

Unit - I

Groups

Definitions

Group :-

A non empty set G is said to be group with the operation $*$ if it satisfies the following

i) closure law

For any $a, b \in G$: $a * b \in G$

ii) Associative law

For any $a, b, c \in G$, $a * (b * c) = (a * b) * c$

These two laws are satisfy then the group are called "Semi Group".

iii) Identity law

There exists $e \in G$ such that $a * e = a = e * a$, $\forall a \in G$

iv) Inverse law

For a given $a \in G$ $\exists a^{-1} \in G$ $\exists$
 $a * a^{-1} = e = a^{-1} * a$

v) Abelian property (or) commutative law.

Let G be a group with $*$.
Then G is said to be abelian if
 $a * b = b * a$, for any $a, b \in G$ ($ab = ba$)

Semi Group

A non empty set G is said to be Semi group with $*$ if it satisfy i) closure law and ii) Associative law.

Monoid

A non empty set G is said to be monoid with $*$ if it satisfy i) closure law, ii) Associative law and iii) Identity law.

Sub group

A non empty subset H of a group $(G, *)$ is said to be subgroup of G if H is also group with $*$.

Examples

1) $G = \mathbb{N}$, $*$ $= +$

i) G satisfies closure law as $a+b \in G$,
 $\forall a, b \in G$

ii) $a, b, c \in G$

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

$\therefore G$ satisfies Associative law.

iii) 0 is identity with $+$

but $0 \notin G = \mathbb{N}$

$\therefore G$ does not satisfy Identity law

$\therefore (G, +)$ is semi group but not

Group.

2) $G = \mathbb{W}$, $*$ $= +$

i) Closure law

$$a, b \in G$$

$$a + b \in G$$

ii) Associative law

$$a, b, c \in G \Rightarrow a + (b + c) = (a + b) + c$$

iii) Identity law

0 is identity with $+$

$$0 \in G = \mathbb{W}$$

$$a \in G, a + 0 = a$$

$$a_1 = -a \notin G, \text{ for } a \neq 0$$

$\therefore G$ does not satisfy inverse law

$\therefore (W, +)$ is monoid

3) $(Z, +)$ is a group

4) $(Q, +)$ is a group

5) $(R, +)$ is a group

6) $(C, +)$ is a group

1. Show that set of Integers ($\mathbb{Z}$) is an abelian group with ' $*$ ' defined by $a * b = a + b + 1$, for $a, b \in \mathbb{Z}$.

i) Closure law

$$a, b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}$$

$$a + b + 1 \in \mathbb{Z}$$

$$a * b \in \mathbb{Z}$$

ii) Associative law

$$a, b, c \in \mathbb{Z}$$

$$a * b = a + b + 1$$

$$(a * b) * c = (a + b + 1) * c$$

$$= a + b + 1 + c + 1$$

$$= a + b + c + 2$$

$$a * (b * c) = a * (b + c + 1)$$

$$= a + b + c + 1 + 1$$

$$= a + b + c + 2$$

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

iii) Identity law

Let e is Identity

$$a * e = a$$

$$a + e + 1 = a$$

$$e = a - a - 1$$

$$e = -1$$

$$e = -1 \in \mathbb{Z}$$

Identity exists in $\mathbb{Z}$

iv) Inverse law

$a \in \mathbb{Z}$, If a is Inverse of a

$$a * a = e$$

$$a + a + 1 = 1$$

$$a = -a - 2 \in \mathbb{Z}$$

$\therefore$ Inverse of a is $-a-2$

v) Commutative law or Abelian law

$$a, b \in \mathbb{Z}$$

$$a * b = a + b + 1$$

$$= b + a + 1$$

$$= b * a$$

$\therefore \mathbb{Z}, *$ is an abelian group.

2Q. The set $G = \mathbb{Q} - \{1\}$ is group. The operation $*$ defined by

$$a * b = a + b - ab, a, b \in G$$

Sol:- $a, b, c \in G$

① closure law

$$a, b \in G \Rightarrow a \neq 1, b \neq 1$$

$$a * b = a + b - ab$$

$$\text{if } a * b = 1$$

$$\text{then } a + b - ab = 1$$

$$a - 1 + b - ab = 0$$

$$(a-1) - b(a-1) = 0$$

$$(a-1)(1-b) = 0$$

$$\Rightarrow a-1=0 \text{ or } 1-b=0$$

$$\Rightarrow a=1 \text{ or } b=1$$

this is contradiction to $a \neq 1$ and $b \neq 1$
 $\therefore a \neq 1$ and $a+b-ab \in \mathbb{Q}$

$$\therefore a \neq b \in \mathbb{Q}$$

② Associative law

$$a \neq (b \neq c) = a \neq (b+c-bc)$$

$$= a+b+c-bc-a(b+c-bc)$$

$$= a+b+c-bc-ab-ac+abc$$

$$(a \neq b) \neq c = (a+b-ab) \neq c$$

$$= a+b-ab+c-(a+b-ab)c$$

$$= a+b-ab+c-ac-bc+abc$$

$$= a+b+c-ab-ac-bc+abc$$

$$\therefore a \neq (b \neq c) = (a \neq b) \neq c$$

③ Identity law:-

$$a \in \mathbb{Q} \Rightarrow a \neq 1$$

If e is identity

$$a \neq e = a$$

$$a+e-ae = a$$

$$a+e-ae-a=0$$

$$e(1-a)=0$$

$$e=0 \text{ (or) } 1-a=0$$

$$\Rightarrow e=0 \text{ or } a=1$$

Since $a \neq 1, e \neq 0$

$$e \neq 0 \in G$$

$\therefore G$ satisfy identity law.

(4) Inverse law

$$a \in G, \Rightarrow a \neq 1$$

If b is Inverse of a

$$a * b = e \neq 0$$

$$a + b - ab = 0$$

$$b - ab = -a$$

$$b(1-a) = -a$$

$$b = \frac{-a}{1-a} = \frac{a}{a-1}$$

$$\text{if } \frac{a}{a-1} = 1 \Rightarrow a = a-1$$

$$a - a = -1$$

$$0 = -1$$

This is contradiction

$$b = \frac{a}{a-1} \in G$$

(5) commutative law

$$a * b = a + b - ab$$

$$= b + a - ba$$

$$= b * a$$

$(G, *)$ is an abelian group

3 Q Show that the set $G = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} : \theta \in \mathbb{R} \right\}$

is a group under matrix multiplication.
is it commutative?

Sol:-

$$A_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

$$A_\beta = \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix}$$

$$A_\gamma = \begin{pmatrix} \cos \gamma & -\sin \gamma \\ \sin \gamma & \cos \gamma \end{pmatrix}$$

$$\alpha, \beta, \gamma \in \mathbb{R}$$

$$\Rightarrow A_\alpha, A_\beta, A_\gamma \in G$$

$$\begin{aligned} A_\alpha A_\beta &= \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix} \\ &= \begin{pmatrix} \cos \alpha \cos \beta - \sin \alpha \sin \beta & -\cos \alpha \sin \beta - \sin \alpha \cos \beta \\ \sin \alpha \cos \beta + \cos \alpha \sin \beta & -\sin \alpha \sin \beta + \cos \alpha \cos \beta \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{pmatrix} \end{aligned}$$

