

## UNIT- IV

### Topic : 1 Algebraic Structures

#### 1) Define Binary Operation with Example:

Let  $A$  be any non-empty sets. The binary operation  $*$  is a function from  $A \times A$  i.e. a rule which assigns to every pair  $(a, b) \in A \times A$ , a unique element  $a*b \in A$ .

##### Example:

Usual addition, multiplication are binary operation defined on the set of real numbers.

Matrix addition and Matrix multiplication are binary operation on the set of  $2 \times 2$  real matrices.

#### 2) Define Algebraic System with Example:

A non-empty set  $A$  together with one or more  $n$ -ary operations  $*$  defined on it, is called an algebraic system or algebraic structure or Algebra.

We denote it by  $(A, *)$

Note:  $+, -, \cdot, \times, *, \cup, \cap$  etc., are some of binary operations.

#### Properties of Binary operations:

Let the binary operation be  $*$  :  $A \times A \rightarrow A$ .

Then we have the following properties

##### 1) Closure Property:

$$a * b \in A \quad \text{for all } a, b \in A.$$

##### 2) Associativity:

$$(a * b) * c = a * (b * c) \quad \text{for all } a, b, c \in A.$$

##### 3) Identity element:

$a * e = e * a = a$ , for all  $a \in A$ , where  $e$  is called the identity element.

4) Inverse element:

If  $a * b = b * a = e$ , then  $b$  is called the inverse of  $a$  and it is denoted by  $a^{-1}$ , (i.e.  $b = a^{-1}$ ).

5) Commutative:

$a * b = b * a$  for all  $a, b \in A$ .

6) Distributive properties: for all  $a, b, c \in A$ .

(i)  $a * (b \cdot c) = (a * b) \cdot (a * c)$  [Left distributive law]

(ii)  $(b \cdot c) * a = (b * a) \cdot (c * a)$  [Right distributive law]

7) Cancellation properties: for all  $a, b, c \in A$

(i)  $a * b = a * c \Rightarrow b = c$  [Left cancellation law]

(ii)  $b * a = c * a \Rightarrow b = c$  [Right cancellation law]

Note:

If the binary operations defined on  $G$  is  $+$  and  $\times$ , then we have the following table

	Properties	For all $a, b, c \in (G, +)$	For all $a, b, c \in (G, \times)$
1.	Closure	$a + b \in G$	$a \times b \in G$
2.	Associativity	$(a + b) + c = a + (b + c)$	$(a \times b) \times c = a \times (b \times c)$
3.	Identity element	$a + 0 = 0 + a = a$ , Here 0 is Additive Identity	$a \times 1 = 1 \times a = a$ , Here 1 is Multiplicative Identity
4.	Inverse element	$a + (-a) = 0$ , Here $(-a)$ is Additive inverse	$a \times \frac{1}{a} = \frac{1}{a} \times a = 1$ , Here $\frac{1}{a}$ is multiplicative inverse
5.	Commutative	$a + b = b + a$	$a \times b = b \times a$

### Notation:

$\mathbb{Z}$ or $I$	The set of all integer.
$\mathbb{Q}$	The set of all rational number.
$\mathbb{R}$	The set of all real number.
$\mathbb{R}^+$	The set of all positive real number.
$\mathbb{Q}^+$	The set of all positive rational number.
$\mathbb{C}$	The set of all complex number.

### Example 1:

The set of integers  $\mathbb{Z}$  with the binary operations  $+$  and  $\times$  is an algebraic system since it satisfies all the above properties.

### Example 2:

The set of real numbers  $\mathbb{R}$  with binary operations  $+$  and  $\times$  is an algebraic system.

### 3) Define Semi group with Example:

**Definition:** If a non-empty set  $S$  together with the binary operation  $*$  satisfying the following two properties.

(a) Closure property

(b) Associative property

is called a semigroup. It is denoted by  $(S, *)$ .

Example:

1. Let  $X$  be any non-empty set. Then the set of all functions from  $X$  to  $X$  is the set  $X^X$ , is a semigroup w.r.to  $*$ , the composition of functions.
2.  $(I, +)$ ,  $(I, \times)$  are semigroups, where  $+$  is the usual addition and  $\times$  is the usual multiplication.
3.  $(P(A), \cap)$  and  $(P(A), \cup)$  are semigroups. Where  $P(A)$  is the powerset of  $A$  (the set of all subsets of  $A$ ).
4.  $N = \{0, 1, 2, \dots\}$  then  $(N, +)$ ,  $(N, \times)$  are semigroups.  $N$  is not a semigroup w.r.to the operation subtraction.

## Solved Examples:

1. Show that the set of all natural numbers  $N$  is a semigroup w.r.to operation  $*$  defined by  $a * b = \max \{a, b\}$ .

### Solution:

$N$  is closed under the operation  $*$ .

For  $a, b, c \in N$

$$a * (b * c) = \max \{a, \max \{b, c\}\} = \max \{a, b, c\} \quad (1)$$

$$(a * b) * c = \max \{\max \{a, b\}, c\}$$

$$(a * b) * c = \max \{a, b, c\} \quad (2)$$

From (1) and (2),

$$(a * b) * c = a * (b * c), \forall a, b, c \in N$$

$\therefore *$  is associative.

$\therefore (N, *)$  is a semigroup.

2. Show that the set of rational numbers  $Q$  is a semigroup for the operation  $*$  defined by  $a * b = a + b - ab$ .

**Solution:**  $Q$  is closed for  $*$ .

$$\begin{aligned} a * (b * c) &= a * (b + c - bc) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + b + c - ab - bc - ca + abc \end{aligned} \quad (1)$$

$$\begin{aligned} (a * b) * c &= (a + b - ab) * c \\ &= a + b - ab + c - (a + b - ab)c \\ &= a + b + c - ab - ac - bc + abc \end{aligned} \quad (2)$$

From (1) and (2),

$$(a * b) * c = a * (b * c), \forall a, b, c \in Q$$

$\therefore *$  is associative.

$\therefore (Q, *)$  is a semigroup.

3. Show that the set of rational numbers  $Q$  is a semigroup for operation  $*$  defined by  $a * b = \frac{ab}{2} \forall a, b \in Q$

**Solution:**  $Q$  is closed for  $*$ .

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

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

$$(a * b) * c = a * (b * c), \forall a, b, c \in Q$$

$\therefore *$  is associative.

$\therefore (Q, *)$  is a semigroup.

4. Let  $(A, *)$  be a semigroup. Show that for  $a, b, c$  in  $A$  if  $a * c = c * a$  and then  $b * c = c * b$  then  $(a * b) * c = c * (a * b)$ .

<b>Solution:</b> L.H.S. $(a * b) * c = a * (b * c)$	$[\because * \text{ is associative}]$
$= a * (c * b)$	$[\because b * c = c * b]$
$= (a * c) * b$	$[\because * \text{ is associative}]$
$= (c * a) * b$	$[\because a * c = c * a]$
$= c * (a * b)$	$[\because * \text{ is associative}]$
$= \text{R.H.S.}$	

5. Let  $(S, *)$  be a commutative semigroup. If  $x * x = x, y * y = y$ , prove that  $(x * y) * (x * y) = x * y$ .

**Solution:** L.H.S.:  $(x * y) * (x * y)$

$$\begin{aligned}
 &= x * (y * (x * y)) \\
 &= x * ((y * x) * y) \\
 &= x * ((x * y) * y) \\
 &= x * (x * (y * y)) \\
 &= x * (x * y) \\
 &= (x * x) * y \\
 &= x * y \\
 &= \text{R.H.S.}
 \end{aligned}$$

6. Let  $(S, *)$  be a commutative semigroup. If  $x * x = x$ ,  $y * y = y$ , prove that  $(x * y) * (x * y) = x * y$ .

**Solution:** L.H.S.:  $(x * y) * (x * y)$   
 $= x * (y * (x * y))$   
 $= x * ((y * x) * y)$   
 $= x * ((x * y) * y)$   
 $= x * (x * (y * y))$   
 $= x * (x * y)$   
 $= (x * x) * y$   
 $= x * y$   
 $= \text{R.H.S.}$

7. Let  $\{\{x, y\}, \cdot\}$  be a semigroup where  $x \cdot x = y$ . Show that

(i)  $x \cdot y = y \cdot x$

(ii)  $y \cdot y = y$ .

