2 GROUP THEORY

2.1 Introduction :

Definition : Binary operation : Let A be a non-empty set.
Then $A \times A = \{(a, b) / a, b \in A\}$.
A function $* : A \times A \to A$ is said to be binary operation on A if $*(a, b) = a * b \in A$.

e.g. **(i)** '+' is binary operation on $\mathbb{N}$
(ii) '×' is binary operation on $\mathbb{R}$
(iii) '–' is not binary operation on $\mathbb{N}$.

Definition : Algebraic structure :

A nonempty set G equipped with one **or** more binary operation is said to be an algebraic structure.

e.g. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{R}, +, \cdot)$

Deifnition : Semigroup :

Let S be a non-empty set and '$*$' be a binary operation on S. Then $(S, *)$ is said to be semigroup if the binary operation '$*$' is associative in S'.

i.e. For every $a, b, c \in S$; $(a * b) * c = a * (b * c)$.

e.g. $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(Z, +)$, $(\mathbb{R}, \times)$.

Definition : Monoid :

Let M be a non-empty set and '$*$' be a binary operation on M. Then $(M, *)$ is said to Monoid if the following conditions are satisfied :

(i) Closure property : M is clossed under '$*$'
i.e. For every $a, b \in M$, $a * b \in M$

(ii) Associative property : '$*$' is associative in M.
i.e. $\forall$ a, b, c $\in$ M, $(a * b) * c = a * (b * c)$

(iii) Existence of identity : There exists an element $e \in M$ such that
$e * a = a * e = a$; $\forall a \in M$

Remark : Every monoid is semigroup but converse is not true in general.
e.g. $(\mathbb{N}, +)$ is semigoup but not monoid.

e.g. (i) $(\mathbb{N}, \times)$, $(Z, \times)$, $(\mathbb{R}, \cdot)$
(ii) Let S be a non-empty set and P (S) be its powerset.

Then (P (S), ∪) and (P (S), ∩) are monoid with the identity ϕ and S respectively.

Definition : Group :

Let G be a non-empty set and '*' be a binary operation on G. Then (G, *) is said to be group if the following conditions are satisfied.

(i) Closure prop. :G is closed under '*'

i.e. For a, b∈G, a * b∈G.

(ii) Associative prop. : For every a, b, c ∈ G

(a * b) * c = a * (b * c).

(iii) Existence of an identity : There exists an element e∈G such that

a * e = a = e * a; ∀a∈G.

(iv) Existence of an inverse : For every a ∈ G, there existts b ∈ G such that a * b = e = b * a.

→ Here $b = a^{-1}$ is siad to be an inverse of a.

Definition : Abelian group or commutative group :

A group (G, *) is said to be an abelian group or commutative group if a * b = b * a; ∀ a, b ∈ G.

e.g. (Z, +), (ℝ, +), (ℝ – (0), ×), (ℚ – (0), ×)

Composition Table :

Let $S = \{a_1, a_2, \ldots a_n\}$ is a finite set having n elements. Let there be a binary operation defînal on S' multiplicatively. All possible binary composition elements of S can be arranged in a tabular form as :

- Write dements of S' in a horizontal row, say it columnheader.
- write elements of S in a vertical column, say it row header
- The elements $a_i * a_j$ associtat with the orderal pair (a_i, a_j) is placed at the intersection of the row headed by a_i and column a_j.

The table so obtain is called composition Table a finite under a grand binary operation.

Exmaple :

(i) Show that the set of square roots of unity form a group under multiplication.

(ii) Show that the set of cube roots of unity form a group under multiplication.

(iii) Show that the set of fourth roots of unity form a group under multiplication.

Solution : (i) Let $x^2 = 1$

$\therefore \quad x^2 - 1 = 0$

$\therefore \quad (x - 1)(x + 1) = 0$

$\therefore \quad x = -1, 1$

i.e. $G = \{-1, 1\}$

composition table :

$\times$	-1	1
-1	1	-1
1	-1	1

(i) Closure prop : From the composition table it is clear that '$*$' is closed in G.

i.e. $\forall\ a, b \in G \quad a \times b \in G$.