$$= A_{\alpha + \beta} \in G$$

① closure law

$$A_\alpha A_\beta = A_{\alpha + \beta}$$

$$\alpha, \beta \in \mathbb{R} \Rightarrow \alpha + \beta \in \mathbb{R}$$

$$\therefore A_{\alpha + \beta} \in G$$

② Associative law

$$(A_\alpha A_\beta) A_\gamma = A_{\alpha+\beta} A_\gamma$$

$$= A_{(\alpha+\beta)+\gamma}$$

$$= A_\alpha + (\beta+\gamma)$$

$$= A_\alpha \cdot A_{\beta+\gamma}$$

$$= A_\alpha (A_\beta A_\gamma)$$

③ Identity law:-

with matrix multiplication identity is

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix} = A_0 \in G$$

④ Inverse law:-

$$A_\alpha \in G$$

$$A_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

$$\alpha \in \mathbb{R}$$

$$A_\alpha^{-1} = \frac{1}{\cos^2 \alpha + \sin^2 \alpha} \begin{pmatrix} \cos \alpha & -(-\sin \alpha) \\ -\sin \alpha & \cos \alpha \end{pmatrix}$$

$$= \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix}$$

$$= A_{-\alpha} \in G$$

⑤ Abelian (or) commutative law:-

$$A_\alpha A_\beta = A_{\alpha+\beta}$$

$$= A_{\beta+\alpha}$$

$$= A_\beta \cdot A_\alpha$$

$\therefore G$ is an abelian group

Prove that the set of n^{th} roots of unity forms an abelian group with usual multiplication

Sol: The n^{th} roots of unity are given by

$$G = \left\{ e^{i \frac{2k\pi}{n}} / k = 0, 1, 2, \dots, n-1 \right\}$$

$$\text{Let } z_1 = e^{i \frac{2k_1\pi}{n}}, z_2 = e^{i \frac{2k_2\pi}{n}}, z_3 = e^{i \frac{2k_3\pi}{n}}$$

$0 \leq k_1, k_2, k_3 \leq n-1$, then $z_1, z_2, z_3 \in G$.

(i) closure law

$$z_1 z_2 = e^{i \frac{2k_1\pi}{n}} \cdot e^{i \frac{2k_2\pi}{n}}$$

$$= e^{i \frac{2k_1\pi}{n} + i \frac{2k_2\pi}{n}}$$

$$= e^{i \frac{2(k_1+k_2)\pi}{n}}$$

(case i): if $0 \leq k_1+k_2 \leq n-1$ then $z_1 z_2 \in G$.

(case ii): if $k_1+k_2 > n-1$ then $k_1+k_2 = n+k'$

where $0 \leq k' \leq n-1$

$$z_1 z_2 = e^{i \frac{2(k_1+k_2)\pi}{n}}$$

$$= e^{i \frac{2(n+k')\pi}{n}}$$

$$= e^{i \frac{2n\pi}{n} + i \frac{2k'\pi}{n}}$$

$$= e^{i2\pi + i \frac{2k'\pi}{n}}$$

$$= e^{i2\pi} \cdot e^{i \frac{2k'\pi}{n}}$$

$$= e^{i \frac{2k'\pi}{n}} \in G$$

① Associative law

$$\begin{aligned}
 (z_1 z_2) z_3 &= \left(e^{i \frac{2k_1 \pi}{n}} \cdot e^{i \frac{2k_2 \pi}{n}} \right) e^{i \frac{2k_3 \pi}{n}} \\
 &= e^{i \frac{2(k_1 + k_2) \pi}{n}} \cdot e^{i \frac{2k_3 \pi}{n}} \\
 &= e^{i \frac{2((k_1 + k_2) + k_3) \pi}{n}} \\
 &= e^{i \frac{2(k_1 + (k_2 + k_3)) \pi}{n}} \\
 &= e^{i \frac{2k_1 \pi}{n}} \cdot e^{i \frac{2(k_2 + k_3) \pi}{n}} \\
 &= e^{i \frac{2k_1 \pi}{n}} \left(e^{i \frac{2k_2 \pi}{n}} e^{i \frac{2k_3 \pi}{n}} \right) \\
 &= z_1 (z_2 z_3)
 \end{aligned}$$

③ Identity law

multiplicative identity is 1 ,

$$k=0 \Rightarrow z_0 = e^{i \frac{2 \cdot 0 \pi}{n}} = 1 \in G$$

④ Inverse law

$$z_0 = 1 \Rightarrow z_0^{-1} = 1^{-1} = 1 \in G,$$

$$z = e^{i \frac{2k\pi}{n}} \in G, \quad 1 \leq k \leq n-1$$

multiplicative inverse of z , is $\frac{1}{z}$

$$\begin{aligned}
 \frac{1}{z} &= \frac{1}{e^{i \frac{2k\pi}{n}}} \\
 &= e^{-i \frac{2k\pi}{n}}
 \end{aligned}$$

$$= e^{i2\pi} \cdot e^{\frac{-i2k\pi}{n}}$$

$$= e^{i2\pi} \cdot e^{\frac{-i2k\pi}{n}}$$

$$= e^{\frac{i2n\pi - i2k\pi}{n}}$$

$$\frac{1}{2} = e^{\frac{i2(n-k)\pi}{n}}$$

$$\text{since } 1 \leq k \leq n-1$$

$$-1 \geq -k \geq -n+1$$

$$n-1 \geq n-k \geq 1$$

$$\Rightarrow \frac{1}{2} = e^{\frac{i2(n-k)\pi}{n}}$$

$$= e^{\frac{i2k'\pi}{n}}, \quad 1 \leq k' \leq n-1$$

$$\therefore \frac{1}{2} \in G.$$

⑤ commutative law:-

$$z_1 z_2 = e^{\frac{i2k_1\pi}{n}} \cdot e^{\frac{i2k_2\pi}{n}}$$

$$= e^{\frac{i2(k_1+k_2)\pi}{n}}$$

$$= e^{\frac{i2(k_2+k_1)\pi}{n}}$$

$$= e^{\frac{i2k_1\pi}{n}} e^{\frac{i2k_2\pi}{n}}$$

$$= z_2 z_1$$

$\therefore (G, \cdot)$ is abelian group

G is also cyclic since $z \in G \Rightarrow z = \left(e^{\frac{i2\pi}{n}}\right)^k, k \in \mathbb{Z}$

Composition table :-

Let $G = \{a_1, a_2, \dots, a_n\}$ be a finite set and $*$ is an operation defined on it

$*$	a_1	a_2	...	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	...	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	...	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	...	$a_n * a_n$

~~① Closure~~

① Closure law

Every element in table belongs to G

② Associative law

$$a_i * (a_j * a_k) = (a_i * a_j) * a_k$$

③ Identity law

There exists a row that is same as top row first element in that row is identity.

④ Inverse law

given an element $a_i \in G$

If there is identity in i^{th} row

Say at j^{th} column
 that is $a_i * a_j$ is identity then $a_i^{-1} = a_j$
 $a_j^{-1} = a_i$

⑤ Commutative law

If the table is symmetric with respect to principal diagonal then G is commutative with $*$

Example :- $G = \{1, -1, i, -i\}$

5. Example :- $G = \{1, -1, i, -i\}$ is abelian group with usual multiplication.

Sol:-

Given:

$*$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

(1) closure law

Every element in table is again in G

(2) Associative law

G is subset of complex numbers

Since complex numbers satisfy associative law,
 G also satisfy associative law

(3) Identity law:-

'1' is Identity

(4) Inverse law:-

$$1^{-1} = 1, (-1)^{-1} = -1$$

$$i^{-1} = -i, (-i)^{-1} = i$$

(5) Commutative law:-

Since the table is symmetric G is abelian.

