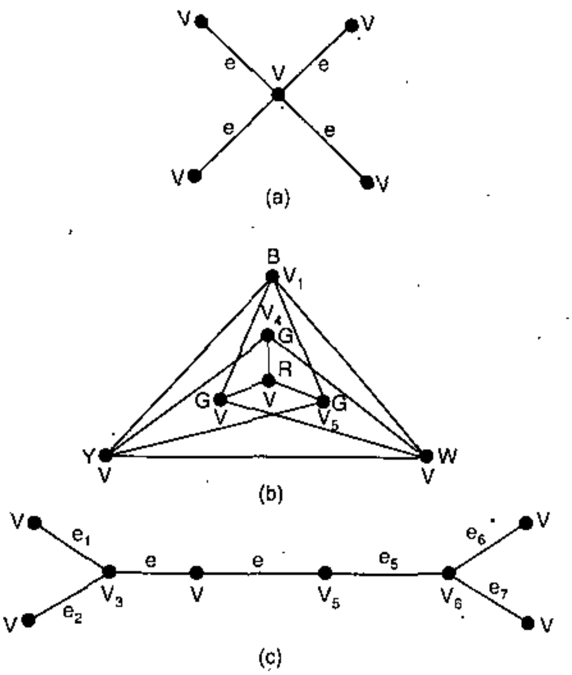



**Fig. 71.** (*a*) Cover, Independence and Dominance (*b*) Colouring (*c*) Matching.

**Theorem 9.** *An edge covering in a graph does not contain a path of at least three edges if and only if it is minimal.*

**Proof.** Let us consider an edge covering containing a path of at least three edges. The second edge of the path can be removed, leaving an edge covering. Hence the original covering is not minimal.

Suppose now that there exists an edge covering which does not contain a path of at least three edges. In this case, each component of the graph is a star. Hence it is impossible to remove an edge from an edge covering of a star, the edge covering is minimal.

We now consider the concept of independence.

**Definitions.** If G = (V, E) is a graph and $E' \subseteq E$, then E′ is said to be an edge independent if no two edges of E′ are adjacent.

If G = (V, E) is a graph and $U \subseteq V$, then U is said to be an vertex independent if no two edges of U are adjacent.

For a given graph G, the cardinality of the set of edges of G which is the largest vertex-independent set of G is said to be the edge dependence number of G and is denoted by $\beta_1(G)$ or $\beta_1$.

For a given graph G, the cardinality of the set of edges of G which is the largest vertex-independent set of G is called the vertex dependence number of G and is denoted by $\beta_0(G)$ or $\beta_0$.

NOTES

An independent set is termed maximal if none of its proper supersets is independent. An independent set in a graph G is called maximum if there is no independent set in G with a greater number of elements.

We demonstrate these ideas with the graph in figure 71($a$). Any one of the edges of the graph constitutes an edge-independent set. Such a singleton set is at once maximal and maximum.

The set $\{v_5\}$ is a maximal vertex-independent set. However it is not maximum because of the existence of the $\{v_1, v_2, v_3, v_4\}$. Thus in this graph $\beta_0 = 4$ and $\beta_1 = 1$.

We make some remarks about edge-independent sets in any graph G.

I(1) *An edge-independent set can always be found in* G contains at least one edge. Any single edge of G constitutes such a set.

I(2) If $G = K_n$, the complete graph on $n$ vertices, then $\beta_1 = [n/2]$, the integer part of $n/2$.

I(3) Every pendant edge in G belongs to at least one maximal edge-independent set.

I(4) It is possible to add a subset of edges (possibly empty) to any edge-independent set in G in order to create a maximal (but not necessarily maximum) edge-independent set in G.

We can make similar observations about vertex-independent sets in G.

I(5) A vertex-independent set exists for G. (Any single vertex of G constitutes such a set).

I(6) If $G = K_n$ then $\beta_0 = 1$.

I(7) Every pendant vertex in G belongs to at least one maximal vertex-independent set.

I(8) It is possible to add a subset of vertices (possibly empty) to any vertex-independent set in G in order to create a maximal (but not necessarily maximum) vertex-independent set in G.

We now give theorems linking the concepts of covering and independence.

## 1.15. SHORTEST PATH IN WEIGHTED GRAPHS

Weighted graphs can be used to represent highways connecting the different cities. The weighted edges represent the distance between different cities and the vertices represent the cities. A common problem with this type of graph is to find the shortest path from one city to another city. There are many ways to tackle this problem one of which is as follows :

**Shortest Paths from Single Source.** We will find shortest paths from a single vertex to all other vertices of the graph. The first algorithm was proposed by **E. Dijkstra** in 1959. Some common terms related with this algorithm are as follows :

**Path Length.** The length of a path is the sum of the weights of the edges on that path.

**Source.** The starting vertex of the graph from which we have to start to find the shortest path.

**Destination.** The terminal or last vertex upto which we have to find the path.

## 1.16. DIJKSTRA'S ALGORITHM



This algorithm maintains a set of vertices whose shortest path from source is already known. The graph is represented by its cost adjacency matrix, where cost being the weight of the edge. In the cost adjacency matrix of the graph, all the diagonal values are zero. If there is no path from source vertex $V_s$ to any other vertex $V_i$, then it is represented by + ∞. In this algorithm, we have assumed all weights are positive.

1. Initially there is no vertex in sets.

2. Include the source vertex $V_s$ in S. Determine all the paths from $V_s$ to all other vertices without going through any other vertex.

3. Now, include that vertex in S which is nearest to $V_s$ and find shortest paths to all the vertices through this vertex and update the values.

4. Repeat the step 3 until $n - 1$ vertices are not included in S if there are $n$ vertices in the graph.

After completion of the process, we get the shortest paths to all the vertices from the source vertex.

**Example 5.** *Find the shortest path between K and L in the graph shown in Fig. 72 by using Dijkstra's Algorithm.*

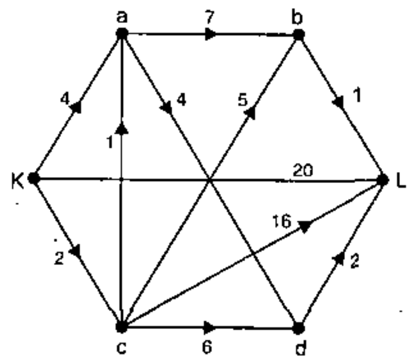



**Fig. 72**

**Sol. Step I.** Include the vertex K in S and determine all the direct paths from K to all other vertices without going through any other vertex.

| S | Distance to all other vertices | | | | | |
|---|---|---|---|---|---|---|
| | K | *a* | *b* | *c* | *d* | L |
| K | 0 | 4(K) | ∞ | 2(K) | ∞ | 20(K) |

**Step II.** Include the vertex in S which is nearest to K and determine shortest paths to all vertices through this vertex and update the values. The nearest vertex is *c*.

