**MCA-205: Mathematics –II (Discrete Mathematical Structures)**

**Lesson No: I** **Written by Pankaj Kumar**

**Lesson: Group theory - I** **Vetted by Prof. Kuldip Singh**

**STRUCTURE**

**1.0 OBJECTIVE:** Objective of this chapter is to gain some knowledge about algebraic structure with one binary operation.

**1.1 INTRODUCTION**: Let us consider the equation x +3 =1; we see that the natural number can not be a solution of it, while an integer is a solution of it. Similarly rotation of an equilateral triangle about their axes of symmetry results into a figure in which the position of the points changes while there is no change in shape of figure. Therefore, keeping the properties of integers and rotation of some figures like a line segment or equilateral triangle about their axes of symmetry, in mind, we come to know about groups, permutations groups. In this chapter, we define groups, permutation groups, subgroups and cosets with suitable examples.

## 1.2 SOME DEFINITIONS

**1.2.1 Definition**: For a non-empty set A, $A \times A$ is called the Cartesian product of A with itself. Therefore, $A \times A = \{ (a, b) \mid a, b \in A \}$.

**1.2.2 Definition**: $*: A \times A \to A$, $*$ is a function from set $A \times A$ to A is called binary operation on A.

**Example** (1) If we add two natural numbers then resultant is again a natural number. Hence addition is a binary operation on set of natural numbers.

(2) Multiplication is binary operation on set of integer while division is not a binary operation on set of integers.

**1.2.3 Notation:** $(G, *)$ is a collection of set G with $*$ as binary operation on it.

## 1.3 GROUP

**1.3.1 Definition**: For $(G, *)$, G is called a group if it satisfies the followings axioms.

(1) $*$ is associative on G, i.e. $a*(b*c) = (a*b) * C \ \forall\ a, b, c \in G$

(2) Identity exits in G i.e., there exist an element $e \in G$ such that

$a*e = e*a = a, \forall\ a \in G$, (Here e is called identity element)

(3) Inverse of every element of G exits in G i.e. for $a \in G$ there exist $b \in G$ such that

$a*b = b*a = e$. We call b as inverse of a.

Beside it if $a*b = b*a \ \forall\ a, b \in G$, then G is called commutative group.

**1.3.2** **Note**: In order to show that a non empty set G is a group, we have to find an operation which is binary on G. In other words we can say that G is closed under that operation and satisfies all the three axioms defined above.

**Example**: I (set of integers) is a group under + i.e. (I, +) is a group

**Solution:** We know that sum of two integers is again an integer; therefore, addition is a binary operation on I.

(1) Ordinary addition is associative since a + (b + c) = (a + b) + c □ a, b, c□G

(2) Zero is an integer such that 0+ a = a + 0 = a □ a □ I; identity exist in I.

(3) For every a□I, we have – a □ I such that a+(-a) = (-a)+a = 0 i.e. inverse of every element exist in I.

As all the axioms of a group are satisfied by elements of I under addition, therefore, it is a group. Further a+b = b+a □ a, b□I. Hence I is commutative group under addition.

**1.3.3** **Note:** Under ordinary addition zero is always identity element and it is called as additive identity while 1 is always multiplicative identity under ordinary multiplication.

**Example**: Q-{0}, the set of all non-zero rational numbers forms a group under multiplication.

**Solution:** Since multiplication of two rational numbers is always a rational number, therefore, multiplication is binary operation on set Q-{0}

(1) Ordinary multiplication is associative because

$$a(bc) = (ab)\,c\ \forall\ a,b,c \in Q\text{-}\{0\}.$$

(2) 1 ∈ Q- {0}, such that 1.a = a.1 = a∀ a∈ Q-{0}. Here 1 acts as identity element.

(3) For a$\in$Q-{0}, we have $\frac{1}{a} \in$ Q-{0} such that a$\frac{1}{a}=\frac{1}{a}$ a=1, therefore, inverse of every element exist in Q-{0}. Hence Q-{0} becomes a group under multiplication.

**Example:** Show that set G of all numbers of the form $a+b\sqrt{2}$, a, b $\in$I forms a group under the operation $(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$ .

**Solution**: Since $(a+c)$ and $(b+d)$ are two integers, therefore,

$(a+b\sqrt{2})+(c+d\sqrt{2})$=$(a+c)+(b+d)\sqrt{2} \in$ G . Hence above operation is binary operation on G.

(1) Since $(a+b\sqrt{2})+((c+d\sqrt{2})+(e+f\sqrt{2}))$

$$=(a+b\sqrt{2})+((c+e)+(d+f)\sqrt{2})$$

$$=(a+c+e)+(b+d+f)\sqrt{2} \qquad (1)$$

Also $((a+b\sqrt{2})+(c+d\sqrt{2}))+(e+f\sqrt{2})$

$$=((a+c)+(b+d)\sqrt{2})+(e+f\sqrt{2})$$

$$=(a+c+e)+(b+d+f)\sqrt{2} \qquad (2)$$

By (1) and (2), we get that associative law holds in G.

(2) $(a+b\sqrt{2})+(0+0\sqrt{2})=(a+0)+(b+0)\sqrt{2}$=$(a+b\sqrt{2})$ i.e. identity exists in G and $0+0\sqrt{2}=0$ is identity element.

(3) For $(a+b\sqrt{2})$ in G we have $(-a-b\sqrt{2})$ exist in G such that

$(a+b\sqrt{2})$+ $(-a-b\sqrt{2})$ = $(-a-b\sqrt{2})$+$(a+b\sqrt{2})$ =0, showing that inverse of every element exist in G.

Since $(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}=(c+a)+(d+b)\sqrt{2}$

= $(c+d\sqrt{2})+(a+b\sqrt{2})$ , therefore, it is commutative group under above binary operation.

**1.3.4 Theorem**: Prove that in a matrix group under matrix multiplication, either all the matrices are singular or non-singular. (Singular matrix is a matrix with zero determinant value and non-singular matrix have non-zero determinant value)

**Proof:** Let M be the matrix group under matrix multiplication as binary operation and E be the identity under multiplication then

$$AE = EA = A \ \forall \ A \in M \qquad (1)$$

If E is singular matrix then the equation (1) is not satisfied by any non-singular matrix A of M. The reason is that if A is non-singular and E is singular then AE is singular and so it cannot be equal to a nonsingular matrix. Therefore if E is singular then every matrix A∈M must be singular.

Now suppose E is non singular matrix .Let A∈M and is singular then there exists no matrix B for which AB=E (since AB will be singular while E is non singular. Thus A does not posses inverse. This contradicts the hypothesis that M is a group. Therefore, if E is non-singular then every matrix in M must be non-singular.

**Note:** By above theorem we see that inverse of a singular matrix also exist. The reason is that if identity element is a singular matrix then we can obtain the inverse of a singular matrix. The following example explains the result.

**Example:** Show that the set of all matrices of the form $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$ where x is non zero real number is a group under matrix multiplication.

**Solution**: let M = {$\begin{bmatrix} x & x \\ x & x \end{bmatrix}$/ x is a non-zero real number} clearly determinant value of this matrix $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$ is zero so it is a singular matrix.

Closure property holds in M because product of two singular matrices is again a singular matrix.

(1) Since matrix multiplication is always associative, associative law holds.

(2) Existence of identity: Let E = $\begin{bmatrix} e & e \\ e & e \end{bmatrix}$ be the identity element, then

AE=EA=A $\forall$ A$\in$M , therefore, $\begin{bmatrix} e & e \\ e & e \end{bmatrix}\begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 2ex & 2ex \\ 2ex & 2ex \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$

$\Rightarrow$ 2ex =x

$\Rightarrow$ e $= \frac{1}{2}$, since x is not zero. Thus E $= \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$.

(3) Existence of inverse: Let A = $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$ be an arbitrary element of M. suppose that B = $\begin{bmatrix} y & y \\ y & y \end{bmatrix}$ is its inverse.

So AB = E $\Rightarrow \begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$

$$\Rightarrow \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \Rightarrow 2\text{xy} = \frac{1}{2} \Rightarrow \text{y} = \frac{1}{4x}$$

Therefore B $= \begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix}$ is inverse of A in M.

**Example:** Show that the set of all real (2×2) matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, ad-bc ≠0 is a group under matrix multiplication as binary operation.

**Solution:** Let G be the set of all real (2×2) matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, ad-bc ≠0. For G to be group it should satisfies the following properties.

(1) Closure property: Let $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ are arbitrary element of G, therefore, $(a_1d_1 - b_1c_1) \neq 0$ and $(a_2d_2 - b_2c_2) \neq 0$.

Now $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$. As

$(a_1a_2 + b_1c_2)(c_1b_2 + d_1d_2) - (c_1a_2 + d_1c_2)(a_1b_2 + b_1d_2)$

$= (a_2d_2 - b_2c_2)\ (a_1d_1 - b_1c_1) \neq 0$. Hence $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in$G.

(2) Associative property: Let A=$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, B=$\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ and C=$\begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$,

then A(BC)

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}\right) = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2a_3 + b_2c_3 & a_2b_3 + b_2d_3 \\ c_2a_3 + d_2c_3 & c_2b_3 + d_2d_3 \end{bmatrix}$$

$$=\begin{bmatrix} a_1(a_2a_3+b_2c_3)+b_1(c_2a_3+d_2c_3) & a_1(a_2b_3+b_2d_3)+b_1(c_2b_3+d_2d_3) \\ c_1(a_2a_3+b_2c_3)+d_1(c_2a_3+d_2c_3) & c_1(a_2b_3+b_2d_3)+d_1(c_2b_3+d_2d_3) \end{bmatrix}$$

$$=\begin{bmatrix} a_1a_2a_3+a_1b_2c_3+b_1c_2a_3+b_1d_2c_3 & a_1a_2b_3+a_1b_2d_3+b_1c_2b_3+b_1d_2d_3 \\ c_1a_2a_3+c_1b_2c_3+d_1c_2a_3+d_1d_2c_3 & c_1a_2b_3+c_1b_2d_3+d_1c_2b_3+d_1d_2d_3 \end{bmatrix}$$

Similarly (AB)C

$$=\begin{bmatrix} a_1a_2a_3+a_1b_2c_3+b_1c_2a_3+b_1d_2c_3 & a_1a_2b_3+a_1b_2d_3+b_1c_2b_3+b_1d_2d_3 \\ c_1a_2a_3+c_1b_2c_3+d_1c_2a_3+d_1d_2c_3 & c_1a_2b_3+c_1b_2d_3+d_1c_2b_3+d_1d_2d_3 \end{bmatrix}$$

=A(BC).

(3) Identity element: As $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$G such that

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix}\in G.$$

(4) Existence of inverse: For $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in$G, we have

$$\begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}\in G \text{ such that}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}=\begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

i.e. inverse of every element exist in G . Hence G is a group.

**Example**: Taking a group {e, x, y, z} of order four, construct two different tables using two binary operation under which this set becomes group. We define two tables as

|  | e | x | y | z |
|---|---|---|---|---|
| e | e | x | y | z |
| x | x | e | z | y |
| y | y | z | e | x |
| z | z | y | x | e |

where $x^2 = y^2 = z^2 = e$ , $xy = z$ ,

(Table 1)

|  | e | x | y | z |
|---|---|---|---|---|
| e | e | x | y | z |
| x | x | y | z | e |
| y | y | z | e | x |
| z | z | e | x | y |

where $x^4 = e$ , x is generator of this group.

(Table 2)

**1.3.5 Definition:** Addition mod m of two integers a and b is written as $a +_m b$ and is the least non-negative integer less then m when sum of a and b is divided by m.

Similarly we define $a \times_m b$ is least non-negative integer less then m when product of a, b is divided by m. This operation is called multiplication mod m.

For example $5 +_5 7 = 2$, $5 +_3 7 = 0$

and $5 \times_3 7 = 2$, $5 \times_2 7 = 1$, $5 \times_{11} 7 = 2$.

**Example:** Set of integers G = {0,1,2… m -1} forms group under addition mod m.

**Solution: -** As we know by definition of division that when an integer is divided by m, its remainder is always less than m, therefore, it is an element of the set G. It is clear by definition of addition mod m that it is binary operation on G.

(i) Associative property holds in G since

$a+_m(b+_mc)$

= $a+_m$ (least non negative remainder when b+c is divided by m)

= Least non-negative remainder when a+(b+c) is divided by m.

= least non negative remainder when (a+b)+c is divided by m.(ordinary addition is associative )

= (Least non negative remainder when a+b is divided by m) $+_mc$

= $(a+_mb)+_mc$ therefore, addition mod is associative.

(ii) Existence of identity: $0 \in G$ acts as identity elements since $0+_ma=a+_m0=a$ □a□G

(iii) Existence of inverse: For □ a□G, we find m-a such that

$a+_m(m-a)=(m-a)+_ma=0$. Therefore inverse of a is m-a. Since $0 \le a \le m$, therefore $m-a \le m$ and hence inverse of a is in G.

Hence G is a group.

**Example:** Show that G ={a / a ∈ $I^+$ (set of positive integers), (a , m) =1 and a < m}i.e set of all positive integers which are less then m( ≥ 2) and are co-prime to m , forms a group under multiplication mod m .

**Note:** (a, m) is notation for greatest common divisor of a and m.

**Solution:** Since by definition of multiplication mod m, $a \times_m b$ always less then m , further a , b ∈ G, therefore, (a, m)=1 and (b, m)=1 and hence $(a \times_m b, m) = 1$ and hence $a \times_m b \in G$ i.e. multiplication mod m is a binary operation on G.

(1) Multiplication is associative as $a \times_m (b \times_m c)$= $a \times_m$(least non-negative remainder when bc is divided by m.

= Least non negative remainder when a(bc) is divided by m

Since ordinary multiplication is associative on set of integers , therefore above expression is

= Least non negative remainder when (ab) c is divided by m

= (Least non negative remainder when ab is divided by m)$\times_m c$

=$(a \times_m b) \times_m c)$

(2) 1 acts as identity element since $1 \times_m b = b \times_m 1$= b for all b in G.

(3) Let a be an arbitrary element of G. Since (a, m) =1, we can find two integer c and d in G such that ac +md =1(this is due to Euler's theorem). Then ac +md-1 is congruent to ac –1 mod m i.e. ac = 1 mod m ⇒ $a \times_m c = 1$ . Hence inverse of every element exists in G. Also $a \times_m b$ is least non-negative remainder when ab is divided by m = least non-negative remainder when ba is divided by m = $b \times_m a$ . Therefore G is a commutative group.

**1.3.6 Note:** -We see that number of elements in a group G, where G is group under addition mod m, is exactly m. But when we take G as a group under multiplication mod m, then number of elements in G is equal to ▨(m),▨ is Euler's function and is calculated as if m=$p_1^{\alpha_1} p_2^{\alpha_2} .........p_n^{\alpha_n}$ then ϕ(m)= ϕ( $p_1^{\alpha_1} p_2^{\alpha_2} .........p_n^{\alpha_n}$ )= ϕ( $p_1^{\alpha_1}$ )ϕ( $p_2^{\alpha_2}$ )…ϕ( $p_n^{\alpha_n}$ )

Where ϕ**(** $p_i^{\alpha_i}$ **)=** $p_i^{\alpha_i - 1}(p_i - 1)$**,** $p_i$ are distinct prime numbers**.**

**1.3.7 Definition:** Let G be a group under * as binary operation, then an element g∈ G is called generator of G if every element of G is equal to $g^t$ for some positive integer t. Here $g^t$ = g*g*g*…*g exactly t times. Such groups are called cyclic group.

**Example:** Set of integers {0,1,2,…,m-1} is a cyclic group under addition modulo m and 1 is the generator of this group

## 1.4 PERMUTATION GROUP

**1.4.1 Definition:** A one-one mapping of G onto itself is called a permutation on G. Generally we take G a finite set. For example if we take G ={1,2}, then number of permutations two exactly two. Let these are $\sigma_1$ and $\sigma_2$ where

$\sigma_1$ is defined as ; $\sigma_1$ (1)=1, $\sigma_1(2)=2$ and

$\sigma_2$ is defined as;$\sigma_2$ (1)=2, $\sigma_2(2)=1$.

Infect if G is a set having n elements then it has n! permutations defined on it.

**1.4.2 Definition**: If f: X→Y and g: Y→Z are two functions, then their product or composition function is defined as fg which is a function from X to Z and for $x \in X$, (x)f g = ((x)f)g. If G has n elements say $a_1, a_2, \ldots, a_n$ then permutation f is represented as $\begin{pmatrix} a_1\ a_2\ a_3 \ldots a_i\ a_k\ a_n \\ a_2\ a_3\ a_i \ldots a_k\ a_n\ a_1 \end{pmatrix}$ gives us that $f(a_1)=a_2$ , $f(a_2)=a_{3,}$ $f(a_i)=a_{k,}$ $f(a_k)=a_{n,}$ $f(a_n)=a_1$ and $f(a_t)=a_t$ for rest of t different from 1,2,3,i,k,n.

**1.4.3 Note:** By a permutation on n symbols means that how many ways we can arrange n different things linearly. If we take G ={$a_1,a_2,a_3$} then number of different arrangement are as follow.$\begin{pmatrix} a_1\, a_2\, a_3 \\ a_1\, a_2\, a_3 \end{pmatrix}$= I,$\begin{pmatrix} a_1\, a_2\, a_3 \\ a_1\, a_3\, a_2 \end{pmatrix}$= $(a_2\ a_3)$,

$\begin{pmatrix} a_1\, a_2\, a_3 \\ a_2\, a_1\, a_3 \end{pmatrix}$= (a$_1$a$_2$), $\begin{pmatrix} a_1\, a_2\, a_3 \\ a_3\, a_2\, a_1 \end{pmatrix}$= (a$_1$a$_3$), $\begin{pmatrix} a_1\, a_2\, a_3 \\ a_2\, a_3\, a_1 \end{pmatrix}$= (a$_1$a$_2$a$_3$),

$\begin{pmatrix} a_1\, a_2\, a_3 \\ a_3\, a_1\, a_2 \end{pmatrix}$= (a$_1$a$_3$a$_2$). These are 3! Permutations i.e. 6 permutations. More over if we write f as (a$_1$,a$_2$,a$_3$,a$_i$,a$_k$,a$_n$) then image of a$_1$ under f is a$_2$ , image of a$_2$ under f is a$_3$ , a$_3$ is a$_i$ , a$_i$ is a$_k$ , a$_k$ is a$_n$ and image of a$_n$ is a$_1$.

**1.4.4 DEFINITION**: A permutation is called cyclic permutation if image of first element is second, image of second is third and so on and image of last element is first element. Number of elements in the cycle is called length of cycle .

**For example** (123) is a cycle of length three.

**1.4.5 Remark** (**1**) A cyclic permutation remains same if we give a cyclic shift to it elements there fore (123)=(231)=(312) but (123)$\neq$ (132).

**(2)** Every permutation on n symbols can be written as product of its cyclic permutation.

**(3)** A cycle of length two is called transposition.

**(4)** A permutation is called even permutation if it product of even number of transpositions other wise it is called odd permutation.

**(5)** Product of even permutations is again an even permutation.

**(6)** Product of two odd permutations is again an even permutation.

**(7)** Product of an odd permutation with an even permutation is an odd permutation.

**(8)** A cycle of odd length is always an even permutation while that off even length is an odd permutation.

**1.4.6** **Note**: If we have two permutations say (123) and (132) then their product is defined as (123) (132)= I. Infect first permutation takes 1 to 2 while second take 2 to 1, therefore their composition takes 1 to 1. Similarly 2 goes to 2 and 3 goes to 3. i.e. resultant permutation is $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ =I.

**1.4.7** **Theorem:** Prove that every permutation on n symbols can be written as product of its cyclic permutations.

**Proof:** Let $a_1,a_2,\ldots,a_n$ are n symbols on which a permutation is taken .Now choose first element say $a_1$ take its image say $a_2$ ,then find image of $a_2$ continue this process till we approaches to $a_1$ which is possible because $a_1$ is also image of some element say $a_i$ .In this way we obtain a cycle $(a_1,a_2,\ldots,a_i)$. Now take $a_t$ which is element of given permutation that does not belongs to the cycle taken above. Repeat the same process for $a_t$. Continuing in this way we get different cycles whose product is given permutation. Hence theorem is proved.

**Example in support of given theorem:** Take a permutation $\begin{pmatrix} 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 4 & 6 & 7 & 8 & 5 & 9 \end{pmatrix}$ i.e. a permutation on nine symbols. It can also be written as $\begin{pmatrix} 2 & 1 & 3 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$ since we can leave those elements, which are left unchanged. Now we start with 1. Image of 1 is 2, image of 2 is 3 and that of 3 is one so we have a cycle (1 2 3) . As 5 is not in cycle (1 2 3) so we start with 5. Clearly image of 5 is 6, image of 6 is 7, Image of 7 is 8 and that of 8 is 5,we get another cycle (5 6 7 8). There fore

$$\begin{pmatrix} 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 4 & 6 & 7 & 8 & 5 & 9 \end{pmatrix} = (1\ 2\ 3)\ (5\ 6\ 7\ 8).$$

**1.4.8 Theorem:** Prove that every cycle of $S_n$ can be written as product of transpositions.

**Proof**: Let ($a_1$ $a_2$ $a_3$ …$a_t$) be a cycle of length t .Now consider the permutation ($a_1$ $a_2$)( $a_1$ $a_3$)…( $a_1$ $a_t$) .we see that under this permutation $a_1$ goes to $a_2$ by first transposition , $a_2$ remains unchanged by rest of transposition of this permutation. So under this permutation $a_1$ goes to $a_2$. Now $a_2$ goes to $a_1$ by first transposition, $a_1$ goes to $a_3$ by second transposition and $a_3$ remains unchanged by rest transposition of this permutation .So $a_2$ goes to $a_3$ .Continuing in this way we get that product of all transposition of this permutation is ($a_1$ $a_2$ $a_3$ …$a_t$) which is a cycle of length t .Hence ($a_1$ $a_2$ $a_3$ …$a_t$) = ($a_1$ $a_2$)( $a_1$ $a_3$)…( $a_1$ $a_t$) .

**Example in support of this theorem:** Take (1 2 3 4) i.e. a cycle of length four, then we can write (1 2 3 4) =(1 2)(1 3)(1 4).

**1.4.9 Corollarary :** Prove that every permutation on n symbols can be written as product of transpositions.

**Proof:** Let f be a permutation on n symbols. We can write f as product of it cyclic permutations (theorem 1.4.7). But we know that every cycle can be written as product of transposition (theorem 1.4.8). So every permutation can be written as product of transposition.

**Example in support of theorem 1.4.9** Take a permutation $\begin{pmatrix} 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 4 & 6 & 7 & 8 & 5 & 9 \end{pmatrix}$ we can write it as a product of different cycles as $\begin{pmatrix} 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 4 & 6 & 7 & 8 & 5 & 9 \end{pmatrix}$**=(1 2 3) (5 6 7 8).** Now we can write (1 2 3) = (1 2)(1 3) and **(5 6 7 8).= (5 6) (5 7) (5 8).** So $\begin{pmatrix} 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 4 & 6 & 7 & 8 & 5 & 9 \end{pmatrix}$**= (1 2)(1 3)(5 6) (5 7) (5 8) .**

**1.4.10 Note (1)** A permutation is called identity permutation if image of every element is same under it i.e. $I(a_i)=a_i$ for all i.

**1.4.11 Theorem**: Prove that $S_n$ i.e. set of all permutations on n symbols becomes a group under composition of mapping as operation.

**Proof**: As we know that composition of mapping which are one –one and onto is again one –one and onto, therefore composition of mapping or permutation is a binary operation on $S_n$

(i) Composition of permutation is associative also as $(a_i)((fg)h)$= $((a_i)(fg))h)$= $((a_if)g)h$=$(a_i)f)(gh)$= $(a_i)(f(gh)$i.e. (fg)h= f(gh)

(ii) Since identity permutation acts as identity element, identity exists in $S_n$

We also know that if a mapping is one –one and onto then its inverse mapping $f^{-1}$ exists and is defined as $f^{-1}(a_i)=a_j$ iff $f(a_j)=a_i$.since every permutation is one-one and onto ,there fore inverse of every element of $S_n$ is in $S_n$ .Hence $S_n$ is a group .It is called group of permutations**.**

**1.4.12 Theorem:** Prove that set of all even permutations is a group and this group is called alternating group of degree n. its order is n!/2 **(**it is generally denoted by $A_n$ ).