$\therefore (G, \cdot)$ is abelian group

G is cyclic since

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

6. Example:- $G = \{1, \omega, \omega^2\}$ is group with multiplication, here $\omega^3 = 1$.

Sol:-

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(1) closure law

Every element in table is again in G

(2) Associative law

G is subset of complex numbers

Since complex numbers satisfy associative law, G also satisfy associative law.

③ Identity law
'1' is Identity

④ Inverse law

$$1^{-1} = 1$$

$$\omega^{-1} = \omega^2$$

$$(\omega^2)^{-1} = \omega$$

⑤ Commutative law:-

Since the table is symmetric G is abelian.

$\therefore (G, \cdot)$ is abelian group & i

G is cyclic since.

$$\omega^1 = \omega, \omega^2 = \omega^2, \omega^3 = 1$$

Modulo arithmetic

If we divide any number with '2' the possible remainders are

divisor	possible remainders
1	0
2	0, 1
3	0, 1, 2
4	0, 1, 2, 3
5	0, 1, 2, 3, 4
...	...
n	0, 1, 2, ..., (n-1)

$+_2$ = Addition modulo 2

$\times_2$ = Multiplication modulo 2

$$G = \{0, 1\}$$

$+_2$

$\times_2$

$$a \equiv x \pmod{n}$$

(a is congruent to x mod n)

$$\Rightarrow n \mid (a - x)$$

$$5 +_2 7 = 0$$

$$5 \times_2 7 = 1$$

$$5 \times_3 7 = 02$$

$$5 \times_5 7 = 0$$

$$5 \times_7 7 = 3$$

$$5 +_7 7 = 0$$

$$5 \times_7 7 = 2$$

$$5 \times_5 7 = 0$$

$$5 +_6 7 = 0$$

$$5 \times_6 7 = 5$$

$$5 \times_7 7 = 0$$

$$5 \times_8 7 = 3$$

$$5 +_7 7 = 5$$

$$5 +_8 7 = 4$$

$$5 \times_8 7 = 3$$

$$a \times b = na$$
$$a \times na = na^2$$

$$\begin{array}{r} 5 \times 8 = 18 \\ 10 \end{array}$$

+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4
+	0	1	2	3	4

Identity
0
1

$$Z_2 = \{0, 1\}$$

$$Z_3 = \{0, 1, 2\}$$

$$Z_4 = \{0, 1, 2, 3\}$$

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

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

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

$$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$Z_n = \{0, 1, 2, \dots, (n-1)\}$$

Rough work

x_2	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$e = 1$$

$$0^{-1} = 1$$

$$2^{-1} = 2$$

x_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

$$0^{-1} = 1$$

$$1^{-1} = 1$$

$$2^{-1} = 3$$

$$3^{-1} = 2$$

x_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

$$0^{-1} = 1$$

$$1^{-1} = 1$$

$$2^{-1} = 2$$

$$3^{-1} = 3$$

2 does not exist

$$3^{-1} = 3$$

x_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

$$0^{-1} = 1$$

$$1^{-1} = 1$$

$$2^{-1} = 3$$

$$3^{-1} = 2$$

x_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

$$0^{-1} = 1$$

$$1^{-1} = 1$$

$$2^{-1} = 2$$

$$3^{-1} = 3$$

x_2	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{0}$	$\bar{0}$

Identity = $\bar{0}$

$$\bar{0}^{-1} = \bar{0}$$

$$\bar{1}^{-1} = \bar{1}$$

x_2	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Identity = $\bar{1}$

$\bar{0}^{-1}$ = does not exist

$$\bar{1}^{-1} = \bar{1}$$

x_3	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Identity = $\bar{0}$

$$\bar{0}^{-1} = \bar{0} \quad \bar{2}^{-1} = \bar{2}$$

$$\bar{1}^{-1} = \bar{2}$$

x_3	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Identity = $\bar{1}$

$\bar{0}^{-1}$ = does not exist

$$\bar{1}^{-1} = \bar{1}$$

$$\bar{2}^{-1} = \bar{2}$$

x_6	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Identity = $\bar{0}$

$$\bar{0}^{-1} = \bar{0}$$

$$\bar{1}^{-1} = \bar{5}$$

$$\bar{2}^{-1} = \bar{4}$$

$$\bar{3}^{-1} = \bar{3}$$

$$\bar{4}^{-1} = \bar{2}$$

$$\bar{5}^{-1} = \bar{1}$$

x_6	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Identity = $\bar{1}$

$$\bar{0}^{-1} = \text{null}$$

$$\bar{1}^{-1} = \bar{1}$$

$$\bar{2}^{-1} = \text{does not exist}$$

$$\bar{3}^{-1} = \text{does not exist}$$

$$\bar{4}^{-1} = \text{does not exist}$$

$$\bar{5}^{-1} = \bar{5}$$

$$0) 8(1)$$

$$0) 10(1)$$

$$0) 9(1)$$

$$0) 6(1)$$

$$0) 3(1)$$

$$0) 12(1)$$

$$0) 15(1)$$

$$0) 11(1)$$

$$0) 1(1)$$

prob:- $Z_n = \{0, 1, \dots, n-1\}$ is abelian group with $+$

Sol:- 1) closure law

$$a +_n b \in Z_n$$

= Since $0 \leq a, b < n$

$$\Rightarrow 0 \leq a+b < n \text{ or } a+b > n$$

$$\text{If } a+b < n \Rightarrow a +_n b \in Z_n$$

$$\text{If } a+b > n \Rightarrow a+b = n + r \text{ for some } r$$

$$\Rightarrow a +_n b \equiv r \pmod{n}$$

$$\Rightarrow a +_n b \in Z_n$$

2) Associative law:-

$$a +_n (b +_n c) = (a +_n b) +_n c \text{ holds for modular arithmetic}$$

3) Identity law:-

0 is identity with $+$

4) Inverse law:-

$$\bar{a} \in Z_n$$

$$\bar{a} +_n \bar{b} = \bar{0}$$

$$\bar{b} = \overline{n-a} \in Z_n$$

5) commutative law:-

$$\bar{a} +_n \bar{b} = \bar{b} +_n \bar{a} \text{ holds for modular arithmetic}$$

arithmetic.

prob:- If P is prime then $Z_P = \{1, 2, \dots, P-1\}$ is abelian group with $\times_P$ (multiplication modulo P).

Sol:- $a, b, c \in Z_P$

(i) closure law

$$a \neq 0, b \neq 0, 1 \leq a, b < P$$

$$a \times_P b \in Z_P$$

$\therefore ab \not\equiv p$ similarly $p \not\equiv ab$

$\therefore ab \equiv x \pmod{p} \Rightarrow 1 \leq x < p$

$$\Rightarrow \overline{ab} = \overline{x} \in \mathbb{Z}_p$$

ii') Associative :-

$$(a \times_p b) \times_p c = a \times_p (b \times_p c) \text{ holds for}$$

modular arithmetic

iii') Identity law :-

1 is identity with $\times_p$

iv') Inverse law :-

$$\overline{a} \in \mathbb{Z}_p$$

G.C.D of a and p is 1

$$\exists x, y \in \mathbb{Z} \quad \exists ax + py = 1$$

$$ax \equiv 1 \pmod{p}$$

$$\Rightarrow \therefore \overline{a}^{-1} = \overline{x} \in \mathbb{Z}_p$$

v') commutative law :-

$$\overline{a} \times_p \overline{b} = \overline{b} \times_p \overline{a}$$

holds for modular arithmetic.

Theorems :-

1. Theorem :- Let G be a group then
SM identity in it is unique.

Proof :-

Suppose G has two identity elements.

say e_1 and e_2

That is, $e_1, e_2 \in G$

$e_1 e_2 = e_1$ (since e_2 is identity)

$e_1 e_2 = e_2$ (since e_1 is identity)

From above equations we have $e_1 = e_2$

Hence identity element in a group is unique.