(ii) Asso. prop : We know that: multiplication of integers is associative.

i.e. $\forall\ a, b, c \in G$; $(a \times b) \times c = a \times (b \times c)$.

(iii) Exist. of identity : From the composition table, it is clear that '1' is the identity.

(iv) Exist. of inverse : from the compostition table

Inverse of -1 is -1

Inverse of 1 is 1

Also, $\forall\ a, b \in G,\ a \times b = b \times a$

Hence, $(G, \times)$ is an abelian group.

(ii) Here $x^3 = 1$

$\therefore \quad x^3 - 1 = 0$

$\therefore \quad (x - 1)(x^2 + x + 1) = 0$

$\therefore \quad x - 1 = 0$ or $x^2 + x + 1 = 0$

$\therefore \quad x = 1$ or $x = \dfrac{-1 \pm \sqrt{3}\,i}{2}$

i.e. $G = \{1, \omega, \omega^2\}$ where $\omega = \dfrac{-1 + \sqrt{3}\,i}{2}$; $\omega^2 = \dfrac{-1 - \sqrt{3}\,i}{2}$

Composition table :

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(i) Closure prop : From the composition table it is dear that G is closed under '×'.

(ii) Asso. prep : From the composition table for every a, b, c∈G We have (a × b) × c = a × (b × c).

(iii) Exist. of identity : From the composition table we see that '1' is the identity.

(iv) Exist. of an inverse : From the composition table

Inverse of 1 is 1
Inverse of ω is ω^2
Inverse of ω^2 is ω

Also, For every a, b ∈ G, a × b = b × a

Hence, (G, ×) is an abelian group.

(iii) Here $x^4 = 1$

$\therefore$ $x^4 - 1 = 0$

$\therefore$ $(x^2 - 1)(x^2 + 1) = 0$

$\therefore$ $x = \pm 1, \pm i$

Let G = {−1, 1, −i, i}

Composition table :

×	−1	1	−i	i
−1	1	−1	i	−i
1	−1	1	−i	i
−i	i	−i	−1	1
i	−i	i	1	−1

(i) Closure prop : From the composition table it is clear that G is closed under '×'.

(ii) Asso. prop : From the composition table. We see that For every a, b, c ∈ G ; (a × b) × c = a × (b × c).

(iii) Exist. of identity : From the composition table it is clear that '1' is the identity.

(iv) Exist. of inverse : From the composition table

Inverse of −1 is −1
Inverse of 1 is 1
Inverse of −i is i
Inverse of i is −i

Also, $\forall\ a, b, \in G, a \times b = b \times a$

Hence, $(G, \times)$ is an abelian group.

Example : Show that the set of all positive rational number forms an abelian group under the composition defined by $a * b = ab/2$.

Solution : Here $G = Q^+$ = The set of all positive rationals and '$*$' be binary operation on G defined as $a * b = \frac{ab}{2}$; $a, b \in G$

(i) Closure prop : Let $a, b \in G$

$$\text{then } a * b = \frac{ab}{2}$$

Now, a & b are +ve rational number,

$\Rightarrow$ $ab/2$ is also +ve rational number

i.e. for any $a, b \in Q^+ \Rightarrow a * b = \frac{ab}{2} \in Q^+$

i.e. Q^+ is closed under '$*$'.

(ii) Asso. prop : Let $a, b, c \in Q^+$

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

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

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

i.e. '$*$' is associative in Q^+.

(iii) Exist. of identity : Let 'e' be the identity of Q^+ under '$*$'.

i.e. for any $a \in G$ $\quad a * e = a$

$$\Rightarrow \frac{ae}{2} = a$$

$$\Rightarrow e = 2$$

i.e, '2' is the identity.