| S | Distance to all other vertices | | | | | |
|---|---|---|---|---|---|---|
| | K | *a* | *b* | *c* | *d* | L |
| K, *c* | 0 | 3(K, *c*) | 7(K, *c*) | 2(K) | 8(K, *c*) | 18(K, *c*) |

**Step III.** The vertex which is 2nd nearest to K is *a*, included in S.

| S | Distance to all other vertices | | | | | |
|---|---|---|---|---|---|---|
| | K | *a* | *b* | *c* | *d* | L |
| K, *c*, *a* | 0 | 3(K, *c*) | 7(K, *c*) | 2(K) | 7(K, *c*, *a*) | 18(K, *c*) |

NOTES

**Step IV.** The vertex which is 3rd nearest to K is $b$, is included in S.

| S | Distance to all other vertices | | | | | |
|---|---|---|---|---|---|---|
| | K | $a$ | $b$ | $c$ | $d$ | L |
| K, $c$, $a$, $b$ | 0 | 3(K, $c$) | 7(K, $c$) | 2(K) | 7(K, $c$, $a$) | 8(K, $c$, $b$) |

**Step V.** The vertex which is next nearest to K is $d$, is included in S.

| S | Distance to all other vertices | | | | | |
|---|---|---|---|---|---|---|
| | K | $a$ | $b$ | $c$ | $d$ | L |
| K, $c$, $a$, $b$, $d$ | 0 | 3(K, $c$) | 7(K, $c$) | 2(K) | 7(K, $c$, $a$) | 8(K, $c$, $b$). |

Since, $n - 1$ vertices included in S. Hence we have found the shortest distance from K to all other vertices.

Thus, the shortest distance between K and L is 8 and the shortest path is K, $c$, $b$, L.

**Example 6.** *Show that $e \geq 3V - 6$ for the connected planar graphs shown in Figs. 73 and 74.*

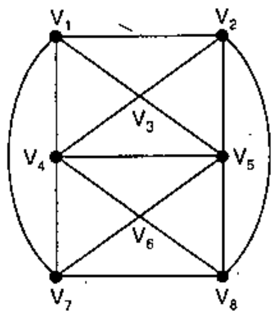



**Fig. 73**

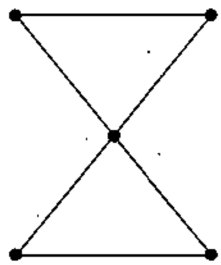


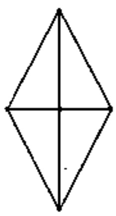
**Fig. 74**

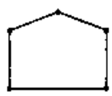
**Sol.** ($i$) The graph shown in Fig. 73 contains vertices V = 8 and edges $e$ = 17. Putting the values we have $e = 3 \times 8 - 6 = 18 \geq 17$. Hence proved.

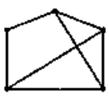
($ii$) The graph shown in Fig. 74 contains vertices V = 5 and edges $e$ = 6. Putting the values, we have $3 \times 5 - 6 = 11 > 6$. Hence proved.

## EXERCISE 3

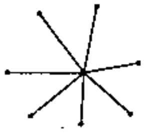
1. Find the chromatic numbers of the following graphs.

(a) 

(b) 

(c) 

(d) 

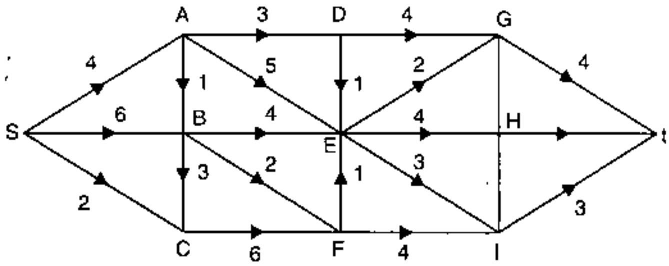
(*e*) 

(*f*) 

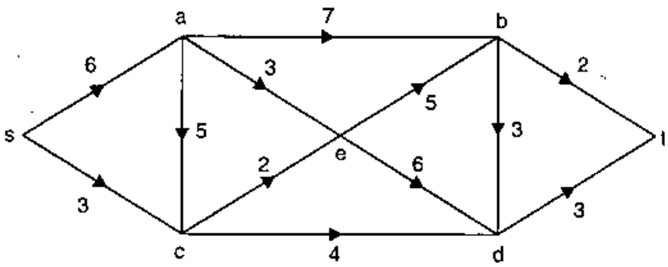
**NOTES**

2. Find the shortest path and its length from *s* to *t* by using Dijkstra's algorithm in the following graph.

(*a*)




(*b*)




## 1.17. TREE

A graph which has no cycle is called an acyclic graph. A tree is an acyclic graph or graph having no cycles.

A tree or general tree is defined as a non-empty finite set of elements called vertices or nodes having the property that each node can have minimum degree 1 and maximum degree $n$. It can be partitioned into $n + 1$ disjoint subsets such that the first subset contains the root of the tree and the remaining $n$ subsets contains the elements of the $n$ subtree. (Fig. 75)

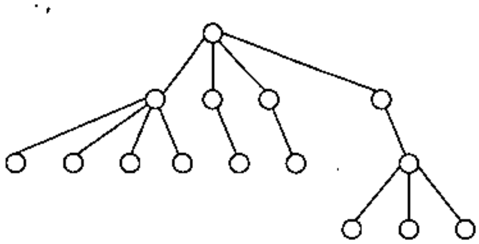


**Fig. 75.** General Tree.

## Directed Trees

A directed tree is an acyclic directed graph. It has one node with indegree 1, while all other nodes have indegree 1 as shown in Figs. 76 and 77.

NOTES

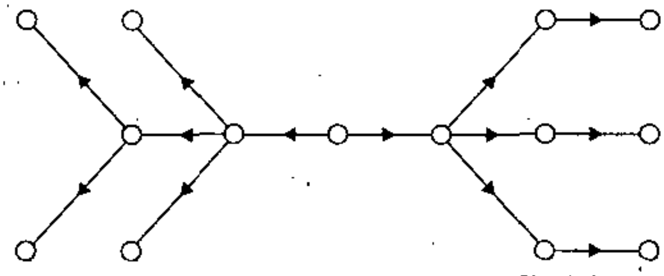



**Fig. 76**

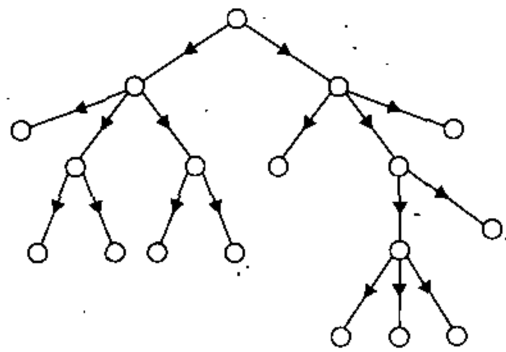


**Fig. 77**

The node which has outdegree 0 is called an external node or a terminal node or a leaf. The nodes which has outdegree greater than or equal to one are called internal nodes or branch nodes.

