UNIT - 2

ALGEBRAIC STRUCTURES

BINARY OPERATIONS: (COMPOSITIONS)

→ Let A be a non empty set then f^n $f: A \times A \to A$ is said to be binary op^r on A.

$g: A \to A$ (Unary op^r on A)

$A \times A \times A \to A$ (Ternary op^r on A) and so on ...

→ Thus binary op^r assigns each ordered pair of A to an element of A

Symbols used: $+, \times, \cdot, \circ, *, \oplus, \cup, \cap, \wedge, \vee$ etc.

Eg $+$ will be a binary op^r on A iff $a+b \in A$ for all $a, b \in A$ (CLOSURE PROPERTY)

also $a * b \in A$.

Illustrations :-

① '+' is binary op^r on set (N), I, Q, R and C also.

② '−' is binary op^r on set I, Q, R, C but not on N becoz $5-8 = -3 \notin N$

ALGEBRAIC STRUCTURE :-

A non empty set G equipped with with one or more binary op^r is called algebraic structure.

eg. $(G, *)$, $(G, \oplus)$, $(G, +, \cdot)$,

$(G, *, \circ, \vee, \wedge)$

PROPERTIES :- (AXIOMS)

Q1) CLOSURE :- $(G, *)$

$\forall\ a, b \in G$. then.

$a * b \in G$

eg $(N, +)$ — Yes.

$(I, +)$ — Yes

[$(I, -)$ — NO
$(N, -)$ — NO.
Example.]

Q2) ASSOCIATIVE PROPERTY :-

$\forall\ a, b, c \in G$.

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

[eqs $(N, +)$
$(N, -)$ — N
$(I, -)$ — No]

Q3) EXISTENCE OF IDENTITY ELEMENT :-

There exist a unique element 'e' $\in S$ such that for any $a \in S$,

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

then 'e' is called Identity Element.

eg $a * b = \frac{ab}{2}$ $(R, *)$

$a * e = e * a = a$

$a * e = \frac{ae}{2} = a$

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

$\boxed{e = 2}$ and $(2 \in R)$

(Q4) EXISTENCE OF INVERSE :-

There exict a unique element $a^{-1} \in S$ for all $a \in S$, such as :

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

then a^{-1} is called inverse of a

eg $(R, *)$ $a * b = \frac{ab}{2}$, find a^{-1}.

$a * e = e * a$

$e = 2$

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

$\frac{a * a^{-1}}{2} = 2$

$\boxed{a^{-1} = \frac{4}{a} \in R}$

(G5) COMMUTATIVE :-

If $\forall\, a, b \in G$ then

$$a * b = b * a.$$

---

(1) GROUPOID :- (G1)

An algebraic structure $(G, *)$ is said to be groupoid if it satisfies closure prop only.

(2) SEMI-GROUP :-

(CLOSURE + ASSOCIATIVE)

(G1, G2)

(3) MONOID :-

(CLOSURE + ASSOCIATIVE + IDENTITY)

(G1, G2, G3)

(4) GROUP :-

Let G be any non empty set together with operation * then A.S. $(G, *)$ is said to be group if it satisfies 4 conditions :-

Closure, associative, identity, inverse

(G1, G2, G3, G4)

ABELIAN GROUP :-

A group 'G' is said to be abelian if it satisfies the commutative property (G5)

(G1, G2, G3, G4, G5)

EXAMPLES OF BINARY OPR :-

(1) Let $A = \{0, 1, -1\}$ '+'

It is not a binary opr as $(-1) + (1) = -2$

$-2 \notin A$.

whereas (*) is a binary opr.

$\forall b, a \in A \quad a * b \in S$.

(2) Let $A = \{0, 1\}$; binary opr $\vee$ and $\wedge$

(COMPOSITE TABLE)

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

(YES)

(3) $S = \{a, b, c, d\}$ * on S defined by formula

$x * y = x$.

*	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

8) $(R, *)$ $a*b = \frac{ab}{2}$. check this associative, commutative, not

Sol^{n})

$$LHS = a*(b*c)$$
$$= \frac{abc}{4}$$
$$RHS = (a*b)*c$$
$$= \frac{abc}{4}$$

$\therefore (R, *)$ is associative.

9) Prepare the composition table for multiplication the element in set $A = \{1, \omega, \omega^2\}$ where ω is the cube root of unity. Show that multip (Abelian group).