**Proof:** Since by remark 1.4.5 (5), we get that product of two even permutations is an even permutation**,** therefore product of permutation is a binary operation on $A_n$ .

(1) This product is associative since $A_n \subset S_n$ and elements of $S_n$ satisfies associative law

(2) As I is an even permutation so $I \in A_n$ acts as identity element.

(3) Let $f \in A_n$ be an even permutation and g be its inverse permutation then fg =I. Since product is even permutation, so by remark 1.4.5 (7) g cannot be odd .So g is even, therefore is an element of $A_n$. Hence proof is over.

**Example in support of this theorem:** Take $S_3$ ={I, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)} then using remark 1.4.5 (8) we get that $A_3$ ={I, (1 2 3), (1 3 2)} is a group as identity exists in $A_3$, inverse of (1 2 3) is (1 3 2).

## 1.5 SOME RESULTS ON GROUP.

**1.5.1 Theorem:** If G is a group, then it has unique identity.

**Proof**: Let if possible e and f be two identity elements of G,

then e.f = e (taking f as identity element ) (1)

and e.f = f (taking e as identity element ) (2)

From (1) and (2) we get e = f i.e. identity is unique.

**1.5.2 Theorem**: In a group inverse of each element is unique.

**Proof:** Let $a \in G$ has two inverse b and c say, then by definition of inverse

$$a.b=b.a=e \qquad (1)$$

$$a.c=c.a=e \qquad (2)$$

Since b.(a.c)=(b.a).c (by associative law) (3)

Also b.(a.c)=b.e=b (4)

and (b.a).c=e.c=c (5)

By (3),(4),(5) we get b=c.

i.e. Inverse of an element is unique in G.

**1.5.3 Theorem**: For a group G, prove that for every a in G, $(a^{-1})^{-1}$=a when operation is multiplicative and -(-a) =a when operation is additive.

**Proof**: Let $a^{-1}$ be inverse of a and $(a^{-1})^{-1}$ be inverse of $a^{-1}$ then by definition of inverse $a^{-1} . a = a . a^{-1} =e$ (1)

and $a^{-1} . (a^{-1})^{-1} = (a^{-1})^{-1} . a^{-1} =e$ (2)

Now using (1), (2) and theorem 1.5.2 we get $(a^{-1})^{-1}$=a.

Similarly we can show second result.

**1.5.4 Theorem**: Prove that for all a and b in a group G we have $(ab)^{-1} = b^{-1}a^{-1}$ and under addition it can be written as –(a+b) =(-b) + (-a).

**Proof:** Let $(ab)^{-1}$ be inverse of ab, then by definition of inverse

$(ab). (ab)^{-1} = (ab)^{-1}.(ab) = e$ (1)

and $(ab). b^{-1}a^{-1} = a(bb^{-1})a^{-1} = a.e.a^{-1} =e$ (2)

$b^{-1}a^{-1} (ab)= b^{-1}(a^{-1} a).b = b^{-1}e.b = e$ (3)

By (2) and (3), $b^{-1}a^{-1}$ is inverse of ab. Now using (1), (2), (3) and theorem 1.5.2 we get $(ab)^{-1} = b^{-1}a^{-1}$.

Similarly we can show second result.

## 1.6 SUBGROUP

**1.6.1 Definition:** Let H be a subset of a group G. If H also becomes a group under the same binary operation as in G, then H is called as a subgroup of G.

**Example:** Take 2I, the set of even integers, then it is a group under ordinary addition. Since $2I \subset I$ , the set of integers which is also a group under ordinary addition, therefore, 2I is a subgroup of I.

**Example**: Take $G=\{1,a,a^2,a^3,a^4,a^5\}$such that $a^6=1$ , then G becomes a group multiplication. Now take $H=\{1,a^3\}$; $a^6=1$. Clearly H is also a group under multiplication and is a subgroup of G.

**1.6.2** **Theorem**: A subset H of a group G will be a subgroup of G if and only if $a^{-1}b \in H \ \forall\ a, b \in H$ (Equivalently, for a subset H of G, $HH^{-1} = H$ if and only if H is a subgroup of G).

**Proof:** Let H be a subgroup of group G, therefore, for a, b $\in$H, $a^{-1}\in H$ and by closure property $a^{-1}b\in H$. Conversely let us suppose that H is a subset of G such that $a^{-1}b\in H\ \forall$ a, $b\in H$. Since H is subset of G, therefore, elements of H satisfies associative property.

Also for $a\in H$, a, a $\in H$ which gives us that $a^{-1}a=e\in H$ i.e. identity exist in G.

Again a, $e\in H \Rightarrow a^{-1}e= a^{-1}\in H\ \forall\ a\in H$ i.e inverse of every element exist in G.

Finally $a\in H \Rightarrow a^{-1}\in H$, therefore, $(a^{-1})^{-1}\cdot b = ab\in H\ \forall\ a,b\in H$ i.e. closure property is satisfied by the element of H.

Since H satisfies all the axioms of a group, it becomes a subgroup of G.

**1.6.3** **Theorem:** Let G is a finite group, then a subset H of G will be a subgroup of G if and only if it is closed under binary operation defined on G i.e. $ab\in H\ \forall$ a, $b\in H$ (Equivalently, for a finite group G, a subset H of G will be a subgroup of G if and only if HH = H).

**Proof**: Let H be a subgroup, then for a,b $\in$H, ab$\in$H (by definition of group).Conversely, let us suppose that ab$\in$H $\forall$ a,b$\in$H, we assert that H is a subgroup of G.

Since H is a subset of G, elements of H satisfy associative law.

For a$\in$H, by assumption, aa=$a^2\in$H. Similarly $a^k\in$H. But H is finite being a subset of finite set, therefore, there exist positive integers s and t such that

$a^s=a^t \Rightarrow a^{s-t}=e\in H$ , showing that identity exist in H.

Also we can write $a^{s-t}= a^{s-t-1}a=e \Rightarrow a^{s-t-1}$ is inverse of a exist in H. Similarly we can show that inverse of every element of H exist in H. Hence H is a subgroup of G.

**Example:** Let G be the group of all real (2×2) matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ , ad-bc $\neq$0 with matrix multiplication as binary operation. Show that the set H $=\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\in G \ / \ ad \neq 0\}$ is a subgroup of G.

**Solution**: Let $h_1$ and $h_2$ be arbitrary elements of H , then $h_1 =\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}$ and $h_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}$ . Now $(h_2)^{-1} = \dfrac{1}{a_2d_2}\begin{bmatrix} d_2 & -b_2 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} \dfrac{1}{a_2} & \dfrac{-b_2}{a_2d_2} \\ 0 & \dfrac{1}{d_2} \end{bmatrix}$.

and h$_1$ (h$_2$)$^{-1}$ = $\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} \frac{1}{a_2} & \frac{-b_2}{a_2 d_2} \\ 0 & \frac{1}{d_2} \end{bmatrix} = \begin{bmatrix} \frac{a_1}{a_2} & \frac{-a_1 b_2}{a_2 d_2} + \frac{b_1}{d_2} \\ 0 & \frac{d_1}{d_2} \end{bmatrix}$ ∈H because

$\frac{a_1}{a_2}\frac{d_1}{d_2} \neq 0$.

**Example:** Show that the set K = $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ is a subgroup of the group H ={$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$/ ad ≠ 0, a, b, c are all real numbers}. H is group under matrix multiplication as binary operation.

**Solution**: let k$_1$ and k$_2$ are two elements of K. we will show that k$_1$ .k$_2$∈K. let k$_1$ =$\begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix}$ and k$_2$ =$\begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix}$, then (k$_2$)$^{-1}$ =$\begin{bmatrix} 1 & -b_2 \\ 0 & 1 \end{bmatrix}$

and k$_1$ (k$_2$)$^{-1}$ =$\begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -b_2 + b_1 \\ 0 & 1 \end{bmatrix}$ which is an element of K.

Hence K is a subgroup H.

**1.6.4** **Note:** The result in Theorem 1.6.3 is true when G is finite. For example if we take G an infinite set say N (set of natural numbers) then G is closed under multiplication but it is not a group.

**1.6.5** **Theorem:** Prove that intersection of two subgroups of a group G is again a subgroup of G.

**Proof**: Let H and K are two subgroups of a group G. If $H \cap K = \{e\}$ then we have nothing to prove, so suppose that h, $k \in H \cap K$. We will show that $hk^{-1}$ belongs to $H \cap K$.

As $h \in H \cap K \Rightarrow h \in H$ and $h \in K$ .

Similarly $k \in H \cap K \Rightarrow k \in H$ and $k \in K$.

Now $h \in H$ and $k \in H \Rightarrow hk^{-1} \in H$ (H is a subgroup of G)

Similarly h K and $k \in K \Rightarrow hk^{-1} \in K$ (K is a subgroup of G)

Adding both results we get that $hk^{-1} \in H \cap K$.

**1.6.6 Theorem:** Prove that arbitrary intersection of subgroups of a group G is a subgroup of G.

**Proof**: Let G be a group and let $\{H_t: t \in T\}$ be any family of subgroups of G. here T is an index set and is such that for all $t \in T$, $H_t$ is a subgroup of G. Let $H = \bigcap_{t \in T} H_t$ =$\{x \in G : x \in H_t \ \forall \ t \in T$.

Now let a and b be any two elements of H. then

$$a \in \bigcap_{t \in T} H_t \Rightarrow a \in H_t \quad \forall t \in T \quad \text{and}$$

$$b \in \bigcap_{t \in T} H_t \Rightarrow b \in H_t \quad \forall t \in T .$$

But for all $t \in T$, $H_t$ is a subgroup of G. therefore $a \in H_t$, $b \in H_t \Rightarrow ab^{-1} \in H_t \ \forall$ $t \in T$. Consequently $ab^{-1} \in \bigcap_{t \in T} H_t \ \forall t \in T$ . There fore $\bigcap_{t \in T} H_t$ is a subgroup.

**1.6.7 Theorem:** Prove that union of two subgroups of a group G is again a subgroup of G if and only if one is contained in the other.

**Proof**: Suppose H and K are two subgroups of a group G. Let us suppose that $H\subset K$ or $K\subset H$ then $H\cup K$ is equal to H or K. But H and K both are subgroup of G , therefore $H\cup K$= H or K is also a subgroup.

Conversely, suppose that $H\cup K$ is a subgroup of G. Let us assume that H is not a subset of K and K is not a subset of H.

Now H is not subset of K $\Rightarrow \exists$ $h\in H$ such that $h\notin K$ (1)

Also K is not a subset of H $\Rightarrow \exists$ $k\in K$ such that $k\notin H$ (2)

But by (1), $h\in H\cup K$ and by (2), $k\in H\cup K$ so $hk \in H\cup K$. Let hk = t, therefore $t\in$ H or K. If t belongs to H then $k = h^{-1}t$ belongs to H, a contradiction. Hence t does not belong to H. Similarly we can show that t does not belong to K. It shows that t does not belongs to $H\cup K$, a contradiction and hence a contradiction to our assumption that H is not a subset of K and K is not a subset of H. Hence either H is subset of K or K is subset of H.

## 1.7 COSET

**1.7.1 Definition:** For a group G and subgroup H of it we define $a*H =\{a*h/ h\in H\}$. This set is called coset of H in G generated by a. a*H is called left coset of H in G. Similarly H*a is called right coset of H in G.* is binary operation on G.

**Example** Take G=(I,+) and H ={2I,+} then 0+Hand 1+H are two different left cosets given as

$0+H = \{0+h/h\in H\}$ = H which is set of even integers and

$1+H = \{1+h/h\in H\}$ which is set of odd integers. We also note that I is union of H and 1+H.

**1.7.2 Theorem:** If $c\in aH$, then cH = aH and $c\in Ha$, then Hc = Ha

**Proof:** Since $c\in aH \Rightarrow c = ah_1$ for some $h_1\in H$,

But then $ch = ah_1h = ah_2 \in aH$.

As ch is arbitrary element of cH, therefore cH$\subseteq$aH.

Now c=ah$_1$ $\Rightarrow$ a= c $(h_1)^{-1}$ $\Rightarrow$ ah = c $(h_1)^{-1}$h $\in$ cH,

Therefore aH $\subseteq$ cH. Hence the result is over**.** Similarly we can prove second part**.**

**1.7.3 Theorem**: For a subgroup H of G, if aH and bH are two left cosets of H in G, then either aH = bH or aH $\cap$ bH = $\phi$.

**Proof:** If aH $\cap$ bH = $\phi$ then we have nothing to prove.

So suppose that c$\in$ aH $\cap$ bH.

This implies that c$\in$ aH and c$\in$bH.

But c$\in$ aH

$\Rightarrow$ cH = aH

and c$\in$ bH

$\Rightarrow$ cH = bH (by theorem 1.7.2).

Therefore aH = bH .

**1.7.4 Theorem**: If a and b are any two element s of a group G and H any subgroup of G, then

Ha = Hb if and only if ab$^{-1}$$\in$ H and aH = bH if and only if a$^{-1}$ b $\in$ H.

**Proof**: Since a is an element of Ha then

Ha = Hb $\Rightarrow$ a $\in$ Hb $\Rightarrow$ ab$^{-1}$$\in$ Hbb$^{-1}$ = H.

Conversely let us suppose that

ab$^{-1}$$\in$ H $\Rightarrow$ ab$^{-1}$b$\in$ Hb $\Rightarrow$ a $\in$ Hb, but then by theorem 1.7.2 Ha = Hb. Similarly we can prove other part .

**1.7.5 Theorem :**If we define that $a \cong b \mod H$ if and only if ab$^{-1}$ $\in$H. then this is an equivalence relation and class of a mod H is right coset of H in G generated by b.

**Proof:** We know a relation is called equivalence relation if it is reflexive, symmetric and transitive. Since aa$^{-1}$ = e $\in$H i.e. relation is reflexive.

Also $a \cong b \mod H$ $\Rightarrow$ that ab$^{-1}$ $\in$H which further gives us that

(a b$^{-1}$ )$^{-1}$ = ba$^{-1}$ $\in$H $\Rightarrow$ $b \cong a \mod H$ i.e. relation is symmetric. Further $a \cong b \mod H$ and $b \cong c \mod H$

$\Rightarrow$ That ab$^{-1}$ $\in$H and bc$^{-1}$ $\in$H $\Rightarrow$ ab$^{-1}$ bc$^{-1}$ $\in$H $\Rightarrow$ ac$^{-1}$ $\in$H i.e. $a \cong c \mod H$.

Hence this relation is an equivalence relation. Now class of a is denoted as [a]={b$\in$H such that $b \cong a \mod H$}. Let b$\in$ [a] then $b \cong a \mod H$ which implies that ba$^{-1}$$\in$H i.e. ba$^{-1}$ a$\in$Ha $\Rightarrow$ b $\in$Ha there fore [a] $\subseteq$ Ha. Conversely let suppose that h$\in$ Ha is an arbitrary element of Ha. But h$\in$ Ha $\Rightarrow$ ha$^{-1}$$\in$h i.e. $h \cong a \mod H$. Hence h $\in$ [a] giving us that Ha $\subseteq$ [a] .there fore [a] =Ha.

Hence the result is proved**.**

**1.7.6 Note:** We know that for every g$\in$G we have a coset gH such that g$\in$ gH. Hence we can write $G = \bigcup_{g \in G} gH = \bigcup_{g \in g} Hg$

**Example**: Find all left cosets of V$_4$ ={I , (1 2)(3 4) ,(1 3)(2 4) , (1 4)(2 3)} in S$_4$

**Solution**: First we will see that V$_4$ is a group. Being a subset of S$_4$ associative law is followed by elements of V$_4$. Also inverse of (1 2)(3 4) is (1 2)(3 4) as (1 2) (3 4). (1 2)(3 4) =I. Similarly each element of V$_4$ is inverse of itself.

Now V$_4$ is **first left coset** which is {I, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}

For **second left coset** we take (1 2 3) $V_4$ = {(1 2 3) I, (1 2 3)(1 2)(3 4), (1 2 3)(1 3)(2 4), (1 2 3)(1 4)(2 3)}

= {(1 2 3), (2 4 3), (1 4 2), (1 3 4)}

For **third left coset** we take

(1 2 4) $V_4$ = {(1 2 4) I, (1 2 4)(1 2)(3 4), (1 2 4) (1 3)(2 4), (1 2 4)(1 4)(2 3)}

= {(1 2 4), (2 3 4), (1 4 3) (1 3 2)}.

For **forth-left coset** we take (1 2 3 4) $V_4$

= {(1 2 3 4) I, (1 2 3 4)(1 2)(3 4), (1 2 3 4) (1 3)(2 4), (1 2 3 4)(1 4)(2 3)}

= {(1 2 3 4), (2 4), (1 4 3 2), (1 3)}

For **fifth left coset** we take (1 2 4 3) $V_4$

= (1 2 4 3) I, (1 2 4 3)(1 2)(3 4), (1 2 4 3) (1 3)(2 4), (1 2 4 3)(1 4)(2 3)}

={(1 2 4 3), (2 3), (1 4), (1 3 4 2)}.

For **sixth left coset** we take (1 3 2 4) $V_4$

= {(1 3 2 4) I, (1 3 2 4)(1 2)(3 4), (1 3 2 4) (1 3)(2 4), (1 3 2 4)(1 4)(2 3)}

= {(1 3 2 4) , (1 4 2 3) , (3 4) , (1 2)}.

**Here we see that union of all left cosets** is {I, (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2 3), (1 2 4), (1 3 4), (2 3 4), (1 3 2), (1 4 2), (1 4 3), (2 4 3), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)} which is $S_4$. i.e. $S_4 = G = \bigcup_{g \in G} gH$ .

Now $V_4$ is **first right coset** which is {I, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}

For **second right coset** we take $V_4$(1 2 3) = {I (1 2 3), (1 2)(3 4) (1 2 3), (1 3)(2 4) (1 2 3), (1 4)(2 3) (1 2 3)}

= {(1 2 3), (1 3 4) , ( 2 4 3), (1 4 2)}

For **third right coset** we take

$V_4$ (1 2 4) = {I (1 2 4), (1 2)(3 4) (1 2 4), (1 3)(2 4) (1 2 4), (1 4)(2 3) (1 2 4) }

= {(1 2 4), (1 4 3), (1 3 2) ,(2 3 4)}.

For **forth right coset** we take $V_4$ (1 2 3 4)

= { I (1 2 3 4), (1 2)(3 4) (1 2 3 4), (1 3)(2 4) (1 2 3 4), (1 4)(2 3) (1 2 3 4) }

= {(1 2 3 4), (1 3), (1 4 3 2), (2 4)}.

For **fifth right coset** we take $V_4$ (1 2 4 3)

= {I (1 2 4 3), (1 2)(3 4) (1 2 4 3), (1 3)(2 4) (1 2 4 3), (1 4)(2 3) (1 2 4 3) }

={(1 2 4 3), (1 4), (2 3) , (1 3 4 2)}.

For **sixth right coset** we take $V_4$ (1 3 2 4)

= {I (1 3 2 4), (1 2)(3 4) (1 3 2 4), (1 3)(2 4) (1 3 2 4) , (1 4)(2 3) (1 3 2 4) }

= {(1 3 2 4), (1 4 2 3), (1 2) , (3 4) }.

**Here we see that union of all right cosets** is {I, (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2 3), (1 2 4), (1 3 4), (2 3 4), (1 3 2), (1 4 2), (1 4 3), (2 4 3), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2), (1 2)(3 4) ,(1 3)(2 4) , (1 4)(2 3)} which is $S_4$ .i.e. $S_4 = \bigcup_{g\in g} Hg$

**1.7.7 Note**: Above result has very fine applications, which are

**(1)** Order of every subgroup of a group divides order of group. (Order of a group means the number of elements it has. It is also called Lagrange's theorem)

**(2)** Order of every element of G divides order of group G. (Order of element $g \in G$ means smallest positive integer t such that $g^{t}$ =e, identity of G.)

**(3)** Number of distinct left or right cosets of H in G is called index of H in G .It is given by $\frac{O(G)}{O(H)}$.

## 1.8 KEY WORDS

Binary operation, groups subgroups, permutation, identity, inverse.

## 1.9 SUMMERY: This chapter contains definition of groups, subgroups, permutation group, cosets and some theorem on groups

## 1.10 SELF ASSESSMENT QUESTIONS

(1) Proves that set of all $(2 \times 2)$ non-singular matrices is a group under multiplication of matrices.

(2) Let G ={$a_0$ , $a_1$ , $a_2$ , $a_3$ , $a_4$ , $a_5$ , $a_6$ } where

ai . aj = ai+j if i+j< 7

ai . aj = ai+j-7 if i+j $\geq$ 7 .( for example $a_4$ .$a_5$ = $a_{5+4-7}$ = $a_{2.)}$

(3) Find all the cosets of H={$1,a^3$} in G ={$1,a,a^2,a^3,a^4,a^5$}such that $a^6$=1 .

(4) Prove that group and subgroup have same identity.

(5) Prove that union of subgroup of G may or may not be a subgroup of G.

(6) Prove or disprove whether the following is a group or not

| × | 1 | a | b | c |
|---|---|---|---|---|
| 1 | 1 | a | b | c |
| a | a | 1 | c | B |
| b | b | c | 1 | A |
| c | c | b | a | 1 |

Where $a^2 = b^2 = c^2 = 1$, ab=c. Also find out $a^{-1}$, $b^{-1}$,$c^{-1}$,$(ab)^{-1}$.

(7) Prove that those elements of a group G which commute with the square of a given element b of G forms a subgroup H of G and those which commute with b it self form a subgroup of H.

(8) (a) Can an abelian group have a non-abelian subgroup.

(b) Can a non abelian group have an abelian subgroup.

(c) Can a non abelian group have a non-abelian subgroup. Give an example in support of your answer.

(9) Prove that following table on relation of elements of set G = {0 1 2 3 4 5} multiplication mod 6 is not a group

|  | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 0 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

(10) Let R be a group under multiplication and Q be a subset of R and is a group under addition . Can it be a subgroup of R?

(11) Let G be the group of integer under addition .let $H_n$ be the set of all integer which are multiple of fixed integer n. Show that it is a subgroup of G .is it a normal subgroup. Determine the index of $H_n$ in G and write all the cosets of $H_n$ in G. also find out $H_n \cap H_m$.

(12) Prove that set of all n th root of unity forms a group under multiplication

**Answer** (1) Yes it is a group.

(2) Yes it is a group.

(3) It has three cosets given as H = $\{1,a^3\}$, aH = $\{a,a^4\}$and $a^2$H= $\{a^2,a^5\}$ it is clear that their union is G.

(6) Yes it is a group and $a^{-1}$=a , $b^{-1}$=b, $c^{-1}$=c,$(ab)^{-1}$= c.

(10) No it cannot be a subgroup because if it is a subgroup of R then Q and R must have binary operation**.**

(11) $H_n \cap H_m$ will contain set of all integers, which are multiple of t, where t is least common multiple of n and m.

## 1.11 SUGGESTED READINGS

(1) I.N. Herstein, Topics in Algebra, Wiley eastern Ltd., New Delhi, 1975.

(2) Surjeet Singh and Quazi Zameeruddin., Modern Algebra.

**MCA-205: Mathematics –II (Discrete Mathematical Structures)**

**Lesson No: 2** **Written by Pankaj Kumar**

**Lesson: Group theory - II** **Vetted by Prof. Kuldip Singh**

## STRUCTURE

**2.0 OBJECTIVE :** Objective of this chapter is to define some more algebraic structure and to find their application in communication and computer.

**2.1 INTRODUCTION :** In Chapter 1, we see that there are subsets of a given group becomes a group in itself under the same operation as in G. We call these subsets as sub-groups of G. In this chapter we define some other condition on subgroup of G. We have defined some more algebraic structure.

At last we have shown the applications of these algebraic structures in modular arithmetic, coding theory and finite state machine.

## 2.2 N0RMAL SUBGROUP

### *2.2.1 **Definition: A** subgroup H of group G is called a normal subgroup of G. If gH = Hg $\forall$ g $\in$ G.*

### *2.2.2 **Theorem :** If G is commutative group, then prove that every subgroup of G is normal in G.*

**Proof**: Let H be a subgroup of G. Now for some C $\in$ gH, C = gh, h $\in$ H. Since h and g both are elements of G and G is commutative, therefore, gh=hg. As hg is element of Hg, therefore C $\in$ Hg. But C is arbitrary element of gH, therefore gH $\subseteq$ Hg.