## Ordered Trees

If in a tree at each level, an ordering is defined, then such a tree is called an ordered tree.

*e.g.,* the trees shown in Figs. 78 and 79 represent the same tree but have different orders.

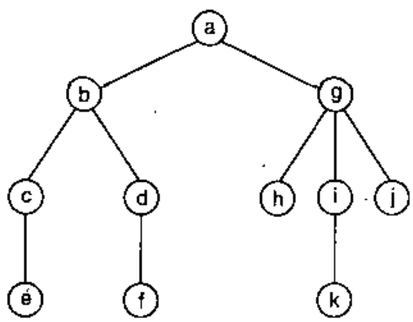



**Fig. 78**

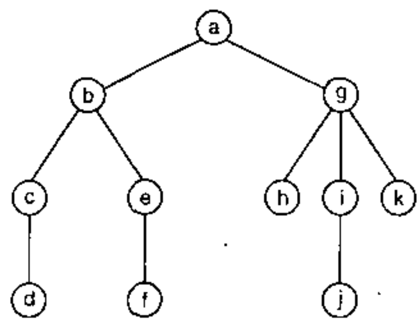



**Fig. 79**

## 1.18. ROOTED TREES

If a directed tree has exactly one node or vertex called root whose incoming degree is 0 and all other vertices have incoming degree one, then the tree is called rooted tree.

* A tree with no nodes is a rooted tree (the empty tree).

* A single node with no children is a rooted tree.

## 1.19. BINARY TREE

If the outdegree of every node is less than or equal to 2, in a directed tree then the tree is called a binary tree. A tree consisting of no nodes (empty tree) is also a binary tree.

## 1.20. TREE TERMINOLOGY

(*a*) **Root.** A binary tree has a unique node called the root of the tree.

(*b*) **Left Child.** The node to the left of the root is called its left child.

(*c*) **Right Child.** The node to the right of the root is called its right child.

(*d*) **Parent.** A node having left child or right child or both is called parent of the nodes.

(*e*) **Siblings.** Two nodes having the same parent are called siblings.

(*f*) **Leaf.** A node with no children is called a leaf. The number of leaves in a binary tree can vary from one (minimum) to half the number of vertices (maximum) in a tree.

(*g*) **Ancestor.** If a node is the parent of another node, then it is called ancestor of that node. The root is an ancestor of every other node in the tree.

(*h*) **Descendent.** A node is called descendent of another node if it is the child of the node or child of some other descendent of that node. All the nodes in the tree are descendents of the root.

(*i*) **Left Subtree.** The subtree whose root is the left child of some node is called the left subtree of that node.

(*j*) **Right Subtree.** The subtree whose root is the right child of some node is called the right subtree of that node.

(*k*) **Level of a Node.** The level of a node is its distance from the root. The level of root is defined as zero. The level of all other nodes is one more than its parent node. The maximum number of nodes at any level N is $2^N$.

(*l*) **Depth or Height of a Tree.** The depth or height of a tree is defined as the maximum number of nodes in a branch of tree. This is one more than the maximum level of the tree *i.e.,* the depth of root is one. The maximum number of nodes in a binary tree of depth $d$ is $2^d - 1$, where $d \geq 1$.

(*m*) **External Nodes.** The nodes which has no children are called external nodes or terminal nodes.

(*n*) **Internal Nodes.** The nodes which has one or more than one children are called internal nodes or non-terminal nodes.

**Theorem 10.** *Let G be a graph with more than one vertex. Then the following are equivalent :*

*(i) G is a tree.*

NOTES

*(ii) Each pair of vertices is connected by exactly one simple path.*

*(iii) G is connected, but if any edge is deleted then the resulting graph is not connected.*

*(iv) G is cycle tree, but if any edge is added to the graph then the resulting graph has exactly one cycle.*

**Proof.** To prove this theorem, we prove that (*i*) ⇒ (*ii*), (*ii*) ⇒ (*iii*), (*iii*) ⇒ (*iv*) and finally (*iv*) ⇒ (*i*). The complete proof is as follows :

(*i*) ⇒ (*ii*) Let us assume two vertices $u$ and $v$ in G. Since G is a tree, so G is connected and there is at least one path between $u$ and $v$. More over, there can be only one path between $u$ and $v$, otherwise G will contain a cycle.

(*ii*) ⇒ (*iii*) Let us delete an edge $e = (u, v)$ from G. It means $e$ is a path from $u$ to $v$. Suppose the graph result from $G - e$ has a path $p$ from $u$ to $v$. Then P and $e$ are two distinct paths from $u$ to $v$, which is a contradiction of our assumption. Thus, there does not exist a path between $u$ and $v$ in $G - e$, so $G - e$ is disconnected.

(*iii*) ⇒ (*iv*) Let us suppose that G contains a cycle $c$ which contains an edge $e = \{u, v\}$. By hypothesis, G is connected but $G' = G - e$ is disconnected with $u$ and $v$ belonging to different components of G′. This contradicts the fact that $u$ and $v$ are connected by the path $P = C - e$, which lies in G′. Hence G is cycle free.

Now, Let us take two vertices $x$ and $y$ of G and let H be the graph obtained by adjoining the edge $e = \{x, y\}$ to G. Since G is connected, there is a path P from $x$ to $y$ in G ; hence $C = Pe$ forms a cycle in H. Now suppose H contains another cycle $C_1$. Since G is cycle free, $C_1$ must contain the edge $e$, say $C_1 = P_1e$.

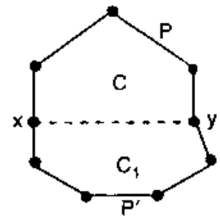


**Fig. 80**

Then P and $P_1$ are two paths in G from $x$ to $y$ as shown in Fig. 80. Thus, G contains a cycle, which contradicts the fact that G is cycle free. Hence H contains only one cycle.

(*iv*) ⇒ (*i*) By adding any edge $C = (x, y)$ to G produces a cycle, the vertices $x$ and $y$ must be connected already in G. Thus, G is connected and is cycle is free *i.e.*, G is a tree.