Sol^{M} $\omega = \sqrt[3]{1}$ $\quad \omega^3 = 1$

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

① Closure :- if composition table contains only the elements of set A then closure law holds $(1, \omega, \omega^2) \in A$.

et Z be set of integers, show that op * on Z defined by $a*b = a+b+1 \quad \forall a, b \in Z$ is multiplicative abelian group.

① Closure :-

$\forall a, b, \in Z$

$a+b+1 \in Z$.

② Commutative :- Yes. $(a+b+1 = b+a+1)$

③ $(a+b+1) * c$ Associative

$\Rightarrow a+b+c+1+1$

$= a+b+c+2.$

$a*(b*c)$

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

$= a+b+c+2.$

LHS = RHS.

④. Identity :- .

$a*e = a = a+e+1 = a$

$e = -1 \in Z.$

So -1 is the identity element for * in Z.

⑤ Inverse :- $a*a^{-1} = e.$

$a*b = -1.$

$a+b+1 = -1$

$\boxed{b = -(2+a}$

(ii) Associative :-

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

$$1 \times (\omega \times \omega^2) = (1 \times \omega) \times \omega^2$$

$$1 \times \omega^3 = \omega^3$$

$$1 = 1.$$

(iii) Identity Element :-

$$a * e = a = e * a.$$

$$(e = 1)$$

(iv) Inverse :-

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

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

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

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

It satisfies the condition also.

as $\forall a \in A \ (a^{-1} \in A)$

(v) Commutative :-

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

In table it satisfies for all a and b $\in A$

(It is symmetric about the diagonals)

Let $A = \{a, b\}$. Which of the tables are monoid / semigroups?

(a)

*	a	b
a	b	b
b	a	a

Closure ✓
Associative ✓
No identity ✗.
(Not Monoid)
It is a semigrp.

(b)

*	a	b
a	a	b
b	b	a.

Closure, associative and identity

$a * e = a$

$\boxed{a * a = a}$

a is identity element

$b * e = b$

$\boxed{b * a = b}$

8) Show that the set of all +ve rational nos forms an abelian grp under the composition defined by $\left(a * b = \frac{ab}{2}\right)$

Sol^{n}) $(Q^+, *)$

① Closure: $\forall a, b \in Q^+$

then. $a * b \in Q^+$.

(ii) Associative :-

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

$$a*(b*c) = a*(bc/2)$$

$$= \frac{a(bc/2)}{2} = \frac{abc/2}{2}.$$

$$=$$

(iii) commutative :-

$$\forall\, a, b \in Q^+.$$

$$a*b = ab/2 = ba/2 = b*a.$$

(iv) Identity element :-

$$a*e = a = a*e.$$

$$a*e = \frac{ae}{2} = a$$

$$\boxed{e = 2} \qquad e \in Q^+.$$

(v) Inverses :-

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

$$\frac{aa^{-1}}{2} = 2$$

$$\boxed{a^{-1} = \frac{4}{a}} \qquad \frac{4}{a} \in Q^+$$

$\therefore (Q^+, *)$ is an Abelian group.

Show that set four roots of unity $(1, -1, i, -i)$ forms an abelian group with respect to multiplication. $(i = \sqrt{-1})$

Sol^{n}

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

Sol^{n} ①

Closure :- $\forall a, b \in G$.

$a \times b \in G$. Yes.

② Associative :-

$(1 \cdot i) \cdot (-i) = 1 \cdot [i(-i)] = 1$

It is associative

③ Identity :-

$a \times e = a = e \times a$

$a \times e = a$

$1 \times 1 = 1$

$i \times 1 = i$

$-i \times 1 = -i$

$e = 1$

(4) Commutative :-

$1(-1) = (-1)1 = -1$. (Yes)

(5) Inverse :-

$a \times a^{-1} = e$.

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

$(-1)^{-1} = -1 \quad \forall\ a^{-1} \in G$.

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

$(i)^{-1} = -i$ $\therefore$ This condition also satisfies.

9) Show that $G = \{1, 2, 3, 4, 5\}$ is not a group under addition modulo 5 and multiplication modulo 6.

Sol^{n}

$(a) +_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

$a \bmod q \Rightarrow$
$a = qn + b$
$n = \lfloor \frac{a}{q} \rfloor$

(Of G.) not closure
Hence not a group.