2. Theorem :- Inverse element for a given
SM element in a group is unique.

Proof :-

Let $a \in G$, suppose $a_1, a_2 \in G$ are
inverse elements for a

$$\text{that is } aa_1 = e = a a_2 \quad \text{--- (1)}$$

$$a a_2 = e = a_1 a \quad \text{--- (2)}$$

Here e is identity in G .

From (1) $aa_1 = e$

$$a_1 (aa_2) = a_1 e$$

$$(a_1 a) a_2 = e \quad (\text{by Associative law})$$

$$e a_2 = a_1 a_2 \quad (\text{from eq (1)})$$

$$a_1 a_2 = e$$

$\therefore$ Inverse element of a given element in G is unique.

3. Theorem :- In a group G the following holds

- (1) $(a^{-1})^{-1} = a$, for any $a \in G$
- (2) $(ab)^{-1} = b^{-1}a^{-1}$ for any $a, b \in G$
- (3) $(a_1, a_2, \dots, a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$
for $a_1, a_2, \dots, a_n \in G$.

proof : ① Let $a \in G$

then $\exists b \in G \ni ab = e$

$$a^{-1} = b \text{ and } b^{-1} = a$$

$$(a^{-1})^{-1} = a$$

② $a, b \in G \Rightarrow ab \in G$ (by closure law)

Then $(ab)^{-1}$ exists

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(b(b^{-1}a^{-1})) \quad (\text{by Associative law in } G) \\ &= a((bb^{-1})a^{-1}) \quad (\text{by associative law in } G) \\ &= a(ea^{-1}) \end{aligned}$$

$$= aa^{-1}$$

$$= e$$

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

③ Let $a_1, a_2, \dots, a_n \in G$

then $a_1 a_2 \dots a_n \in G$ (by closure law)

we know $a_i^{-1} = a_i^{-1}$

Suppose

$$(a_1, a_2, \dots, a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \dots a_1^{-1} \rightarrow \text{①}$$

then

$$\begin{aligned} (a_1, a_2, \dots, a_k, a_{k+1})^{-1} &= a_{k+1}^{-1} (a_1, a_2, \dots, a_k)^{-1} \quad (\because (ab)^{-1} = b^{-1}a^{-1}) \\ &= a_{k+1}^{-1} a_k^{-1} \dots a_2^{-1} a_1^{-1} \quad (\text{by ①}) \end{aligned}$$

$\therefore$ From mathematical induction

$$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$$

for any n .

④ Theorem:- Cancellation laws hold in a group i.e., if G is a group then

i) $a, b, c \in G$, $ab = ac \Rightarrow b = c$

ii) $a, b, c \in G$, $ba = ca \Rightarrow b = c$

Let G be a group
and $a, b, c \in G$

i) Assume $ac = bc$

Since $c \in G \Rightarrow c^{-1} \in G$

$$(ac)c^{-1} = (bc)c^{-1} \quad (\text{by using Associative law})$$

$$a(cc^{-1}) = b(cc^{-1})$$

$$ae = be$$

$$\Rightarrow a = b$$

$\therefore$ Right cancellation law holds in G

ii) Assume $ca = cb$

$$c^{-1}(ca) = c^{-1}(cb) \quad (\text{by using Associative law})$$

$$(c^{-1}c)a = (c^{-1}c)b$$

$$ea = eb$$

$$\Rightarrow a = b$$

$\therefore$ Left cancellation law holds in G

5. Theorem :- In a group G , the system of equations $ax = b$ and $ya = b$ have unique solutions for $a, b \in G$

Let G be a group
and $a, b \in G$ and $a^{-1}, b^{-1} \in G$

(i) consider $ax = b$

$$a^{-1}(ax) = a^{-1}b \quad \text{by associative law}$$

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

$$ex = a^{-1}b$$

$x = a^{-1}b$ is solution for

$$ax = b \text{ and } a^{-1}b \in G$$

Suppose x_1, x_2 are two solutions
for $ax = b$

$$\text{then } ax_1 = b$$

$$ax_2 = b$$

$$\Rightarrow ax_1 = ax_2$$

By left cancellation law $x_1 = x_2$

$\therefore ax = b$ has unique solution in G

ii) consider $ya = b$

$$(ya)a^{-1} = ba^{-1} \quad (\text{by using associative law})$$

$$y(aa^{-1}) = ba^{-1}$$

$$ye = ba^{-1}$$

$y = ba^{-1}$ is solution for $ya = b$

and $ba^{-1} \in G$,

Suppose y_1, y_2 are two solutions
for $ya = b$

then $y_1 a = b$
 $y_2 a = b$

$$\Rightarrow y_1 a = y_2 a$$

By right cancellation law $y_1 = y_2$

$\therefore y a = b$ has unique solution in G .

6. Theorem: In a group G if $a^{-1} = a$ for every $a \in G$ then G is abelian.

Let $a, b \in G \Rightarrow ab \in G$ and $ba \in G$

Since $a^{-1} = a$ for any $a \in G$

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

$$\boxed{a^{-1} = a \text{ and } b^{-1} = b}$$

$$b^{-1} a^{-1} = ab$$

$$ba = ab$$

$\therefore G$ is abelian.

7. Theorem: In a group G if $a^2 = a$ for every $a \in G$ then G is abelian.

Let $a, b \in G \Rightarrow ab \in G$ and $ba \in G$

Since $a^2 = a$ for any $a \in G$

$$(ab)^2 = ab$$

$$(ab)^2 = a^2 b^2 \quad (\because a^2 = a, b^2 = b)$$

$$abab = aabb$$

$$a^{-1} ab ab b^{-1} = a^{-1} a a b b b^{-1}$$

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

$$ba = ab$$

$\therefore G$ is abelian.

8. Theorem:- In a group G if $a^n = e$ for any $a \in G$ then G is abelian

Imp
5m

$$a, b \in G \Rightarrow a b \in G$$

$$(ab)^2 = e \quad (\because a^n = e \text{ for any } a \in G)$$

$$(ab)^4 = e$$

$$(ab)^4 = a^4 b^4$$

$$a b a b = a a b b$$

$$a^{-1} a b a b b^{-1} = a^{-1} a a b b b^{-1}$$

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

$$\Rightarrow b a = a b$$

$\therefore G$ is abelian.

9. Theorem:- In a group G if $(ab)^n = a^n b^n$

Imp
10m

for consecutive integers then G is abelian.

Let $a, b \in G$

Assume $(ab)^n = a^n b^n$

for $n=m, n=m+1, n=m+2$

$$\Rightarrow (ab)^m = a^m b^m$$

$$(ab)^{m+1} = a^{m+1} b^{m+1}$$

$$(ab)^{m+2} = a^{m+2} b^{m+2}$$

$$(ab)^{m+2} = a^{m+2} b^{m+2}$$

$$(ab)^{m+1} (ab) = a^{m+2} b^{m+2}$$

$$a^{m+1} b^{m+1} (ab) = a^{m+1} a b^{m+1} b$$

By left cancellation law

$$b^{m+1}ab = ab^{m+1}b$$

By Right cancellation law

$$b^{m+1}a = ab^{m+1}$$

$$b^m b a = ab^{m+1}$$

multiplying a^m on both sides

$$\Rightarrow a^m b^m b a = a^m a b^{m+1}$$

$$(ab)^m b a = a^{m+1} b^{m+1}$$

$$(ab)^m b a = (ab)^{m+1}$$

$$(ab)^m b a = (ab)^m ab$$

By left cancellation law

$$ba = ab$$

$\therefore G$ is abelian.