## ILLUSTRATIVE EXAMPLES

**Example 1.** *For the tree as shown in Fig. 81.*

*(i) Which node is the root ?*

*(ii) Which nodes are leaves ?*

*(iii) Name the parent node of each node.*

NOTES

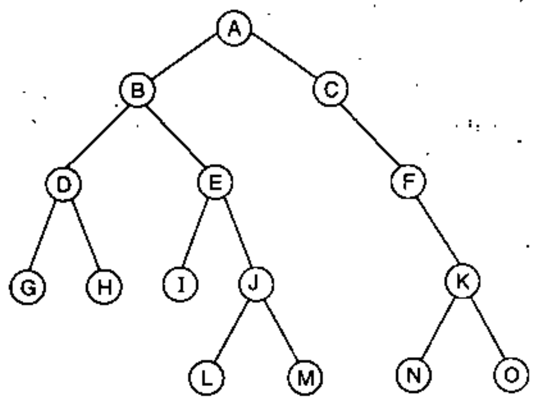



**Fig. 81**

**Sol.** (*i*) The node A is the root node.

(*ii*) The nodes G, H, I, L, M, N, O are leaves.

(*iii*)

| Nodes | Parent |
|---|---|
| B, C | A |
| D, E | B |
| F | C |
| G, H | D |
| I, J | E |
| K | F |
| L, M | J |
| N, O | K |

**Example 2.** *For the tree as shown in Fig. 82.*

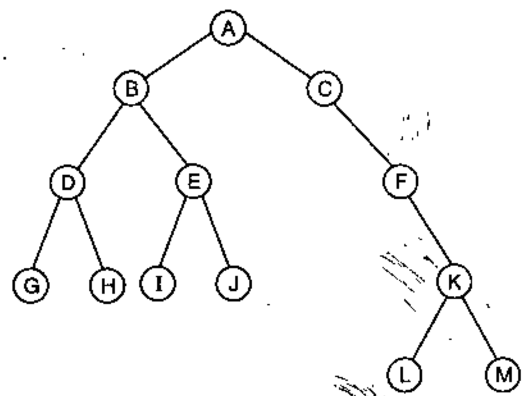



**Fig. 82**

(*i*) *List the children of each node.* (*ii*) *List the siblings.*

(*iii*) *Find the depth of each node.* (*iv*) *Find the level of each node.*

**Sol.** (*i*) The children of each node is as follows :

| Node | Children |
|---|---|
| A | B, C |
| B | D, E |
| C | F |
| D | G, H |
| E | I, J |
| F | K |
| K | L, M |

NOTES

(*ii*) The siblings are as follows :

**Siblings**

B and C

D and E

G and H

I and J

L and M are all siblings.

(*iii*)

| **Node** | **Depth or Height** |
|---|---|
| A | 1 |
| B, C | 2 |
| D, E, F | 3 |
| G, H, I, J, K | 4 |
| L, M | 5 |

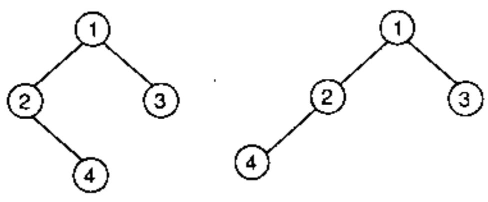
(*iv*)

| **Node** | **Level** |
|---|---|
| A | 0 |
| B, C | 1 |
| D, E, F | 2 |
| G, H, I, J, K | 3 |
| L, M | 4 |

**Example 3.** (*a*) *How will you differentiate between a general tree and a binary tree ?*

(*b*) *Define a rooted tree with an example and show how it may be viewed as directed graph.*

**Sol.** (*a*)

| ***General Tree*** | ***Binary Tree*** |
|---|---|
| 1. There is no such tree having zero nodes or an empty general tree. | 1. There may be an empty binary tree. |
| 2. If some node has a child, then there is no such distinction. | 2. If some nodes has a child, then it is distinguished as a left child or a right child. |
| 3. The trees shown in figure are same, when we consider them as general trees.   (i) (ii) | 3. The trees shown in figure are distinct, when we consider them as binary trees, because in (*i*), 4 is right child of 2 while in (*ii*), 4 is left child of 2. |

(*b*) **Rooted tree:** We first define the term '*directed tree*'. A directed graph is said to be a directed tree if it becomes a tree when the directions of the edges are ignored. For example, the Fig. 83 is a *directed tree*.

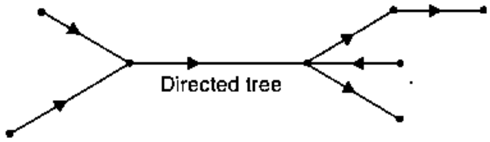
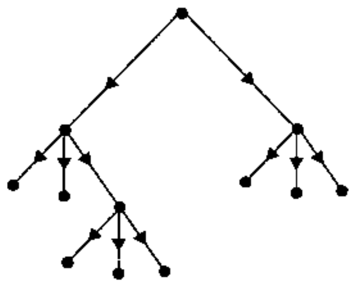



**Fig. 83**

A directed tree is called a *rooted tree* if there is exactly one vertex whose incoming degree is 0 and incoming degree of all other vertices are 1. The vertex with incoming degree 0 is called the *root* of the *rooted tree*. The Fig. 84 is an example of a rooted tree.



Rooted tree

**Fig. 84**

In a rooted tree, a vertex whose outgoing degree is 0 is called a *leaf* or a *terminal code* and a vertex whose *outgoing degree is non zero, is called a branch node or an internal node.*

**Rooted tree may be viewed as directed graph.** We know that a tree is a graph which is connected and without any cycles. A rooted tree T is a tree with a designated vertex *r*, called the root of the tree. Since there is a unique simple path from the root *r* to any other vertex *v* in T, this determines a direction to the edges of T. Thus T may be viewed as a directed graph.

## 1.21. SPANNING TREE

Consider a connected graph G = (V, E). A spanning tree T is defined as a sub-graph of G if T is a tree and T includes all the vertices of G.

**Example 4.** *Draw all the spanning trees of the graph G shown in Fig. 85.*

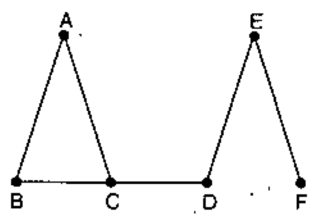



**Fig. 85.** Graph G.

NOTES

**Sol.** All the spanning trees of graph G is as shown in Fig. 86.

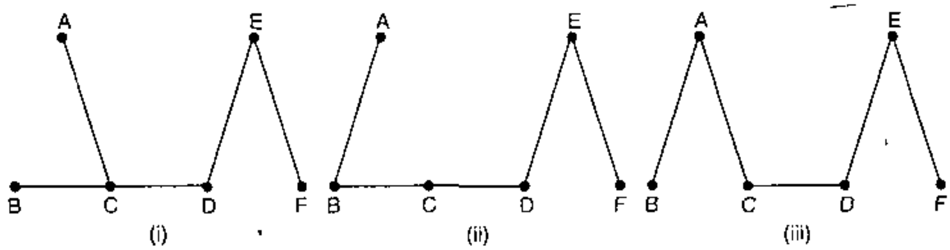



**Fig. 86**

## 1.22. MINIMUM SPANNING TREE

*Consider a connected weighted graph* G = (V, E). A minimal spanning tree T of the graph G is a tree whose total weight is smallest among all the spanning trees of the graph G. The total weight of the spanning tree is the sum of the weights of the edges of the spanning trees.