(iv) Exist. of inverse : Let $a \in Q^+$ and b be inverse of a. Then we have

$a * b = 2 = b * a$

$$\frac{ab}{2} = 2 \quad \therefore b = 4/a$$

i.e. $\forall a \in G$, $4/a$ is the inverse of a in Q^+

(v) Commutative prop : For any $a, b \in \mathbb{Q}^+$

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

Hence, $(\mathbb{Q}^+, *)$ is an abelian group.

Example : Show that $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0,\ a, b, c, d \in \mathbb{R} \right\}$ is group under matrix multiplication.

Solution : Here, $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0,\ a, b, c, d \in \mathbb{R} \right\}$

(i) Closure prop : Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in G$

i.e. $a_1d_1 - b_1c_1 \neq 0,\ a_2d_2 - b_2c_2 \neq 0$ ..... (Δ)

$$A \cdot B = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

Now $(a_1a_2 + b_1C_2)(c_1b_2 + d_1d_2) - (a_1b_2 + b_1d_2)(c_1a_2 + d_1c_2)$

$= (a_1a_2c_1b_2 + a_1a_2d_1d_2 + b_1c_2c_1b_2 + b_1c_2d_1d_2$

$- a_1b_2c_1d_2 - a_1b_2d_1c_2 - b_1d_2c_1d_2 - b_1d_1d_2c_2$

$= a_1a_2d_1d_2 - a_1b_2d_1c_2 - b_1c_1d_2a_2 + b_2c_2c_1b_2$

$= a_1d_1(a_2d_2 - b_2c_2) - b_1c_1(a_2d_2 - b_2c_2)$

$= (a_1d_1 - b_1c_1)(a_2d_2 - b_2c_2)$

$\neq 0$, $(\because (\Delta))$

$\Rightarrow A \cdot B \in G$

i.e. G is closed under matrix multiplication.

(ii) Asso. prop : We know that : for every $A, B, C \in G$

$(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

(iii) Exist of identity : Let $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$

then for any $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$

$$A \cdot e = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = A$$

i.e. $A \cdot e = A = e \cdot A$; $\forall A \in G$

i.e. 'e' be the identity of G.

(iv) Exist of inverse : Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ i.e. $ad - bc \neq 0$

Then $A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in G$

Hence, is a group under matrix multiplication

Now for $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix} \in G$

$$A \cdot B = \begin{bmatrix} 7 & 4 \\ 15 & 8 \end{bmatrix} \quad \& \quad B \cdot A = \begin{bmatrix} 1 & 2 \\ 9 & 8 \end{bmatrix}$$

i.e. $AB \neq BA$

Hence, G is not abelian.

2.2 Properties of group :

Theorem 1 : Let e be an identity element in group (G $*$), then 'e' is unique.

Proof : Suppose e end e' are two identity elements in G.

Then we have

$ee' = e$ if e' is identity

$ee' = e'$ if e is idnetity

Since ee' is unique element in G

$\therefore e = e'$.

Theorem 2 : Inverse of each element of a group (G, $*$) is unique.

Proof : Let a be any element of G and e the identity of G.

Suppose b and c are two different inverse of a in G. Then we have

$a * b = e = b * a$ if b is an inverse of a

and $a * c = e = c * a$ if c is an inverse of a

Now, $b = b * e$

$= b * (a * c)$

$= (b * a) * c$ ($\because$ asso. prop)

$= e * c = c$

Thus 'a' has unique inverse.

Theorem 3 : If a^{-1} is the inverse of an element a of group $(G, *)$, then $(a^{-1})^{-1} = a$.

Proof : Let e be the identity of group $(G, *)$

Then we have

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

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

$\Rightarrow ((a^{-1})^{-1} * a^{-1}) \cdot a = (a^{-1})^{-1}$ ($\because$ asso. prop)

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

$\Rightarrow (a^{-1})^{-1} = a.$

Theorem 4 : If $(G, *)$ be a group then for any two elements a and b of $(G, *)$, prove that $(a * b)^{-1} = b^{-1} * a^{-1}$ rule of reversal.