**Solution:** (i)  $x \cdot (x \cdot x) = (x \cdot x) \cdot x$  (Since  $\cdot$  is associative)

Given  $x \cdot x = y$

$\therefore x \cdot y = y \cdot x$

(ii) To prove:  $y \cdot y = y$

Since the set  $\{x, y\}$  is closed for operation ' $\cdot$ ',

$x \cdot y = x$  (or)  $x \cdot y = y$

Assume  $x \cdot y = x$

$y \cdot y = y \cdot (x \cdot x)$

$= (y \cdot x) \cdot x$

$= (x \cdot y) \cdot x$

$\therefore y \cdot y = y$

Next consider the case  $x \cdot y = y$ ,

$y \cdot y = (x \cdot x) \cdot y$

$= x \cdot (x \cdot y)$

$\therefore y \cdot y = y$

8. Let  $(A, *)$  be a semi group. Further more for every  $a, b \in A$ , if  $a \neq b$  then

$$a * b \neq b * a$$

- (i) Show that for every  $a \in A$ ,  $a * a = a$
- (ii) For every  $a \in A$ ,  $a * (b * a) = a$ .
- (iii) For every  $a, b, c \in A$ ,  $(a * b) * c = a * c$ .

**Solution:**

$$(i) \quad a * (b * c) = (a * b) * c$$

Put  $b = a$  and  $c = a$

$$a * (a * a) = (a * a) * a$$

Since  $(A, *)$  is not commutative,  $a * a = a$ .

(ii) Let us assume that  $b \in A$  then

we have for  $b \in A$ ,  $b * b = b$ .

$$\text{Let } a * (b * b) = a * b \quad [\because b * b = b]$$

$$(a * b) * b = a * b \quad [\because \text{associative}]$$

$$\text{Hence } a * b = a \underline{\hspace{2cm}} (1) \quad (\text{Using Right Cancellation law})$$

$$\therefore a * (b * a) = (a * b) * a \quad \text{From } [\because \text{associative}]$$

$$= a * a$$

$$= a$$

$$(iii) \quad (a * b) * c = a * c \quad [\because a * b = a]$$

X.....X

# Monoids

## 1) Define Monoid with Example:

A semigroup  $(S, *)$  with an identity element w.r.t.  $'*'$  is called Monoid.

It is denoted by  $(M, *)$ .

In other words, a non-empty set 'M' with respect to  $*$  is said to be a monoid, if  $*$  satisfies the following properties.

- (a) Closure property
- (b) Associative property
- (c) Identity property

### Examples:

1.  $N = \{0, 1, 2, \dots\}$  then  $(N, +)$ ,  $(N, \times)$  are monoids.
2.  $(Z, \times)$ ,  $(Z, +)$  are monoids.
3. The set of even integers  $E = \{\dots, -4, -2, 0, 2, 4, \dots\}$ , Then  $(E, +)$  is a monoid and  $(E, \times)$  is a semigroup but not a monoid.
4.  $(P(A), \cup)$  is a monoid with identity element  $\emptyset$ .  
 $(P(A), \cap)$  is a monoid with identity element  $A$ , where  $A$  is any set.

### Problem:

2) Show that the set of integers, is a monoid for the operation  $*$  defined by  $a*b = a + b - ab$ , for  $a, b \in I$ .

### Solution:

$I$  is closed for the operation  $*$ .

Further  $*$  is associative.

The element  $0 \in I$  is the identity Element

Since  $x * 0 = x + 0 - x \cdot 0 = x$  and  $0 * x = 0 + x - 0 \cdot x = x, \forall x \in I$ .

$\therefore (I, *)$  is a monoid with identity  $0 \in I$ .

X.....X



## Topic 2: GROUPS

### 1) Define Group with Example :

A non-empty set  $G$  with binary operation  $*$  is called a group if the following axioms are satisfied.

1.  $*$  is associative, i.e.  $(a*b)*c = a*b*c \forall a, b, c \in G$ .
2. There exists an element  $e \in G$  such that  $a*e = e*a = a, \forall a \in G$ .  
( $e$  is the identity element).
3. For every  $a \in G, \exists$  an element  $a^{-1} \in G$ , such that  $a*a^{-1} = a^{-1}*a = e$ .  
( $a^{-1}$  is called the inverse element of  $a$ ).

### 2) Define Abelian Group (or) Commutative Group

A group  $(G,*)$  is called abelian if  $a*b=b*a, \forall a, b \in G$ . i.e.  $*$  is commutative in  $G$ .

Example:

1.  $(\mathbb{I}, +)$  is a group called the additive group of integers.
2.  $M_2(\mathbb{R})$ , the set of all  $2 \times 2$  matrices is a group w.r.to matrix addition.
3. The set of all non-singular  $2 \times 2$  matrices is a group w.r.to matrix multiplication.
4. The set of  $n^{\text{th}}$  roots of unity  $\{1, w, w^2, \dots, w^{n-1}\}$  is a group w.r.to the operation multiplication of complex numbers.
5.  $G = \{1, -1, i, -i\}$ . In  $G$ , the operation  $\cdot$  is defined by the following table.  
Then  $(G, \cdot)$  is an abelian group.

$\cdot$	<b>1</b>	<b>-1</b>	<b>i</b>	<b>-i</b>
<b>1</b>	1	-1	i	-i
<b>-1</b>	-1	1	-i	i
<b>i</b>	i	-i	-1	1
<b>-i</b>	-i	i	1	-1

Here  $\cdot$  is the multiplication of complex numbers.

### Examples :

1. Show that  $[Z_5, +_5]$  is an abelian group.

**Solution:** The table for addition modulo 5 is.

$+_5$	[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]

- (i) Closure property:  
 $[a] +_5 [b]$  = remainder when the sum is divided by 5.
- (ii) Associative Property:  
From the table for  $[a], [b], [c] \in Z_5$   
 $[a] +_5 ([b] +_5 [c]) = ([a] +_5 [b]) +_5 [c]$
- (iii ) Identity:  
 $[0] \in Z_5$  is the identity
- (iv ) Inverse:  
The inverse of  $[1]$  is  $[4]$ .  
The inverse of  $[2]$  is  $[3]$ .  
The inverse of  $[3]$  is  $[2]$ .  
The inverse of  $[4]$  is  $[1]$ .  
The element  $[0] \in Z_5$  has self-inverse.
- (v ) Commutative property:  
Further  $[a] +_5 [b] = [b] +_5 [a], \forall [a], [b] \in Z_5$ .

$\therefore (Z_5, +_5)$  is an abelian group.

2. Show that  $[\{1,2, 3, 4\}, x_5]$  is an abelian group.

**Solution:** The table for the  $x_5$  is as follows

$Z_5 = \{1,2,3,4\}$  and  $x_5$  is multiplication operation

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(i) Closure Property:

Here  $a \in Z_5$  means  $a = [a]$

$a \times_5 b = \text{remainder when } ab \text{ is divisible by } 5.$

(ii) Associative Property:

For  $a, b, c \in Z_5.$

$$a \times_5 (b \times_5 c) = (a \times_5 b) \times_5 c$$

(iii) Identity:

$1 \in Z_5;$  is the identity element.