Similarly we can show that Hg $\subseteq$ gH. Hence gH = Hg $\forall$ g $\in$ G. It proves the result.

### *2.2.3 **Theorem: A** subgroup H of a group G will be normal in G if and only if $g^{-1}hg$ $\in$ H for all g $\in$ G and h $\in$ H.*

**Proof**: Let H be a normal subgroup of G, then by definition of normal subgroup gH = Hg $\forall$ g $\in$G. On multiplying both sides by $g^{-1}$, we get that $g^{-1}gH = g^{-1}$ Hg $\forall$ g $\in$G i.e $g^{-1}Hg$ = H $\forall$ g $\in$ G which implies that $g^{-1}$ hg $\in$ H $\forall$ h $\in$ H and g $\in$ G.

Conversely let us suppose that $g^{-1}hg$ $\in$ H $\forall$ g $\in$ G and h $\in$ H. Now $g^{-1}hg$ $\in$ H that implies $gg^{-1}hg$ $\in$ gH $\Rightarrow$ hg $\in$ gH. As hg is general element of Hg, hence Hg $\subseteq$ gH.

Moreover number of elements in Hg is equal to number of elements in gH. Hence gH = Hg, i.e. H is normal in G. Hence the result is proved.

***2.2.4 Remark:*** *Number of elements in Hg is equal to number of elements in gH and it can be shown by defining a mapping from gH to Hg as f: gH $\rightarrow$ Hg by f(gh) = h'g for some h' $\in$ H.*

***2.2.5 Theorem:*** *Let G be a group. If index of subgroup H in G is two, then H is normal subgroup of G.*

**Proof**: As we know that H is a coset of H itself given by e $\in$ G. If gH is another coset [$\because$ index of H in G is two] then

G = H $\cup$ gH … (i) [$\because$ G is union of all distinct cosets of H in G].

Similarly we can write G = H $\cup$ Hg … (ii)

By (i) and (ii) we get that Hg = gH $\forall$ g $\in$ G. i.e. H is normal in G.

**2.2.6 Theorem:** A subgroup N of a group G is normal in G if and only if the product of two-left coset of N in G is again a left coset in G. (or product of two right cosets of N in G is again a right coset).

**Proof:** first we suppose that N is a normal subgroup of G. let aN and bN are its two left cosets of N in G given by a and b then

(a N).(b N) = (a .(N b)N) (By associative property of group G).

= a (b N) N (Since N is normal therefore N b = b N ).

= ab N = cN for ab = c which is again a left coset.

Conversely suppose that

$g_1N \,.\, gN = g_2 N$

$\Rightarrow (g_2)^{-1}\ g_1N \,.\, gN \subseteq (g_2)^{-1} g_2 N \subseteq N$

$\Rightarrow g^1 N g N \subseteq N$ where $g^1 = (g_2)^{-1} g_2\ \forall\ g \in G$.

$\Rightarrow$ Ng N $\subseteq$ $(g^1)^{-1}$N

$\Rightarrow$ Ng $\subseteq$ $(g^1)^{-1}NN^{-1}=(g^1)^{-1}N$ $\forall$ g$\in$G (1) (For a subgroup N, $NN^{-1}$=N )

But g$\in$ g N $\Rightarrow$ g$\in$ $(g^1)^{-1}$N $\Rightarrow$ g N = $(g^1)^{-1}$N ( by theorem 1.7.2 ) (2)

Now using (1) and (2) we get

Ng $\subseteq$ g N

As order of Ng and g N is same , therefore,

Ng = gN $\forall$ g$\in$G

Hence N is a normal subgroup of G .

**2.2.7** Theorem: **Let N and M be the normal subgroups of a group G such that N$\cap$M = (e). Prove that for any n$\in$N, m$\in$M we have nm =mn.**

Proof: **Let us consider an element $n^{-1}m^{-1}nm$ for n$\in$N and m$\in$M. Because N is normal in G, $m^{-1}nm$ belongs to N. Since $n^{-1}$ also belongs to N, we have $n^{-1}m^{-1}nm$$\in$N.**

**Similarly, as M is also normal, $n^{-1}m^{-1}n$ $\in$ M and hence $n^{-1}m^{-1}nm$ belongs to M. Therefore,**

$$n^{-1}m^{-1}nm \in N\cap M .$$

**But by given condition N$\cap$M = (e), therefore,**

$$n^{-1}m^{-1}nm = e \Rightarrow mn\, n^{-1}m^{-1}nm = mn$$

**$\Rightarrow$ nm = mn. Hence the theorem is proved.**

**2.2.8** Theorem: **If we define NM {nm / n$\in$ N, m$\in$ M}. Prove that if N is a normal subgroup of G then NM is also a subgroup of G. If both N and M are normal subgroups of G then NM is also a normal subgroup of G.**

Proof: **Let nm and rt be two elements of NM. Then $(rt)^{-1} = t^{-1} r^{-1}$ is in G .we will show that nm $(rt)^{-1}\in$NM.**

**Since nm $(rt)^{-1}$ = nm $t^{-1} r^{-1} = n(m t^{-1})r^{-1} (m t^{-1})^{-1}m t^{-1}$ .**

**Now $r^{-1}$ belongs to N, therefore, $(m t^{-1})r^{-1} (m t^{-1})^{-1}$ also belongs to N (because N is normal) and hence $n(m t^{-1})r^{-1} (m t^{-1})^{-1}$ belongs to N.**

**Further $mt^{-1}$ belongs to M implies that $n(m t^{-1})r^{-1} (m t^{-1})^{-1}m t^{-1}$ = nm $(rt)^{-1}$ belongs to NM. Hence NM is a subgroup of G.**

**Now we will show that $g^{-1}nm\,g \in$ NM. As**

**$g^{-1}nm\,g = g^{-1}ngg^{-1}\,m\,g$**

**belongs to NM { because $g^{-1}ng \in$N (N is normal in G) and $g^{-1}\,m\,g \in$M (M is normal in G)}. Hence NM is a normal subgroup of G.**

**Example**: Show that $V_4$ is normal in $A_4$ where $V_4$ is {I , (1 2)(3 4) ,(1 3)(2 4) , (1 4)(2 3)} and $A_4$ is {I, , (1 2 3), (1 2 4), (1 3 4), (2 3 4), (1 3 2), (1 4 2), (1 4 3), (2 4 3), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}.

**Solution: we will show that every left coset is equal to right coset.** Now $V_4$ is **first left coset** which is {I, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)} and corresponding **right coset** is {I, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}.

More over (1 2)(3 4) $V_4$ = (1 3)(2 4) $V_4$ = (1 4)(2 3) $V_4$ = $V_4$ = $V_4$ (1 2)(3 4) = $V_4$ (1 3)(2 4) = $V_4$ (1 4)(2 3). (by use of theorem 1.7.2)

## Now we calculate left coset of $V_4$ generated by (1 2 3)

(1 2 3) $V_4$ = {(1 2 3) I, (1 2 3)(1 2)(3 4), (1 2 3) (1 3)(2 4), (1 2 3)(1 4)(2 3)}

= {(1 2 3), (2 4 3), (1 4 2), (1 3 4)}.

## And corresponding right coset is

$V_4$ (1 2 3) = {I (1 2 3), (1 2)(3 4) (1 2 3), (1 3)(2 4) (1 2 3), (1 4)(2 3) (1 2 3)}

= {(1 2 3), (1 3 4), ( 2 4 3), (1 4 2)}.

We get (1 2 3) $V_4$ = $V_4$ (1 2 3).

(2 4 3)$V_4$ = (1 4 2) $V_4$ =(1 3 4) $V_4$ = (1 2 3) $V_4$ = $V_4$ (1 2 3). =$V_4$ (1 3 4) = $V_4$ (2 4 3) = $V_4$ (1 4 2) . by use of theorem 1.7.2

**For third left coset we get**

(1 2 4) $V_4$ = {(1 2 4) I, (1 2 4)(1 2)(3 4), (1 2 4) (1 3)(2 4), (1 2 4)(1 4)(2 3)}

= {(1 2 4), (2 3 4), (1 4 3) (1 3 2)}.

**For third right coset we get**

$V_4$ (1 2 4) = {I (1 2 4), (1 2)(3 4) (1 2 4), (1 3)(2 4) (1 2 4), (1 4)(2 3) (1 2 4)}

= {(1 2 4), (1 4 3), (1 3 2) ,(2 3 4)}. We get that (1 2 4) $V_4$ = $V_4$ (1 2 4).

From above we get that each left coset of $V_4$ in $A_4$ is equal to a right coset of $V_4$ in $A_4$. Hence $V_4$ is normal in $A_4$.

**Example:** Show by an example that we can find three subgroups E, F and G of a group such that $E \subset F \subset G$. E is normal in F and F is normal G but E is not normal in G.

**Solution:** Let us take $S_4$ (symmetric group of degree 4 over the set{1, 2, 3, 4}). Take E = {I , (1 2)}, F = $V_4$ and G =$A_4$.

First we se that E is a subset of F. More over E is also a group (See problem 1) under the same operation as F is. Therefore, E is a subgroup of F. Since index of E in F is two, therefore by Theorem 2.2.5, E is normal in F .By previous example F is normal in G. We will show that E is not Normal in G. for it we will show that there exist an element of G for which left coset of E is not equal to right coset of E.

**Calculate left coset of E given by (1 2 3)**

(1 2 3)E = { (1 2 3)I , (1 2 3)(1 2) } = {(1 2 3) , (2 3)} …….(1)

**And right coset of E given by (1 2 3)**

E (1 2 3) = { I (1 2 3) , (1 2)(1 2 3) } = { (1 2 3) , ( 1 3) }……(2) .we see that set given in (1) is not equal to set given in (2) so

**(1 2 3)E $\neq$ E (1 2 3),**therefore, E is not normal in G.

***2.2.7 Remark:*** *For a finite group G, $(g)^{0(G)} = e \ \forall g \in G$. This result is due to Lagrange's theorem.*

## 2.3 SEMI GROUP AND FREE SEMI GROUP

***2.3.1 Definition: A** set G is called semi group if there is a binary operation on G which is associative on G. i.e. if it is a binary operation then a . (b . c) = (a . b) . c $\forall$ a, b, c $\in$ G.*

**Example**: Set of natural number is a semi group under ordinary addition. Since sum of two natural numbers is a natural number and

$a + (b + c) = (a + b) + c \; \forall \; a, b, c \in N$.

**2.3.3** Remark: Every group is a semi group but converse may not be true. Above example shows this case.

**2.3.4** Definition: For a given set G = {$a_1$, $a_2$, …, $a_n$} we define $a_1$, $a_2$, $a_1$, $a_2$, … or $a_1a_2a_3a_1a_4a_1$ as the sequence of elements of G. If G* is set of all finite sequences and for $\alpha$, $\beta \in$ G* where $\alpha = a_1a_2 \ldots a_k$, $\beta = a_1a_2a_1a_2a_3$ then $\alpha.\beta = a_1a_2 \ldots a_k \, a_1a_2a_1a_2a_3$. Under this relation which is a binary operation on G* becomes a semi group is called free semigroup generated by set G.

## 2.4 APPLICATION OF ALGEBRAIC STRUCTURE IN MODULAR ARITHMATICS.

***2.4.1 In modular arithmetic:** As we know that set of all positive integers less than m and coprime to m forms a group under multiplication mod m, which is denoted by $Z_m^x$. Now the number of positive integers less than m and co prime to m are exactly $\phi$ (m). Since for a $\in Z_m^x$ we have $a^{0(Z_m^x)} \equiv 1$ mod m. In fact we have $a^{\phi(m)} = 1$ mod m for all positive integers. For example take m = 12, then $Z_{12}^x$ = {1, 5, 7, 11}, it is group* *under multiplication mod 12. As multiplication mod 12 is associative, 1 acts identity element and inverse of 1 is 1, 5 is 5, 7 is 7 and 11 is 11 itself mod 12.*

Now by remark 2.2.7, $a^{\phi(12)} = 1 \text{ mod } 12$, $a \in Z_{12}^{x}$

But $\phi(12) = \phi(4)\ \phi(3) = \phi(2^2)\ \phi(3) = 2\times2 = 4$.

Hence $a^4 = 1 \text{ mod } 12$, as $1^4 = 1 \text{ mod } 12$, $5^4 = 1 \text{ mod } 12$, $7^4 = 1 \text{ mod } 12$ and $11^4 = 1 \text{ mod } 12$. In fact $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \text{ mod } 12$.

***2.4.2 Definition:*** *Let $a \in Z_m^x$, then order of a mod m is smallest positive integer t such that $a^t \equiv 1$ mod m and it is denoted by 0(a).*

***2.4.3 Note :****In above example 0 (1) = 1, 0(5) = 2, 0(7) = 2, 0(11) = 2. It is also clear that order of every element also divides order of group $Z_m^x$. So we have an idea about order of a $\in Z_m^x$ by order of $Z_m^x$.*

**2.4.4 Example**: Find remainder when $3^{200}$ is divided by 7.

**Solution**: Take group of integer mod 7 we see that {1, 2, 3, 4, 5, 6} are the positive integer less than 7 which forms group under multiplication mod 7. So $3^{\phi(7)} \equiv 1 \text{ mod } 7$ i.e. $3^6$ gives us remainder 1 when divided by 7.

[Here 0 (3) = 6].

We write it as $3^{6}_{\text{mod } 7} = 1$.

$\therefore\ 3^6 = (7k + 1)$ [$\because$ if an integer gives us remainder 1 when divided by 7 it is of the form 7k + 1]

Now $3^{200} = 3^{(6 \times 33 + 2)} = (3^6)^{33}.9 = (7k + 1)^{33} . 9$

Hence $3^{200}_{\text{mod } 7} = 9$ [$\because$ $(7k + 1)^{33}$ gives us remainder 1 when divided by 7 using the result that if $a \equiv 1 \mod m$ then $a^t \equiv 1 \mod m$]

Now $9_{\text{mod } 7} = 2$

Hence $3^{200}_{\text{mod } 7} = 2$.

## 2.5 SOME DEFINITION AND RESULTS ABOUT CODE WORDS AND CODES

**1**. Code is made of code words. Weight of a code word is number of non-zero entries in that code word. For example 010101 is a code word of weight three.

**2.** When we talk about linear code of length n, it mean code words are n tuples and set of all code words forms a subgroup of group of all n tuples [Here 5 tuple mean a sequence contains exactly 5 elements i.e. 01010 is a 5 tuple].

If we take n tuple over the set {0, 1} then $B^n$ is that set which contains all n tuple and is called set of binary n tuple. For example elements of $B^3$ are {(0,0,0), (0,0,1), (0,1,0), (1,0,0), (1,1,0), (1,0,1), (0,1,1), (1,1,1)} i.e. eight elements. The set $B^n$ forms a group under component wise addition mod 2 i.e.

$(a, b, c) + (a', b', c) = (a +_2 a^1, b +_2 b^1, c +_2 c^1)$

$\therefore$ (1, 1, 0) + (0, 1, 0) = (1+0, 1+1, 0+0) = (1,0,0).

Now we take a subset of $B^3$ = {(000), (110), (011), (101)} it is a subgroup of group $B^3$ under component-wise addition mod 2. then this is code of 3 tuples.

**3** Distance between two code words is the numbers of position at which they differ with each other for example distance between (101) and (110) is 2.

**4**. In this case we take received word and take its distance with code words. We choose that code word which has minimum distance with received word and assume that the above code word was sent.

## 2.6 COSET LEADER DECODING

Now we define coset leader decoding. As we know that if H is a subgroup of $B^n$, then $B^n$ can be written as union of distinct cosets of H in $B^n$. Since received word is an n tuple lies in $B^n$ and hence lies in a coset also we choose the word of minimum weight in a coset as coset leader and we subtract that word from received word and obtain the required code word which was sent. So we use cosets to obtain correct code word.

**For example** in $B^3$ we see that H = {(000), (101), (110), (011)} is a subgroup. Then we get following cosets.

(0,0,0) + H={(0,0,0), (1,0,1), (1,1,0), (0,1,1)}

(1,0,0) + H={(1,0,0), (0,0,1), (0,1,0), (1,1,1)}

are two cosets.

Here (0,0,0) is coset leader for first coset.

And (1,0,0) is coset leader for second coset.

Now if we receive (111) as a word we see that it lies in second coset with coset leader (1,00), hence we decode it to (111) – (1,00) = (011) is code word which was sent.

## 2.7 LANGUAGES

We considered the set S* consisting of all finite strings of elements from the set S. There are many possible interpretations of the elements of S*, depending on the nature of S. If we think of S as a set of “words”, then S* may be regarded as the collection of all possible “sentences” formed from words in S. Of course, such “sentences” do not have to be meaningful or even sensibly constructed. We may think of a language as a complete specification, at least in principle, of three things. First, there must be a set S consisting of all "words" that are to be regarded as being part of the language. Second, a subset of S* must be designated as the set of "properly constructed sentences" in the language. The meaning of this term will depend very much on the language being constructed. So if S is any set, then a subset of free semi group generated by S is called languages on S.

## 2.8 FINITE-STATE MACHINES

We think of a machine as a system that can accept input, possibly produce out put, and have some sort of internal memory that can keep track of certain information about previous inputs. The complete internal condition of the machine and all of its memory, at any particular time, is said to constitute the state of the machine at that time. The state in which a machine finds itself at any instant summarizes its memory of past inputs and determines how it will react to subsequent input. When more input arrive the given state of the machine determine (with the input) the next state to be occupied, and any output that may be produced. If the number of states is finite, the machine is a finite-state machine.

Suppose that we have a finite set $S = \{s_0, s_1, \ldots, s_n\}$, a finite set I, and for each $x \in 1$, a function $f_x: S \to S$. Let $\mathcal{F} = |f_x|\ x \in I|$. the triple $(S, I, \mathcal{F})$ is called a finite-state machine, S is called the state set of the machine, and the elements of S are called states. The set I is called the input set of the machine. For any input $x \in I$, the function $f_x$ describes the effect that this input has on the states of the machine and is called a state transition function. Thus, if the machine is in state is and input x occurs, the next state of the machine will be $f_x$ (is).

Since the next state $f_x$ (is) is uniquely determined by the pair (is, x), there is a function $F: S \times I \to S$ given by

F (is, x) = $f_x$ (is).

The individual functions $f_x$ can all be recovered from a knowledge of F. Many authors will use a function F : S × I → S, instead of a set $|f_x|$ x ∈ I}, to define a finite-state machine. The definitions are completely equivalent.

**Example 1**. Let S = {$s_0$, $s_1$} and I = {0, 1}. Define $f_0$ and $f_l$ as follows:

$F_0$ ($s_0$) = $s_0$,  $f_l$ ($s_0$) = $s_1$,

$F_0$ ($s_1$) = $s_1$,  $f_l$($s_{1)}$ = $s_0$.

This finite-state machine has two states $s_0$ and $s_i$ and accepts two possible inputs, 0 and 1. The input 0 leaves each state fixed, and the input 1 reverses states. We can think of this machine as a model for a circuit (or logical) device and visualize such a device as in Fig. 2.1. The output signals will, at any given time, consist of two voltages, one higher than the other. Either line 1 will be at the higher voltage and line 2 at the lower, or the reverse. The first set of output conditions will be denoted $s_0$ and the second will be denoted $s_1$. An input pulse, represented by the symbol 1, will reverse output voltages. The symbol 0 represents the absence of an input pulse and so results in no change of output. This device is often called a T flip-flop and is a concrete realization of the machine in this example. We summarize this machine in Fig. 2.2. The table shown there lists the states down the side and inputs across the top. The column under each input gives the values of the function corresponding to that input at each state shown on the left.

The arrangement illustrated in Fig. 2.2 for summarizing the effect of inputs on states is called the state transition table of the finite-state machine. It can be used with any machine of reasonable size and in a convenient method of specifying the machine.

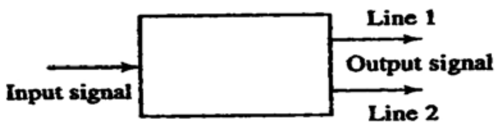
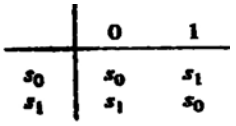


Fig. 2.1



| | 0 | 1 |
|---|---|---|
| $s_0$ | $s_0$ | $s_1$ |
| $s_1$ | $s_1$ | $s_0$ |

Fig. 2.2

**Example 2**: Consider the state transition table shown in Fig. 2.3. Here a and b are the possible inputs, and there are three states, $s_0$, $s_1$ and $s_2$. The table shows us that

$f_a(s_0) = s_0$, $f_a (s_1) = s_2$, $f_a (s_2) = s_1$

and $f_b(s_0) = s_0$, $f_b (s_1) = s_2$, $f_b (s_2) = s_2$

| | a | B |
|---|---|---|
| $s_0$ | $s_0$ | $s_0$ |
| $s_1$ | $s_2$ | $s_1$ |
| $s_2$ | $s_1$ | $s_2$ |

fig. 2.3

If M is a finite-state machine with states S, inputs I, and state transition functions {fx |x ∈ I}, we can determine a relation $R_M$ on S in a natural way. If is, $s_j \in S$, we say that is $R_M s_j$ if there is an input x so that $f_x$ (is) = $s_j$.

Thus is $R_M s_j$ means that if the machine is in state is, there is some input x ∈ I that, if received next, will put the machine in state $s_j$. The relation $R_M$ permits us to describe the machine M as a labelled digraph of the relation $R_M$ on S, where each edge is labelled by the set of all inputs that cause the machine to change states as indicated by that edge. **We see that output in a finite state machine is an element of permutation group of input symbols.**

## 2.9 KEYWORDS AND SUMMARY

In this chapter we have shown the application of Algebraic structure. Keywords are, semigroup codes and finite state machine.

## 2.10 SELF ASSESSMENT QUESTION

1. Find the remainder when $2^{100}$ is divided by 11.
2. Prove that a group is always a semigroup and converse may not be true.
3. Define coset leader decoding on $B^4$ taking its subgroup.
4. Define outputs of a finite state machine.

5 Show that E ={I, (1 2) is a group.

## 2.11 SUGGESTED READINGS

(1) I.N. Herstein, Topics in Algebra, Wiley eastern Ltd., New Delhi, 1975.

(2) Surjeet Singh and Quazi Zameeruddin., Modern Algebra.

(3) Seymour Lepschutz, Finite Mathematics (International edition 1983), McGraw-Hill Book Company , New York.

**MCA-205: Mathematics –II (Discrete Mathematical Structures)**

**Lesson No: 3** **Written by Pankaj Kumar**

**Lesson: Graph theory - I** **Vetted by Prof. Kuldip Singh**

**STRUCTURE**

**3.0 OBJECTIVE:** Objective of this chapter is to gain some knowledge about graphs, which has wide application in computer net working, circuits etc**.**

**3.1 INTRODUCTION:** In this chapter we have defined graph which is pictorial representation of relations on sets. We have defined directed graph, undirected graphs, paths, circuits and matrix associated with graphs.

**3.2 GRAPH: A** pair of set {V, E}, V≠ϕ, constitute a graph. Elements of set V are called vertices while elements of set E are called edges or lines or curves. Generally lines and points of plane represent the edges and vertices of the graph.

**Note:** 1. If V is a finite set then we say that graph is finite graph.

2. Each edge is represented by a pair of vertices say u and v, these vertices are called end point of edges we will denote it by $E_{(u,\ v)}$.

### 3.2.1 Directed graphs

If we put u and v as an ordered pair then edge is called directed from u to v and such a graph in which each edge is directed is called directed graph. For example, figures given below are directed graphs.

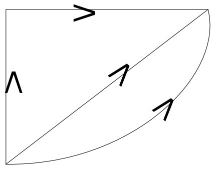


Fig. 3.1

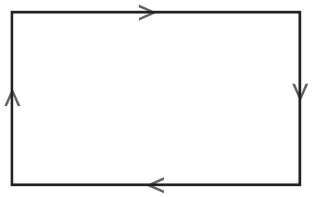
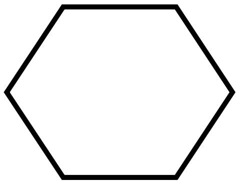


Fig. 3.2

Another example is graph of a relation is always directed graph.