The minimum weight of the spanning tree is unique but the spanning tree may not be unique because more than one spanning tree are possible when more than one edges exist having the same weight.

## 1.23. KRUSKAL'S ALGORITHM

This algorithm finds the minimum spanning tree T of the given connected weighted graph G.

1. Input the given connected weighted graph G with $n$ vertices whose minimum spanning tree T, we want to find.

2. Order all the edges of the graph G according to increasing weights.

3. Initialise T with all vertices but do not include any edge.

4. Add each of the graph G in T which does not form a cycle until $n - 1$ edges are added.

**Example 5.** *Determine the minimum spanning tree of the weighted graph shown in Fig. 87.*

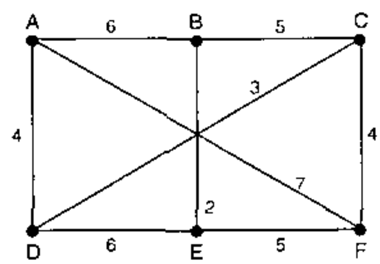



**Fig. 87**

**Sol.** Using Kruskal's algorithm, arrange all the edges of the weighted graph in increasing order and initialise spanning tree T with all the six vertices of G. Now start adding the edges of G in T which do not form a cycle and having minimum weights until five edges are not added as there are six vertices. (Fig. 88).

| Edges | Weights | Added or Not |
|---|---|---|
| (B, E) | 2 | Added |
| (C, D) | 3 | Added |
| (A, D) | 4 | Added |
| (C, F) | 4 | Added |
| (B, C) | 5 | Added |
| (E, F) | 5 | Not added |
| (A, B) | 6 | Not added |
| (D, E) | 6 | Not added |
| (A, F) | 7 | Not added. |

**Minimum Spanning Tree**

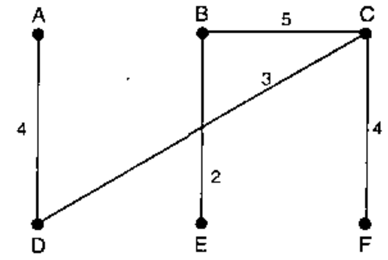



**Fig. 88**

**Example 6.** *Find a minimum spanning tree of the labelled connected graph shown in Fig. 89.*

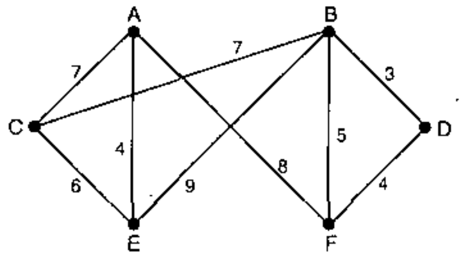



**Fig. 89**

**Sol.** Using KRUSKAL'S ALGORITHM, arrange all the edges of the graph in increasing order and initialize spanning tree with all the vertices of G. Now, add the edges of G in T which do not form a cycle and have minimum weight until $n - 1$ edges are not added, where $n$ is the number of vertices. The spanning tree is shown in Fig. 90.

| Edges | Weights | Added or Not |
|---|---|---|
| (B, D) | 3 | Added |
| (A, E) | 4 | Added |
| (D, F) | 4 | Added |
| (B, F) | 5 | Not added |
| (C, E) | 6 | Added |
| (A, C) | 7 | Not added |
| (B, C) | 7 | Added |
| (A, F) | 8 | Not added |
| (E, B) | 9 | Not added |

**Minimum Spanning Tree**

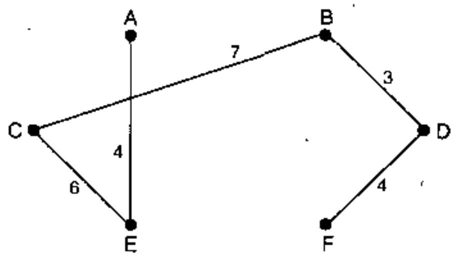



**Fig. 90**

The minimum weight of spanning tree is = 24.

**Example 7.** *Find all the spanning trees of graph G and find which is the minimal spanning tree of G shown in Fig. 91.*

NOTES

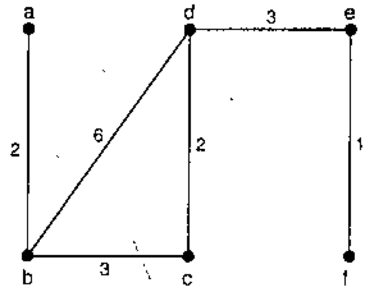



**Fig. 91**

**Sol.** There are total three spanning trees of the graph G which are as shown in Fig. 92.

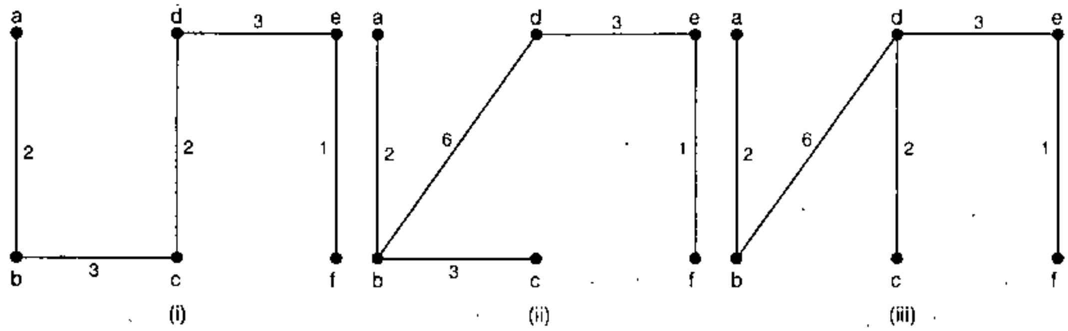



**Fig. 92**

To find the minimal spanning tree, use the KRUSKAL'S ALGORITHM. The minimal spanning tree is shown in Fig. 93.

| Edges | Weights | Added or Not |
|---|---|---|
| (E, F) | 1 | Added |
| (A, B) | 2 | Added |
| (C, D) | 2 | Added |
| (B, C) | 3 | Added |
| (D, E) | 3 | Added |
| (B, D) | 6 | Not added. |

**Minimal Spanning Tree**

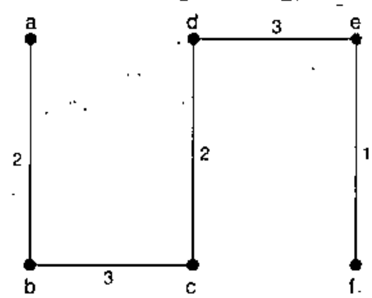



**Fig. 93**

The first one is the minimal spanning having the minimum weight = 11.