Proof : Let a^{-1} and b^{-1} are inverse of a and b respectively and e be the identity

Then we have $a * a^{-1} = e = a^{-1} * a$

$b * b^{-1} = e = b^{-1} * b.$

Now, $(a * b) * (b^{-1} * a^{-1}) = [(a * b) * b^{-1}] * a^{-1}$ ($\because$ asso. prop)

$= [(a * (b * b^{-1})] * a^{-1}$ ($\because$ asso. prop)

$= [a * e] * a^{-1}$

$= a * a^{-1}$

$= e$

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

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

This shows that : $b^{-1} * a^{-1}$ is inverse of $a * b$.

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

Cancellation law :

Theorem : If a, b and c be any three elements of a group $(G, \cdot)$ then

$ab = ac \Rightarrow b = c$ left Cancellationlaw

and $ba = ca \Rightarrow b = c$ rigth Cancellationlaw

Proof : Let $a \in G \Rightarrow$ there exists $a^{-1} \in G$ s.t. $aa^{-1} = e = a^{-1}a$

Where e is the identity of G.

Now, $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$ ($\because$ Multi. both sides on left by a^{-1})

$\Rightarrow (a^{-1}a) \cdot b = (a^{-1}a) \cdot c$ ($\because$ Asso. prop.)

$\Rightarrow e \cdot b = e \cdot c$

$\Rightarrow b = c$

Also $ba = ca$

$\Rightarrow (ba)\, a^{-1} = ((a)\, a^{-1}$ (∴ Multi bothside on right by a^{-1})

$\Rightarrow b\ (aa^{-1}) = c\ (aa^{-1})$ (∴ Asso. prop.)

$\Rightarrow b \cdot e = c \cdot e$

$\Rightarrow b = c.$

Exmaple : If a and b are any two elements of a group (G, ·) then show that the equations $ax = b$ and $ya = b$ have unique solution in G.

Soln : (a) Here $a \in G \Rightarrow \exists\ a^{-1} \in G$ s.t. $a \cdot a^{-1} = e = a^{-1} \cdot a$ where e is the identity of G.

Now, $a^{-1} \in G,\ b \in G \Rightarrow a^{-1} b \in G$

Now, substituting $x = a^{-1} b$ in the left side of $ax = b$.

We have $ax = a\ (a^{-1} b)$

$= (a\ a^{-1})\ b$ (∵ asso prop)

$= e \cdot b$

$= b$

Thus $a^{-1} b$ is a solution of the equation $ax = b$.

For uniqueness.

Let x_1 and x_2 are two different solution of the equation $ax = b$.

i.e. $ax_1 = b$ and $ax_2 = b$

$\Rightarrow ax_i = ax_2$

$\Rightarrow x_1 = x_2$ (by left can_law).

i.e. solution is unique

Similarly, We can prove for $ya = b$.

EXERCISES

Example : Show that the set $G = \{a + b\sqrt{2} \mid a, b \in Q\}$ is a group with repeat to addition.

Example : Show that the set of matrices

$$A\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \quad : \text{Where } \alpha \in \mathbb{R},$$

Form a group under matrix multiplication.

Example : Show that $G = \{I, A, B, C\}$ where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},\ B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

is an abelian group under matrix multiplication.

2.3 Modulorelation :

Let Z be the set of integers.

Define the relation a = b (mod n) read as a congruent to b mod n iff a – b is divisible by n

i.e. $n \mid (a - b)$

e.g. 13 – (–17) = 30 = 2·3·5 gives us

13 = –17 (mod 2)

13 = –17 (mod 3)

13 = –17 (mod 5)

13 = –17 (mod 6)

13 = –17 (mod 10)

13 = –17 (mod 15)

13 = –17 (mod 30)

→ [a] is called congruence class (mod n) of a (equivalance class For the relation congruence mod n)

→ If we denote the set of congruence classes (mod 5) by Z_5 them

$Z_5 = \{[0], [1], [2], [3], [4]\}$

Similarlly, lly $Z_n = \{[0], [1], [2] \ldots [n - 1]\}$

Note : [a] Can be written as $\bar{a}$.