(iv) Inverse:

The inverse of 1 is 1

The inverse of 2 is 3

The inverse of 3 is 2

The inverse of 4 is 4

(v) Commutative property:

Further  $a \times_5 b = b \times_5 a, \forall a, b \in Z_5.$

$\therefore [\{1,2, 3, 4\}, x_5]$  is an abelian group.

X.....X

### Topic :3 Properties of Group

#### Property 1:

The identity element in a group is unique.

**Proof:** If  $(G, *)$  be a group and  $e_1$  and  $e_2$  be two identity elements of  $G$ .

Let  $x \in G$ ;  $x * e_1 = x$  and  $x * e_2 = x$

$\therefore x * e_1 = x * e_2$ ,

By using left cancellation law, we get  $e_1 = e_2$

$\therefore$  Identity element is unique

#### Property 2:

The inverse of every element in a group is unique.

**Proof:** Let  $(G, *)$  be a group, with identity element  $e$ .

Let  $b$  and  $c$  be inverses of a element  $a \in G$ .

$$a * b = b * a = e$$

$$a * c = c * a = e$$

$$b = b * e$$

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

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

$$= e * c$$

$$b = c$$

#### Property 3:

If  $a$  is an element in a group  $(G, *)$  then  $(a^{-1})^{-1} = a$ .

#### Property 4:( Reversal law)

If  $a$  and  $b$  are two elements in a group  $(G, *)$  then

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

[ prove  $(a * b) * (b^{-1} * a^{-1}) = e$  and  $(b^{-1} * a^{-1}) * (a * b) = e$ ]

### Property 5: Cancellation laws

In a group  $(G, *)$ , for every  $a, b, c \in G$ , then

(i)  $a * c = b * c$  implies  $a = b$  (Right Cancellation law)

(ii)  $c * a = c * b$  implies  $a = b$  (Left Cancellation law)

### Property 6:

In a group  $(G, *)$ , the equations  $x * a = b$  and  $a * y = b$  has unique solution.

#### Proof:

Consider  $x * a = b$  Post

multiplying by  $a^{-1}$

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

$$\text{i.e. } x * e = b * a^{-1}$$

$$\therefore x = b * a^{-1}$$

#### Proof of Uniqueness

Let  $x_1$  and  $x_2$  be two solutions of  $x * a = b$ .

Then  $x_1 * a = b$  and  $x_2 * a = b$ .

$$\therefore x_1 * a = x_2 * a$$

$$\Rightarrow x_1 = x_2 \quad [\text{By Right cancellation law}]$$

$\therefore$  The solution is unique.

In a similar manner, the equation  $a * y = b$  has a solution  $y = a^{-1} * b$  and it has unique solution.

### Examples

1. Show that a group  $(G, *)$  is abelian iff  $(a * b)^2 = a^2 * b^2$

**Solution:** First we assume that  $(G, *)$  is abelian,

$$(a * b)^2 = (a * b) * (a * b)$$

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

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

Since  $G$  is abelian,  $a * b = b * a$ .

$$\begin{aligned}\therefore (a * b)^2 &= a * ((a * b) * b) \\ &= (a * a) * (b * b) \\ &= a^2 * b^2\end{aligned}$$

**Conversely,**

we assume that  $(a * b)^2 = a^2 * b^2$ .

To prove :  $G$  is abelian

$$\begin{aligned}(a * b)^2 &= a^2 * b^2 \\ (a * b) * (a * b) &= (a * a) * (b * b) \\ a * (b * (a * b)) &= a * (a * (b * b)) \\ b * (a * b) &= a * (b * b) && \text{[by Left cancellation law]} \\ (b * a) * b &= (a * b) * b \\ b * a &= a * b && \text{[by Right cancellation law]} \\ \therefore a * b &= b * a, \forall a, b \in G \\ \therefore G &\text{ is abelian.}\end{aligned}$$

**2.** Show that  $(G, *)$  is abelian iff  $(a * b)^{-1} = a^{-1} * b^{-1}$ .

**Solution:** Assume that  $G$  is Abelian.

$$\begin{aligned}\therefore (a * b) &= (b * a), \forall a, b \in G \\ (a * b)^{-1} &= (b * a)^{-1} \\ &= a^{-1} * b^{-1}\end{aligned}$$

**Conversely**

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

But  $a^{-1} * b^{-1} = (b * a)^{-1}$  (By Reversal law)

$$\therefore (a * b)^{-1} = (b * a)^{-1} \quad \text{From given}$$

Taking inverses both sides,

$$\begin{aligned}((a * b)^{-1})^{-1} &= ((b * a)^{-1})^{-1} \\ \Rightarrow a * b &= b * a, \forall a, b \in G \\ \therefore (G, *) &\text{ is abelian}\end{aligned}$$

3. Show that if every element in a group is its own inverse, then the group is abelian.

**Solution:** Let  $G$  be a group such that every element in  $G$  is its own inverse.

$$\therefore \text{For } a \in G, a^{-1}=a$$

Let  $a, b \in G$ , then  $(a * b) \in G$  and so

$$(a * b)^{-1} = a * b \quad (1)$$

$$\text{But } (a * b)^{-1} = b^{-1} * a^{-1}$$

$$\text{Since } b^{-1} = b, a^{-1} = a.$$

$$\Rightarrow (a * b)^{-1} = b * a \quad (2)$$

From (1) and (2) we have  $a * b = b * a \forall a, b \in G$

$\therefore G$  is abelian.

4. Prove that if for every element  $a$  in a group  $(G, *)$ ,  $a^2 = e$  then  $G$  is an abelian group.

**Solution:** Let  $a, b \in G$

$$\text{Then } (a * b) \in G \text{ and so } (a * b)^2 = e \text{ (1)}$$

$$\text{Since } a \in G, a^2=e \Rightarrow a * a = e$$

$$b \in G, b^2=e \Rightarrow b * b = e$$

$$\text{From (1)} \quad (a * b)^2 = e$$

$$\Rightarrow (a * b) * (a * b) = e * e$$

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

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

$$b * (a * b) = a * (b * b) \quad [\text{by Left cancellation law}]$$

$$\text{i.e. } (b * a) * b = (a * b) * b$$

$$\therefore b * a = a * b \quad [\text{by Right cancellation law}]$$

$\therefore G$  is abelian.

X.....X

## Topic 4: Symmetric Groups ( $S_n$ )

### 1) Define Permutation with Example:

A permutation of a set  $A$  is a one-to-one and onto function from set  $A$  to itself.

#### Example.:

If  $A = \{1, 2, 3, 4, 5\}$ , then a permutation is function  $\sigma$  where:  $\sigma(1)=4$ ,  $\sigma(2)=2$ ,  $\sigma(3)=5$ ,  $\sigma(4)=3$ ,  $\sigma(5)=1$ . This can be represented with permutation notation

$$\text{as: } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

### 2) Define Symmetric Set:

If  $S$  is a finite set having  $n$  distinct elements then we shall have  $n!$  distinct permutations of the sets. The set of all distinct permutations of degree  $n$  defined on the set  $S$  is denoted by  $S_n$  called symmetric set of permutations of degree  $n$ .

**Note:**  $O(S_n) = n!$ .

### Problems:

1. List all elements of the symmetric set  $S_3$ , where  $S = \{1, 2, 3\}$  and prove that  $(S_3, \circ)$  is a non abelian group.

**Solution:** Given  $S = \{1, 2, 3\}$ .

Total number of permutation on  $S = 3! = 6$ .

Elements of symmetrical set  $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$

where

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

The operation ' $\circ$ ' product of permutations defined on the set  $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$  is given in the table.