10. Theorem :- A finite semigroup
satisfying cancellation laws is a group

V Imp
10M

Let G be a finite semi-
group that satisfying cancellation
laws.

$$G = \{a_1, a_2, \dots, a_n\}$$

$$\text{Let } a \in G$$

$$aa_1, aa_2, \dots, aa_n \in G \quad (\because \text{By closure law})$$

$aa_1, aa_2, \dots, aa_n$ are disjoint elements

if $aa_i = aa_j$ for some $i \neq j$
 $\Rightarrow$ By left cancellation law $a_i = a_j$

This is contradiction

$\therefore aa_i \neq aa_j$ for $i \neq j$.

Since $aa_1, aa_2, \dots, aa_n \in G$ and aa_i

aa_k for some k

Since a is arbitrary element in G

$a_k = e$ is identity in G

$\Rightarrow G$ satisfy identity law

Since $a_k = e \in G$ and $a \in G$

$aa_j = a_k = e$ for some j

$\Rightarrow aa_j \in G$

Inverse law holds in G

Since G is semigroup and

It satisfies identity law and

Inverse law.

$\therefore G$ is a group.

NOTE:- The set of integers $\mathbb{Z}$,
with multiplication is semi group
that satisfy cancellation laws how
ever it is not a group with
multiplication As it is not a finite
set.

2. Sub Groups

Complex:-

Definition: If G is a group and $H \subseteq G$, then H is called a complex of G .

Ex:- The set of all even integers is a complex of the group $(\mathbb{Z}, +)$.

Definition:- If H and K are two complexes of a group G , then the complex $(H \cdot K)$ is called the product of H and K .

Definition:- If H is a complex of a group G , then the complex H^{-1} is called Inverse complex of H in G .

* Sub Group:-

Definition:- Let G be a group. A subset H of G is ~~said~~ to be a Sub group of G if H is a group with respect to the operation $\cdot$ of G .

① Theorem:- If H is a sub group of a group G then $HH = H$

proof:- Let $x \in HH \Rightarrow h_1 h_2$

where $h_1, h_2 \in H$

$\forall h_1, h_2 \in H$, H is a sub group

$\Rightarrow x \in H$

$\therefore HH \subseteq H$ — ①

Let $h \in H$ then $h = h e \in HH$

$\therefore H \subseteq HH$ — ②

$\therefore$ from ① & ② we have

$$HH = H$$

② Theorem:- If H is a sub group of a group G then $H^{-1} = H$

proof:- Let $x \in H^{-1} \Rightarrow x = h^{-1}$

where $h \in H$

$h \in H$, H is a sub group

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

$\Rightarrow x \in H$

$\therefore H^{-1} \subseteq H$ — ①

$h \in H$, H is a sub group

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

$\Rightarrow h = (h^{-1})^{-1} \in H^{-1}$

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

$\therefore H \subseteq H^{-1}$ — ②

from ① & ② we have

$$H^{-1} = H$$

③ Theorem:-

Necessary and sufficient conditions

for a subgroup:-

Theorem:-

Statement: A non empty complex H of a group G is a subgroup of G if and only if

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

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

necessary (or) sufficient (or) $(\Rightarrow)$ these are same

proof:- Suppose H is a subgroup of G .

G .

Then H is a group with respect to the operation of G .

Thus, $a, b \in H \Rightarrow ab \in H$

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

Conversely

conversely

suppose

that H is a

non empty

complex

such that

$a, b \in H \Rightarrow ab \in H$ — ①

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

from ① it follows that ' $\cdot$ ' is a

binary operation in H .

Let $a, b, c \in H \Rightarrow$

$\Rightarrow a, b, c \in H, H \subseteq G$

$\Rightarrow a, b, c \in H \subseteq G$

$$\Rightarrow (ab)c = a(bc) \text{ (Associative)}$$

$\therefore \cdot$ is associative in H

$$\text{Let } a \in H \Rightarrow a^{-1} \in H$$

$$a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H$$

$$e \in H$$

If $a \in H$, then $a \in G$ and hence

$$ae = ea = e \text{ (Identity)}$$

$\therefore e$ is the identity in H

Let $a \in H$ then $a^{-1} \in H$ also

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

$\therefore$ every element in H has

inverse in H

$\therefore H$ is a group with respect

to the operation $\cdot$ of G .

$\therefore H$ is a subgroup of G .

(H) Theorem: A non empty complex H of a group G is a subgroup of G

if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof: Suppose H is a subgroup of G

$\therefore H$ is a group with respect to the operation $\cdot$ of G

Let $a, b \in H$

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

$$a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$$

$$\therefore a, b \in H \Rightarrow ab^{-1} \in H$$

conversely Suppose that H is non empty
sub^{set} of G such that $a, b \in H \Rightarrow ab^{-1} \in H$

Since H is non-empty, Let $a \in H$

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

$\therefore$ Identity element e of G is in H

and hence it is the identity
element of H .

Let $a \in H$

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

$\therefore$ Every element in H has inverse in H

Let $a, b \in H$

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

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

$$\therefore a, b \in H \Rightarrow ab \in H$$

$\therefore$ $\cdot$ is a binary operation in H

Let $a, b, c \in H$

$$a, b, c \in H, H \subseteq G \Rightarrow a, b, c \in G \Rightarrow (ab)(c) = a(bc)$$

$\therefore \cdot$ is an associative binary

operation in H .

Thus H is a group w.r.t. the binary
operation $\cdot$ of G .

$\therefore H$ is a subgroup of G .

⑤ Theorem:-

A finite non empty complex H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab \in H$

Proof:

Suppose H is a subgroup of the group G .

Thus H is a group with respect to the operation $\cdot$ of G and hence is a binary operation in H .

$$a, b \in H \Rightarrow ab \in H$$

Conversely suppose that H is a non empty complex of G such that $a, b \in H \Rightarrow ab \in H$.

Since H is non empty, let $a \in H$

$$aa \in H, a \in H \Rightarrow a^2 \in H$$

By induction $a^n \in H$ for each $n \in \mathbb{N}$

$$\therefore \{a, a^2, a^3, \dots\} \subseteq H$$

Since H is finite, $a^x = a^y$

where $x, y \in \mathbb{N}$ and $x > y$

$$x > y \Rightarrow x - y > 0$$

$$x - y \in \mathbb{N}$$

$$a^{x-y} = a^x a^{-y}$$

$$= a^x (a^y)^{-1}$$

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

if $x-y=1$ then, $a=e$ and

hence $a^{-1}=e^{-1}=e \Rightarrow a \in H \Rightarrow a^{-1} \in H \Rightarrow a \in H$

if $x-y > 1$

$$x-y-1 > 0$$

$$x-y-1 \in \mathbb{N}$$

$$a^{x-y-1} \in H$$

$$a^{x-y} = e$$

$$aa^{x-y-1} = e$$

$$a^{-1} = a^{x-y-1} \in H$$

$$\therefore a \in H \Rightarrow a^{-1} \in H$$

$\therefore H$ is a subgroup of G .

Theorem:

algebra of subgroups

① Theorem:-

If H and K are two subgroups of a group G . Then $H \cap K$ is also a subgroup of G .

proof:-

Since H is a subgroup of G , $e \in H$

Since K is a subgroup of G , $e \in K$

$$e \in H, e \in K \Rightarrow e \in H \cap K$$

$\therefore H \cap K$ is a non empty subset

of G

let $a, b \in H \cap K$

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

$a, b \in H$, H is a subgroup of $G \Rightarrow ab^{-1} \in H$

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

$a, b \in K$, K is a subgroup of G
 $G \Rightarrow ab^{-1} \in K$

$$ab^{-1} \in H, ab^{-1} \in K$$

$$\Rightarrow ab^{-1} \in H, ab^{-1} \in K \Rightarrow ab^{-1} \in H \cap K$$

$\therefore H \cap K$ is a subgroup of G

Note:- The union of two subgroups of a group need not be a subgroup.