### 3.2.2 Undirected graph

If a graph is not directed is called undirected graph in such graphs edges are given as $E_{(u,\ v)}$. Figure 3.3 and 3.4 are undirected graph



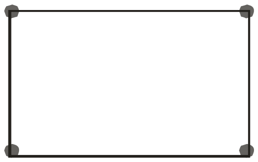


Figure 3.3 Fig. 3.4

**Note**: (1) Edge $E_{(u, u)}$ is called a self loop. A graph with no self loop and no parallel edge is called a simple graph otherwise it is called non-simple. For example graph of a relation which is neither reflexive nor symmetric is simple and that of reflexive relation is not simple. Figure 3.5 and 3.6 are graph which are non-simple and simple respectively.

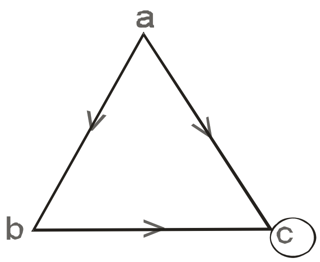


Fig. 3.5

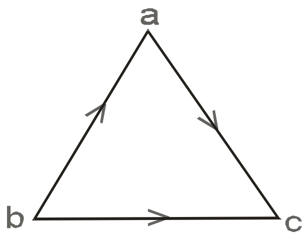


Fig. 3.6

(2) Edges $e_1$ and $e_2$ are parallel edges if they have same vertices. Here $e_1$ and $e_2$ are parallel edges.

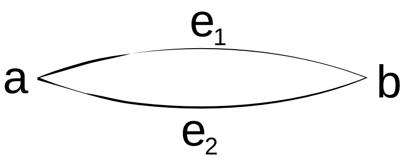


Fig.3.7

## 3.3 PATH AND CIRCUIT

In the following figure, we have $e_{(a_1,a_2)}$, $e_{(a_2,a_3)}$, $e_{(a_3,a_4)}$ $e_{(a_4,a_5)}$, $e_{(a_5,a_6)}$ are the edges so that we move from $a_1$ to $a_6$ along these edges without using an edge more than once.

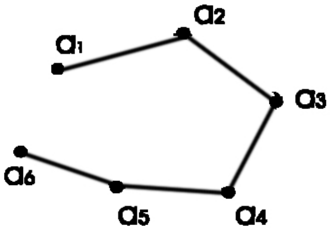


Fig. 3.8

Now we define the following:

***3.3.1 Walk.*** *Let G be a graph. Then a sequence of vertices $v_0$, $v_1$, $v_2$, ……. $v_t$ each adjacent to the next and there is always an edge between $v_i$, and $v_{i+1}$, is called a **walk**. The vertex $v_0$ is called the initial vertex and the vertex $v_t$ is called terminate vertex of the path. Number of edges in a walk is called its length. A walk is called **open walk** if it has different beginning and end points and is called **closed walk** if it's beginning and end points are same.*

***3.3.2 Definition:*** *A **Trail** is a walk having all distinct edges. A **Path** is a walk in which all vertices are distinct. A closed trail is called a **Circuit**. A circuit in which vertices (except the first and last) do not repeat is called a **Cycle.***

***3.3.3 Note:*** *A path is always a trail but a trail need not be a path. Similarly a cycle is always a circuit but a circuit is not a cycle always.*

In figure given below for the graph aba, one is circuit while other is not a circuit.

Fig. 3.9

is not a circuit

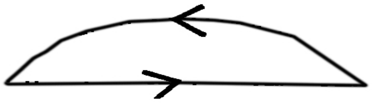


Fig. 3.10

is a circuit and cycle

In Figure 3.11,

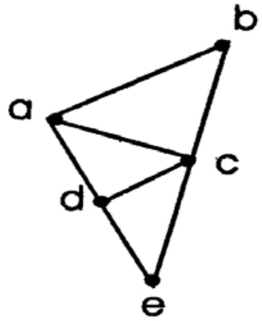


Fig. 3.11

(i) a b c d a c is a trail as no edge repeats

(ii) a b c d e , a d c b and a d e c b are paths

(iii) a c d e c b a is a circuit but not a cycle

(iv) a b c a , a b c d a and a b c e d a are cycles.

## 3.4 SOME DEFINITIONS WITH EXAMPLES

### ***3.4.1 Degree of a vertex:*** *In a non-directed graph G, the degree of a vertex v is determined by counting each loop on v twice and each other edge once. It is denoted by d (v).*

**Example:** d ($V_1$) = 1, d ($V_2$) = 2, d ($V_3$) = 3 are the degrees of $V_1$, $V_2$ and $V_3$ in following figure.

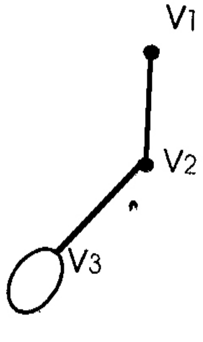


Figure 3.12

### 3.4.2 Theorem: *The sum of $d(v_i)$ for each $v_i$ of a undirected graph G (V, E) is twice the number of edges in G*

**Proof**: Since G is undirected graph, each edge of G is incident with two vertices, therefore, contributes 2 to the sum of degree of all the vertices of the undirected graph. Therefore, the sum of degrees of all the vertices in G is twice the number of edges in G.

**Example:** Draw a simple graph with three vertices i.e. draw a graph with no self loop and no parallel edges.

**Solution**: Figure shown below is a simple graph.

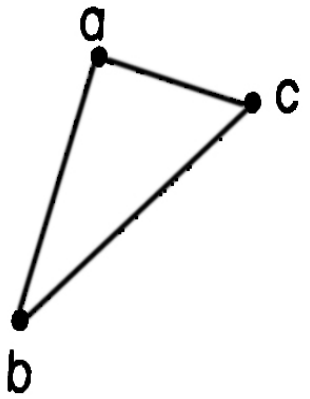


Fig. 3.13

### 3.4.3 REMARK

If we see following graph

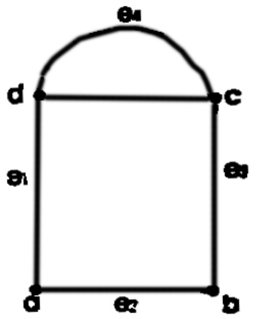


Fig. 3.14

There are five edges in this graph in which edge $e_4$ and $e_5$ has same vertices (c, d). Therefore these edges are parallel edges. Further sum of degrees of the vertices is 2+2+3+3=10 = 2.5= 2 times the number of edges.

### 3.4.4 Definitions

1. Isolated vertex: A vertex on which no edge incident is called isolated vertex, i.e. a vertex v such that d (v) = 0.

2. Null graph: A graph G = (V, E) such V ≠ ϕ and E = ϕ is called null graph, therefore null graph in which every vertex is isolated.

**3.4.5 Theorem:** In a non-directed graph, the number of vertices of odd degree is always even.

**Proof:** Let the number of vertices in a graph G be n. Wlog suppose that the degree of first k vertices say $v_0$, $v_1$, $v_2$, …. $v_k$ be even and remaining n-k vertices be odd i.e. the vertices with odd degree.

$$\text{Now } \sum_{i=1}^{n} d(v_i) = \sum_{i=1}^{k} d(v_i) + \sum_{i=k+1}^{n} d(v_i) \qquad \text{... (1)}$$

But we know by Theorem (3.4.2) that L.H.S. of (1) is even. As $d(v_i)$ in first term of R.H.S. is even, therefore, $\sum_{i=1}^{k} d(v_i)$ is also even. It gives us that $\sum_{i=k+1}^{n} d(v_i)$ must be even. But each d ($v_i$) in that $\sum_{i=k+1}^{n} d(v_i)$ is odd. Moreover we know that sum of odd number is even if they are taken even number of times. So here n-k must be even. i.e. odd number vertices in the graph must be even. Hence the proof is over.

## 3.5 CONNECTED AND DISCONNECTED GRAPHS.

### 3.5.1 Definition: *If in a graph we can move from any vertex to the any other vertex of the graph then such graphs are called connected graphs otherwise it is called disconnected graph. Simple we can say that if there exists a path between every pair of vertices the graph is called connected.*

For example, Graph in Fig. 3.15 is connected graph while in Fig. 3.16 it is disconnected.

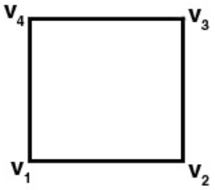


Fig. 3.15

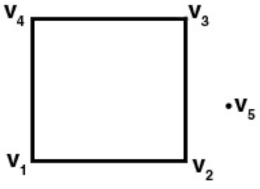


Fig. 3.16

### 3.5.2 Definition

1. Let G be a connected graph. The edge connectivity of G is the minimum number of lines (Edges) whose removal results in a disconnected or trivial graph. It is generally denoted by δ(G).
2. Vertex connectivity of a graph G is the minimum number of vertices whose removal results in a disconnected or trivial graph is called the vertex connectivity of G. It is generally denoted by k(G).

### 3.5.3 Theorem. *The edge connectivity of a connected graph G cannot exceed the minimum degree of G, i.e. $\lambda(G) \leq \delta(G)$.*

**Proof**: Let G be a connected graph and v be a vertex of minimum degree in G. Then the removal of edges incident with the vertex v disconnects the vertex v from the graph G. Thus the set of all edges incident with the vertex v forms a cut set of G. But from the definition, edge connectivity is the edge connectivity of G cannot exceed the minimum degree of v, i.e. $\lambda$ (G) ≤ $\delta$ (G).

### 3.5.4 Theorem: *The vertex connectivity of a graph G is always less then or equal to the edge connectivity of G, i.e., k (G) $\leq$ $\lambda$ (G).*

**Proof**: If graph G is disconnected or trivial the k (G) = λ (G) = 0. If G is connected and has a bridge e, then λ = 1. In this case K = 1, since either G has a cut point incident with e or G is $K_2$.($\therefore$ k (G) ≤ λ (G) when λ (G) = 0 or 1). Finally let us suppose that λ (G) ≥ 2. The G has λ lines whose removal disconnects G. Clearly the λ-1 of these edges produces a graph with a bridge e = {u, v}. For each of these λ-1 edges select an incident point which is different from u or v. The removal of these points (vertices) also removes λ-1 edges and if the resulting graph is disconnected then k ≤ λ-1 < λ. If not the edge e = {u, v} is a bridge and hence the removal of u and v will result in either a disconnected or a trivial graph. Hence k ≤ λ in each case and this completes the proof of the theorem.

Thus, the vertex connectivity of a graph does not exceed the edge connectivity and edge connectivity of a graph cannot exceed the minimum degree of G. Hence the theorem given below.

### 3.5.5 Corollary :*For any graph G, k(G) $\leq \lambda$ (G) $\leq \delta$(G) is disconnected.*

### 3.5.6 Theorem :*A graph is disconnected if V can be written as union of two non-empty, disjoint subsets $V_1$ and $V_2$ such that there exist no element of E whose one vertex in $V_1$ and other in $V_2$.*

**Proof**: Let us suppose that G be a connected graph. Take any vertex v in G. Let $V_1$ be the collection of all these vertices, which are joined by paths to v. Since G is not connected $V \neq V_1$ [if $V = V_1$ then G will be connected]. So take

$v_2$ a set having all vertices of G which are not in all vertices of V which are not in $V_1$. Therefore $V_1$ and $V_2$ are required subsets of V.

Conversely, suppose that $V = V_1 \cup V_2$, $v_1 \neq \Phi$, $v_2 \neq \Phi$, $V_1 \cap V_2 = \phi$, then if we take $v_1 \in V_1$ and $v_2 \in V_2$ then there exist no edge between $v_1$ and $v_2$ i.e. graph is disconnected.

### *3.5.7 Component of a graph means maximal connected subgraph of graph G (V, E). For example in Fig. 3.18.*

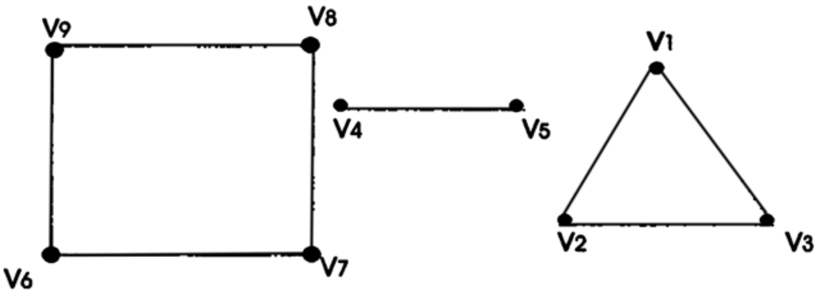


Fig. 3.18

$\{v_1,v_2,v_3\}$, $\{v_4,v_5\}$, $\{v_6,v_7,v_8,v_9\}$, are components. **Further it is clear that a graph is connected if and only if it has exactly one component.**

### ***3.5.8 Theorem**: A simple graph with m vertices and r components can have at most (m-r) (m – r + 1)/2 edges.*

**Proof**: Let G (V, E) be a graph with m vertices and r components let $m_0$, $m_1$, … $m_r$ be the number of vertices in each components of G (V, E). Then we have

$$\Sigma mi = m \text{ and } \quad m_i \geq 1 \qquad (1)$$

Now from (1) we get

$$\sum_{i=1}^{r}(m_i - 1) = m - r \qquad (2)$$

Squaring (2) on both sides we get

$$\left(\sum_{i=1}^{r}(m_i - 1)\right)^2 = m^2 + r^2 - 2mr$$

But $\left(\sum_{i=1}^{r}(m_i - 1)\right)^2 = \sum_{i=1}^{r}(m_i - 1)^2 + 2(m_i - 1)(m_j - 1) = m^2 + r^2 - 2mr$

$$\Rightarrow \sum_{i=1}^{r}(m_i - 2m_i) + r \leq m^2 + r^2 - 2mr \;\; (\because (m_i - 1) \geq 0 \quad \mathit{and} \; (m_j - 1) \geq 0\,)$$

$$\Rightarrow \sum_{i=1}^{r} m_i^2 - 2\sum_{i=1}^{r} m_i \leq m^2 + r^2 - 2mr - r$$

$$\Rightarrow \sum_{i=1}^{r} m_i^2 \leq m^2 + r^2 - 2mr - r + 2m$$

We also know that in a simple graph with $m_i$ vertices have at most $m_i$ ($m_i$ -1)/2. Thus the maximum number of edges in G is

$$\sum_{i=1}^{r}\frac{1}{2}m_i(m_i - 1) = \left[\frac{1}{2}\sum_{i=1}^{r}m_i^2 - \sum_{i=1}^{r}m_i\right] = \frac{1}{2}\left[m^2 - (r-1)(2m - r) - m\right]$$

$$< \frac{1}{2}(m - r)(m - r + 1)$$

This completes the proof.

**3.5.9 Definition:** Two vertices u and v in a digraph are said to be mutually reachable if G contains both directed u-v walk and a directed v-u walk. A digraph is said to be strongly connected if every two of its vertices are mutually reachable.

**Example:** Digraph shown in the figure 3.10 is strongly connected.

## 3.6 MATRIX REPRESENTATION OF GRAPHS

Since we know that it is very easy to manipulate matrices. We take the matrix associated with different graphs. There are two ways of representing graph- (1) incidence matrix; (2) Adjacency matrix.

***3.6.1 Incidence matrix:*** *Let $v_1$, $v_2$, ….. $v_n$ be n vertices and $e_1$, $e_2$, …, $e_m$ be m edges of graph G. Then an n × m matrix I = $[a_{ij}]$ whose n rows correspond to n vertices and m columns corresponds to m edges where $a_{ij}$ is as*

$$a_{ij} = \begin{cases} 0 & \text{if } v_i \text{ is not an end po int of edge } e_j \\ 1 & \text{if } v_i \text{ is not an end po int of edge } e_j \\ 2 & \text{if } e_j \text{ is self loop on } v_i \end{cases}$$

this matrix I = $[a_{ij}]$ is called incidence matrix.

**Example**: Write the incidence matrix of the graph in Figure is

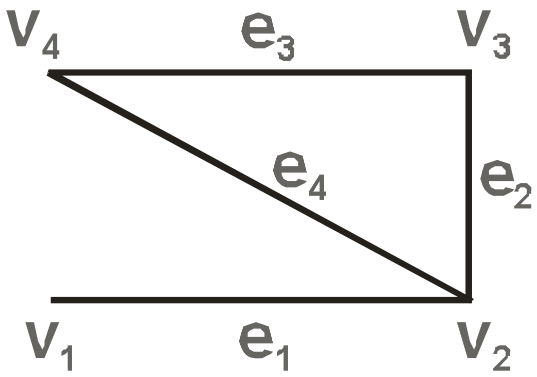


Fig. 3.18

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array}\begin{array}{c} \begin{array}{cccc} e_1 & e_2 & e_3 & e_4 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Some facts about incidence matrix of a graph without self loop.

(i) Number of one's in each column is exactly two since each edge incident exactly on two vertices.

(ii) With given incidence matrix there always exists a graph.

(iii) Sum of entries of any row of matrix gives us the degree of corresponding vertex.

(iv) A row with all zeroes represents an isolated vertex.

### 3.6.2 Adjacency matrix: *Let us consider a graph with n vertices say $v_1, v_2, \dots, v_n$ . Then a square matrix $X = [x_{ij}]$ of order n, where*

$$x_{ij} = \begin{cases} \text{the number of edges between } v_i \text{ and } v_j \text{ if } v_i \neq v_j \\ \text{the number of self loops at } v_i \text{ if } v_i = v_j \end{cases}$$

**Example**: Write the adjacency matrix of the graph given below:

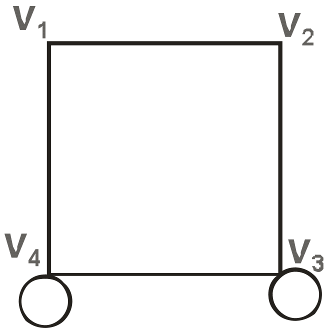


Fig. 3.19

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Some facts about adjacency matrix

(1) X (G) is symmetric matrix.

(2) If G has no self loops then diagonal entries of adjacency matrix are zero. If $i^{th}$ diagonal entry is 1, then it indicates that there is a self loop at $i^{th}$ vertex $v_i$.

**3.6.3 Adjacency matrix of a digraph** (i.e. a directed graph) is defined as

A (G) = $[x_{ij}]_{nxn}$ where G is a graph with n vertices and no parallel edges and

$$x_{ij} = \begin{cases} \text{the number of edges directed from } v_i \text{ to } v_j \text{ if } v_i \neq v_j \\ \text{the number of self loops at } v_i \text{ if } v_i = v_j \end{cases}$$

By definition it is clear that the sum of elements of $i^{th}$ row of adjacency matrix is equal to the out going degree of vertex $v_i$ i.e. the number of edges going out of vertex $v_i$.

**Example**: Write the Adjacency matrix of the diagraph given below:

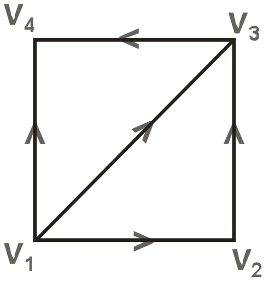


Fig. 3.20

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

**Example**: Write the adjacency matrix of the following digraph:

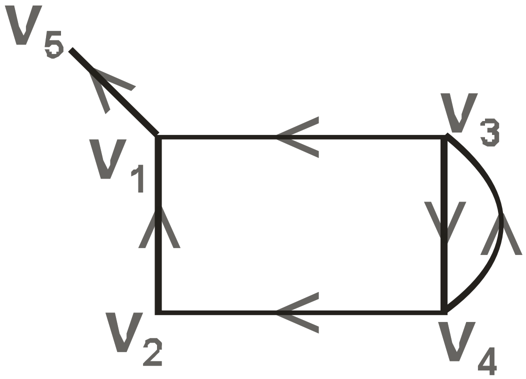


Fig. 3.21

| | V1 | v2 | v3 | v4 | v5 |
|---|---|---|---|---|---|
| v1 | 0 | 0 | 0 | 0 | 1 |
| v2 | 1 | 0 | 0 | 0 | 0 |
| v3 | 1 | 0 | 0 | 1 | 0 |
| v4 | 0 | 1 | 1 | 0 | 0 |
| v5 | 0 | 0 | 0 | 0 | 0 |

Therefore the matrix associated with above graph is

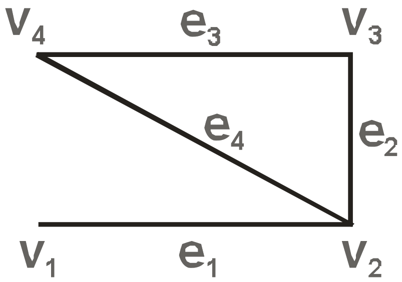
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

## 3.7 KEYWORDS AND SUMMARY

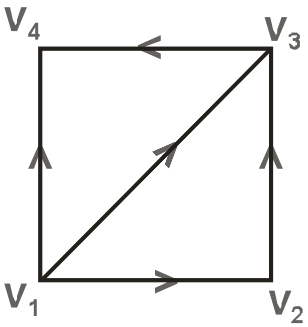
In this chapter we have defined graphs, digraphs and matrix representation of graphs. Graphs, matrix, paths, circuits are key words.

## 3.8 SELF ASSESSMENT QUESTIONS

1. Write the adjacency matrix associated with the graph shown below:



2. Write incidence matrix of following graphs



3 Draw a graph corresponding to given adjacency matrix.

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

4. Draw the diagraph of the incidence matrix.

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

## 3.9 SUGGESTED READING

(1) Seymour Lepschutz, Finite mathematics (International edition 1983), McGraw-Hill Book Company , New York.

(2) N.Deo, Graph Theory with application and computer science , Pentile Hall of India.

**MCA-205: Mathematics –II (Discrete Mathematical Structures)**

**Lesson No: 4** **Written by Pankaj Kumar**

**Lesson: Graph Theory II** **Vetted by Prof. Kuldip Singh**

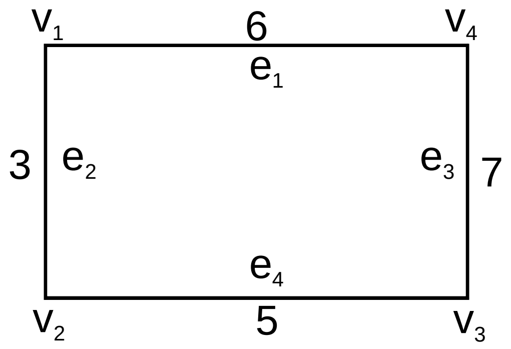
## STRUCTURE

**4.0 OBJECTIVE.** Objective of this chapter is to gain knowledge about trees, weighted graphs e.t.c.

**4.1 INTRODUCTION.** In chapter 3 we studied some definition and matrices associated with graph. In this chapter we will know about trees weighted graphs and shorted path problem in graph theory.

## 4.2 WEIGHTED GRAPHS

**4.2.1 Weighted graph:** A graph G (V, E) is called weighted graph of each of its edge is assigned by some positive real number. That real number is called the weight of that edge. Let us see the following figure



Here weight of edge $e_1$ is 6, $e_2$ is 3, $e_3$ is 7 and $e_4$ is 5.

## 4.3 SHORTEST PATH IN WEIGHTED GRAPH

Let G be a simple weighted graph. The length of an edge from vertex i to a vertex j is denoted by $d_{ij}$. If there is no edge from vertex i to vertex j then $d_{ij}$ = [ ]. The shortest path problem is to find the shortest possible path from a specified vertex A to another specified vertex L. There are several well-known procedures to solve this problem. Here we shall discuss an algorithm due to Dijkstra.

### *4.3.1 Dijkstra algorithm*

This algorithm labels the vertices of the given graph. The algorithm starts by assigning a permanent label O to the starting vertex A and temporary label [ ] to the remaining n-1 vertices. At each iteration in the algorithm, another vertex gets a permanent label according to the following rules:

1.Every vertex *j* which is not yet permanently labelled gets a new temporary label whose value is given by

min [old label of j, old label of i + $d_{ij}$],

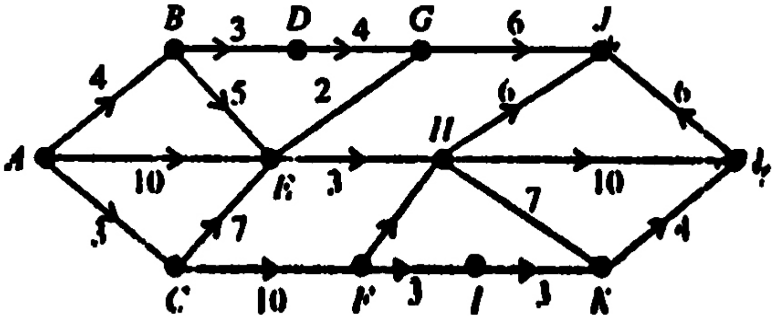
where i is the latest vertex permanently labelled, in the previous iteration and $d_{ij}$ is the length of the edge between vertices i and j. If i and j are not joined by edge then $d_{ij} = \propto$

2. The smallest value among all the temporary labels is found and this becomes the permanent label of the corresponding vertex. In case of a tie, select any one of the vertices for permanent labelling.