$\circ$	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$
$P_1$	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$
$P_2$	$P_2$	$P_1$	$P_4$	$P_3$	$P_6$	$P_5$
$P_3$	$P_3$	$P_5$	$P_1$	$P_6$	$P_4$	$P_2$
$P_4$	$P_4$	$P_6$	$P_2$	$P_5$	$P_1$	$P_3$
$P_5$	$P_5$	$P_3$	$P_6$	$P_1$	$P_4$	$P_2$
$P_6$	$P_6$	$P_4$	$P_5$	$P_2$	$P_3$	$P_1$

To prove:  $(S_3, \circ)$  is a non abelian group.

(i) Closure: Since the body of the table contains only the elements of  $S_3$ .

$\therefore (S_3, \circ)$  is closed.

(ii) Associativity: We know composition of function  $S_3$  is associative and so it is true in  $S_3$  also.  $(S_3, \circ)$  is associative.

$$P_1 \circ (P_3 \circ P_4) = P_1 \circ P_6 = P_6.$$

$$(P_1 \circ P_3) \circ P_4 = P_3 \circ P_4 = P_6.$$

$$\therefore P_1 \circ (P_3 \circ P_4) = (P_1 \circ P_3) \circ P_4.$$

(iii) Identity:  $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$  is the identity element of  $S_3$ .

(iv) Inverse: From the above table

$$P_1^{-1} = P_1; P_2^{-1} = P_2; P_3^{-1} = P_3; P_4^{-1} = P_5; P_5^{-1} = P_4; P_6^{-1} = P_6. \text{ Thus inverse exists}$$

for every element. Hence inverse axiom is verified.

$\therefore (S_3, \circ)$  is a group.

(v) Commutative: From the table;  $P_3 \circ P_4 = P_6$  and  $P_4 \circ P_3 = P_2$ .

$\therefore P_3 \circ P_4 \neq P_4 \circ P_3$ . Hence  $(S_3, \circ)$  is not commutative.

X.....X

## Topic 5: SUBGROUP

### 1) Define SUBGROUP with Example:

**Definition:** Let  $G, *$  be a group. Let  $e$  be the identity element in  $G$  and let  $H \subseteq G$ . If  $H$  itself is a group with the same operation  $*$  and the same identity element  $e$ .  
(or)

Let  $G, *$  be a group and  $H \subseteq G$ .  $H, *$  is called a subgroup of  $G, *$ , if  $H$  itself is a group with respect to  $*$ .

**Example:**  $(Q, +)$  is a subgroup of  $(R, +)$ .

### 2) Define TRIVIAL SUBGROUP OR IMPROPER SUBGROUP

**Solution:** For any group  $G, *$ ,  $\{e, *\}$  and  $G, *$  are subgroups, called trivial subgroups.

### 3) Define NON TRIVIAL SUBGROUP OR PROPER SUBGROUP

**Solution:** All other subgroups other than  $\{e, *\}$  and  $(G, *)$  are called non trivial subgroup.

### 4) What is the CONDITION FOR A NON-EMPTY SUBSET H to be subgroup of G

$H, *$  is said to be a subgroup of  $G, *$  if

(i).  $H$  is closed for the operation  $*$ ,  $\forall a, b \in H, a * b \in H$ .

(ii).  $H$  contains the identity element  $e$   
(i.e)  $e \in H$  where  $e$  is the identity of  $G$ .

(iii). For any  $a \in H, a^{-1} \in H$ .

## Topic 6 : Theorems on Subgroups

### 1) Theorem 1: State and Prove NECESSARY AND SUFFICIENT CONDITION For a subgroup :

**Statement:** A non-empty subset  $H$  of a group  $G$ ,  $*$  is a subgroup of  $G$  if and only if  $a * b^{-1} \in H$  for all  $a, b \in H$ .

#### **PROOF: Necessary Condition:**

Let  $H$  be a subgroup of a group  $G$  and  $a, b \in H$ .

To prove:  $a * b^{-1} \in H$ .

Since  $H$  is a subgroup and  $b \in H$ ,  $b^{-1}$  must exist and  $b^{-1} \in H$ .

Now,  $a \in H, b^{-1} \in H \Rightarrow a * b^{-1} \in H$ . [By closure property]

#### **Sufficient Condition:**

Assume  $a \in H, b \in H \Rightarrow a * b^{-1} \in H$ .

To prove:  $H$  be a subgroup of a group  $G$ .

#### (i). **IDENTITY:**

Now,  $a \in H, a^{-1} \in H \Rightarrow a * a^{-1} \in H \Rightarrow e \in H$ .

Hence the identity element,  $e \in H$ .

#### (ii). **INVERSE:**

$e \in H, a \in H \Rightarrow e * a^{-1} \in H \Rightarrow a^{-1} \in H$ .

$\Rightarrow$  Every element ' $a$ ' of  $H$  has its inverse  $a^{-1}$  is in  $H$ .

#### (iii). **CLOSURE:**

If  $b \in H$  then  $b^{-1} \in H$ .  $a \in H, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$ .

#### (iv). **ASSOCIATIVE:**

Now  $H \subseteq G$  and the associative law hold good for  $G$ , as  $G$  is a group.

Hence it is true for the element of  $H$ .

Thus all axioms for a group are satisfied for  $H$ .

Hence  $H$  is subgroup of  $G$ .

**2) Prove:** The intersection of two subgroups of a group  $G, *$  is also a subgroup of  $(G, *)$  & The Union need not be a Subgroup .

**PROOF:**

Let  $H$  and  $K$  are subgroups of  $(G, *)$

To prove that:  $H \cap K$  is subgroup of  $(G, *)$ .

We have  $H \cap K \neq \emptyset$ . [ $\because$  atleast identity element is common to both  $H$  and  $K$ ].

Let  $a, b \in H \cap K \Rightarrow a \in H \cap K$  and  $b \in H \cap K$

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

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

Now,  $a \in H, b \in H \Rightarrow a * b^{-1} \in H$  [ $H$  is a subgroup , Theorem 1],

$a \in K, b \in K \Rightarrow a * b^{-1} \in K$  [ $K$  is a subgroup , Theorem 1].

Therefore,  $a * b^{-1} \in H \cap K$ .

Thus  $a \in H \cap K$  and  $b \in H \cap K \Rightarrow a * b^{-1} \in H \cap K$ .

$H \cap K$  is a subgroup of  $G$ . [By Theorem 1]

**ALSO,** The union of two subgroups need not be a subgroup.

**Example:**

Let  $(\mathbb{Z}, +)$  is a group.

Let  $H$  and  $K$  are subgroup of  $(\mathbb{Z}, +)$

where  $H = \{ \dots -4, -2, 0, 2, 4, 6 \dots \} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$

$K = \{ \dots -6, -3, 0, 3, 6, 9 \dots \} = \{0, \pm 3, \pm 6, \pm 9, \dots\}$

$H \cup K = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \dots\}$

$3, 8 \in H \cup K$  but  $3 + 8 = 11 \notin H \cup K$ .

Therefore,  $H \cup K$  is not closed with respect to addition.

Therefore,  $H \cup K$  is not a subgroup of  $G$ .

**3) Prove:** The union of two subgroups of a group  $G$  iff one is contained in the other.

**PROOF:**

Assume  $H$  and  $K$  are subgroups of  $G$  and  $H \subseteq K$  or  $K \subseteq H$ .

To prove that.  $H \cup K$  is a subgroup.

$\because H$  and  $K$  are subgroups and  $H \subseteq K \Rightarrow H \cup K = K$ .

(or)  $H$  and  $K$  are subgroups and  $K \subseteq H \Rightarrow H \cup K = H$ .

Therefore,  $H \cup K$  is a subgroup.

**Conversely,**

Suppose  $H \cup K$  is a subgroup.

To prove that, one is contained in the other (i.e)  $H \subseteq K$  or  $K \subseteq H$ .

Suppose,  $H \not\subseteq K$  or  $K \not\subseteq H$ .