2.3.1 Addition modulo m.

Let a and b are any interger and m is a fixed positive interger, then addition modulo m written as $a +_m b$ as

$$a +_m b = r,\ 0 \leq r < m$$

Where r is the least non–negative remainder when a + b is devided by m

e.g. $17 +_3 3 = 2$

2.3.2 Multiplication modulo P :

Let a and b are any integers and P is a fixed positive integer then "multiplication modulo p" written as $a \times p^b$ is defined as

$$a \times_P b = r; \qquad 0 \leq r < p$$

Where r is the least non–negative remainder when a–b is divided by P.

e.g. $3 \times_7 8 = 3$

Definition : Order of a group :

Let (G, *) be finite group then the number of distinct elements in G is called order of a group G and is donoted by O(G) **or** |G|

e.g. (i) Let G = { 1, −1, i, −i} is a group under multiplication

$\Rightarrow$ O (G) = |G| = 4

(ii) G = { 1, w, w^2 } is a group under multiplication

$\Rightarrow$ O (G) = |G| = 3

Example : Let S be a non-empty set and P (S) be its power set. Then (P (S), $\cap$) and (P (S), $\cup$) are monoids with the idontities S and ϕ respectively.

e.g. Consider (p (S), $\cup$) where S = {a, b}

p (S) = {{a}, {b}, {a, b}, ϕ}

Composition table is

$\cup$	{a}	{b}	{a, b}	ϕ
{a}	{a}	{a, b}	{a, b}	{a}
{b}	{a, b}	{b}	{a, b}	{b}
{a, b}	{a, b}	{a, b}	{a, b}	{a, b}
ϕ	{a}	{b}	{a, b}	ϕ

From the composition table it is clear that

(i) Closure property : For any X, Y $\in$ P (S)

We have X $\cup$ Y $\in$ P (S)

i.e. P (S) is closed under $\cup$

(ii) Asso. property : From the composition table it is clear that : $\cup$ is assocoative in p (S)

i.e. $\forall$ X, Y, Z $\in$ p (S) We have X $\cup$ (Y $\cup$ Z) = (X $\cup$ Y) $\cup$ Z

(iii) Exist of identity : From the composition table it is clear that ϕ is identity w.r. to $\cup$.

i.e. X $\cup$ ϕ = X = ϕ $\cup$ X ; $\forall$ X $\in$ p(S)

Hence, (p (S), $\cup$) is a monoid.

→ Similarly, we can prove that (p (S), $\cap$) is a monoid.

Example : Prove that the set G = { 0, 1, 2, 3, 4, 5} is a finite abelian group of order 6 w.r.to addition modulo 6.

Sol. : First we construct the composition table :

$+_6$	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

(i) Closure prop : From the composition table it is clear that : For every $a, b \in G$

$\rightarrow a +_6 b \in G$

(ii) Asso. prop : From the composition table we say that $+_6$ is associative in G i.e. $\forall$ a, b, c $\in$ G we have

$$a +_6 (b +_6 c) = (a +_6 b) +_6 C$$

(iii) Exist of identity :

From the composition table we say that '0' is the identity in G i.e. $\forall a \in G$ We have

$$a +_6 0 = a = 0 +_6 a$$

(iv) Exist of an inverse : From the composition table it is clear that

Inverse of 0 is 0
Inverse of 1 is 5
Inverse of 2 is 4
Inverse of 3 is 3
Inverse of 4 is 2
Inverse of 5 is 1

$\} \in G$

Hence, $(G +_6)$ is a group.

Also, it is clear that

$$a +_6 b = b +_6 a ; \forall a, b \in G$$

Hence, $(G, +_6)$ is an abelian group.

Example : Show that : $(Z_5, \times_5)$ is not a group.