Steps 1 and 2 stated above are repeated alternately until the destination vertex L gets a permanent label.

The first vertex to be permanently labelled is the starting vertex A. The second vertex to get a permanent label is the vertex nearest to A. The next vertex to be permanent label is the vertex nearest to A. The next vertex to be permanently labelled is the next nearest vertex to A. Thus the permanent label of each vertex is the shortest distance of that vertex from A. We illustrate Dijkstra procedure with the help of the following example:

**Example**: find the shortest path from A to L in the following weighted graph:



**Solution**: We shall use an array of length eleven (no. of vertices) to show the temporary and permanent labels of the vertices as we go through the solution. The permanent labels will be shown enclosed in a square and the latest vertex assigned permanent label in the array is indicated by a mark [ ]*. The labelling proceeds as follows:

| i | A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0. | [0]* | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ |
| 1. | [0] | 4 | [3]* | ∞ | 10 | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ |
| 2. | [0] | [4]* | [3] | ∞ | 10 | 13 | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ |
| 3. | [0] | [4] | [3] | [7]* | 9 | 13 | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ |
| 4. | [0] | [4] | [3] | [7] | [9]* | 13 | 11 | ∞ | ∞ | ∞ | ∞ | ∞ |
| 5. | [0] | [4] | [3] | [7] | [9] | 13 | [11]* | 12 | ∞ | ∞ | ∞ | ∞ |
| 6. | [0] | [4] | [3] | [7] | [9] | 13 | [11] | [12]* | ∞ | 17 | ∞ | ∞ |
| 7. | [0] | [4] | [3] | [7] | [9] | [13]* | [11] | [12] | ∞ | 17 | 19 | 22 |
| 8. | [0] | [4] | [3] | [7] | [9] | [13] | [11] | [12] | [16]* | 17 | 19 | 22 |
| 9. | [0] | [4] | [3] | [7] | [9] | [13] | [11] | [12] | [16] | [17]* | 19 | 22 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10. | [0] | [4] | [3] | [7] | [9] | [13] | [11] | [12] | [16] | [17] | [19]* | 22 |
| 11. | [0] | [4] | [3] | [7] | [9] | [13] | [11] | [12] | [16] | [17] | [19] | [22]* |

Thus the shortest distance from A to L is 22. Note that this method gives only the shortest distance. The shortest path can be easily obtained by going back word from the terminal vertex such that we go to that predecessor (vertex) whose label differs exactly by the length of the connecting edge. A tie indicates more than one shortest path. We can also determine the shortest path by keeping a record of the vertices from which each vertex was labelled permanently. This record can be stored in another array of length n, such that whenever a new permanent label is assigned to vertex j, the vertex from which j is directly reached is recorded in the jth position of this array. In the above example, the shortest path is A → B → E → H → L.

## 4.4 TREE

### *4.4.1 **Definition:** A tree is a connected graph without any circuits.*

From the definition it is clear that a tree is a connected and acyclic graph. It has neither self loops nor parallel edges and is depoted by the symbol T. Since trees are acyclic, we adopt a convention similar to that used for Hasse diagrams. Trees may be directed or non-directed.

### *4.4.2 **Directed tree.** A connected, a cyclic, directed graph is called a directed tree.*

The graph in Fig. is non-directed tree and graph shown in Fig. 4.2 is a directed tree 4.1.

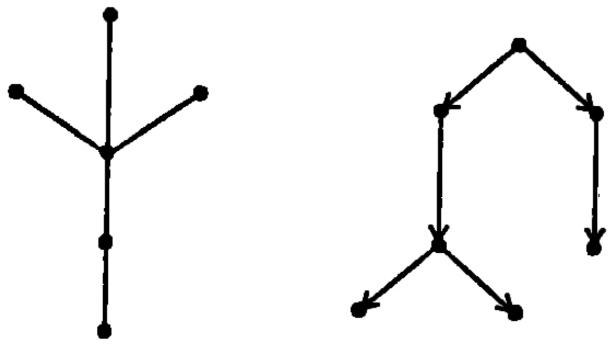


Fig. 4.1 and 4.2

If T is a tree, then it has a unique simple non-directed path between each pair of vertices. A tree with only are vertex is called trivial tree. If T is a not a trivial tree then it is called a non-trivial tree. The vertex set (i.e., the of nodes) of a tree is a finite set. In most cases the vertices of a tree are labelled.

### 4.4.3 **Theorem:** *A simple non-directed graph G is a tree if and only if G is connected and has no cycles*

**Proof**: Let G be a tree. Then each pair of vertices of G are joined by a unique path, therefore G is connected. Let u and v be two distinct vertices of G. Such that G contains a cycle containing u and v. Then u and v are joined by at least two simple paths, one along one portion of the cycle and the other path completing the cycle. This contradicts our hypothesis that there is a simple unique path between u and v. Hence tree has no cycle.

Conversely let G be a connected graph having no cycles. Let $v_1$ and $v_2$ be any pair of vertices of G and let there be two different simple paths say $P_1$ and $P_2$

from $v_1$ to $v_2$. then we can find a cycle in G as follows: Since the paths $P_1$ and $P_2$ are different, there must be a vertex say u, which is on both $P_1$ and $P_2$ but its successor on $P_1$ is not on $P_2$. If u is the next point on $P_1$ which is also on $P_2$, the segments of $P_1$ and $P_2$ which are between $P_1$ and $P_2$ form a cycle in G. A contradiction. Hence there is atmost one path between any two vertices of G. Which shows that G is a tree.

### ***4.4.4 Theorem :*** *Any non-trivial tree has at least one vertex of degree 1.*

**Proof**: Let G be a non-trivial tree, then G has no circuits. Let $v_1$ be any vertex of G. If deg $(v_1) = 1$, then the theorem is at once established. Let deg $(v_1) \neq 1$ move along any edge to a vertex $v_2$ incident with $v_1$. If deg $(v_2) \neq 1$ then continue to another vertex say $v_3$ along a different edge. Continuing the process we get a path $v_1 - v_2 - v_3 - v_4$ - … in which none of the $v_i$ s is repeated. Since the number of vertices in a graph is finite, the path must end some where. The vertex at which the path ends is of degree are, since we can enter the vertex but cannot leave the vertex.

### ***4.4.5 Theorem*** *A tree T with n vertices has exactly (n – 1) edges*

**Proof**: The theorem will be proved by mathematical induction on the number of vertices of a tree. If n = 1 then there are no edges in T. Hence the result is trivial.

If n = 2 then the number of edges connecting the vertices is one i.e., n – 1. Hence the theorem is true for n = 2. Assume that the theorem, holds for all trees with fewer than n vertices. Consider a tree T with n vertices. Let V be a vertex in T of degree 1 and let T' denote the graph obtained by removing the vertex v and edge e associated with it from T. Consider T' = T – e. T' has n – 1, vertices and fewer edges than T. If $v_1$ and $v_2$ are any two vertices in T', then there is a unique simple path from $v_1$ to $v_2$ which is not affected by the removal of the vertex and edge. T' is connected and no edges in it, therefore T' is a tree T' has n-1 vertices and n – 1 – 1 = n – 2 edges. T has are more edge than T'.

Therefore, the number of edges in T = n – 2 + 1 = n – 1. Hence T has exactly n – 1 edges.

**4.4.6 Definition.** *If G is connected graph and u and v are any two vertices of G, the length of the shortest path between u and v is called the distance between u and v and is denoted by d (u, v).*

The distance function on defined above has the following properties. If u, v and w are any three vertices of a connected graph then.

(i) $d(u, v) \geq$ and $d(u, v) = 0$ iff – $u = v$

(ii) $d(u, v) = d(v, u)$

and (iii) $d(u, v) \leq d(u, w) + d(w, v)$

from the above it is clear that distance in a graph is a metric.

**Example**: In the graph shown in Fig. 4.3

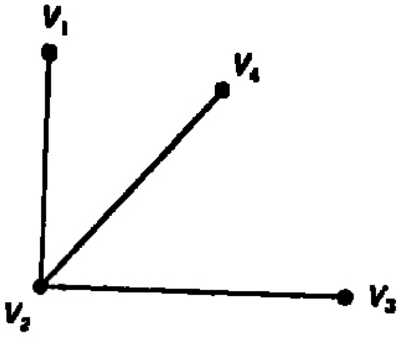


Fig. 4.3

## 4.5 Spanning tree

Let G be a connected graph. The sub graph H of G is called a spanning tree of G if

(i) H is a tree and

(ii) H contains all the vertices of G.

**Example.** In Fig. 4.4 H is spanning tree of Fig. 4.4.

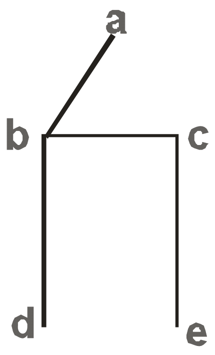


Fig. 4.5

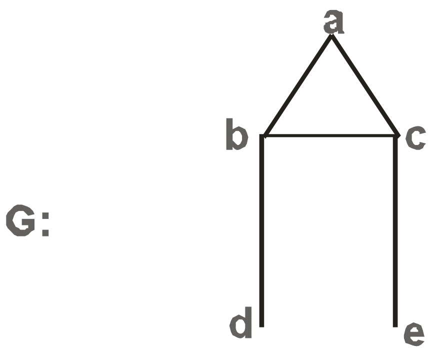


Fig. 4.4

### 4.5.2 Minimal spanning tree : *Let G be a connected weighted graph. A minimal spanning tree of G is a spanning tree of G whose total weight is as small as possible.*

There are various methods to find a minimal spanning tree in connected weighted graph. Here we consider algorithms for generating such a minimal spanning tree.

### 4.5.3 Algorithm

A connected weighted graph with n vertices.

**Step 1**: Arrange the edges of G in the order of decreasing weights.

**Step 2**: Proceed sequentially, and delete each edge of G, that does not disconnect the graph G until n – 1 edges remain.

**Step 3**: Exit.

**Example 1**: Consider the graph G given below:

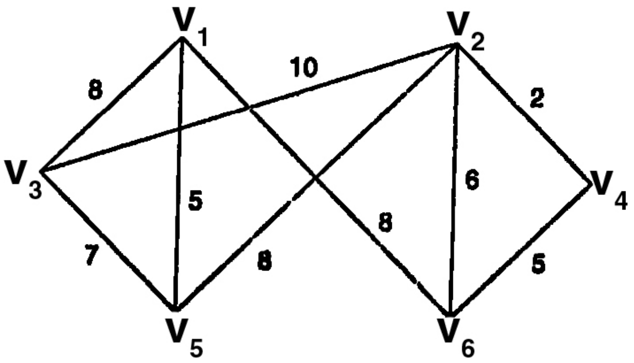


Fig. 4.6

Number of vertices in G = n = 6.

We apply the algorithm given above.

We order the edged by decreasing weights and delete the edges of G until n – 1 =  6 – 1 = 5 edges remain.

| Edges | ($v_2$, $v_3$) | ($v_1$, $v_6$) | ($v_1$, $v_3$) | ($v_2$, $v_5$) | ($v_3$, $v_5$) | ($v_2$, $v_6$) |
|---|---|---|---|---|---|---|
| Delete | Yes | Yes | Yes | No | No | Yes |
| Edges | ($v_1$, $v_5$) | ($v_4$, $v_6$) | ($v_2$, $v_4$) |  |  |  |
| Delete | No | No | No |  |  |  |

The minimal spanning tree of G is shown in Fig. 4.7.

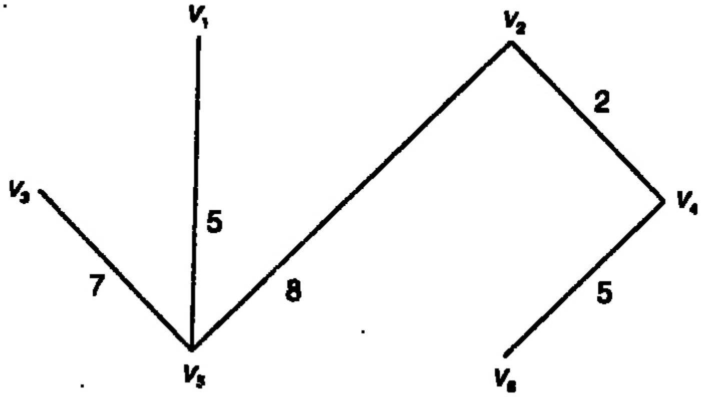


Fig. 4.7

The weight of the minimum spanning tree = 8 + 7 + 5 + 5 + 2 = 27.

## 4.6 KURUSKAL ALGORITHM

Input: A connected weighted graph G with n vertices.

**Step 1**: Arrange the edges of in order of increasing weights and select the edge with minimum weight.

**Step 2**: Proceed sequentially, add each edge which does not result in a cycle until n – 1, edges are selected.

**Step 3**: Exit.

**Example**: Consider the graph in Fig. 4.6.

We have n = 6

We order the edges by increasing weights ($V_2$, $V_4$) is edge with minimum weight. Select the edge ($V_2$, $V_4$) we successively add edges to ($V_2$, $V_4$), without forming cycles until 6 – 1 = 5 edges are selected. This yields:

| Edges | ($V_2$, $V_4$) | ($V_1$, $V_5$) | ($V_4$, $V_6$) | ($V_2$, $V_6$) | ($V_3$, $V_5$) | ($V_1$, $V_3$) | ($V_1$, $V_6$) | ($V_2$, $V_5$) | ($V_2$, $V_3$) |
|---|---|---|---|---|---|---|---|---|---|
| Weight | 2 | 5 | 5 | 6 | 7 | 8 | 8 | 8 | 10 |
| Add? | Yes | Yes | Yes | No | Yes | No | Yes | No | No |

Edges in the minimum spanning tree are

($V_2$, $V_4$), ($V_1$, $V_5$), ($V_4$, $V_6$), ($V_3$, $V_5$), ($V_1$, $V_6$)

The resulting minimal (optimal) spanning tree is shown in Fig. 4.8.

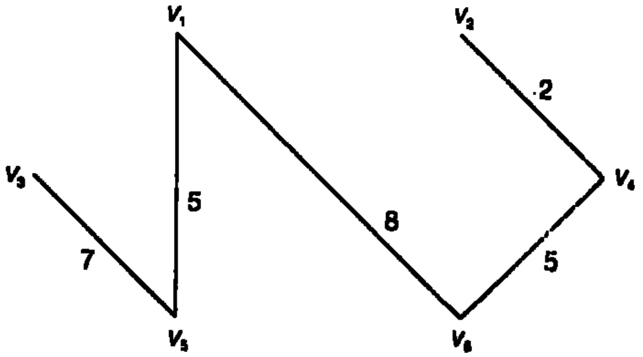


Fig. 4.8

We apply the steps of Kruskal's algorithm to the graph of Fig. 8.96; as follows:

($V_2$, $V_4$) is the edge with minimum weight, therefore we select the edges ($V_2$, $V_4$).

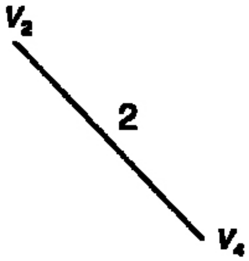


Fig. 4.9 (a)

The next edge with minimum weight ($V_1$, $V_5$), selection of ($V_1$, $V_5$) does not result in a cycle.

∴ edge ($V_1$, $V_5$) is selected.

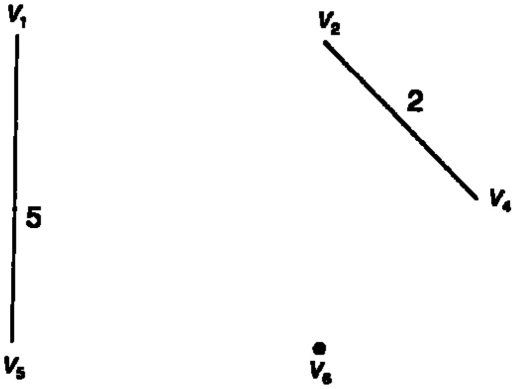


Fig. 4.9 (b)

The edge to be considered, next is ($V_4$, $V_6$).
The next edge to be selected is ($V_4$, $V_6$).

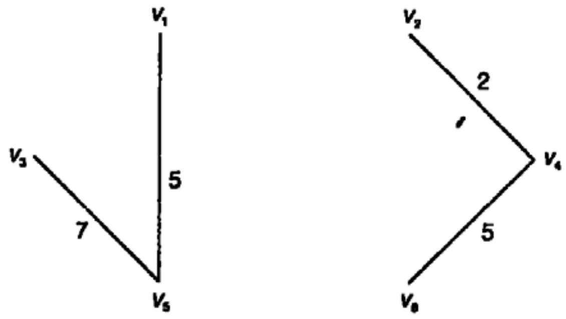


Fig. 4.9 (c)

Selection of the edge ($V_2$, $V_6$) for the spanning tree results in a cycle. Therefore ($V_2$, $V_6$) is not selected we consider the edge ($V_3$, $V_5$) selection of edge ($V_3$, $V_5$) does not result in a cycle. Hence ($V_3$, $V_5$) is selected.

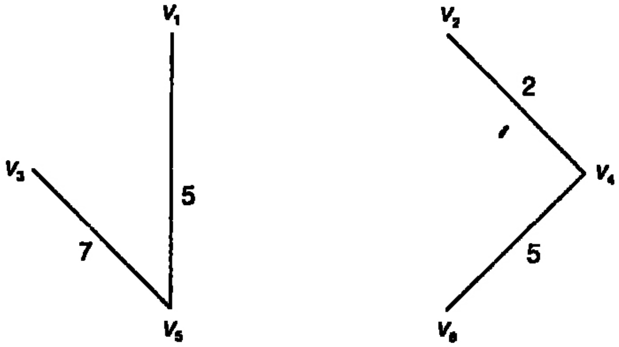


Fig. 4.9 (d)

Next we consider the edge ($V_1$, $V_3$) from the list. Selection of the edge ($V_1$, $V_3$) result in a cycle. Therefore edge ($V_1$, $V_3$) is not selected. Consider the edge ($V_1$, $V_6$) selection of edge ($V_1$, $V_6$) does not result in a cycle. Hence ($V_1$, $V_6$) is selected.

Number of edges selected is 5. We stop, and obtain the spanning trees as shown in Fig. 4.9(e).

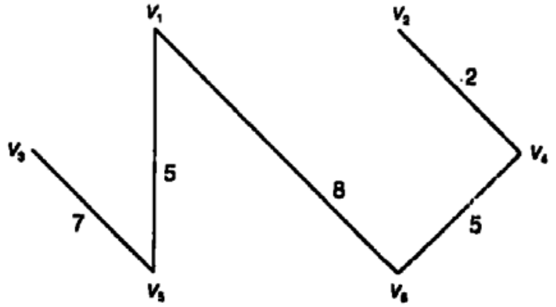


Fig. 4.9 (e)

The weight of the minimal spanning tree.
= 2 + 5 + 5 + 7 + 8 = 27

## 4.7 PRIMS ALGORITHM

Input: A connected weighted graph G with n vertices.

**Step 1**: Select an arbitrary vertex $v_1$ and an edge $e_1$ with minimum weight incident with vertex $v_1$.

**Step 2**: Having selected the vertices $v_1, v_2, \ldots, v_1$ and $e_1, e_2, \ldots, e_{i-1}$; select an edge $e_i$ such that $e_i$ connects a vertex of the set $(v_1, v_2, \ldots, v_i)$ and a vertex of $V = (v_1, v_2, \ldots, v_i)$ and of all such edges $e_i$ has the minimum weight.

**Step 3**: Stop if n – 1, edges are selected, else go to step 2.

**Example 1**: Consider the graph shown in Fig. 4.10

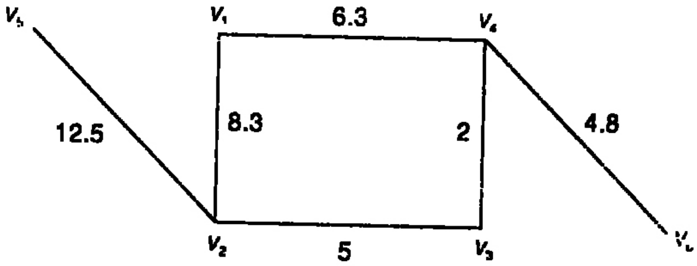


Fig. 4.10

Let $e_1 = (V_1, V_2)$, $e_2 = (V_2, V_3)$

$e_3 = (V_3, V_4).e_4 = (V_4, V_1)$

$e_3 = (V_2, V_5)$ and $e_6 = (V_4, V_6)$.

Denote the edge of G.

We apply prims algorithm to the graph as follows:

The edge $e_3 = (V_3, V_4)$ is an edge with minimum weight. Hence we start with the vertex $V_3$ and select the edge $e_3$ incident with $v_3$.

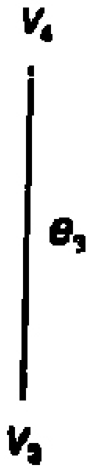


Fig. 4.11 (a)

We next consider the edges connecting a vertex {V$_3$, V$_4$} with the vertex of the set V – {V$_3$, V$_4$}. We observe that e$_6$ the edge with minimum weight.

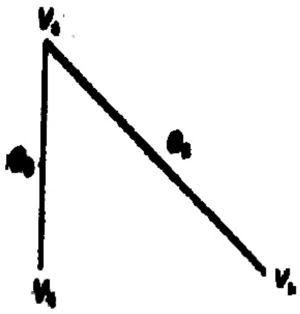


Fig. 4.16 (b)

Consider the edges connecting the vertices of the set {V$_3$, V$_4$, V$_6$} with the vertices of V – {V$_3$, V$_4$, V$_6$}. The edge e$_2$ has the minimum weight. The edge e$_2$ is selected.

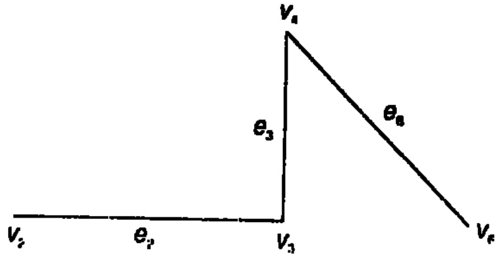


Fig. 4.11 (c)

Of the connecting the vertices of {V$_2$, V$_3$, V$_4$, V$_6$}; with the vertex set V – {V$_2$, V$_3$, V$_4$, V$_6$}, e$_4$ has minimum weight, therefore e$_4$ is selected.

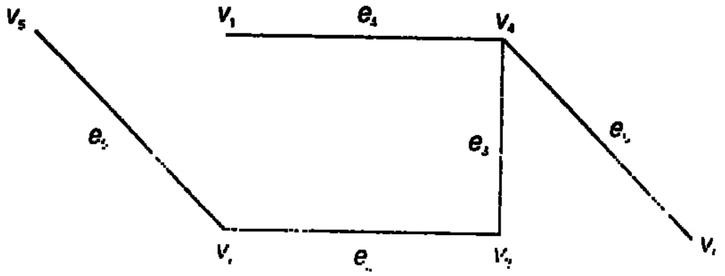


Fig. 4.11 (d)

$e_1$, $e_5$ are the edges remaining. $e_5$ is the only edge connecting {$V_1$, $V_2$, $V_3$, $V_4$, $V_5$, $V_6$} and {$V_5$} such that the inclusion of $e_5$ does not result in a cycle. Hence $e_5$ is selected.

Since number of edges selected is 5 we stop.

The minimal spanning tree obtained is shown in Fig. 4.11 (e).