Then,  $\exists$  elements  $a$ , such that  $a \in H$  and  $a \notin K$  -----(1)

$b \in K$  and  $b \notin H$  -----(2)

Clearly,  $a, b \in H \cup K$ .

Since,  $H \cup K$  is a subgroup of  $G$ ,  $ab \in H \cup K$ .

Hence,  $ab \in H$  or  $ab \in K$ .

**Case 1:** Let  $ab \in H$ .  $\because a \in H, a^{-1} \in H$ .

Hence,  $a^{-1}ab = b \in H$ , which is a contradiction (2).

**Case 2:** Let  $ab \in K$ .  $\because b \in K, b^{-1} \in K$ .

Hence,  $b^{-1}ab = a \in K$ , which is a contradiction (1).

Therefore, Our assumption is wrong.

Thus,  $H \subseteq K$  or  $K \subseteq H$ .

## PROBLEMS:

1. Find all the non-trivial subgroup of  $(Z_6, +_6)$ .

**Solution:**  $Z_6 = \{0, 1, 2, 3, 4, 5\}$  of  $H$  is a subgroup of  $Z_6$

Hence,  $O(H) = 1, 2, 3$ , or  $6$ .

Subgroups are

$$\Rightarrow H = [0]$$

$$\Rightarrow H = [0], [3]$$

$$\Rightarrow H = [0], [2], [4]$$

$+_6$	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	3
5	5	0	1	2	3	4

2. Find all the subgroups of  $(Z_9, +_9)$ .

**Solution:**

$$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

Here,  $O(H) = 1, 3$ .

Subgroups are

$$\Rightarrow H = \{0\}$$

$$\Rightarrow H = \{0, 3, 6\}$$

$+_9$	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

$\times_9$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

- 3.. Check whether  $H_1 = \{0, 5, 10\}$  and  $H_2 = \{0, 4, 8, 12\}$  are subgroups of  $Z_{15}$  with respect to  $+_{15}$ .

**Solution:**  $H_1 = \{0, 5, 10\}$

$$H_1 = \{0, 5, 10\}$$

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

$$(H_1, +_{15})$$

$$H_2 = \{ 0, 4, 8, 12 \}$$

$+_{15}$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

$$(H_2, +_{15})$$

Table 1:  
 $(H_1, +_{15})$ : All the entries in the addition table for  $H_1$  are the elements of  $H_1$ .  
 Therefore,  $H_1$  is a subgroup of  $Z_{15}$ .

Table 2:  
 $(H_2, +_{15})$ : All the entries in the addition table for  $H_2$  are not the elements of  $H_2$ .  
 Therefore,  $H_2$  is a subgroup of  $Z_{15}$ .

X.....X

## Topic 7: NORMAL SUBGROUPS

### 1) Define NORMAL SUBGROUPS with Example.

**Definition:** A subgroup  $(H, *)$  of  $(G, *)$  is called normal subgroup of  $G$

if  $aH = Ha, \forall a \in G$ .

### 2) Theorem: Every subgroup of an abelian group is normal

**Proof:** Let  $(G, *)$  be a abelian group and  $(H, *)$  be a subgroup of  $G$ .

Let  $a \in G$  be any element.

Then  $aH = \{a * h / h \in H\}$

$$= \{h * a / h \in H\} \quad (\text{since } G \text{ is abelian}) = Ha$$

Since  $a$  is arbitrary,  $aH = Ha \forall a \in G$

Therefore  $H$  is a normal subgroup of  $G$ .

### 3) Theorem: $(N, *)$ is a normal subgroup of $(G, *)$ iff $a * n * a^{-1} \in N$

$\forall n \in N$  and  $\forall a \in G$ .

**Proof:** Let  $(N, *)$  is a normal subgroup of  $(G, *)$ . Therefore  $aN = Na \quad \forall a \in G$

$$\Rightarrow a * N * a^{-1} = N * a * a^{-1} = N * e = N$$

Therefore for any  $n \in N, a * N * a^{-1} \in N$

Conversely, if  $a * N * a^{-1} \in N, n \in N, \forall a \in G$ ,

To prove  $a * N = N * a$

Let  $x \in a * N \Rightarrow x = a * n$  for some  $n \in N$

$$x = a * n * e \Rightarrow x = a * n * (a^{-1} * a)$$



$$\Rightarrow x = a * n * a^{-1} * a \in N * a$$

$$\Rightarrow a * N \subseteq N * a \dots\dots\dots(1)$$

Let  $y \in N * a \Rightarrow y = n * a$  for some  $n \in N$

$$\text{Then } y = a * a^{-1} * n * a = a * (a^{-1} * n * a^{-1}^{-1}) \in a * N$$

$$\text{Therefore } y \in N * a \Rightarrow y \in a * N \text{ therefore } N * a \subseteq a * N \dots\dots\dots(2)$$

Therefore from (1) and (2) we get  $a * N = N * a, \forall a \in G$ .

Hence  $N$  is a normal subgroup of  $G$ .

**4)Theorem:** prove that intersection of two normal subgroup of  $(G, *)$  is a normal subgroup of  $(G, *)$ .

**Proof:** Let  $(N_1, *)$  and  $(N_2, *)$  be two normal subgroups of  $(G, *)$ .

To Prove  $(N_1 \cap N_2, *)$  is a normal subgroup of  $(G, *)$ .

$$a * n * a^{-1} \in N_1 \cap N_2 \text{ (by previous theorem)}$$

Since  $N_1$  and  $N_2$  are normal subgroup of  $G$ , they are basically subgroups.

We know  $N_1 \cap N_2$  is a subgroup of  $G$ .

Now we shall prove it is a normal subgroup of  $G$ .

Let  $n \in N_1 \cap N_2$  be any element and  $a \in G$  be any element

Then  $n \in N_1$  and  $n \in N_2$ , Since  $N_1$  and  $N_2$  are normal,  $a * n * a^{-1} \in N_1$  and

$a * n * a^{-1} \in N_2$ , Therefore  $a * n * a^{-1} \in N_1 \cap N_2$ .

Hence  $N_1 \cap N_2$  is normal.

x.....x

## Topic 8: Group Homomorphism:

### 1) Define **Group Homomorphism**.

Let  $G, *$  and  $G_1, \circ$  be two groups. A mapping  $g: G \rightarrow G_1$  is called group homomorphism if  $g(a * b) = g(a) \circ g(b)$  for all  $a, b \in G$ .

### 2) Properties of group homomorphism:

A group homomorphism preserves identities, inverses and sub groups.

**Theorem 1:** Homomorphism preserves identities.

(or)

If  $f(e) = e_1$  where  $e$  and  $e_1$  are the identity elements of  $G$  and  $G_1$  respectively.

**Proof:** Let  $a \in G$ , If  $e$  is the identity element  $G$ ,

then  $a * e = e * a = a$

$$\Rightarrow f(a * e) = f(a)$$

$$\Rightarrow f(a) \circ f(e) = f(a) \quad \because f \text{ is homomorphism}$$

$$\Rightarrow f(e) = e_1$$

$\therefore f$  preserves identities.

**Theorem 2:** Homomorphism preserves inverse (or)  $f(a^{-1}) = [f(a)]^{-1}$

**Proof:**

Let  $a \in G, a^{-1} \in G \Rightarrow a * a^{-1} = a^{-1} * a = e$

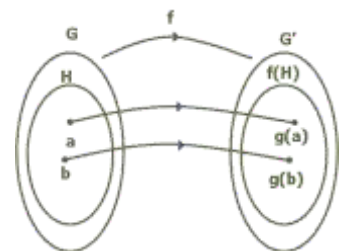
Since  $a * a^{-1} = e$

$$\Rightarrow f(a * a^{-1}) = f(e)$$

$$\Rightarrow f(a) \circ f(a^{-1}) = f(e_1) \quad \because f \text{ is homomorphism}$$

$$\therefore f(a^{-1}) = [f(a)]^{-1}.$$

$\therefore f$  preserves inverse



**Theorem 3:** Homomorphism preserves subgroup  
(or)

If  $H$  is a subgroup of  $G$ , then  $f(H)$  is a subgroup of  $G_1$ .