**Example 8.** *What are the properties of minimum spanning tree.*

**Sol. Properties of Minimum spanning tree** .

A minimum spanning tree T of a graph G is a tree whose total weight is the smallest among all the spanning trees of the graph G. It has the following properties.

(*i*) The total weight of the spanning tree is the sum of the weights of the edges of the spanning trees.

(*ii*) The minimum weight of the spanning tree is unique.

## 1.24. PRIM'S ALGORITHM

NOTES

Let G be a graph with $n$ vertices and $e$ edges.

**Step 1.** First assign a label for all vertices of G

**Step 2.** Form a matrix such that whose elements are the weight of the edges of G (as keep the incidenship of end vertices).

**Step 3.** Set the weight of non existent edge as ∝.

**Step 4.** Select the smallest entry from first row of the matrix. (that is to a vertex other than $V_i$ and $V_j$ has smallest entry in the row 1 and column $j$) let this new vertex be $V_j$. Step 4: Next regard $V_1$, $V_i$ and $V_j$ as one sub graph and repeat the process until all the $n$ vertices have been connected by $n - 1$ edges.

### ILLUSTRATIVE EXAMPLES

**Example 1.** *Find the minimal spanning tree for the following graph by using Prim's algorithm*

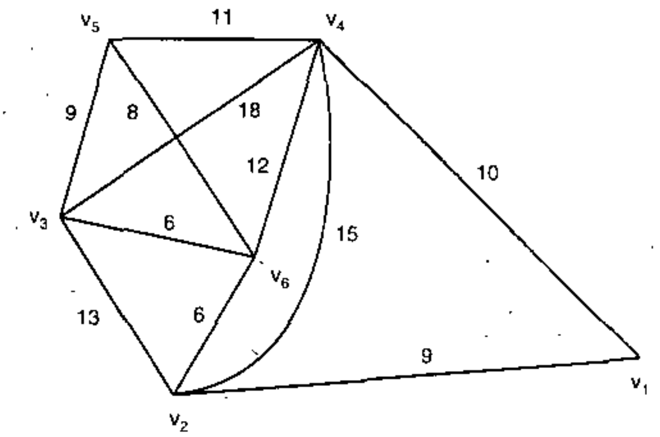



**Fig. 94**

**Sol.**

| | $V_1$ | $V_2$ | $V_3$ | $V_4$ | $V_5$ | $V_6$ |
|---|---|---|---|---|---|---|
| $V_1$ | — | 9 | ∝ | 10 | ∝ | ∝ |
| $V_2$ | 9 | — | 13 | 15 | ∝ | 6 |
| $V_3$ | ∝ | 13 | — | 18 | 9 | 6 |
| $V_4$ | 10 | 15 | 18 | — | 11 | 12 |
| $V_5$ | ∝ | ∝ | 9 | 11 | — | 8 |
| $V_6$ | ∝ | 6 | 6 | 12 | 8 | — |

NOTES

The edges are in the minimal spanning tree are

$$(V_1, V_2) \rightarrow (V_2, V_6) \rightarrow (V_6, V_3) \rightarrow (V_3, V_5) \rightarrow (V_5, V_4) \rightarrow (V_4, V_1)$$

The minimal spanning tree

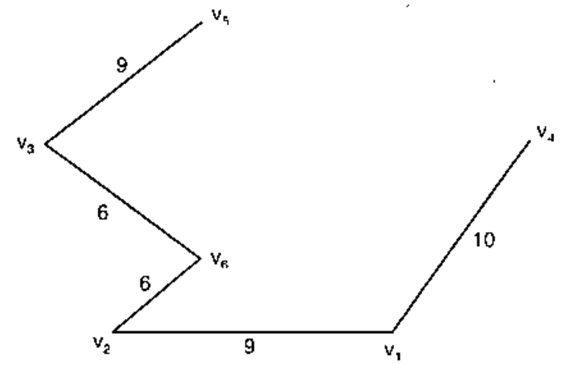



**Fig. 95**

**Example 2.** *Find the minimum spanning tree by using Prim's algorithm.*

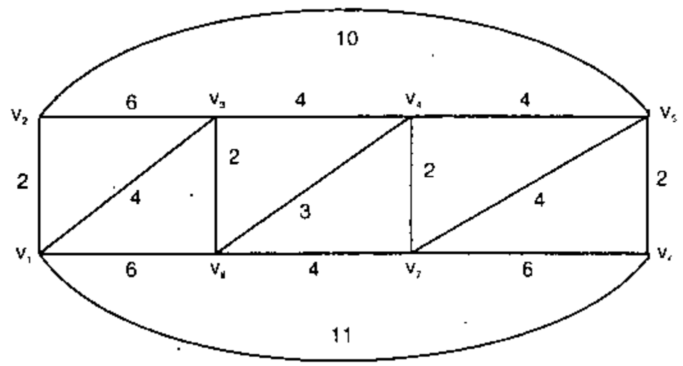



**Fig. 96**

**Sol.**

| | $V_1$ | $V_2$ | $V_3$ | $V_4$ | $V_5$ | $V_6$ | $V_7$ | $V_8$ |
|---|---|---|---|---|---|---|---|---|
| $V_1$ | — | 2 | 4 | α | α | 11 | α | 6 |
| $V_2$ | 2 | — | 6 | α | 10 | α | α | α |
| $V_3$ | 4 | 6 | — | 4 | α | α | α | 2 |
| $V_4$ | α | α | 4 | — | 6 | α | 2 | 3 |
| $V_5$ | α | 10 | α | 6 | — | 2 | 4 | α |
| $V_6$ | 11 | α | α | α | 2 | — | 6 | α |
| $V_7$ | α | α | α | 2 | 4 | 6 | — | 4 |
| $V_8$ | 6 | α | 2 | 3 | α | α | 4 | — |

The edges are selected

$(V_1, V_2) \rightarrow (V_2, V_3) \rightarrow (V_3, V_8) \rightarrow (V_8, V_4) \rightarrow (V_4, V_7) \rightarrow (V_7, V_5)$

The minimal spanning tree is

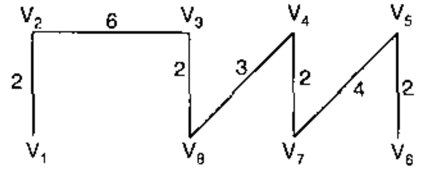



**Fig. 97**

## 1.25. APPLICATIONS OF GRAPH THEORY

Graph theory is playing an increasingly important role in the design, analysis, and testing of computer programs. Its importance is derived from the fact that flow of control and flow of data for any program can be expressed in terms of directed graphs. From the graph representing the flow of control, called the program graph, many other can be derived that either partially or completely preserve the program control structure. One derived graph known as a *cyclomatic tree* is of particular value in program testing. It is so named because the number of leaves of the tree is equal to the cyclomatic number of the program graph.