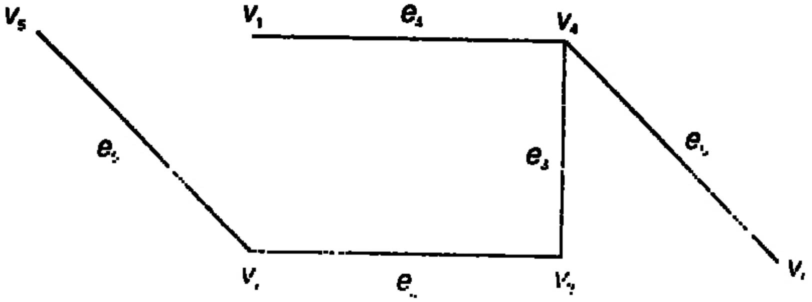


Fig. 4.11 (e)

Weight of the minimal spanning tree

= 2 + 4.8 + 5 + 6.3 + 12.5

= 30.6.

***4.7.1 Expression trees:*** *Algebraic expressions involving addition, subtraction, multiplication and division can be represented as ordered rooted trees called expression trees. The arithmetic expression $3 + 5 \times 9 - 7 \times 6^2$ can be represented as the tree shown in Fig. 4.12.*

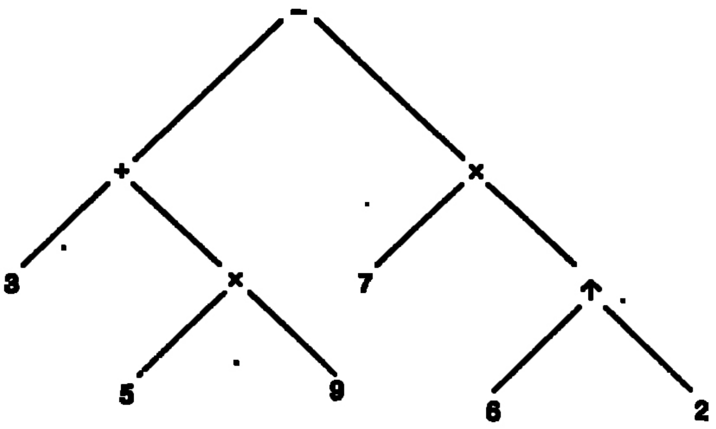


Fig. 4.12

The variables in the algebraic expression appear as the other vertices. In the polish prefix representation, we place the binary operational symbol before the argument and avoid parentheses. The expression {(a – b)/(c × d) + e} can be expressed as i – ab + × cde.

**Example**: Write the following expression as a tree

[(a × b) × c + (d + e) – (f – (g × h)]

**Solution**: The arithmetic expression [(a × b) × c + (d + e) – (f – (g × h))] can be represented as the tree.

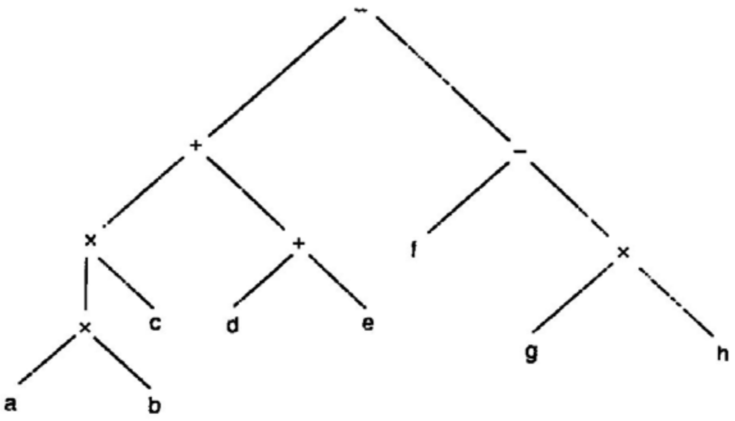


Fig. 4.13

### *4.7.2* ***Definition :****A tree in which there is exactly one vertex of degree two, and each of the remaining vertices of degree one or three, is called a binary tree.*

**Example**: Show that the number of vertices in a binary tree is odd.

**Solution**: Let T be a binary tree with n vertices. T contains exactly one vertex of degree 2 and the remaining vertices of T are of degree one or three. Therefore number of odd degree vertices in T is n – 1. But the number of odd degree vertices in a graph is even. Therefore n – 1 is even. Hence n is odd.

## 4.8 POLISH NOTATION AND FLOW ION NETWORK

### *4.8.1* ***Definition: The*** *process of visiting each vertex of a tree in some specified order is called searching the tree or walking or traversing the tree****.***

We now discuss methods of searching a tree.

**1. Preorder search method**

Input: The root v of a binary tree.

Output: Vertices of a binary tree using pre-order traversal

1. Visit v
2. If $v_1$ (left child of v) exists, then apply the algorithm to (T ($v_1$), ($v_1$)
3. If $V_R$ (right child of v) exists, then apply this algorithm to (T ($v_R$), $v_R$).

End of Algorithm preorder.

In other words, preorder search of a tree consists of the following steps.

Step 1. Visit the root.

Step 2. Search the left subtree if it exists.

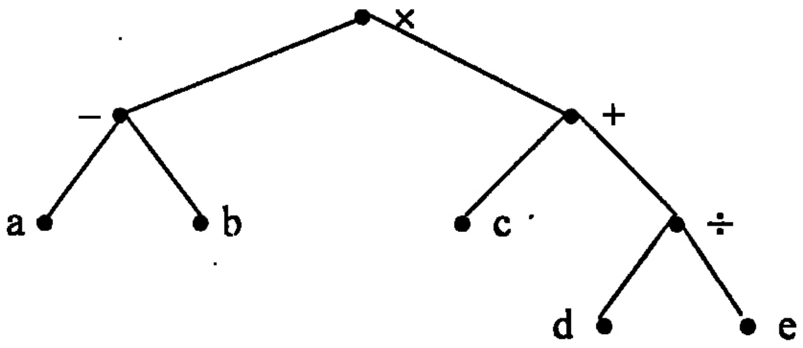
Step 3. Search the right subtree if it exists.

**Example**: Find binary tree representation of the expression

(a – b) × (c + (d ÷ e)

and represent the expression in string form using pre-order traversal.

**Solution**: In the given expression, x is the central operator and therefore shall be the root of the binary tree. Then the operator- acts as $v_1$ and the operator + acts as $v_R$. Thus the tree representation of the given expression is



The result of the pre-order traversal to this binary tree is the string

x – ab + c ÷ de

This form of the expression is called prefix form or polish form of the expression

(a – b) × (c + (d ÷ e))

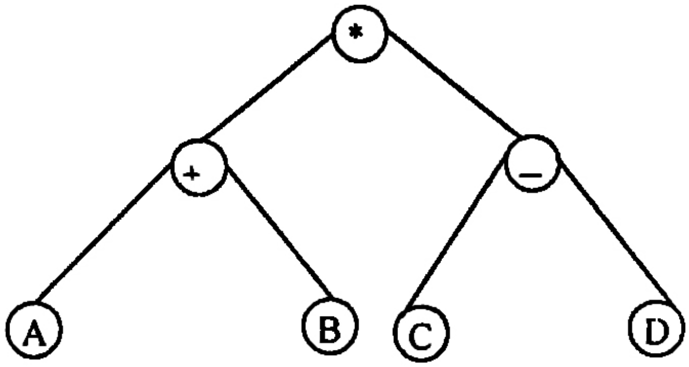
In a polish form, the variables a, b, c, …, are called operands and - +, x, ×, ÷ are called operators. We observe that, in polish form, the operands follows the operator.

**Example**: Represent the expression

(A + B) * (C – D)

as a binary tree and write the prefix form of the expression.

**Solution**: Here * is the central operator. Further + and – operators are $v_t$ and $v_R$. Hence the binary tree is



Using pre-order traversal, the prefix expression for it is

* + AB – CD

### 4.8.2 Procedure to evaluate an expression given in polish form

To find the value of a polish form, we proceed as follows:

Move from left to right until we find a string of the form K xy, where K is operator and x, y are operands.

Evaluate x K y and substitute the answer for the string K x y. Continue this procedure until only one number remains.

**Example**: Find parenthesized form of the polish expression

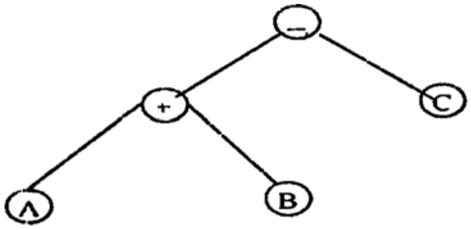
- + ABC

**Solution**: The parenthesized form of the given polish expression is derived as follows:

- (A + B) C

(A + B) – C

The corresponding binary tree is



**Example**: Evaluate the polish form

x – 64 + 5 ÷ 22

**Solution**: We have the following steps in this regard

1. × (6 – 4) + 5 ÷ 22
2. × 2 + 5 ÷ 22
3. × 2 + 5 (2 ÷ 2)
4. × 2 + 51
5. × 2 (5 + 1)
6. × 26
7. 2 × 6
8. 12, which is the required value of the expression.

## 4.8.3 P0ST ORDER SEARCH METHOD

**Algorithm**

Step 1. Search the left sub tree if it exists.

Step 2. Search the right sub tree if it exists

Step 3. Visit the root

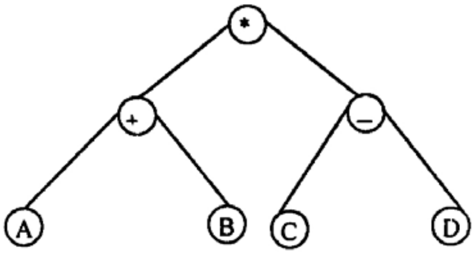
End of algorithm

**Example**: Represent the expression

(A + B) * (C – D)

as a binary tree and write the result of post order search for that tree.

**Solution**: The binary tree expression (as shown earlier) of the given algebraic expression is



The result of postorder search of this tree is

AB + CD –*

This form of the expression is called postfix form of the expression or reverse polish form of the expression.

In postfix form, the operator follows its operands.

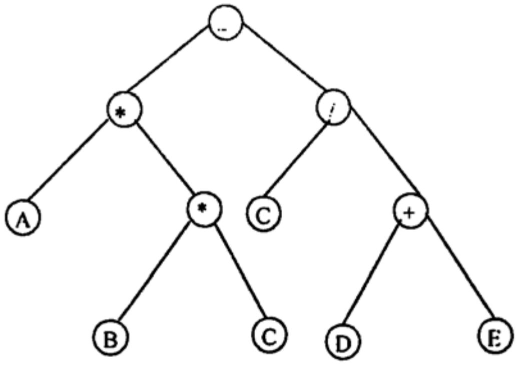
**Example**: Find the parenthesized form of the postfix form

ABC ** CDE +/-

**Solution**: We have

1. ABC ** CDE +/-
2. A (B * C) * C (D + E)/-
3. (A*(B*C)) (C/ (D + E))-
4. (A * (B * C)) – (C / (D + E))

The corresponding binary tree is



**Example 8.19.10.** Evaluate the postfix form

21 – 342 ÷ + ×

**Solution**. We have

21 – 342 ÷ + ×

= (2 – 1) 342 ÷ + ×

= 13 (4 ÷ 2) + ×

= 132 + ×

= 1 (3 + 2 )×

= 15 ×

= 1 × 5

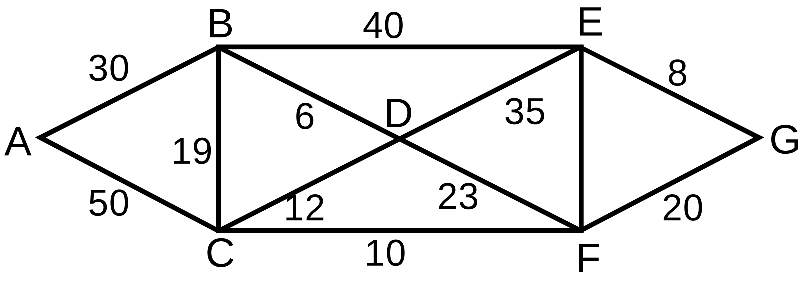
= 5.

## 4.9 KEY WORDS AND SUMMARY

In this chapter we studied weighted graph, trees, some algorithms about shortest path in graphs. Weighted graph, Trees. Prime Algorithm are keywords.

## 4.10 SELF ASSESSMENT QUESTION

Q (1) Use shortest path algorithm to find a shortest path from A to G in the weighted graph.



Q (2) Evaluate the expression given in polish form

(a) 21 - 342 ÷ + ×.

(b) AB + CD –

## 4.11 SUGGESTED READING

(i) Seymour Lepschutz, Finite mathematics (International edition 1983), McGraw-Hill Book Company , New York.

(ii) N.Deo, Graph Theory with application and computer science , Pentile Hall of India.

(iii) Babu Ram, Discrete mathematics, V publication, New Delhi.

**MCA-205: Mathematics –II (Discrete Mathematical Structures)**

**Lesson No: 5** **Written by Pankaj Kumar**

**Lesson: Boolean Algebra I** **Vetted by Prof. Kuldip Singh**

**STRUCTURE**

**5.0 OBJECTIVE:** Objective of this chapter is to study algebraic structure like Boolean algebra, which has much application in computers.

**5.1 INTRODUCTION:** In this chapter we have defined one more algebraic**.** We have defined partial order relation Boolean algebra, lattices and logic gates with their truth tables

## 5.2 PARTIALLY ORDER RELATION:

**5.2.1 Definition -** Let A be non empty set, then the set A×A= {(a, b) | a, b∈A} is called Cartesian product of A with itself.

Any subset R of A×A is called a relation on A. If R satisfies the following conditions

(1) R is reflexive i.e. $(a, a) \in R$ for all $a \in A$.

(2) R is antisymmetric i.e. $(a, b) \in R$ and $(b, a) \in R \Rightarrow a=b$.

(3) R is called transitive i.e. if $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$.

Then R is called partial ordered relation. A set A together with partial order relation R is called partially ordered set or poset and is generally denoted by $(A, \leq)$.

**Example:** Let T be any non empty set, then its power set p(T)(i.e. set of all subsets of T) is a partially ordered set under the relation that $A \leq B$ iff $A \subseteq B$.

(1) Since $A \subseteq A$ for all $A \in P(T)$, i.e. $(A \leq A)$ $\forall$ $A \in P(T)$, R is reflexive relation.

(2) If $A \subseteq B$, $B \subseteq A$, $\Rightarrow A=B$ i.e. relation is antisymmetric

(3) If $A \subseteq B$, and $B \subseteq C$ then we know that $A \subseteq C$ i.e. $A \leq B$ and $B \leq C$ gives us $A \leq C$ so relation is transitive also.

Hence $\subseteq$ is a partial order relation and $(P(T), \subseteq)$ is partially ordered set.

**Example:** On the set N of natural numbers. Relation aRb iff $a \leq b$ is a partially ordered relation

**Proof:** (1) since $a \leq a$ for all $a \in N$ i.e. relation is reflexive.

(2) Since $a \leq b$ and $b \leq a \Rightarrow a = b$ i.e. relation is antisymmetric.

(3) If $a \leq b$ and $b \leq c \Rightarrow a \leq c$ i.e. relation is transitive. Hence less then is a partially ordered relation and $(N, \leq)$ is a partial order set.

**5.2.2 Definition-** If R= $\{(a, b) \mid a\ R\ b\ a, b \in A\}$ then inverse relation on A is $R^{-1} = \{(b,a) \mid (a, b) \in R\}$

**Example**: Prove that if R is p.o.r (partially ordered relation on X) then so is $R^{-1}$ i.e.$R^{-1}$ is also a p.o.r.

(1) $R^{-1}$ is reflexive since $(a, a) \in R \Rightarrow (a, a) \in R^{-1}$ for all $a \in A$

(2) For a $R^{-1}$ b and b $R^{-1}$ a we will show that a=b . As a $R^{-1}$ b $\Rightarrow$ b R a. Also b $R^{-1}$ a $\Rightarrow$ a R b. Now combining a R b and b R a we get a=b i.e. $R^{-1}$ is antisymmetric.

(3) Now a $R^{-1}$ b and b $R^{-1}$ c we will prove that a $R^{-1}$ c . As a $R^{-1}$ b $\Rightarrow$ b R a. Also b $R^{-1}$ c $\Rightarrow$ c R b. Now combining c R b and b R a we get c R a. but then a $R^{-1}$ c i.e. $R^{-1}$ is transitive.

Hence $R^{-1}$ is a partially ordered relation and (X, $R^{-1}$ ) is a partially ordered set.

**5.2.3 Definition**: - Let $\leq$ be a partial order on A then a, b $\in$A are said to be comparable if $a \leq b$ or $b \leq a$. If we have a and b are two elements of A such that neither $a \leq b$ nor $b \leq a$. We say that a and b are non comparable.

**5.2.4 Definition**: Let (A, $\leq$) be a partially ordered set and If every a and b belonging to A either $a \leq b$ or $b \leq a$. Then A is called totally ordered set or a chain simply we can say that every two elements of A are comparable.

**Example**: On set N of natural numbers with partial order $\leq$ is a totally ordered as for a,b $\in$ N either $a \leq b$ or $b \leq a$. But if we take $a \leq b$ iff a / b, then it is not totally ordered on set of N of natural numbers as 3, 5 $\in$ N neither 3/5 nor 5/3 i.e. neither $3 \leq 5$ nor $5 \leq 3$.

**5.2.5 Definition**: If (A, ≤) is a partially ordered set, then **l.u.b** {a,b} means smallest element c of A such that a ≤ c and b ≤ c and **g.l.b** ({a, b}) is greatest element g ∈ a such that g ≤ a and g ≤ b.

**Example**: Take A=N (set of natural numbers) and a ≤ b iff a is less then b for a, b ∈ N. Then l.u.b ({a, b})= b or a , accordingly if a is less then b, or b is less then a. The g.l.b({a,b})= a or b , accordingly if a is less then b, or b is less then a.

**Example:** Take A=N (set of natural numbers) and a ≤ b iff a divides b for a, b ∈ N. Then l.u.b ({a, b})= least common multiple of a and b which is generally written as l.c.m (a,b) and g.l.b({a,b})= greatest common divisor of a and b which is generally denoted by g.c.d (a,b) are respectively least upper bound and greatest lower bound of a and b.

**5.2.6 Dual order**: As we have show that if ≤ is Partial order then so is $\leq^{-1}$ on a set A. The ordered set (A,$R^{-1}$ ) is called dual order of (A,R).

## 5.3 LATTICE

**5.3.1 Lattice**: - A lattice is a partially ordered set (A, ≤ ) in which every subset of cardinality two has a least upper bound and a greatest lower bound in A. If {a,b} is such a set then l.u.b ({a,b}) denoted by a V b and is called joint or sum of a and b. Similarly g.l.b ({a,b}) is denoted by a ∧ b and is called meet or product of a and b.

Another definition is that

A non empty set L together with two binary operations ∧ (meet) and ∨ (join) is said to be a lattice if the following conditions are satisfied.

(i) Commutative laws holds in L under ∧ and ∨ i.e.

$a \wedge b = b \wedge a$ and $a \vee b = b \vee a$ for all a, b belonging to L.

(ii) Associative properties holds in L under $\wedge$ and $\vee$ i.e.

$a \wedge (b \wedge c) = (a \wedge b) \wedge c$ and $a \vee (b \vee c) = (a \vee b) \vee c$ for all a, b and c belonging to L.

(iii) Absorption laws holds in L under $\wedge$ and $\vee$ i.e.

$a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$.

**Example:** - If we take N set of natural number, then relation R between two elements that aRb iff $a \le b$ is a partially order on N. Here N is a lattice also as if we take $\text{l.u.b}(\{a, b\})$ = l.c.m (a,b) and $\text{g.l.b}(\{a, b\})$ = g.c.d (a,b).

**Example**: - If we take (P (A), $\le$ ) partial ordered set such that P(A) is power set of A and $A_1 \le A_2$ iff $A_1 \subseteq A_2$ , $A_1$ and $A_2$ are subsets of A. Then it is a lattice such that

$\text{l.u.b}(\{A_1, A_2\})$ =Union of $A_1$ and $A_2$ sets and $\text{g.l.b}(\{A_1, A_2\})$ = intersection of $A_1$ and $A_2$ .

**5.3.2 Theorem**: - If $(A_{1,} \le_1)$ and $(A_{2,} \le_2)$ are two partial order set, then so is $(A_1 \times A_{2,} \le )$ under the relation $(a_{1,}a_2) \le (b_{1,}b_2)$ iff $a_1 \le_1 b_1$ and $a_2 \le_2 b_2$ for $a_1, b_1$ belonging to $A_1$ and $a_2$ , $b_2$ belonging to $A_2$ .

**Proof:-**(1) since $a_1 \le_1 a_1$ and $a_2 \le_2 a_2$ $\forall a_1 \in A_1$ and $a_2 \in A_2$ therefore $(a_{1,}a_2) \le (a_{1,}a_2)$ i.e. $\le$ is reflexive.

(2) $(a_{1,} a_2) \le (b_{1,}b_2)$ gives us that $a_1 \le_1 b_1$ and $a_2 \le_2 b_2$-----------(1)

And $(b_{1,}b_2) \le (a_{1,}a_2)$ gives us that $b_1 \le_1 a_1$ and $b_2 \le_2 a_2$----------(2)

From (1) and (2) we get that

$a_{1=} b_1$ and $a_{2=}b_2$

Therefore $(a_{1,}\, a_2) = (b_1\, ,b_2)$.

Hence r is antisymmetric

(iii) Since $(a_{1,}a_2) \leq (b_{1,}b_2) \Rightarrow a_1 \leq_1 b_1$ and $a_2 \leq_2 b_2$-----------(3)

and $(b_{1,}b_2) \leq (c_{1,}c_2) \Rightarrow b_1 \leq_1 c_1$ and $b_2 \leq_2 c_2$-----------(4)

from (3) and (4) we get $a_1 \leq_1 c_1$ and $a_2 \leq_2 c_2$ . [ $\because \leq_1$ and $\leq_2$ are transitive]

Hence $(a_{1,}a_2) \leq (c_{1,}c_2)$ which proves the result.

On same line we can prove that cartesion product of two lattices $(A_{1,} \leq_1)$ and $(A_{2,} \leq_2)$ is a lattice (see problem 1).

**5.3.3 Theorem**: - Let L be a lattice, then for every a and b in L.

(1) $a\vee b = b$ iff $a \leq b$

(2) $a \wedge b= a$ iff $a \leq b$

(3) $a \wedge b = a$ iff $a\vee b=b$

**Proof**:-(1) Let us given that $a\vee b = b$--------------- (1)

We know that $a \leq a\vee b$ [by definition of l.u.b of a and b]

Now using (i) we get $a \leq b$--------------- (2)

Then $b \leq a\vee b$ [by definition of l.u.b]

But b is upper bound of a and b (by (2))

Hence $b\leq a\vee b\leq b \Rightarrow b=a\vee b$

(2) See problem (2)

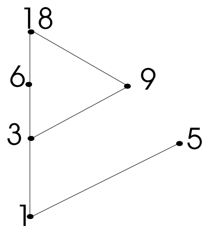
(3) By (2) we get $a\wedge b=a \Leftrightarrow a \leq b$, Now using (1) we get that $a \leq b \Leftrightarrow a\vee b=b$

$\therefore a \wedge b= a \Leftrightarrow a\vee b=b$.

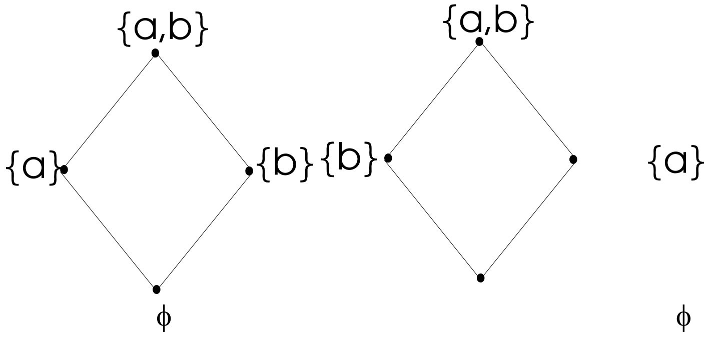
## 5.4 HASSE DIAGRAM

**5.4.1 Definition: -** Hasse diagram is pictorial representation of a finite partial order on a set. In this diagram the elements are shown by vertices (or dots). The two related vertices in Hasse diagram of a partial order are connected by a line.