**Proof:**

Let  $H$  be a subgroup of  $G \Rightarrow$  for  $a, b \in H, a * b^{-1} \in H$  [ $\because H$  is a subgroup]

Let  $f(a) \in f(H)$  and  $f(b) \in f(H)$ .

To prove  $f(a) \circ f(b^{-1}) \in f(H)$

Consider  $f(a) \circ f(b^{-1}) = f(a * b^{-1}) \in f(H)$  [ $\because a * b^{-1} \in H$ ]

$\Rightarrow f(a) \circ f(b^{-1}) \in f(H) \quad \forall f(a) \in f(H) \text{ and } f(b) \in f(H)$ .

$\therefore f(H) \subseteq G_1$  is a subgroup of  $G_1$ .

**Theorem 4:** Let  $f: G \rightarrow G'$  be a group homomorphism and  $H$  is a subgroup of  $G'$ .  
Then  $f^{-1}(H)$  is a subgroup of  $G$ .

**Proof:**

Clearly  $f^{-1}(H)$  is a non empty subset of  $G$  [ $\because H$  is a subgroup of  $G'$ .]

Now let us consider  $a = f^{-1}(c) \in f^{-1}(H)$  and  $b = f^{-1}(d) \in f^{-1}(H)$ .

For  $c, d \in H$  with  $f(a) = c$  and  $f(b) = d$ .

Let  $a, b \in f^{-1}(H) \Rightarrow f(a), f(b) \in H$  [ $\because H$  is a subgroup.]

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

$\Rightarrow f(a * b^{-1}) \in H$  [ $\because f$  is homomorphism.]

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

$\therefore a, b \in f^{-1}(H) \Rightarrow a * b^{-1} \in f^{-1}(H)$

Hence  $f^{-1}(H)$  is a subgroup of  $G$ .

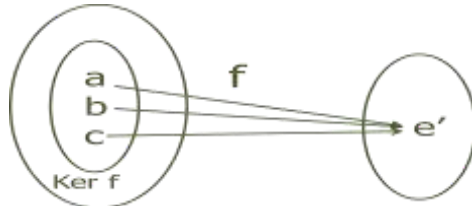
X.....X

## Topic 9: KERNEL OF A HOMOMORPHISM:

1) Define **KERNEL OF A HOMOMORPHISM** with Example:

Let  $f: G \rightarrow G'$  be a group homomorphism. The set of elements of  $G$  which are mapped into  $e'$  (identity element in  $G'$ ) is called the kernel of  $f$  and it is denoted by  $\ker f$ .

$\ker f = \{x \in G / f(x) = e'\}$ ,  $e'$  is identity of  $G'$ .



then  $\ker f = \{a, b, c\}$

**Example:** 1.  $f: (Z, +) \rightarrow (Z, +)$  defined by  $f(x) = 2x$  then  $\ker f = \{0\}$   
2.  $f: (R^*, \cdot) \rightarrow (R^+, \cdot)$  defined by  $f(x) = |x|$ , then  $\ker f = \{1, -1\}$ .

2) If  $f: G \rightarrow G'$  is a homomorphism then  $\ker f = \{e\}$  iff  $f$  is 1-1.

**Proof:**

Assume  $f$  is one to one Then

$$f(e) = e'$$

$$\therefore \ker f = \{e\}$$

Conversely,

Assume  $\ker f = \{e\}$

Now  $f(x) = f(y)$

$$\Rightarrow f(x) * f(y^{-1}) = f(y) * f(y^{-1})$$

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

$$\Rightarrow xy^{-1} \in \ker f$$

$$\Rightarrow xy^{-1} = e$$

$$\Rightarrow x = y$$

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

Hence  $f$  is one to one.

3) Prove that Kernel of a homomorphism is a normal subgroup of  $G$ .

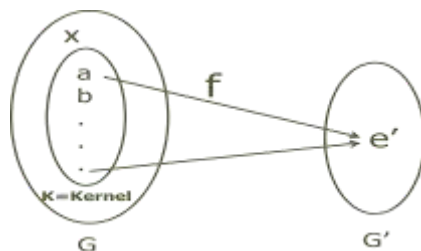
**Proof:**

Let  $(G, *)$  and  $(G', \cdot)$  be the groups and  $f: G \rightarrow G'$  is a group homomorphism.

By the definition of homomorphism,  $f(a * b) = f(a) \cdot f(b) \forall a, b \in G$ .

By the definition of kernel,  $K = \{a \in G / f(a) = e'\}$

i.e.,  $f(a) = e' \forall a \in K$  and  $e'$  is the identity element of  $H$ .



To prove that 'K' is a normal subgroup of G.

i.e., To prove

- i) K is nonempty
- ii)  $a * b^{-1} \in K, \forall a, b \in K$
- iii)  $x * h * x^{-1} \in K, \forall h \in K, x \in G$

i) Identity element 'e' of G is mapped to identity element of  $e'$  of  $G'$ .

i.e.,  $f(e) = e'$

$\therefore e \in K \Rightarrow K$  is non-empty.

ii) Let  $a, b \in K \subseteq G$

$\Rightarrow f(a) = f(b) = e'$

$f(a * b^{-1}) = f(a) \cdot f(b^{-1}) \{ \because f \text{ is homomorphism} \}$

$= e' \cdot (e')^{-1}$

$= e' \cdot e' = e'$

$\therefore a * b^{-1} \in K$ .

Hence  $K = \ker f$  is a subgroup

iii) Let  $x \in G$  and  $h \in K$  be any element.

$\Rightarrow f(h) = e'$

$f(x * h * x^{-1}) = f(x) \cdot f(h) \cdot f(x^{-1})$

$= f(x) \cdot e' \cdot f(x^{-1}) = f(x) \cdot f(x^{-1}) = e'$

$\therefore x * h * x^{-1} \in K$

Hence  $K = \ker f$  is a normal subgroup of G.

X.....X

## Topic : 10 Fundamental Theorem Of Group Homomorphism

State and prove the Fundamental Theorem Of Group Homomorphism.

**Statement:** Let  $(G, *)$  and  $(G', \cdot)$  be two groups.

Let  $f: G \rightarrow G'$  be a homomorphism of groups with kernel  $K$ ,  
then  $G/K$  is isomorphic to  $(G)$ .

i.e.,  $G/K \cong G'$

**Proof:** Given that  $f: G \rightarrow G'$  be a homomorphism of groups with kernel  $K$ .

Define the map  $\phi (K * a) = f(a)$  ,  $\forall a \in G$

i)  $\phi$  is well defined:

Let  $a, b \in G$  such that

$$K * a = K * b$$

$$\Rightarrow a * b^{-1} \in K \quad \text{-----} \rightarrow (1)$$

$$\Rightarrow f(a * b^{-1}) = e' \quad \{\because K \text{ is kernel}\}$$

$$\Rightarrow f(a) * f(b^{-1}) = e' \quad \{\because f \text{ is homomorphism}\}$$

$$\Rightarrow f(a) * f(b)^{-1} * f(b) = e' * f(b)$$

$$\Rightarrow f(a) = f(b)$$

$$\Rightarrow \phi(K * a) = \phi(K * b)$$

$\therefore \phi$  is well defined.

ii)  $\phi$  is one to one:

To prove that  $\phi(K * a) = \phi(K * b) \Rightarrow K * a = K * b$

We know that  $\phi(K * a) = \phi(K * b) \Rightarrow f(a) = f(b)$

$$\Rightarrow f(a) * f(b^{-1}) = f(b) * f(b^{-1})$$

$$= f(b * b^{-1})$$

$$= f(e)$$

$$\Rightarrow f(a) * f(b^{-1}) = e'$$

$$\Rightarrow f(a * b^{-1}) = e'$$

$$\Rightarrow a * b^{-1} \in K$$

$$\Rightarrow K * a = K * b$$

$\therefore \phi$  is one to one.

iii)  $\phi$  is onto:

Let  $y \in G'$

Since  $f$  is onto, there exists  $a \in G$  such that  $f(a) = y$

$$\Rightarrow \phi(K * a) = y \quad \{ \because f(a) = \phi(K * a) \}$$

Thus every element of  $G'$  has preimage in  $G/K$

$\therefore \phi$  is onto.