Graph theory is becoming increasingly significant as it is applied to other areas of mathematics, science and technology. It is being actively used in fields as varied as biochemistry (genomics), electrical engineering (communication networks and coding theory), computer science (algorithms and computation) and operations research (scheduling). The powerful combinatorial methods found in graph theory have also been used to prove fundamental results in other areas of pure mathematics.

The best known of these methods are related to a part of graph theory called *matchings*, and the result from this area are used to prove Dilworth's chain decomposition theorem for finite partially ordered sets. An application of matching in graph theory shows that there is a common set of left and right *coset* representatives of a subgroup in a finite group. This result played an important role in Dharwadker's 2000 proof of the four-colour theorem. The existence of matching in certain infinite bipartite graphs played an important role in Laczkovich's affirmative answer to Tarski's 1925 problem of whether a circle i piecewise congruent to a square. The proof of the existence of a subset of the real numbers **R** that is non-measurable in the Lebesgue sense is due to Thomas. Surprisingly, the theorem can be proved using only discrete mathematics (bipartite graphs). There are many such example of applications of graphs to other parts of mathematics.

Applications of graphs theory are primarily, but not exclusively, concerned with labelled graphs and various specializations of these. Structures that can be represented, as graphs are ubiquitous, and many problems of practical interest can be represented by graphs. The link structure of a website could be represented by a directed graph: the vertices are the web pages available at the website and directed edge from page A to page B exists if and only if A contains a link to B. A similar approach can be taken to problems in travel, biology, computer chip design, and many other fields. The development of algorithms to handle graphs is therefore of major interest in computer science.

NOTES

Assigning a weight to each of the graph can extend a graph structure. Graphs with weights, or weighted values. For example if a graph represents a road network, the weights could represent the length of each road. A digraph with weighted edge in the context of graph theory is called a network.

Networks have many uses in the practical side of graph theory, network analysis (for example, to model and analyze traffic networks). Within network analysis, the definition of the term "network" varies, and may often refer to a simple graph.

Many applications of graph theory exist in the form of network analysis. These split broadly into three categories. Firstly, analysis to determine of the graph. A vast number of graph measures exist, and the production of useful ones for various domains remains an active area of research. Secondly, analysis to find a measurable quantity within the network, for example, for transportation networks, the level of vehicular flow within any portion of it. Thirdly, analysis of dynamical properties of networks.

Graph theory is also used to study molecules in chemistry and physics. In condensed matter physics, the three dimensional structure of complicated simulated atomic structures can be studied quantitatively by gathering statistics on graph-theoretic properties related to the topology of the atoms. For example, Franzblau's shortest-path (SP) rings. In chemistry a graph makes a natural model for a molecule, where vertices represent atoms and edge bonds. This approach is especially used in computer processing of molecular structures, ranging from chemical editors to database searching.

Graph theory is also widely used in sociology as a way, for example, to measure actors' prestige or to explore diffusion mechanism, notably through the use of social network analysis software.

### Graphs in Computer Science

In computer science, graphs are used in many areas such as in computer designing, scheduling problems in operating system, file management in database management system, data-flow control between networks, network of interconnected networks etc. In day-to-day applications, graphs find their importance as representations of many kinds of physical structure.

The structure of digital computer is shown in figure 98.

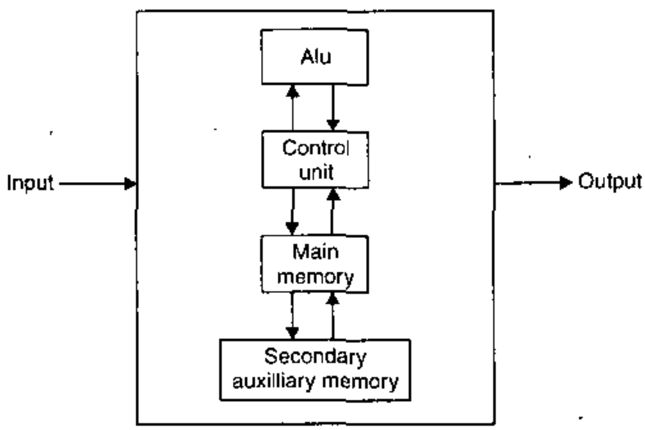



**Fig. 98**

and in form of graph as

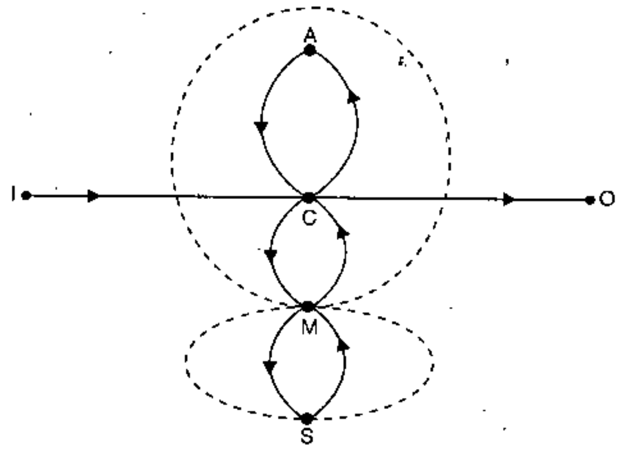



**Fig. 99**

We may use the cutset to show the different main components of computer such as input device, output device, CPU and auxilliary secondary memory.

The theoretical or mathematical concepts of graphs such as connectedness, bioconnected, bipartite, planarity, duality etc..are used for designing the circuits and simulate the effects of implementation before actual implementation.

- Concept of *planar graph* is used for designing the internal architecture of computer in chip (Motherboard).
- The edges *i.e.*, links/buses used to connect the components/nodes may be directed or undirected. Normally all the properties of digraphs can be used to handle the problem of data transmission.
- In case of multiprocessor systems, components may be partitions into a number of separate modules without loss of integrity of system by the help of cutset theory.
- Maximum flow of data through links can be determined by the concept of network flow with the help of weights, where weights are nothing but the storage capacity of each bus.
- Minimal spanning tree help us to determine the path from processor to a memory module in multistage interconnection networks of processors and memories.
- Concept of connectivity, separability and vulnerability is applicable on connected graphs such the after the separation of the remaining components (multiprocessor) can still continue to "communicate" the data.

**Miscellaneous Applications**

This is virtually no end to the list of problems that can be solved with graph theory.

In a modern information retrieval system each document carries a number of index terms (also called descriptors). The index terms are represented as vertices and if two index terms $v_i$ and $v_j$ are closely related (such as "graph" and "tree") they are joined with an edge $(v_i, v_j)$. The simple, undirected large graph thus produced is called *similarity graph*. For retrieval, one specifies some relevant index terms, and the maximal complete subgraph that includes the corresponding vertices will give the complete list of index terms which specify the needed documents.

Graphs have been used in linguistics to depict parsing diagrams. The vertices represent words and word strings and the edges represent certain syntactical relationships between them.