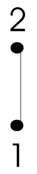
**Example**. Let A={1,3,5,6,9,18} and partial order relation that aRb iff a/b. Its Hasse diagram is as



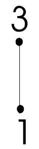
Hasse diagram of (P (A), ≤) where A={a, b} and $A_1 \leq A_2$ iff $A_1 \subseteq A_2$, P (A) is power set of A then its Hasse diagram is



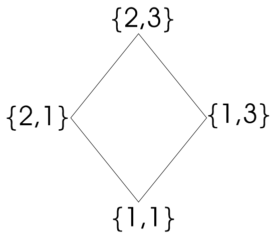
**Example**: -Let $L_1$\{1,2\} and $L_2$\{1,3\} be the chains of divisors of 2 and 3 with partial order of divisibility. Then Hasse diagram of chain $L_1$ is



And that of chain $L_2$ is



Then Hasse diagram of $L_1\times L_{2=}$ {(1,1), (1,3), (2,1), (2,3)} i.e. lattice $L_1\times L_{2\text{ is}}$



## 5.5 BOOLEAN ALGEBRA AND PROPOSITIONS

**5.5.1 Definition** A non empty set B with $\vee$ and $\wedge$ as to binary operation, as unary operation and two elements 0 and 1 is called a Boolean Algebra if following axioms holds for a,b and c $\in B$

(1) Both binary operations are commutative on B i.e. $a\vee b=b\vee a\ \forall\ a,b\in B$

(2) Distributive laws holds in B

i.e. $a\wedge(b\vee c)=a\wedge b\vee a\wedge c$ and $a\vee(b\wedge c)=a\vee b\wedge a\vee c\ \forall\ a, b,c \in B$

(3) Identity element exist under both binary operations. i.e.

$a\vee 0=a$ and $a\wedge 1=a\ \forall\ a\in B$

(4) Complement laws $a \vee a' = 1$ and $a \wedge a' = 0$ where 0 is called zero element, 1 is called unit element and $a'$ the complement of a.

We will denote Boolean algebra by (B,∨, ∧, ‘, 0,1)

**Example**:-If we take P (A), power set of a non empty set A. Then for two binary operation ∪ (set union), ∩ (set intersection), and unary operation complement of set, (P (A),∪, ∩, -,ϕ,A) acts as Boolean Algebra.

**Solution**: - We will show that all the axioms of Boolean algebra holds

(1) ∪, ∩ are commutative since B∪C=C∪B and B∩C=C∩B for all B, C∈ P (A)

(2) We also know that in sets B, C, D

B∪(C∩D)=(B∪C) ∩ (B∪C) and

B ∩(C∪D)=(B∩C) ∪ (B∩D) there for both distributive laws holds.

(3) Now B∪ϕ=B (and B∩A=B ∀ B∈P(A)

I.e. identity laws holds since ϕ and A acts as identity element under ∪ and ∩ respectively

(4) $B \cup \overline{B}$=A and $B \cap \overline{B} = \phi$ is complement of B. which proves the result.

**5.5.2 Proposition Definition**: -Proposition is a declarative sentence that is either true or false but not both.

**Example**: - (1) Sun rises in the west.

It is proposition since this sentence is declaration but not true

(ii) 2+2=4 is again a proposition

(ii) x .y > 0, x ,y∈I is not a proposition as x.y may be greater than zero. For x=2,y=1 it is greater than zero, but for x=-2 and y=1 x .y < 0

**Note: -** (i) We generally denote propositions by lower letters p,q,r,s

(ii) A proposition is also called a statement.

**5.5.3 Definition**: - If more than one propositions are connected then proposition is called compounded. A proposition, which is not compound, is called primitive.

**For Example**: -Peacock is national bird of India and cow is national animal India

This is a compounded statement which is connected by and.

We have two primitive statements

(1) Peacock is national bird of India.

(2) Cow is national animal of India.

## 5.6 LOGICS WITH THEIR TRUTH TABLES

There are three basic logical operations

(1) Negation

(2) Conjunction

(3) Disjunction

Which correspond to not, and, or respectively.

**5.6.1 Negation** of a statement p is which contradicts the statement p. It is denoted by ~p. The relation between truth values of ~p and p has truth table given below

| p | -p |
|---|---|
| T | F |
| F | T |

i.e. when p is true ~p is false and when p is false it negation is true.

**Example**: - If p is "there exist a and b for which ab≠ba", then ~p is "For all a and b, ab=ba."

**5.6.2 Conjunction**: -The conjunction of two-statement p and q is generally denoted by $p \wedge q$.

The true table for conjunction of two statements is given below

| P | q | $p \wedge q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

i.e. conjunction is true only when both p and q are true otherwise it is false.

**5.6.3 Disjunction**: - Disjunction of two statements is denoted by $p \vee q$ its truth table is given below.

| P | q | $p \vee q$ |
|---|---|---|
| T | F | T |
| T | T | T |
| F | T | T |
| F | F | F |

We define some other truth tables as for $p \rightarrow q$

| P | q | p→q |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

Truth table for p↔q i.e. it is conjunction of p→q and q→p

Its truth table is as

| p | q | p→q | q→ p | p→q ∧ q→p |
|---|---|---|---|---|
| T | T | T | T | T |
| T | F | F | T | F |
| F | T | T | F | F |
| F | F | T | T | T |

Therefore reduced form of true table is

| P | q | p→q ∧ q→p |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

**Example** Find the truth table for p∧(q∨r) and for p∧q∨p∧r and hence show that both are equivalent.

Truth table for p∧(a∨r)

| P | q | r | $q\vee r$ | $p\wedge(q\vee r)$ | $p\wedge q$ | $p\wedge r$ | $p\wedge q \vee p\wedge r$ |
|---|---|---|---|---|---|---|---|
| T | T | T | T | T | T | T | T |
| T | T | F | T | T | F | F | T |
| T | F | T | T | T | T | T | T |
| T | F | F | F | F | F | F | F |
| F | T | T | T | F | F | F | F |
| F | F | T | T | F | F | F | F |
| F | T | F | T | F | F | F | F |
| F | F | F | F | F | F | F | F |

This table shows that $p\wedge(q\vee r) \cong (p\wedge q) \vee( p\wedge r)$

Another example of Boolean algebra

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

| . | 1 | 0 |
|---|---|---|
| 1 | 1 | 0 |
| 0 | 0 | 0 |

And $1'=0$ and $0'=1$ then B is a Boolean Algebra infect if we take 1=T and 0= F then sum is equivalent to truth table for $p\vee q$ and is truth table for $p\wedge q$.

## 5.7 KEY WORDS AND SUMMERY

In this chapter we have studied partial order relation Boolean algebra, lattices and logic gates with their truth tables.por, lattice, Hasse diagram, Boolean algebra, logics are key words.

## 5.8 SELF ASSESSMENT QUESTIONS

Q (1) Prove that cartesion product of two lattices ($A_{1,}$ $\leq_1$) and ($A_{2,}$ $\leq_2$) is a lattice

Q (2) Let L be a lattice, then for every a and b in L, $a \wedge b = a$ iff $a \leq b$.

Q (3) Let A={1,3,5,6,9,18} and partial order relation that aRb iff $a \leq b$. Draw Its Hasse diagram.

Q (4) Prove that every chain is a distributive lattice.

## 5.9 SUGGESTED READINGS

(3) Seymour Lepschutz, Finite mathematics (International edition 1983), McGraw-Hill Book Company , New York.

(4) N.Deo, Graph Theory with application and computer science , Pentile Hall of India.

**MCA-205: Mathematics –II (Discrete Mathematical Structures)**

**Lesson No: 6** **Written by Pankaj Kumar**

## Lesson: Boolean Algebra- II Vetted by Prof. Kuldip Singh

**STRUCTURE**

**6.0 OBJECTIVE :** Objective of this chapter is to gain more knowledge about Boolean algebra and their application in electric circuits.

**6.1 INTRODUCTION:** In this chapter we study some more results about Boolean algebra, Boolean functions, switching circuits, logics gates e.t.c.

### 6.2 SOME MORE RESULTS OF BOOLEAN ALGEBRA

**6.2.1 Theorem**: - $\forall$ a $\in$B, a+a=a and a. a=a (idem potent laws in Boolean Algebra)

**Proof**: -(i)We know by Boolean Algebra Axiom a.1=a

$\therefore$ (a+a) = (a+a).1

= (a+a). (a+a') [$\because$(a+a')=1]

= a+ a. a' [using distributive law]

=a

(ii) a=a.1=a. (a+a')=a.a+a.a'=a.a+0=a.a

**6.2.3 Bounded ness law**:- If (B,+, . ,' ,) is a Boolean Algebra, then

(i) (a+1)=1 and a.0=0∀ a∈B

**Proof**: -(i) Since

(a+1) = (a+1).1

= (a+1). (a+a') [∵(a+a')=1]

=a+(1.a' ) [using distributive law]

=a+(a'.1)=a+a'=1

(ii) a.0=(a.0)+0 [∵0=a.a']

=a.0+a.a'=a.(0+a') [using distributive law]

= a.(a'+0)=a.a'=0

**6.2.4 Theorem**:-Absorption law:- a+(a.b)=a and a. (a+b)=a ∀ a,b ∈B, B is Boolean Algebra

**Proof**: -(i) a+a.b

=a.1+a.b= a.(1+b) [using distributive law]

=a.1 [∵1+b=1 ∀ b∈ B]

(i) (a+b)

=(a+0).(a+b) [∵ a+0=a' ∀ a∈ B]

=a+0.b

=a

**6.2.5 Theorem**:- If (B,+,.,') is a Boolean algebra, then

(i) (a+b)'=a'.b' ∀a, b ∈B

(ii) $(a.b)' = a'+b' \ \forall a, b \in B$

**Proof**: - (i) $(a+b)+a^{1}.b^{1}$

$=(a+b+a').\ (a+b+b')$ [using distributive law]

$=(a+b+a').\ (a+1)$ [$\because$ $b+a'=a'+b$, $b+b'=1$]

$=(1+b).\ (a+1)$ [$a+a'=1$]

$=1.1$

$=1$

also $(a+b).a'.b'$

$=(a'.b').(a+b)$ [by commutative law]

$=a'.b'.a+a'.b'.b$ [by distributive law]

$=a'.a.b'=a'.0$ [$\because$ $b'.b=0$ and $a.a'=0$]

$=0.b'+a'.\ 0=0+0=0$ [by Bounded ness law]

$\therefore$ We get that $a'.b'=(a+b)'$

(ii) See problem (1)

**6.2.6** **Theorem**:- cancellation law in a Boolean Algebra

(i) If $a+b=a+c$ and $a'+b=a'+c$, then $b=c$

(ii) If $a.b=a.c$ and $a'.b=a'.c$, then $b=c$

**Proof:-** (i) $b=b+0$

$=b+a.a'$ [$\because$ $a.a'=0 \forall\ a \in B$]

$=(b+a).(b+a')$ [by distributive law]

$=(a+b).(a'+b)$ [by commutative law]

$=(a+c).(a'+c)$ [by given condition]

$=(c+a).(c+a')$ [by commutative law]

$=c+a.a'=c+0=c$

(ii)$b=b.1$

$=b.(a+a')$ [$\because$ $a.a'=0 \forall\ a \in B$]

$=b.a+b.a'$ [by distributive law]

$=a.b+a'.b$ [by commutative law]

$=a.c+a'.c$ [by given condition]

$=c.a+c.a'$ [by commutative law]

$=c+(a+a')=c.1=c$

**Example**: - In a Boolean Algebra show that $a.b+a.b'+a'.b+a'.b'=1$

**Solution**: - L.H.S:- $a.b+a.b'+a'.b+a'.b'$

$= a.(b+b')+a'.(b+b')$ [by distributive law]

$=a1+a'.1$ [$\because b+b'=1$]

$=a+a'=1$

**Example**:- Prove that Boolean Algebra cannot have three elements

**Solution**:- If possible, let Boolean Algebra have exactly three elements. Let a be third element of B other then 1 and 0 since $0'=1$, $1'=0$, we must have $a'=a$ ($\because$ if $a'=0 \Rightarrow a''=0'=1 \Rightarrow a=1$ a contradiction similar $a'\neq1$)

We have $a.a'=0$

$\because a.a=0$

$a=0$ this is not possible because $a \neq 0$, our assumption is wrong.

Hence prove the result.

## 6.3 BOOLEAN FUNCTION

**6.3.1 Definition** :- Let (B,+, . ,' ) be a Boolean Algebra . The element of B is called constants in B. A symbol representing an arbitrary element of B is called a variable in B. A variable in B is denoted by letters a,b,c,--- ------------ ,p,q,r, ------------x,y,z etc.

**6.3.2 Definition :-** In (B,+, . ,' ,0,1), a variable or a well formed expressions involving Boolen operation '+','.',' and a finite number of variable is called Boolen function.

**For Example** $x+y+z$, $x.y+z'$. etc

**Note**: - In a B having n variable a product of the form $y_{1.}y_2$-----------$y_n$ wher $y_i=x_i$ or $x_i'$ for I=1,2,______,n is called a minterm in n varialble. Simple calculatioln shows that we have $2^n$ minterm in B having n variable.

Bool's expansion theorem:- Statement of (B,+, . ,' ,0,1) be a Boolean Algebra and $f(x_{1,}x_2$-----------$x_n)$ be a Boolean function in n variable $x_{1.}x_2$------------$x_{n,}$ then

$f(x_{1,}x_2$------------$x_n)$= f(1,1,1,-- ------,1) $x_{1.}x_2$------------$x_n$ +f(0,1,-- ------,1) $x_{1,}x_2'$------------$x_n$ +f(1,0,1,-- ------,1) $x_{1.}x_2'.x_3$------------$x_n$ +----+f(0,0,-- ------,0) $x_1',x_2'$------------$x_n'$

**Example**:- Let (B,+, . ,' ,0,1) be a Boolean Algebra and let f(x,y ) be Boolean function of the variable x and y. By using the following table find the expression for f(x,y)

| x | y | f(x,y) |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

**Solution**:- From given table

f(1,1)=0, f(1,0)=1, f(0,1)=0, f(0,0)=1

Now Boole's expansion theorem, we have

$f(x,y)= f(1,1).x.y + f(1,0)x.y' + f(0,1).x'.y+ f(0,0).x'.y'$

$=0.x.y+1.x.y' +0.x'.y +1.x'.y'$

$=0+x.y' +0 +x'.y'$ $\quad$ $[\because 0.a=0 \ \forall \ a\in B]$

$=x.y' +x'.y'$

$=(x+x').y'$ $\quad$ [by distributive law]

$=1.y'$ $\quad$ $[\because x+x'=1]$

$=y'$

## 6.4 APPLICATION OF BOOLEAN ALGEBRA IN SWITCHING CIRCUITS.

**6.4.1 Definition: -** Switching circuit is a arrangement of wires and switches connected together to the terminal of a battery. A switch is a two state device used for allowing current to pass through it or not to pass through it.

A switch in a circuit are denoted by letter a,b,c………………p,q,r,…………………,x,y,z etc.

There are two methods of connecting two switches

(1) Connecting switches in parallel is as

The lamp is on if at least one switch is on.

(2) Connecting switches in series

The lamps is on iff x and y are both are on.

**Note**: If we denote 0, when switch is off and 1 stands when switch is on. Then we observe following Table when switches are parallel i.e. is

| x | y | x+y | y+x |
|---|---|---|---|
| 0 |  | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 |

1

And when switched are in series, following table show their output

| x | y | x-y | y.x |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 |

2

If we take switch is off when switch x is on and is on when switch x is off. Its Table is as

| x | x' | x+x' | x.x' |
|---|---|---|---|
| 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 |

3

**6.4.2 Theorem:-** Prove that if we denote x+y when switches are parallel and x.y when switches are in series and x' denoting switch is off when x is off. Then this switching circuit is a Boolean algebra

**Proof**: - (1) By table (1) and (2) we get that both operations are commutative

(2) For all x,y,z belonging to B

| x | y | z | y.z | x+y.z | x+y | x+z | (x+y).(x+z) |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

This table show that distributive law x+y.z=(x+y).(x+z) holds . Similarly we can show that x.(y+z)=x.y+x.z for all x,y,z belonging to B.

(3)

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

| x | 1 | x.1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 1 |

i.e. identity laws holds in which 0 and 1 acts as zero element and identity element of B.

(4)

| x | x' | x+x' |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 1 |

| x | x' | x-x' |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 0 | 0 |

i.e. $x+x' =1$ and $x.x'=0 \ \forall \ x \in B$. Showing that complement laws holds.

Hence we have proved that it is Boolean algebra.

**Example**:- Find Boolean function corresponding Boolean switching circuits

**Solution:-** In the circuit y and x' are parallel which is represented by y+x', $\therefore$ Boolean function $\forall$ x.(y+x').z.

**Example**:- Simply X'.Y'+X.Y'+X'.Y

**Solution**:- Here Boolean function

f(x,y)=X'.Y'+X.Y'+X'.Y

= (X'+X).Y'+X'.Y

=1.Y'+X'.Y [$\because$X+X'=1]

=Y'+X'.Y [$\because$1.a=a]

= (Y'+X').(Y'+Y)

=(Y'+X').1

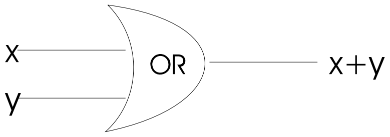
= Y'+X'

## 6.5 LOGIC GATE

**Definition: -** A logic gate is simply and electronic circuit which operate on one or more input signal to produce standard output signals. There logic gates are the building blocks of all the circuits in a computer . There are three basic logic gates called or **GATE, AND GATE AND NOT GATE**.

**Note**: We shall use the convention that the lines entering the gate symbol from the left are input lines and the single line on the right is the output line.

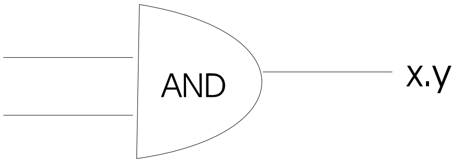
**6.5.1 OR GATE**: - It is an electronic circuit that generates the output signal of 1 if any one of the input signals is 1. Two or more switches connected in parallel behave



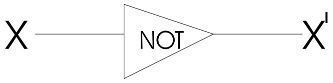
as an OR GATE

### 6.5.2 Switches in parallel

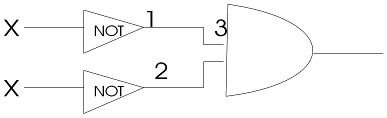
**AND GATE**:- It is an electronic circuit that generates the output signal 1 only if all input signals are 1. Two or more switches connected in series behave as an



**6.5.3 NOT GATE**:- It is an electronic circuit that generates an output signal which is reverse of the input signal.



**Example**:- Find the Boolean expression for the output of the given logic circuit. Also draw the truth table for the given logic circuit



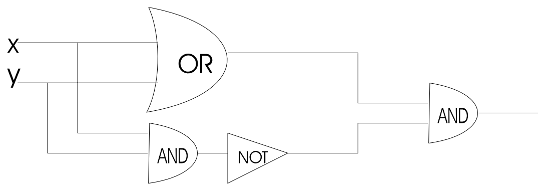
**Solution**:- The inputs are x and y. At point 1 the output of NOT gate is X', at point 2, the output of NOT gate is y'. The input to the OR gate at point 3 are X' and Y' whose output is X'+Y'.

**Truth table is**

| Inputs | | | | Output |
|---|---|---|---|---|
| x | y | x' | y' | x'+y' |
| 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 |

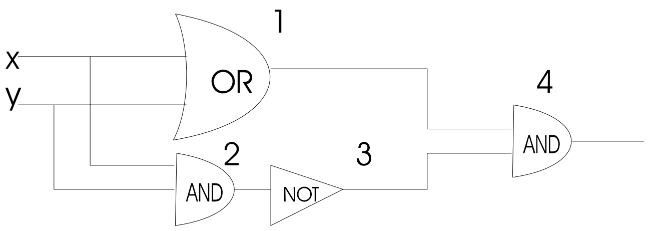
| | | | | |
|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 |

**Example**: - find the Boolean expression for the output of the given logic circuit



Also draw the truth table for the given logic circuit

**Solution**:- Given circuit is shown Below



At point 1, the output of the OR gate is x+y

At point 2, the output of the AND gate is x.y

At point 3, the output of the NOT gate is (x.y)'

At point 4, the output of the AND gate is (x+y).(x.y)'

Its truth table is

| Inputs | | | | Output | |
|---|---|---|---|---|---|
| x | y | x+y | x.y | (x.y) | (x+y).(x.y)' |
| 0 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 0 |

## 6.6 KEY WORDS AND SUMMERY

In this chapter we have studied some more results about Boolean algebra, Boolean functions, switching circuits, logics gates e.t.c. Switching circuit, gates are key words

## 6.7 SELF ASSESSMENT QUESTION

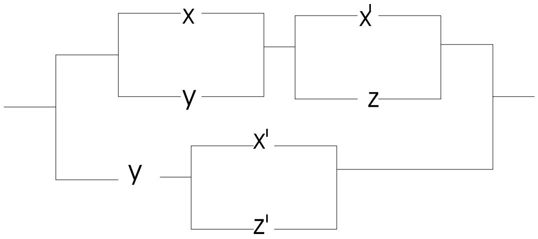
Q (1) If (B,+,.,') is a Boolean algebra, then $(a.b)'= a'+b' \ \forall a, b \in B$

Q (2) Let B={1,2,3,4,6,12} be the set of positive divissor of 12. If we define +,. And ' by a+b= lcm(a,b), a.b=gcd(a,b) and a'=12/a respectively $\forall$ a,b $\in$B. Then show that (B,+, . ,') is not a Boolean Algebra.

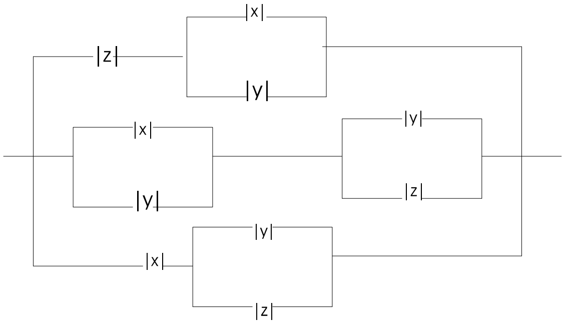
Q (3) B is set positive divisors of 6. We define the binary and unary operation as defined in exercise 2, show that (B,+, . ,') is a Boolean Algebra in this case.

Q (4) Simplify the circuits given below

(a)



(b)



Q (5) Find out the logic circuit corresponding to the following input tables

| Input | | Output |
|---|---|---|
| X | Y | |
| 0 | 0 | 1 |
| 1 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 1 | 0 |

## 6.8 SUGGESTED READINGS

(1) Seymour Lepschutz, Finite mathematics (International edition 1983), McGraw-Hill Book Company , New York.

(2) N.Deo, Graph Theory with application and computer science , Pentile Hall of India

**MCA-205: Mathematics –II (Discrete Mathematical Structures)**

**Lesson No: 7** **Written by Pankaj Kumar**

**Lesson: Integral Domains** **Vetted by Prof. Kuldip Singh**

**STRUCTURE**

**7.0 OBJECTIVE:** Objective of this chapter is to gain some knowledge about algebraic structure with two binary operations**.**

**7.1 INTRODUCTION:** In chapter first we have studied algebraic structure with one binary operation. In this chapter, we will study the algebraic structure with two binary operations. We define rings, integral domains, fields and ring of polynomials over the field. We will also know about extension field containing all the roots of given polynomial.

## 7.2 SOME DEFINITIONS (STRUCTURE, RING)

**7.2.1 Definition:** We define structure is a non empty set with at least n ary operation defined on it and under which elements of the set satisfies certain axioms. For example group is an algebraic structure.

**7.2.2 Definition:** Let R be a non empty set with two operations (+, .) generally called addition and multiplication. If elements of R satisfies following axioms

(1) R is commutative group under addition

(2) It is closed under multiplication i.e. multiplication is binary operation on R

(3) Multiplication is associative on R i.e. $a.(b.c)=(a.b).c \ \forall$ a, b and c $\in R$,

(4) Distributive laws holds in R i.e.

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

Then R is called a ring. More over if

$$a.b=b.a \quad \text{and} \quad a.e=e.a=a \ \forall \ a, b \in R,$$

then R is called commutative ring with unity.