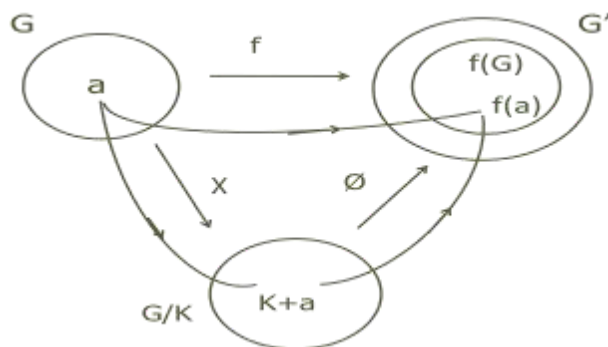
i)  $\phi$  is a homomorphism:

$$\begin{aligned} \phi(K * a * K * b) &= \phi(K * a * b) \\ &= f(a * b) \\ &= f(a) * f(b) \\ &= \phi(K * a) * \phi(K * b) \end{aligned}$$

$\therefore \phi$  is a homomorphism.

Since  $\phi$  is one to one, onto and homomorphism,  $\phi$  is isomorphism between  $G/K$  and  $G'$ .

$$\therefore G/K \cong G'$$



2) **State and prove the Cayley's representation theorem.**

(or)

**Prove that every finite group of order 'n' is isomorphic to a permutation group of order 'n'.**

**Proof:**

To prove the theorem, we have to show the following.

- To form a set  $G$  of permutation
- To prove  $G'$  is a group
- Exhibit an Isomorphism  $\phi: G \rightarrow G'$ .

a. To form a set  $G$  of permutation:

Let  $G$  be a finite group of order ' $n$ ' and  $a \in G$  be any element.

Corresponding to ' $a$ ' we define a map  $f_a(x) = a * x, \forall x \in G$  then  $f$  is one to one.

$$\because f_a(x) = f_a(y)$$

$$\Rightarrow a * x = a * y$$

$$\Rightarrow x = y \text{ (by left cancellation law)}$$

Now  $y \in G$  (Co-domain), then

$a^{-1} * y \in G$  such that

$$f_a(a^{-1} * y) = a * (a^{-1} * y) = (a * a^{-1}) * y = e * y = y$$

$\therefore f_a$  is onto.

Thus  $f_a$  is a one to one and onto function from  $G \rightarrow G$  and so it is a permutation on  $G$ .

b. To prove  $G'$  is a group:

Let  $f_a, f_b \in G'$  be any two elements, then

$$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b * x) = a * (b * x) = (a * b) * x = f_{a*b}(x)$$

$\therefore G'$  is closed.

Composition mapping is also associative.

Since ' $e$ ' is the identity element of  $G$ ,  $f_e \in G'$  is identity mapping.

Let  $a \in G \Rightarrow a^{-1} \in G$

$$f_{a^{-1}} f_a(x) = f_{a^{-1}}(a * x) = (a^{-1} * a) * x = e * x = f_e(x)$$

$$\therefore f_{a^{-1}} \in G'$$

Hence  $G'$  is a group.

c. Isomorphism  $\phi: G \rightarrow G'$ :

To prove  $G$  and  $G'$  are isomorphic.

Let  $\phi: G \rightarrow G'$  be defined by  $\phi(a) = f_a, \forall a \in G$

$$\text{Now for any } a, b \in G, \phi(a * b) = f_{a*b} = f_a * f_b = \phi(a) \phi(b)$$

$\therefore \phi$  is a homomorphism.

Suppose  $\phi(a) = \phi(b)$  then

$$f_a = f_b \Rightarrow f_a(x) = f_b(x), \forall x \in G \Rightarrow a * x = b * x \Rightarrow a = b \text{ \{Right Cancellation law\}}$$

$\therefore \phi$  is one to one

Since  $f_a$  is onto,  $\phi$  is onto.

Thus  $G \cong G'$



## Topic 11: COSETS and LAGRANGE'S THEOREM:

### 1) Define cosets with Example:

**Definition:** Let  $(H, *)$  be a subgroup of  $(G, *)$ . Let  $a \in G$  be any element. Then

$aH = \{a * h / h \in H\}$  is called the left coset of  $H$  in  $G$  determined by  $a$ .

Sometimes  $aH$  can be written as  $a * H$ .

The set  $Ha = \{h * a / h \in H\}$  is called the right coset of  $H$  in  $G$  determined by  $a$ .

### Points to remember:

1. Since  $e \in H$ ,  $a * e \in aH \Rightarrow a \in aH$  and  $e * a = a \in Ha$

2. Also  $eH = e * h / h \in H = h / h \in H = H$

and  $He = h * e / h \in H = h / h \in H = H$

So  $H$  itself is a left coset as well as right coset.

3. In general,  $aH \neq Ha$ .

But if  $G$  is abelian, then  $aH = Ha$  That is every left coset is a right coset.

### Problems:

1. Find the left cosets of  $H = (5Z, +)$  which is a subgroup of  $(Z, +)$

**Solution:** If  $H = 5Z$  then  $(H, +)$  is a subgroup of  $(Z, +)$ .

Then the distinct left cosets of  $H$  in  $Z$  are

$$0 + H = H = 0 + 5x \text{ where } x \in Z$$

$$1 + H = 1 + 5x \text{ where } x \in Z$$

$$2 + H = 2 + 5x \text{ where } x \in Z$$

$$3 + H = 3 + 5x \text{ where } x \in Z$$

$$4 + H = 4 + 5x \text{ where } x \in Z$$

$$5 + H = 5 + 5x \text{ where } x \in Z$$

$$= 5(1 + x) \text{ where } x \in Z = H$$

$$6 + H = 6 + 5x/x \in Z = 1 + 5(1 + x) \text{ where } x \in Z = 1 + H \text{ and so}$$

on. Therefore number of different left cosets of  $H$  in  $G$  is 5.

**2)Theorem:** Let  $(H,*)$  be a subgroup of  $(G,*)$ . Then the set of all left cosets of  $H$  in  $G$  form a partition of  $G$ .

**Proof:** Let  $aH$  and  $bH$  be any two left cosets.

We shall prove either  $aH = bH$

$$(\text{or}) aH \cap bH = \emptyset.$$

Suppose  $aH \cap bH \neq \emptyset$ , then there exists an element

$$x \in aH \cap bH \Rightarrow x \in aH \text{ and } x \in bH$$

$$\Rightarrow x = a * h_1 \quad x = b * h_2, \text{ for some } h_1, h_2 \in H \dots\dots\dots(1)$$

$$\text{Therefore, } a * h_1 = b * h_2, \Rightarrow a * h_1 * h_1^{-1} = b * h_2 * h_1^{-1}$$

$$\Rightarrow a * (h_1 * h_1^{-1}) = b * (h_2 * h_1^{-1})$$

$$\Rightarrow a * e = b * (h_2 * h_1^{-1})$$

$$a = b * (h_2 * h_1^{-1}) \dots\dots\dots(2)$$

If  $x$  is any element in  $aH$ , then  $x = a * h$

$$\Rightarrow x = b * (h_2 * h_1^{-1}) * h$$

$$\Rightarrow x = b * (h_2 * h_1^{-1}) * h \in bH$$

$$\text{Therefore } x \in aH \Rightarrow x \in bH \text{ therefore } aH \subseteq bH \dots\dots\dots(2)$$

$$\text{Similarly we can prove } bH \subseteq aH \dots\dots\dots(3)$$

From (2) and (3) we get  $aH = bH$ .