⑦ Theorem:-

Let H and K be two subgroups of a group G . Then $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

Proof:-

Suppose that $H \cup K$ is a subgroup of G .

Suppose if possible $H \not\subseteq K, K \not\subseteq H$,
 ~~$H \not\subseteq K \Rightarrow$~~ there exist $(\exists) a \in H$

$$H \not\subseteq K \Rightarrow \exists a \in H \exists a \notin K$$

$$K \not\subseteq H \Rightarrow b \in K \exists b \notin H$$

$$a \in H \Rightarrow a \in H \cup K$$

$$b \in K \Rightarrow b \in H \cup K$$

$$a, b \in H \cup K \Rightarrow ab \in H \cup K$$

$$\Rightarrow ab \in H \text{ or } ab \in K$$

If $ab \in H$ then $b = a^{-1}(ab) \in H$

which is not true

If $ab \in K$ then $a = a(b)b^{-1} \in K$

which is not true

it is a contradiction

$$H \subseteq K \text{ or } K \subseteq H$$

Conversely suppose that either $H \subseteq K$ or

$$K \subseteq H.$$

if subgroups $H \subseteq K$ then $H \cup K = K$

a subgroup of G

if $K \subseteq H$ then

$$H \cup K = H$$

a subgroup of G .

$\therefore H \cup K$ is a subgroup of G .

③ Theorem:-

Let H and K be two subgroups of a group G then HK is a subgroup of G if and only if $HK = KH$

Proof:-

H is a subgroup of G

$$\Rightarrow H H^{-1} = H$$

$$\text{and } H H^{-1} = H$$

K is a subgroup of G

$$\Rightarrow K^{-1} = K \text{ and } K K^{-1} = K$$

Suppose HK is a subgroup of G

HK is a subgroup of G

$$\Rightarrow (HK)^{-1} = HK \Rightarrow HK = (HK)^{-1} = K^{-1}H^{-1} = KH$$

clearly suppose that

$$(HK)(HK)^{-1} = KKK^{-1}H^{-1} = HKH^{-1} = KH = HK$$

$\therefore HK$ is a subgroup of G

second proof:

conversely

suppose that HK is a subgroup of G .

Let $x \in HK$.

$$x \in HK \Rightarrow x^{-1} \in HK \Rightarrow x^{-1} = h'k' \text{ where}$$

$$h' \in H, k' \in K$$

$$h \in H \Rightarrow h^{-1} \in H; k \in K \Rightarrow k^{-1} \in K$$

$$\therefore x = (hk)^{-1} = k^{-1}h^{-1} \in KH. \therefore HK \subseteq KH$$

Let $x \in KH$

$$x \in KH \Rightarrow x = kh; k \in K, h \in H$$

$$h \in H \Rightarrow h^{-1} \in H; k \in K \Rightarrow k^{-1} \in K$$

$$h^{-1} \in H \text{ and } k^{-1} \in K \Rightarrow h^{-1}k^{-1} \in HK \Rightarrow (kh)^{-1} \in HK$$

$$\Rightarrow [(kh)^{-1}]^{-1} \in HK \Rightarrow kh \in HK \Rightarrow x \in HK$$

$$\therefore KH \subseteq HK$$

$$HK \subseteq KH, KH \subseteq HK \Rightarrow HK = KH$$

conversely suppose that $HK = KH$

$$H \neq \emptyset, K \neq \emptyset \Rightarrow HK \neq \emptyset$$

Let $a, b \in HK$

$a \in HK \Rightarrow a = h_1 k_1$, where $h_1 \in H, k_1 \in K$
 $b \in HK \Rightarrow b = h_2 k_2$ where $h_2 \in H, k_2 \in K$.
 $k_2 \in K \Rightarrow k_2^{-1} \in K; h_2 \in H \Rightarrow h_2^{-1} \in H$

$$k_1, k_2^{-1} \in K \Rightarrow k_1 k_2^{-1} \in K$$

$$k_1 k_2^{-1} h_2^{-1} \in KH = HK \Rightarrow k_1 k_2^{-1} h_2^{-1} = h_3 k_3$$

where $h_3 \in H, k_3 \in K$

$$ab^{-1} = (h_1 k_1) (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_3 k_3 \in HK$$

$\therefore HK$ is a subgroup of G .

Cyclic Subgroups

Let G be a group and

$a \in G$ the subgroup generated by set $\{A\}$ is called cyclic

subgroup of G generated by a .

The element a is called generator of the cyclic subgroup.

This cyclic subgroup is denoted by $\langle a \rangle$ (generator of a)

① Theorem: - If it is a subgroup of a group G and if $g \in G$ and $gHg^{-1} = H$

$\{g h g^{-1} : h \in H\}$, then prove that

$g H g^{-1}$ is a subgroup of G

proof :-

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

clearly gHg^{-1} is a non empty subset of G .

Let $a, b \in gHg^{-1} \Rightarrow a = gh_1g^{-1}$,

where $h_1 \in H$

$$b \in gHg^{-1} \Rightarrow b = gh_2g^{-1}$$

where $h_2 \in H$

$h_1, h_2 \in H$, H is a subgroup of G

$$\Rightarrow h_1h_2^{-1} \in H$$

$$\text{Now } ab^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1g^{-1}(g^{-1})^{-1}h_2^{-1}g^{-1}$$

$$= gh_1h_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}$$

$\therefore gHg^{-1}$ is a subgroup of G .

Cosets definition :-

Let H be a subgroup of a group G and $a \in G$. Then $Ha =$

$\{ha : h \in H\}$ is called right

coset of H in G and $aH =$

$\{ah : h \in H\}$ is called left coset

of H in G .

① Theorem: - Let H be a subgroup of a group G , and $a \in G$. Then

$$(i) a \in H \Leftrightarrow Ha \supseteq H$$

$$(ii) a \in H \Leftrightarrow aH \supseteq H$$

Proof: -

i) Suppose $a \in H$

Let $x \in Ha \Rightarrow x = ha$ where $h \in H$

$$h \in H, a \in H \Rightarrow ha \in H \Rightarrow x \in H$$

$$\therefore Ha \subseteq H.$$

Let $x \in H$

$$x \in H, a \in H \Rightarrow xa^{-1} \in H$$

Let $h = xa^{-1} \in H$. Then $x = ha \in Ha$.

$$\therefore H \subseteq Ha$$

$$Ha \subseteq H, H \subseteq Ha \Rightarrow Ha \supseteq H$$

Conversely suppose that $Ha \supseteq H$.

$$\text{Now } a = ea \in Ha \supseteq H \Rightarrow a \in H$$

ii) Suppose $a \in H$

Let $x \in aH \Rightarrow x = ah$ where $h \in H$

$$h \in H, a \in H \Rightarrow ah \in H \Rightarrow x \in H$$

$$\therefore aH \subseteq H.$$

Let $x \in H$

$$x \in H, a \in H \Rightarrow xa^{-1} \in H$$

Let $h = xa^{-1} \in H$. Then $x = ah \in aH$

$$\therefore H \subseteq aH$$

$$aH \subseteq H, H \subseteq aH \Rightarrow aH = H$$

Conversely suppose that $aH = H$.

$$\text{Now } a = ea \in aH = H \Rightarrow a \in H$$

Corollary: Let H be a subgroup of group G and $a \in G$. Then $a \in H \Leftrightarrow aH = H = Ha$.
 write the proof of above theorem.