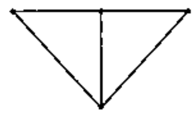
**NOTES**

Digraphs under the name *sociograms* have been used to represent relationships among individuals in a society. Members are represented by vertices and the relationship by directed edge connectdness, separability, complete subdigraphs, size of fragments and so forth, in a sociogram can be given immediate significance.

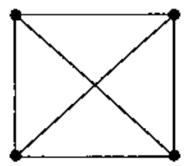
Graph theory has also been used in economics, logistic cybernetics, artificial intelligence, pattern recognition, genetics theory, fault diagnosis in computers.

## EXERCISE 4

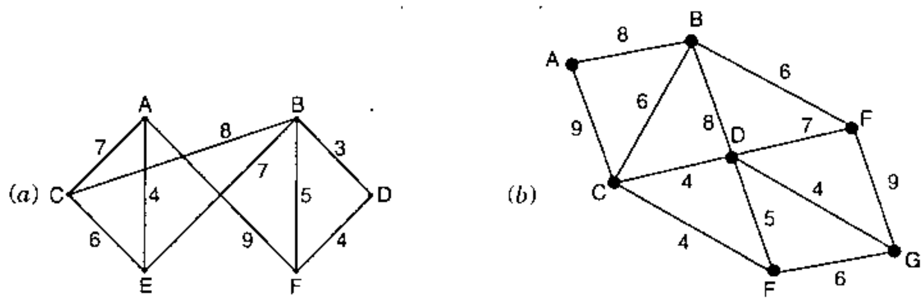
1. Find all spanning trees of the graph shown below :



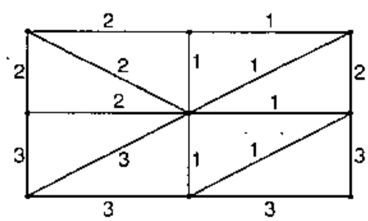
2. Find all spanning trees of the graph shown in the following figure.



3. Find the minimal spanning tree of the following graph




(c) Find the minimal spanning tree T for the weighted graph shown below :




4. Show that the sum of the degrees of the vertices of a tree with $n$ vertices is $2n - 2$.

## SUMMARY

- The graph consist of points or nodes called vertices which are connected to each other by way of lines called edges.
- A graph containing only vertices and no edge is called a discrete or null graph.
- Two vertices are called adjacent if they are connected by on edge.
- The path is called simple one if no edge is repeated in the path.
- A graph G is said to be planar if it can be drawn in a plane so that no edges cross.
- A graph G is said to be non-planar if it cannot be drawn in a plane so that no edges cross.
- A colouring is proper if any two adjacent vertices $u$ and $v$ have different colours otherwise it is called improper colouring.
- The minimum number of colours needed to produce a proper colouring of a graph G is called the chromatic number of a graph G.
- A vertex in a graph is said to cover the edges with which it is incident.
- An edge in a graph G is called to dominate those other edges in G with which it is adjacent.
- Dijkstra's algorithm maintains a set of vertices whose shortest path from source is already known.
- A tree is an acyclic graph or graph having no cycles.
- A directed tree is an acyclic directed graph.
- If the outdegree of every node is less than or equal to 2, in a directed tree then the tree is called a binary tree.
- Kruskal's algorithm finds the minimum spanning tree T of the connected weighted graph G.

## TEST YOURSELF

1. What is the difference between directed and undirected graph?
2. Differentiate between paths and circuits.
3. Let G be a finite connected planner graph with at least three vertices. Show that G has at least one vertex of degree 5 or less.
4. (*a*) Suppose a graph G contains two distinct paths from a vertex $a$ to vertex $b$. Show that G has a cycle.

   (*b*) If a graph G has more than two verticals of odd degree, then prove that there can be no Euler Path.
5. Draw the following graphs

   (*a*) $K_{2,5}$ (*b*) $K_4$

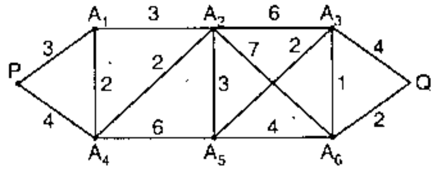
   (*c*) $K_{2,3}$
6. If G is a simple, connected and planner graph with more than one edge, then

   (*i*) $2 \mid E \mid \geq 3 \mid R \mid$

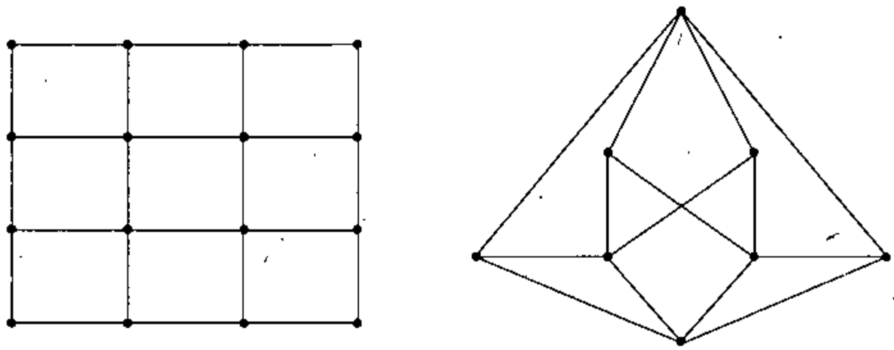
   (*ii*) $\mid E \mid \leq 3 \mid V \mid - 6$, where $\mid E \mid$ denotes the number edges, $\mid R \mid$, the number of regions and $\mid V \mid$, the number of vertices.
7. Show that $K_{3,3}$ is non-planar graph.

**NOTES**

**8.** Find the shortest path, by using either Breadth first search or Dijkstra's algorithm, from P to Q in the following weighted graph.




**9.** Find the chromatic number of the following graphs.

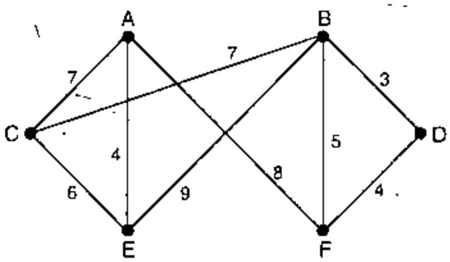


**10.** Draw all trees with exactly six vertices.

**11.** Draw all trees with five or fewer vertices.

**12.** Find the number of trees with seven vertices.

**13.** Find a minimum spanning tree of the weighted graph shown below:




**14.** Discuss the various applications of graph in computer science in detail.

**15.** Draw graphs of the following chemical compounds:

(*a*) $CH_4$ (*b*) $C_2H_6$

(*c*) $C_6H_6$ (*d*) $N_2O_3$

**16.** Name 10 situations that can be represent by means of graphs. Explain what the vertices and the edge denote.