Thus any two left cosets are either equal or disjoint. Further  $\bigcup_{a \in G} aH \subseteq G$  since union of subsets is a subset. If  $x$  is any element in  $G$ , then  $x = x * e \in xH$

Therefore  $x$  is a left coset and hence  $x \in \bigcup_{a \in G} aH$ . Hence  $\Rightarrow x \in G \Rightarrow x \in \bigcup_{a \in G} aH \Rightarrow G \subseteq \bigcup_{a \in G} aH$ . Therefore  $G = \bigcup_{a \in G} aH$ . Thus all the left cosets forms partition of  $G$ .

### 3) State and prove Lagrange's theorem:

Statement: The order of a subgroup  $H$  of a finite group  $G$  divides the order of the group. (i.e) order of  $H$  divides order of  $G$ .

**Proof:** Let  $(G, *)$  be a group of order  $n$  and  $(H, *)$  be a subgroup of order  $m$ .

Since  $G$  is a finite group, the number of left cosets of  $H$  in  $G$  is finite.

Let  $r$  be the number of left cosets of  $H$  in  $G$

Let the  $r$  cosets be  $a_1H, a_2H \dots a_r H$ .

We know that the left cosets of  $G$  forms a partition of  $G$ . (by previous theorem)

Therefore  $G = a_1H \cup a_2H \cup \dots \cup a_r H$

Therefore  $o(G) = o(a_1H \cup a_2H \cup \dots \cup a_r H)$

$$= o(a_1H) + o(a_2H) + \dots o(a_rH)$$

But  $o(a_iH) = o(H)$  (by previous theorem)

Therefore  $o(G) = o(H) + o(H) + \dots o(H)$

*r times*

$$\Rightarrow o(G) = r o(H)$$

Thus  $O(H)$  divides  $o(G)$

## Topic 12: RINGS AND FIELDS

### 1) Define Ring with Example:

**Definition:** A non-empty set  $R$  with two binary operations  $+$  and  $\cdot$  called addition and multiplication is called ring if the following axioms are satisfied.

- (i)  $(R, +)$  is an abelian group with 0 as identity
- (ii)  $(R, \cdot)$  is a semigroup
- (iii) The operation  $\cdot$  is distributive over  $+$   
(i.e)  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  
 $(b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$

### 2) Define commutative ring.

**Definition:** A ring  $(R, +, \cdot)$  is said to be commutative if  $a \cdot b = b \cdot a \quad \forall a, b \in R$

### 3) Define Ring with Identity.

**Definition:** A ring  $(R, +, \cdot)$  is said to be a ring with identity if there exists an element  $1 \in R$  such that  $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

### 4) Define Ring with zero divisor.

**Definition:** If  $R, +, \cdot$  is a commutative ring, then  $a \neq 0 \in R$  is said to be a zero- divisor if there exists a non-zero  $b \in R$  such that  $ab = 0$ .

### 5) Define Ring without zero divisors

**Definition:** If in a commutative ring  $(R, +, \cdot)$ , for any  $a, b \in R$  such that  $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$  then the ring is without zero divisors.

In a ring without zero divisors,  $a \cdot b = 0 \Rightarrow a = 0$  or  $b = 0$ .

### 6) Define Integral domain:

**Definition: Integral domain:** A commutative ring  $(R, +, \cdot)$  with identity and without zero divisors is called an integral domain.

### 7) Define Field.

**Definition: Field:** A commutative ring  $(R, +, \cdot)$  which has more than one element such that every non zero element of  $R$  has a multiplicative inverse in  $R$  is called a field.

**Problems:**

1. Show that  $Z_5 = \{0, 1, 2, 3, 4\}$  is an integral domain under  $+_5$  and  $\times_5$ .

**Solution:**

$+_5$	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

$\times_5$	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

We can easily verify  $(Z_5, +_5, \times_5)$  is a commutative ring with identity 1. From the table for  $\times_5$ , we see product of non zero elements is non zero and so  $(Z_5, +_5, \times_5)$  ring without zero divisors is an integral domain.

2. Prove the set  $Z_4 = \{0, 1, 2, 3\}$  is a commutative ring with respect to  $+_4$  and  $\times_4$ .

**Solution:**

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- (i) All entries in both the tables  $+_4, \times_4$ , belongs to  $Z_4$ .  
Therefore  $Z_4$  is closed under  $+_4, \times_4$ .

- (ii) The entries of the first row is same as those of first column.

- (iii) Hence  $Z_4$  is commutative with respect to  $+_4, \times_4$

(iv) If  $a, b, c \in Z_4$  we can verify

$$a +_4 b +_4 c = a +_4 b +_4 c$$

$$a \times_4 b \times_4 c = a \times_4 b \times_4 c$$

Also the law is true for  $+_4, \times_4$ .

(iv)  $0 +_4 a = a +_4 0 = a \forall a \in Z_4$

$$1 \times_4 a = a \times_4 1 = a \forall a \in Z_4$$

0 is the additive identity and 1 is the multiplicative identity of  $Z_4$  with respect to  $+_4, \times_4$ .

(v) From the table  $+_4$  additive inverse of 0,1,2,3 are 0,3,2,1 respectively. And multiplicative inverse of non zero element 1,2,3 are 1,2,3 respectively.

(vi) Also we can verify distributive law

$$(vii) a \times_4 (b +_4 c) = a \times_4 b +_4 (a \times_4 c)$$

$$b +_4 c \times_4 a = b \times_4 a +_4 (c \times_4 a)$$

Hence  $(Z_4, +_4, \times_4)$  is a commutative ring with unity.

3. Prove that every field is an integral domain.

**Proof:** Let  $F$  be a field.

(i.e)  $(F, +, \cdot)$  is a commutative ring with identity and non zero element has a multiplicative inverse.

To prove  $F$  is an integral domain we have to show it has no zero divisors.

Suppose  $a, b \in F$  with  $a \cdot b = 0$  let  $a \neq 0$ , since  $a$  is a non zero element, its multiplicative inverse exists (i.e)  $a^{-1}$  exists.

$$\text{Therefore } a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 \Rightarrow a^{-1} \cdot a \cdot b = 0 \Rightarrow 1 \cdot b = 0$$

Thus  $a \cdot b = 0 \Rightarrow a \neq 0 \Rightarrow b = 0$ . Therefore  $F$  has no zero divisors.

Hence  $(F, +, \cdot)$  is an integral domain.

4) Show that  $(\mathbb{Z}, +, \cdot)$  is an integral domain where  $\mathbb{Z}$  is set of all integers.

**Proof:** We know commutative ring with identity and without zero divisors is called integral domain.

If  $\mathbb{Z}$  is set of all integers, then

(i)  $(\mathbb{Z}, +)$  is an abelian group.

(ii)  $(\mathbb{Z}, \times)$  is a semi ring.

(iii)  $a \times b = b \times a \quad \forall a, b, c \in \mathbb{Z}$

(iv)  $a \times b + c = a \times b + a \times c \quad \forall a, b, c \in \mathbb{Z}$

Hence  $(\mathbb{Z}, +, \cdot)$  is a commutative ring with identity.

If  $a \neq 0, b \neq 0 \in \mathbb{Z}$  then we know  $ab \neq 0$ . So  $\mathbb{Z}$  is without zero divisors.

Hence  $(\mathbb{Z}, +, \cdot)$  is an integral domain.

X.....X