## 7.3 INTEGRAL DOMAIN

**7.3.1 Zero divisor**: For two elements a, b belong to a ring R such that a.b=0, neither $a\neq 0$ nor $b\neq 0$, then we call a as zero divisor.

**Example:** The set {0, 1, 2, 3, 4, 5} forms a ring under addition and multiplication modulo 6 which can be shown easily. Now

$2 \times_6 3 = 0$; neither 2 is zero nor 3 is equal to

**7.3.2 Definition**: A commutative ring is an integral domain if it is with out zero divisor.

**Example**: (1) I (+,.) (Set of integers) is an integral domain under ordinary addition and multiplication.

**Solution**: Since ordinary addition and multiplication of two integers is again an integer hence both operations are binary operation.

We also know (in chapter I) that under addition the set of integer is a commutative group. Hence the first condition holds.

(2) Since the product of two integers is again an integer, multiplication is binary operations on set of integer.

(3) Since a.(b.c)=(a.b).c $\forall$ a,b,c$\in$I ,ordinary multiplication is associative .

(4) We also know that a.(b+c)=a.b+a.c and (a+b).c=a.c+b.c i.e distributive law holds in I.

(5) a.b=b.a $\forall$ a,b,$\in$I ,ordinary multiplication is commutative in I.

(6) Since a.b=0 $\Rightarrow$ either a=0 or b=0, therefore I is without zero divisor.

We see that set of integers satisfies all the axioms of integral domain Hence (I,+,x) is an integral domain.

**Example:** (2) Set D={0,1,2,3,4}$_{+,x\ (5)}$ i.e. set of integers from 0 to 4 is an integral domain under addition and multiplication mod 5.

**Solution: -** As by definition of $a+_5b$ is least non-negative remainder when the sum of a and b is divided by 5, it certainly belongs to D. Similarly a $\times_5$ b belongs to D i.e. addition and multiplication mod 5 are binary operations on D. Now we will show that D satisfies all the conditions of integral domain.

(1) The following Table 1, shows that D is a commutative group under addition mod 5 since by table 1, 0+a=a $\forall$ a$\in$I ,0 acts as identity element, inverse of 0 is 0,1is 4 and 2 is 3.More over ij th entry of matrix is equal to ji th entry of the table i.e. $a+_5b=b+_5a$ .

| $+_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

Table 1

| $\times_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Table 2

By Table 2, we see that ij th entry of matrix in table 2 is equal to ji th entry i.e. $a\times_5 b=b\times_5 a$. Hence multiplication mod 5 is commutative on D. Also by the use of both tables we get

$2\times_5(3+_5 4)$

$=2\times_5 2$ (By table 1)

$=4$ (By table 2)…(1)

$(2\times_5 3)+_5(2\times_5 4)$

$=1+_5 3$ (By table 2)

$=4$ (By table 1)…(2)

Since (1)=(2), distributive laws also holds

Moreover $a\times_5 b=0$ iff $a=0$ or $b=0$ (by table 2) shows that D is without zero divisors. Hence D is an integral domain. This is an example of finite integral domain.

**7.3.3 Note:** If D is an integral domain with unity such that each of its non zero elements has an inverse under multiplication then D is called **field**. It is generally denoted by F, so set F will be a field under addition and multiplication if

(1) It is **abelian** group under **addition**.

(2) **Distributive** laws hold in F

(3) **F- {0}** is **commutative group** under **multiplication**.

**Example:** The set of rational numbers is a field under ordinary addition and multiplication as binary operations. Another example is the set {0, 1, 2, 3, 4} under addition and multiplication mod 5. Generally, the set {0, 1, …, p-1} is afiled under under addition asnd multiplication mod p , p is prime number.

## 7.4 POLYNOMIALS

**7.4.1 Polynomial**: Let F be a field. A polynomial over F is a polynomial in indeterminate x whose coefficients are element of the field F. We write $f(x) \in F[x]$.

For example $x^2+1$ is a polynomial over Q (field of rational numbers)

$x^2+i$, $i=\sqrt{-1}$ is a polynomial over C (the field of complex numbers)

$x^2+\sqrt{2} \notin Q[x]$ as coefficient $\sqrt{2} \notin Q$

**7.4.2 Theorem:** If F is a field then F [x], the set of all polynomials over F, forms an integral domain.

**Proof**: Take $f(x)= a_0+ a_1x^1+ a_2x^2+\ldots+ a_nx^n$ and

$g(x)= b_0+ b_1x^1+ b_2x^2+\ldots+ b_nx^n$ , and define addition of two polynomials as $f(x)+ g(x) = (a_0+ b_0 )+(a_1+b_1)x^1+(a_2+b_2)x^2+\ldots+ (a_n+b_n)x^n$ (i.e. component wise addition) and multiplication of two polynomials as

$f(x).\ g(x)=\sum d_i x^i$ , $d_i = \sum\limits_{l+r=i} a_l b_r$ where sum runs over all positive integers l and r whose sum is i.

$\therefore\ d_0=a_0b_0$

$d_1=a_0b_1+ a_1b_0$.

$d_2=a_0b_2+a_1b_1+a_2b_0$. and so on.

Clearly addition and multiplication of two polynomials is again a polynomial over F, therefore addition and multiplication are binary operations on F[x].

Now for f(x), g(x), t(x) in F [x] where t(x) is $c_0+ c_1x^1+ c_2x^2+\ldots+ c_nx^n$ ,

$(f(x)+ (g(x)+ t(x))= (a_0+ a_1x^1+ a_2x^2+\ldots+ a_nx^n)+(( b_0+ b_1x^1+ b_2x^2+\ldots+ b_nx^n )+ (c_0+ c_1x^1+ c_2x^2+\ldots+ c_nx^n ))$

$=(a_0+ a_1x^1+ a_2x^2+\ldots+ a_nx^n)+( (b_0+ c_0 )+ (b_1+ c_1 )x^1+ (b_2+ c_2 )x^2+\ldots+$

$(b_n+ c_n )x^n )$

$= (a_0+(b_0+ c_0 ))+ (a_1+(b_1+ c_1 ))x^1+ (a_2+(b_2+ c_2 ))x^2+\ldots+ (a_n+(b_n+ c_n ))x^n$

$= ((a_0+b_0)+ c_0 )+ ((a_1+b_1)+ c_1 )x^1+ ((a_2+b_2)+ c_2 )x^2+\ldots+ (a_n+b_n)+ c_n ))x^n$

($\because$ $a_i,b_i,c_i$ are elements of F and addition is associative in F)

$=((a_0+b_0)+ (a_1+b_1)x^1+ (a_2+b_2)x^2+\ldots+$

$(a_n+b_n)x^n$ )+( $c_0 + c_1 x^1 + c_2 x^2 + \ldots + c_n x^n$ )

= (f(x)+ g(x))+ t(x) i.e. addition is associative.

Also $0 \in F[x]$ and for $f(x) \in F[x]$ ,- $f(x) \in F[x]$ such that

f(x)+(- f(x)= (- f(x)+ f(x)=0 implies that identity and inverse of every element in F(x) exists .Finally

f(x)+g(x) $= \sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i)x^i = \sum (b_i + a_i)x^i =$

$\sum b_i x^i + \sum a_i x^i$ =g(x)+f(x).

From above results we get that (F[x],+) is a commutative group.

(2) f(x).( g(x). t(x))=(f(x).g(x)).t(x)(see problem 1) showing that multiplication is associative.

(3) f(x).( g(x)+ t(x))= f(x).g(x)+f(x).t(x)

L.H.S.= f(x).( g(x)+ t(x))= $(\sum a_i x^i).(\sum (b_i + c_i)x^i) = (\sum h_i x^i)$ …………(1) where $h_i = \sum_{l+r=i} a_l (b_r + c_r)$

and R.H.S.= f(x). g(x)+ f(x).t(x)= $(\sum a_i x^i).(\sum b_i x^i) + (\sum a_i x^i).(\sum c_i x^i)$

$= (\sum d_i x^i) + (\sum e_i x^i) = (\sum (d_i + e_i)x^i)$ …(2)

Where $d_i = \sum_{l+r=i} a_l b_r$ and $e_i = \sum_{l+r=i} a_l c_r$ . Now $d_i + e_i = \sum_{l+r=i} a_l (b_r + c_r) = h_i$ , we see that L.H.S.=R.H.S. Hence distributive law holds in F[x].

(4) Finally we will show that F[x] is without zero divisor

$f(x).\ g(x) = 0 \Rightarrow \sum d_i x^i = 0\ ,\ d_i = \sum_{l+r=i} a_l b_r$

$\therefore\ d_0=0 \Rightarrow a_0b_0 = 0 \Rightarrow a_0=0$ or $b_0=0$ or both are zero

w.l.o.g. suppose that $a_0=0$ and $b_0\neq 0$

$d_1=0 \quad \Rightarrow a_0b_1+ a_1b_0=0$

$\Rightarrow a_1b_0=0 \Rightarrow a_1=0$

$d_2=0 \ \Rightarrow a_0b_2+a_1b_1+a_2b_0= 0$

$\Rightarrow\ a_2b_0=0$ i.e. $a_2=0$.Continuing in this way we get $a_i=0\ \forall\ i$ , hence $f(x)=0$ .similarly we can prove that $g(x)=0$,therefore $f(x).\ g(x) =0\Rightarrow$ either $f(x) =0$ or $g(x) =0$, there fore $f(x)$ is without zero divisor which complete the proof that $F[x]$ is an integral domain.

## 7.5 IRREDUCIBLE POLYNOMIALS

**7.5.1 Definition**: -A polynomial f(x) over F is called irreducible over F if it can not be written as product of two non constant polynomials over F, otherwise it is called reducible polynomial. For example $x^2$-3 is a polynomial over field of rational. We can write

$$x^2-3=(x-\surd 3)(x+\surd 3) \text{ but } (x-\surd 3) \text{ and } (x+\surd 3) \notin Q[x]$$

Hence $x^2$-3 is irreducible over Q.

**7.5.2 Remarks (1)** Irreducibly of a polynomial depends on the field.

$x^2$-3 is not irreducible (or reducible over field of real number as (x-√3) and (x+√3) ∈R[x]

**(2)** A non-constant polynomial is a polynomial of degree at least one.

**(3)** A polynomial f(x)= $a_0$+ $a_1x^1$+ $a_2x^2$+…+ $a_nx^n$ is called primitive polynomial if gcd($a_0$, $a_1$, $a_2$,…., $a_n$)=1. Also if f(x) is a primitive polynomial which is factored as product of two polynomials having rational coefficient, then it can be factored as product of two polynomials having integer coefficients.

**(4**) If a polynomial is not primitive, then it can be made primitive polynomial over that field.

**7.5.3 Theorem** Let f(x)= $a_0$+ $a_1x^1$+ $a_2x^2$+…+ $a_nx^n$ be a polynomial with integer coefficient such that for a prime p,p/$a_0$,……….., p/$a_{n-1}$, $p^2 \nmid a_0$, $p \nmid a_n$ (here p/$a_0$ means p divides $a_0$ and $p^2 \nmid a_0$ means p does not divides $a_0$ ) then f(x) is irreducible over Q.

**Proof**: W.l.o.g. we may take f(x) as primitive polynomial. If f(x) factors as product of two polynomials with rational coefficient then we can always write f(x) as product of two polynomials with integer coefficients (Remark (3), 7.5.2). Let if possible f(x) is not irreducible over F, then it is reducible i.e f(x) =g(x)t(x) (1)

where g(x)= $b_0$+ $b_1x^1$+ $b_2x^2$+…+ $b_rx^r$ and t(x**)** is $c_0$+ $c_1x^1$+ $c_2x^2$+…+ $c_sx^s$ , g(x) and t(x) are non constant polynomials. Now by (1), we get $a_0 = b_0c_0$.

Since $p/\ a_0 \Rightarrow p/\ b_0c_0 \Rightarrow$ either $p/\ b_0$ or $p/\ c_0$ ($\because$ if p divides $b_0$ and $c_0$ then $p^2/\ b_0c_0$ i.e. $p^2/a_0$ , a contradiction to our assumption), therefore, w.l.o.g. we suppose that $p/\ b_0$ and $p \nmid c_0$

Let k be the least positive integer so that $p \nmid b_k$ ( because if p divides all $b_k$ then p/f(x), a contradiction to our assumption that f(x) is primitive polynomial). Since

$a_k= b_0c_k+ b_1c_{k-1}+ b_2c_{k-2}+\dots +b_kc_0$ and $p/a_k$

$\Rightarrow$ $p/\ b_0c_k+ b_1c_{k-1}+ b_2c_{k-2}+\dots +b_kc_0$

Further by assumption, p divides $b_0$ , $b_1$, …,$b_k$ , therefore $p/\ b_kc_0$ also

But p neither divides $b_k$ nor divides $c_0$, a contradiction. Hence f(x) can not be written as product of two non constant polynomials. Therefore, f(x) is irreducible.

**7.5.4 Theorem**: Prove that f(x) is irreducible if and only of f(x+1) is irreducible

**Proof:** Let us suppose that f(x) is irreducible and f(x+1) is reducible, then we can write f(x+1)= g(x+1)t(x+1).

If we put (x+1) = y then we get f(y)= g(y)t(y)$\Rightarrow$ f(x)= g(x)t(x), a contradiction to our assumption that f(x) is irreducible. Hence f(x+1) is irreducible. Similarly we can prove converse part of the theorem.

**Example:** Show that $x^4+ x^3+ x^2+ x+1$ is irreducible over Q.

**Solution:** Let us take $f(x) = x^4+x^3+x^2+x^1+1$, than

$f(x+1)=(x+1)^4+(x+1)^3+ (x+1)^2+(x+1)+1$

$=(x^4+4x^3+6x^2+4x+1)+(x^3+3x^2+3x+1)+(x^2+2x+1)+(x+1)+1$

$= x^4+ 5x^3+ 10x^2+ 10x+5.$

Now we get that 5 is a prime number that divides all the coefficients of polynomial f(x+1) and $5^2$ does not divides $5=a_0$. Hence f(x+1) is irreducible by Theorem 7.5.3. Now using Theorem 7.5.4, we get that f(x) is irreducible.

**Example:** Prove that $x^2 + 2x +2$ is irreducible over Q.

**Solution:** Since 2 is a prime number that divides every coefficient of the given polynomial except the leading coefficient and $2^2=4$ does not divides the constant coefficient of the polynomial. Hence by Theorem 7.5.3, the polynomial $x^2 + 2x +2$ is irreducible over Q.

## 7.6 ROOTS OF A POLYNOMIAL

**7.6.1 Definition**: For a polynomial f(x), if f(a)=0, then a is called root of f(x). More over if $f(x)=(x-a)^m g(x)$ such that $g(a)\neq 0$ then a is called root of f(x) with multiplicity m.

For example if $f(x)=(x-3)^2(x+2)$ then 3 is a root with multiplicity 2 and –2 is a simple root of f(x).

**7.6.2 Field extension**: Let F be a field and K be another field containing F, then K is called extension of F and F is called subfield of K.

**For example** C the field of complex number is an extension of R, the field of real numbers. Here R is a subfield of C.

**7.6.3 Theorem (3)** A polynomial of degree n over a field can have at most n roots in any extension field.

**Proof:** We will prove the result by induction on the degree of the polynomial p(x) . If p(x) is of degree 1, then it must be of the form ax+b where a, b are in F and a≠0. If $\alpha$ is a root of p(x) then $a\alpha+b=0\Rightarrow\alpha=(-b/a)\in F$ i.e. p(x) has a unique root (-b/a).Whence conclusion of theorem certainly hold in this case.

Now assume that result to be true in any field for all polynomials of degree less then n. Let us suppose that p(x) is of degree n and K be an extension of F . If p(x) has no root in K then certainly our result holds for the number of roots in K, namely zero roots is certainly at most n. So suppose that p(x) has at least one root a in K and its multiplicity is m say. Since $(x-a)^m /p(x)$, m≤n follows. We get $p(x) = (x-a)^m r(x)$ where $r(x) \in K[x]$ is of degree n-m . Now $(x-a)^{m+1} \nmid p(x) \Rightarrow (x-a) \nmid r(x)$ i.e. a can not be a root of r(x). Also if b is a root of r(x) i.e. r(b) =0, b is also a root of p(x). Since degree of r(x) is less then degree of p(x), by induction hypothesis it has at most (n-m) roots in any extension. Hence it has at most n-m roots in K. Therefore, it is clear that p(x) has at most m + (n-m) = n roots in K. This completes the induction and proves the theorem.

**7.6.4 Note: (1)** This theorem holds when $p(x) \in F[x]$, F is a field. If F is not a field, then a polynomial of degree n may have more then n roots in some extension. For example $x^2+1$ has three roots over the ring {1,-1, i, -i, j, -j, k, -k}.

**(2)** If p(x) is a polynomial of degree n ≥1 over F and it is irreducible over F, then there is an extension E of F such that [E: F]= n[i.e. dimension of E as a vector space over F since every extension act as a vector space over its subfield.] in which p(x) has a root.

**(3)** If $E_0$ is a finite extension of F and E is finite extension $E_0$ then E is finite extension of F also. More over $[E: F] = [E: E_0]\,[E_0: F]$.

**7.6.5 Theorem:** For f(x) $\in$F [X], which is a polynomial of degree n $\geq$1, there exist an extension E of F of degree at most n! in which f(x) has n roots. (a root of multiplicity m is counted m times). In-fact we can say that there always exits an extension E of F which contains a full complements of roots of f(x) $\in$F[X].

**Proof**: We know that if f(x)$\in$F[X] has an irreducible factor say p(x), then there exist an extension $E_0$ of F such that [$E_0$: F]$\leq$ n in which p(x) has a root (by 7.6.4(2)). But every root of p(x) is a root of f(x), therefore, $E_0$ is an extension of F in which f(x) has a root. Thus in $E_0$ we can write f(x) = (x-$\alpha$)q(x) where q(x) is of degree n-1. Now repeating the above process for q(x) we get an extension of $E_1$ of $E_0$ in which has q(x) has a root and [$E_1$:$E_0$]$\leq$n-1. At last we get an extension say E which contains all the roots of f(x) and [E:F]= [E:$E_n$] [$E_n$:$E_{n-1}$]… [$E_1$:$E_0$] [$E_0$: F]$\leq$n(n-1)(n-2)….1=n!.(By note 7.6.4,(3)) Hence proof is over.

## 7.7 SPLITTING FIELD

**7.7.1 Definition:** for f(x) $\in$F[X] , a finite extension E of is said to be splitting field of f(x) over F if over E , but not over any proper subfield of E , f(x) can be written as a product of linear factors.

**7.7.2 Remark (1):** By theorem 7.6.5, we came to know that such an extension always exists.

**(2)**: For any field f, F(a) is called smallest field containing F and a. If a is a root of an irreducible polynomial p(x) ,then [F(a):F]= degree of p(x). For example $x^2$+1 is an irreducible polynomial over Q. As i is a root of it there fore [Q(i):Q]=2. Similarly $x^2$-3 is irreducible over Q as its root $\sqrt{3}$ does not lies in Q. Now [Q ($\sqrt{3}$): Q]=2.

**Example:** Find out splitting fields of some polynomials given below.

(1) $x^4 +1$

(2) $x^4 +x^2 +1$

(3) $x^3 -2$

**Proof: (**1) we can write

$x^4 +1= (x^4 +2 x^2 +1)- 2x^2$

$= (x^2 +1)^2-2x^2 \quad = (x^2 +1)^2-(\sqrt{2}x)^2 =$

$(x^2 +1-\sqrt{2}x) (x^2 +1+\sqrt{2}x) \quad (\because a^2-b^2 =(a-b)(a+b))$

we see that if $\alpha$ is a root of $(x^2 +1-\sqrt{2}x)$ then $-\alpha$ is a root of $(x^2 +1+\sqrt{2}x)$.so we have to find root of $(x^2 +1-\sqrt{2}x)$ .its root $\alpha$ is given as $\alpha = \dfrac{-\sqrt{2} \pm \sqrt{2-4}}{2} = \dfrac{-\sqrt{2} \pm \sqrt{-2}}{2} = \dfrac{-\sqrt{2} \pm \mathrm{i}\sqrt{2}}{2} = \dfrac{\sqrt{2}(-1 \pm i)}{2}$ .

We see that $Q(\sqrt{2}, i)$ is the smallest field containing $\dfrac{\sqrt{2}(-1 \pm i)}{2}$. Hence $Q(\sqrt{2}, i)$ is the required splitting field and

$[Q(\sqrt{2},i):Q]= [Q(\sqrt{2},i):Q(\sqrt{2})][Q(\sqrt{2}):Q]=2\times2=4$.( $\because$ $\sqrt{2}$ satisfies an irreducible polynomial $x^2-2$ over Q hence $[Q(\sqrt{2}):Q]=2$ . Similarly i satisfies an irreducible polynomial $x^2+1$ over Q, therefore, it satisfies $x^2+1$ over $Q(\sqrt{2})$ also hence $[Q(\sqrt{2},i):Q(\sqrt{2})]=2$.)

(2) We can write

$$x^4+x^2+1 = x^4+2x^2+1- x^2 = (x^2+1)^2- (x)^2 = (x^2+x+1 )(x^2-x+1).$$

We see that if $\alpha$ is a root of $(x^2 +x+1)$ then $-\alpha$ is a root of $(x^2 -x+1)$, therefore we have to find root of $(x^2 +x+1)$. Its root $\alpha$ is given as $\alpha=\frac{-1\pm\sqrt{1-4}}{2}=\frac{-1\pm\sqrt{-3}}{2}=\frac{-1\pm i\sqrt{3}}{2}= \omega$ (complex cube root of unity). But $\omega$ satisfies second degree irreducible polynomial over Q. Hence $[Q(\omega):Q]=2$.

(3) For $f(x) =x^3-2$. Its roots are $(2)^{\frac{1}{3}}, \omega(2)^{\frac{1}{3}}, \omega^2(2)^{\frac{1}{3}}$, where $\omega$ is complex cube root of unity. Now $Q((2)^{\frac{1}{3}}, \omega)$ is smallest field containing $(2)^{\frac{1}{3}}$ and $\omega$ .

Now $(2)^{\frac{1}{3}}$ satisfies $x^3-2$, an irreducible polynomial of degree three over Q. Hence $[Q((2)^{\frac{1}{3}}):Q]=3$. Since $\omega$ is complex number, it is not contained in $Q((2)^{\frac{1}{3}})$ which is subset of real numbers. Also $\omega$ satisfies an irreducible polynomial $x^2+x+1$ over Q, therefore it satisfies $x^2+x+1$ over $Q((2)^{\frac{1}{3}})$ also. Hence $[Q((2)^{\frac{1}{3}}, \omega): Q((2)^{\frac{1}{3}})]= 2$. Hence

$$[Q((2)^{\frac{1}{3}}, \omega):Q]= [Q((2)^{\frac{1}{3}}, \omega):Q((2)^{\frac{1}{3}})][Q((2)^{\frac{1}{3}}):Q]=2.3=6=3!.$$

**7.7.3 Remark** In first example we see that degree of extension of splitting field is equal to degree of polynomial, in second we see that it is equal to degree of polynomial and in last example we see that degree of extension of splitting field is equal to 3! which is maximum degree extension according to Theorem 7.6.5.

**7.8 KEY WORD AND SUMMERY:** In this chapter we have defined polynomial over field, irreducibility of that polynomial over given field and splitting field of polynomial.

Polynomials, irreducibility, splitting field are key words

## 7.9 SELF ASSESSMENT QUESTIONS

(1) Prove that over any field F, f(x).( g(x). t(x))=(f(x).g(x)).t(x) where f(x), g(x) and t(x) are polynomials over F.

(2) Prove that $(D,+\times_n)$ is an integral domain iff n is a prime number(operations are addition and multiplication mod n).

(3) Prove that in integral domain F[x], degree (f(x). g(x)) =degree f(x)+ degree g(x) but result does not holds over arbitrary ring.

(4) Find out splitting field of polynomials $x^6+x^3+1$, $x^4-1$ and $x^3-3$ over Q.

(5) Show that $x^n-p$ and $x^{10}+x^9+\ldots+x^2+x^1+1$ are irreducible over Q

## 7.11 SUGGESTED READINGS:

(1) I.N. Herstein, Topics in Algebra, Wiley eastern Ltd., New Delhi, 1975.
(2) Surjeet Singh and Quazi Zameeruddin., Modern Algebra.