Sol. : Here $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

or $Z_5 = \{[0], [1], [2], [3], [4]\}$

First, we construct composition table

$\times_5$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

From the composition table

(i) Closure prop : Z_5 is closed under $\times_5$

i.e. $\forall\ \bar{a}, \bar{b} \in Z_5$ We have $\bar{a} \times_5 \bar{b} \in Z_5$

(ii) Associative prop : $\times_5$ is associative in Z_5

i.e. $\forall\ \bar{a}, \bar{b}, \bar{c} \in Z_5$

$\bar{a} \times_5 (\bar{b} \times_5 \bar{c}) = (\bar{a} \times_5 \bar{b}) \times_5 \bar{c}$

(iii) Exist. of a identity : $\bar{1}$ is the identity in Z_5 w.r.to χ_5

i.e. $\bar{a} \times_5 \bar{1} = a = \bar{1} \times \bar{a}$

(iv) Exist. of inverse :

Inverse of $\bar{1} = \bar{1}$

Inverse of $\bar{2} = \bar{3}$

Inverse of $\bar{3} = \bar{2}$

Inverse of $\bar{4} = \bar{4}$

but inverse of $\bar{0}$ does not exists on Z_5 w.r. to χ_5

$\therefore$ $(z_5, \times_5)$ is not a group

$\therefore$ $(z_5, \times_5)$ is monoid

Note that : $(z_5', \times_5)$ is a group

where $z_5' = z_5 - \{\bar{0}\}$

Remark : An element [m] in Z_n has a multiplicative inverse iff (m, n) = 1

2.4.1 Permutations :

Let S be a finite set having n–district elements. Then a one–one mapping of S on to itself is called a permulation of degree n.

The number of elements in the finite set S is known as the degree of permulation.

e.g. Let $S = \{a_1, a_2, \ldots a_n\}$

than permutation $f = \begin{pmatrix} a_1 & a_2 & a_n \\ b_1 & b_2 & b_n \end{pmatrix}$

where $f : S \to S$ as $f(a_i) = b_i$ where $b_i \in S \ \forall i$

→ If S = {a, b} than set of all permulation on S is

$$\left\{\begin{pmatrix} a & b \\ a & b \end{pmatrix}, \begin{pmatrix} a & b \\ b & a \end{pmatrix}\right\}$$

2.4.2 Equality of two Permulation :

Let S be any finite set. Then two permution f and g of degree n on S are said to be equal if we have $f(a) = g(a) : \forall a \in S$

e.g. if S' = {1, 2, 3, 4} and

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \& \quad g = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

are two permutation of degree 4 then we have f = g

→ If P_n be the set consisting of all permutation of degree n, then the set P_n will have n! distinct elements.

→ This set P_n is called the symmetric set of permutations of degree n.

→ Sometimes it is also denoted by S_n.

Thus, P_n = {f : f is a permutation of degree n}

e.g. If S = {1, 2, 3} then the set P_3 of all permutations of degree 3 will have 3! distinct elements.

$$P_3 = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$$

2.4.3 Identity Permutation :

If I is a permutiation of degree n such that $I(a) = a : \forall a \in S$, then I is called the identity permulation of degree n

Thus if S = (1, 2, 3, ...n)

then $I = \begin{pmatrix} 1 & 2 & 3 \ldots n \\ 1 & 3 & 3 \ldots n \end{pmatrix}$ is an identity

permutation on S of degree n.

2.4.4 Product or Composition of two permutation :

The product or compsite of two permutations f and g of degree n donoted by f·g, is obtained by first carrying out the operation defined by f and then by g.

Suppose P_n is the set of all permutation of degree n let.

$f = \begin{pmatrix} a_1 & a_2 \dots & a_n \\ b_1 & b_2 \dots & b_n \end{pmatrix}$ and $g = \begin{pmatrix} b_1 & b_2 \dots & b_n \\ c_1 & c_2 \dots & c_n \end{pmatrix}$ be any two elements of P_n.