2. Theorem :- Let H be a subgroup of a group G and $a, b \in G$. Then

$$i) a \in Hb \Leftrightarrow Ha \subseteq Hb$$

$$ii) a \in bH \Leftrightarrow aH \subseteq bH$$

Proof :-

(i) Suppose $a \in Hb$

$$a \in Hb \Rightarrow a = hb \text{ where } h \in H \Rightarrow b = h^{-1}a \\ \text{where } h^{-1} \in H$$

$$\text{Let } x \in Ha$$

$$x \in Ha \Rightarrow x = h_1 a \text{ where } h_1 \in H \Rightarrow x = h_1 (hb) \\ = (h_1 h) b \in Hb$$

$$\therefore Ha \subseteq Hb$$

$$\text{Let } x \in Hb$$

$$x \in Hb \Rightarrow x = h_2 b \text{ where } h_2 \in H \Rightarrow x = h_2$$

$$(h^{-1} a) = (h_2 h^{-1}) a \in Ha$$

$$\therefore Hb \subseteq Ha$$

$$Ha \subseteq Hb, Hb \subseteq Ha \Rightarrow Ha = Hb$$

conversely Suppose that $Ha = Hb$

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

ii) Suppose that $a \in bH$

$$a \in bH \Rightarrow a = bh \text{ where } h \in H \Rightarrow b = ah^{-1}$$

where $h^{-1} \in H$

$$\text{Let } x \in aH$$

$$x \in aH \Rightarrow x = ah, \text{ where } h \in H \Rightarrow x = (bh)h^{-1} = b(hh^{-1}) \in bH$$

$$\text{Let } x \in bH$$

$$x = bh_1 \text{ where } h_1 \in H$$

$$\Rightarrow x = (ah^{-1})h_1 = a(h^{-1}h_1) \in aH$$

$$\therefore bH \subseteq aH$$

$$aH \subseteq bH, bH \subseteq aH \Rightarrow aH = bH$$

conversely $aH = bH$

$$\text{Now } a = ae \in aH = bH \Rightarrow a \in bH$$

Theorem:-

① Let H be a subgroup of a group G

and $a, b \in G$ then

$$(1) Ha = Hb \Leftrightarrow ab^{-1} \in H$$

$$(2) aH = bH \Leftrightarrow ab^{-1} \in H$$

Theorem:-

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

5. Theorem:-

Any two right cosets of a subgroup
of a group are either disjoint or
identical.

Any two left cosets of a subgroup
of a group are either disjoint or
identical.

Proof:-

Let H be a subgroup of a group G .

① Let Ha, Hb be two right
cosets of H in G .

Suppose $Ha \cap Hb \neq \emptyset$.

Let $c \in Ha \cap Hb$.

$$c \in Ha \cap Hb \Rightarrow c \in Ha, c \in Hb$$

$$c \in Ha \Rightarrow Hc \subseteq Ha$$

$$c \in Hb \Rightarrow Hc \subseteq Hb$$

$$Ha \supseteq Hc \subseteq Hb$$

$\therefore$ Any two right cosets of H in G
are either disjoint or identical.

② Let aH, bH be left cosets of H in G .

Suppose $aH \cap bH \neq \emptyset$

Let $c \in aH \cap bH$

$c \in aH \cap bH \Rightarrow c \in aH, c \in bH$

$c \in aH \Rightarrow cH = aH$

$c \in bH \Rightarrow cH = bH$

$aH = cH = bH$

$\therefore$ Any two left cosets of H in G

are either disjoint or identical.

6. Theorem:-

Note:-

① If H is a subgroup of a group G then there exists a one one correspondence between any two left

coset of H in G

$$f(x_1) = f(x_2)$$

$$\Rightarrow x_1 = x_2$$

② If H is a subgroup of a finite group of G then any two left or right cosets of H have the same number of elements.

⑦

Theorem :-

If H is a subgroup of G then there exist a one to one correspondence between the set of all distinct left cosets of H in G and the set of all distinct right cosets of H in G .

Let L be the set of all left cosets and R be the set of all right cosets of H in G .

Thus, $L = \{aH : a \in G\}$, $R = \{Ha : a \in G\}$

define f from L to R as

$$f(aH) = Ha^{-1} \quad \forall aH \in L$$

If $aH \in L$

Then, $f(aH) = Ha^{-1} \in R$

Let $aH, bH \in L$ and $aH = bH$

$$aH = bH \Rightarrow a^{-1}b \in H$$

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

$$\Rightarrow Ha^{-1} = Hb^{-1}$$

$$f(aH) = f(bH)$$

$\therefore f: L \rightarrow R$ is a mapping

Let $aH, bH \in L$ & $f(aH) = f(bH)$

$$Ha^{-1} = Hb^{-1}$$

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

$$\Rightarrow a^{-1}b \in H$$

$$\Rightarrow aH = bH$$

$\therefore f: L \rightarrow R$ is one-one

Let $Ha \in R$

$$Ha \in R \Rightarrow a \in G$$

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

$$\Rightarrow a^{-1}Ha \in L$$

$$\text{Now } f(a^{-1}H) = H(a^{-1})^{-1} = Ha$$

$\therefore f: L \rightarrow R$ is onto

$\therefore f: L \rightarrow R$ is one one, and onto.

$\therefore$ There exist a one to one correspondence between the set of all left cosets of H in G and the set of all right cosets of H in G .

Congruent Module a subgroup of H.

Let H be a subgroup of group G and $a, b \in G$ then a is said to be congruent to b module H if

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

It is denoted by $a \equiv b \pmod{H}$.

① Theorem :- If H is a subgroup of a group then the relation congruent modulo H is an ^{equivalence relation} in G .

proof :-

Let $a \in G$ now

$$\text{now } aa^{-1} = e \in H \Rightarrow a \equiv a \pmod{H}$$

$\therefore$ congruent modulo H is reflexive

Let $a, b \in G$ and $a \equiv b \pmod{H}$

$$\Rightarrow a \equiv b \pmod{H}$$

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

$$(ab^{-1})^{-1} \in H$$

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

$$ba^{-1} \in H$$

$$\Rightarrow b \equiv a \pmod{H} \quad (\text{by definition})$$

$\therefore$ congruent modulo H is symmetric.

Let $a, b, c \in G$ and $a \equiv b \pmod{H}$,

$$b \equiv c \pmod{H}, \forall a, b, c$$

$$a \equiv b \pmod{H} \Rightarrow ab^{-1} \in H$$

$$b \equiv c \pmod{H} \Rightarrow bc^{-1} \in H$$

$$ab^{-1} \in H, bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) \in H$$

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

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

$$a^{-1} \in H$$

$$a \equiv c \pmod{H}$$

$\therefore$ congruent modulo H is transitive

$\therefore$ congruent modulo H is an equivalence relation.