Then $f \cdot g = \begin{pmatrix} a_1 & a_2 \dots & a_n \\ c_1 & c_2 \dots & c_n \end{pmatrix} \in P_n$

Example 1 : Let $S = \{1, 2\}$ and let S_2 be the set of permutation on S'.

i.e. $S_2 = \{P_1, P_2\}$ where $P_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$; $P_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ composition table

·	P_1	P_2
P_1	P_1	P_2
P_2	P_2	P_1

$$P_1 \cdot P_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = P_1$$

$$P_1 \cdot P_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = P_2$$

$$P_2 \cdot P_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = P_2$$

$$P_2 \cdot P_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = P_1$$

(i) Closure Prop : From the composition table it is clear that for every $P_i, P_j \in S_2$

We have $p_i \cdot p_j \in S_2 \quad 1 \le i, j \le 2$

(ii) Asso. Prop : From the composition table we say that composition of permutation is associative in S_2.

(iii) Exist. of identy : From the composition we say that $P_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ is an identity in S_2.

(iv) Exist. of inverse : From the composition table

Inverse of P_1 is $P_1 \in S_2$

Inverse of P_2 is $P_2 \in S_2$

$\therefore$ $(S_2, \cdot)$ is a group

Also, $P_i \cdot P_j = P_j \cdot P_i \; ; \; \forall P_i, P_j \in S_2$

Hence, $(S_2, \cdot)$ is a comutative group.

Que. Give an example of a non-abelion group of order 6.

OR

Example 2 : Show that : The set S_3 of all permulations on three symbols 1, 2, 3 is a finite non-abelian group of order 6 w.r.to. composition of permutation.

Sol. : Let $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$

where $P_1, P_2, \ldots\ldots P_6$ are defined as under :

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Composition table '$\cdot$' = product of permutations.

$\cdot$	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_6	P_5	P_4	P_3
P_3	P_3	P_5	P_1	P_6	P_2	P_4
P_4	P_4	P_6	P_5	P_1	P_3	P_2
P_5	P_5	P_3	P_4	P_2	P_6	P_1
P_6	P_6	P_4	P_2	P_3	P_1	P_5

From the composition table

(i) Closure Prop : It is clear that for way $P_i, P_j, \in S_3$, $1 \le i, j \le 6$

We have $P_i \cdot P_j \in S_3$

(ii) From the composition table it is clear that composition of permutation is associative in S_3.

(iii) From table it is clear that : $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ is the identity element in S_3 w.r.to. composition of permutation.

i.e. $\forall\ P_i \in S_3 \qquad 1 \le i \le 6$

We have $P_i \cdot P_1 = P_i$

(iv) From the composition table

Inverse of P_1 is P_1
Inverse of P_2 is P_2
Inverse of P_3 is P_3
Inverse of P_4 is P_4
Inverse of P_5 is P_6
Inverse of P_6 is P_5

$\Big\} \in S_3$

Hence, $(S_3, \cdot)$ is a group

Also $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ & $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$$P_3 \cdot P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_6$$

&

$$P_4 \cdot P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_5$$

i.e. $P_3 \cdot P_4 \neq P_4 \cdot P_3$

Hence, S_3 is a non-abelian group of order 6 w.r.to composition of pemutation.

Example : Show that if every element of a group G is its own inverse, then G is abelian.

Let $a, b \in G$

$\Rightarrow$ $a * b \in G$ (by closure prop.)

Now, $a^{-1} = a$ & $b^{-1} = b$

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

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

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

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

Thus, We have $a * b = b * a$; $\forall$ $a, b \in G$

$\therefore$ (G, $*$) is an abelian group.

Example : Show that in a group (G, $*$), if for any $a, b \in G$, $(a * b)^2 = a^2 * b^2$ then (G, $*$) must be abelian.

$\rightarrow$ Let (G, $*$) be a group and let $a, b \in G$

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

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

$\Rightarrow$ $a * (b * a) * b = a * (a * b) * b$ ($\therefore$ asso. prop.)

by left and right cancellation law

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

Thus, we have $a * b = b * a$: $\forall$ $a, b \in G$

Hence, (G, $*$) is an abelian group.

2.5 Sub group :

Let G be a group under the binary operation '$*$'. A non-empty subset H of a group G is said to be a subgroup of G if H is itself a group under the same binary operation of a group G.