Note:-

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

The equivalence class containing a with respect to the equivalence relation congruent modulo H is denoted by $[a]$.

$$\text{Now } [a] = \{x \in G : x \equiv a \pmod{H}\}$$

Lagrange's theorem:

Imp

Statement:-

(1)

If H is a subgroup of a finite group G then order of H divides order of G ($|H| \mid |G|$)

Proof:- Since H is a subgroup of G and G is finite, there are $|H|$ cosets of H in G and the number of right cosets of H in G is also finite. Since, there is a one to one correspondence between any

two right cosets of H in G .

for any $a \in G$ $|O(Ha)| = |O(He)| = |O(H)|$

Let $Ha_1, Ha_2, \dots, Ha_k$ be the disjoint right cosets of H in G

Since, G is the union of disjoint right cosets of H in G .

$$\therefore G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$$

Thus order of G (or $|G|$)

$$|G| = |Ha_1 \cup Ha_2 \cup \dots \cup Ha_k|$$

$$= |Ha_1| + |Ha_2| + \dots + |Ha_k|$$

$$= |H| + |H| + \dots + |H|$$

$$= k |H|$$

k times order of H

$\therefore |H|$ divides $|G|$

Definition :-

If H is a subgroup of group G then the cardinal number of disjoint right cosets of H in G is called index of H in G . it is denoted by $[G:H]$ or $I_G(H)$

order of an element in a group :-

Definition :- Let G be a group and $a \in G$. if there exist a positive integer n such that

$a^n = e$ is called order of a . it is denoted by $o(a) = n$. if there exist no positive integer n such that $a^n = e$ then the order of a is denoted to be ∞ or infinity.

① problem:-

Find the order of each element of the multiplicative group $\{1, -1, i, -i\}$

proof:-

$$\Rightarrow 1^1 = 1$$

order of 1 is 1

$$\Rightarrow (-1)^2 = 1$$

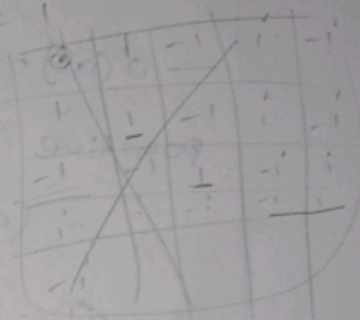
order of -1 is 2

$$\Rightarrow (i)^4 = 1$$

order of i is 4

$$\Rightarrow (-i)^4 = 1$$

order of $-i$ is 4



② And the order of each element of the group $(\mathbb{Z}_6, +)$

order of (0) is 1

$$o(1) = 6$$

$$o(2) = 3$$

$$o(3) = 2$$

$$o(4) = 3$$

$$o(5) = 6$$

Theorem :-

Let G be a group if $a \in G$
then order of a $o(a) = o(a^{-1})$

Proof :- Let $o(a) = m$, $o(a^{-1}) = n$

$o(a) = m \Rightarrow m$ is the least
positive integer such that

$$a^m = e$$

$o(a^{-1}) = n \Rightarrow n$ is the least
positive integer such that

$$(a^{-1})^n = e$$

$$a^n = (a^{-1})^{-1} = [(a^{-1})^n]^{-1}$$

$$= e^{-1} = e \Rightarrow m \leq n$$

$$(a^{-1})^m = a^{-m} = (a^m)^{-1} = e^{-1} = e \Rightarrow n \leq m$$

$$m \leq n, n \leq m \Rightarrow m = n$$

$$o(a) = o(a^{-1})$$

Theorem :-

The order of every element
in a finite group is finite.

proof :- Let G be a finite group
and $a \in G$

$$a \in G \Rightarrow a^2 \in G$$

$$a, a^2 \in G \Rightarrow a^3 \in G$$

by Induction

$$a^n \in G \quad \forall n \in \mathbb{N}$$

$$\therefore \{a, a^2, a^3, \dots\} \subseteq G$$

Since G is finite, $a^x = a^y$

for some positive integers x and y

Such that, $x > y$

Now $x - y \in \mathbb{N}$ and $a^{x-y} = a^x a^{-y}$

$$\begin{aligned} a^{x-y} &= a^x a^{-y} \\ &= a^y a^{-y} \\ &= a^y (a^y)^{-1} \\ &= e \end{aligned}$$

$$a \cdot a^{-1} = e$$

$$\text{let } S = \{m \in \mathbb{N} : a^m = e\}$$

clearly $x - y \in S$

Thus, S is non empty subset of $\mathbb{N}$.

by well ordering principle, S has least element. Let n be the

least element in S .
 $\therefore n$ is the least positive integer

such that $a^n = e$

$\therefore o(a) = n$ which is finite.

Let G be a group and $a \in G$
 such that $o(a) = n$ then $a^n = e$

Suppose that $a^m = e$.

$0 \neq n, m \in \mathbb{Z} \Rightarrow$ by division algorithm
 there exist $q, x \in \mathbb{Z} \Rightarrow n = nq + x$

where $0 \leq x < n$

Now

$$\begin{aligned} a^x &= a^{m-nq} \\ a^x &= a^{m-nq} \\ &= a^m a^{-nq} \\ &= a^m (a^n)^{-q} \\ &= e (a^n)^{-q} \\ &= e (e)^{-q} \\ &= e \end{aligned}$$

$$a^n = e$$

~~also~~ $o(a) = n \Rightarrow n$ is the least
 positive integer such that $a^n = e$

$$a^x = e, 0 \leq x < n$$

$$\Rightarrow x = 0$$

$$\therefore m = nq$$

$$n/m$$

conversely suppose that n/m

$n/m \Rightarrow m = na$ for some integer a

x and n
are
same

$$a^m = a^n$$

~~is~~

$$2(a^n)^2$$

$$= e^2 = e$$

if G is a finite group and $a \in G$

$$\text{then } o(a) \leq o(G)$$

proof:- $a \in G \Rightarrow \langle a \rangle$ ^{generated by a} is a subgroup of G

$$\Rightarrow \langle a \rangle \subseteq G$$

$$\Rightarrow o(\langle a \rangle) \leq o(G)$$

$$o(a) \leq o(G)$$

corollary:-

if G is a finite group and $a \in G$ and then

$$o(a) \mid o(G)$$

proof:- $a \in G$ $\langle a \rangle$ is a

subgroup of G by Lagrange's theorem

$$o(\langle a \rangle) \mid o(G)$$

$$\Rightarrow o(a) \mid o(G)$$

(write the proof of Lagrange's theorem)

In a group G for $a, b \in G$, if $o(a) = 5$, $b \neq e$ and $aba^{-1} = b^4$, find $o(b)$.

Sol:

$$(aba^{-1})^2 = aba^{-1}aba^{-1} = abeba^{-1} = abba^{-1} = aba^{-1} \\ = aaba^{-1}a^{-1} = a^2ba^{-2}$$

$$\Rightarrow (aba^{-1})^4 = [(aba^{-1})^2]^2 = (a^2ba^{-2})^2 = a^4ba^{-4} \\ = a^4b^4a^{-4} = a^4aba^{-1}a^{-4} = a^3ba^3$$

$$\Rightarrow (aba^{-1})^8 = [(aba^{-1})^4]^2 = (a^3ba^3)^2 = a^3ba^3a^3ba^3 \\ = a^3b^4a^{-3} = a^3aba^{-1}a^{-3} = a^4ba^{-4}$$

$$\Rightarrow (aba^{-1})^{16} = [(aba^{-1})^8]^2 = (a^4ba^{-4})^2 = a^4ba^4a^4ba^{-4} \\ = a^4b^4a^{-4} = a^4aba^{-1}a^{-4} = a^5ba^5$$

But $o(a) = 5 \Rightarrow a^5 = e, a^5 = e$.

$$\therefore (aba^{-1})^{16} = a^5ba^5 = ebe = b$$

$$\Rightarrow (b^4)^{16} = b$$

$$\Rightarrow b^{64} = e$$

$$\Rightarrow o(b) | 64.$$

Since 31 is a prime, $o(b) = 1$ or $o(b) = 31$.

But $b \neq e$, hence $o(b) = 31$.