$\times_6$	1	2	3	4	5	$\notin G$
1	1	2	3	4	5	
2	2	4	0	2	4	
3	3	0	3	0	3	
4	4	2	0	4	2	
5	5	4	3	2	1	

$0 \notin G$

$(G, \times_6)$ is not a group.

Q). Prove $G = \{0, 1, 2, 3, 4\}$ is a finite abelian group under addition modulo 5. $(+_5)$

Sol^n

$+_5$	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

Yes it an Abelian grp.

$e = 0$

INVERSE

$\{ 0 - 0,\ 1 - 4,\ 2 - 3,\ 3 - 2,\ 4 - 1 \}$.

RESIDUE CLASSES of set of integers :—

Let $I = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$ be set of integers. Let $a, b \in I$ and m be the fixed +ve integer.

Relation of "congruence modulo m" in I.

Def:- Let m be a +ve integer, then the two integers a and b are said to be 'congruent modulo m" if $(a-b)$ is divisible by m as,

$$a \equiv b \pmod{m}$$

which is read as,

"a is congruent to b modulo m".

Eg:

(a) $8 \equiv 3 \pmod 5$

$\Rightarrow (8-3) = 5$ divisible by 5.

(b) $27 \equiv -3 \bmod 5$

$= 27 - (-3)$

$= 30$ which is divisible by 5.

(1) The identity element in a group is unique

PROOF

Let $a \in G$ and e, e' be two identities of G

$e \in G \quad a \in G \Rightarrow ae = a$ — (1)

$e' \in G \quad a \in G \Rightarrow ae' = a$ — (2)

$ae = ae'$

$\boxed{e = e'}$

(2) The inverse of each element of group is unique :—

PROOF Let $a \in G$ and $e \in G$.

Let a_1^{-1} and a_2^{-1} be inverses of $a, \in G$.

$a \in G \quad a_1^{-1} \in G \Rightarrow a a_1^{-1} = e$ — (1)

$a \in G \quad a_2^{-1} \in G \Rightarrow a a_2^{-1} = e$ — (2)

then, $a a_1^{-1} = a a_2^{-1}$

$a_1^{-1} = a_2^{-1}$

The inverse of product of two elements of group G is the product of inverse taken in reverse order. i.e

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

Proof: Let $a, b \in G$. If a^{-1} and b^{-1} are inverses of a and b. then

$$a^{-1}.a = e = aa^{-1}.$$
$$b^{-1}.b = e = bb^{-1}.$$

$(aa^{-1} = e)$ show this.

Now $(ab)(b^{-1}a^{-1})$

$$= a(bb^{-1})a^{-1}$$
$$= a.e.a^{-1}$$
$$= aa^{-1} = e$$

Also, $(b^{-1}a^{-1}).ab = b^{-1}(a^{-1}.a)b$

$$= b^{-1}.(eb)$$
$$= b^{-1}b$$
$$= e.$$

Thus $b^{-1}a^{-1}$ is the inverse of ab.

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

Proved

(4). For any element 'a' in a group G, prove that $(a^{-1})^{-1} = a$

PROOF Let 'e' be the identity of group G.

Then $a^{-1} \in G$.

So, $a \cdot a^{-1} = a^{-1} \cdot a = e$.

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

and $(a^{-1})^{-1}$ is inverse of (a^{-1})

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

Multiplying by 'a' both sides.

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

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

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

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

(5) CANCELLATION LAWS:-

(1) Left cancellation law:-

If a, b, c are any elements of G then

$ab = ac \Rightarrow b = c$

Right Cancellation law :-

If $a, b, c \in G$, and

$$b \cdot a = c \cdot a \Rightarrow b = c$$

Eg. $(\mathbb{Z}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{Z}, *)$ holds both laws.

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

$$ab = ac$$

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

$$(a^{-1}a)b = (a^{-1}a)c \quad \text{(Associative law)}$$

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

$$b = c$$

Also

$$ba = ca.$$

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

$$b(aa^{-1}) = c(aa^{-1}) \quad \text{(Associative law)}$$

$$be = ce$$

$$b = c$$

ORDER OF THE ELEMENTS of a Group :-

Let G be a group. By the order of the element $a \in G$, we mean the least positive integer 'n' such that

$$\boxed{a^n = e}$$

& 'e' is the identity element in G.

If there does not exist an integer 'n' satisfying $a^n = e$ then we say that the element $a \in G$ is of infinite order or zero order.

The order of element 'a' is denoted as

$$\boxed{o(a)}.$$

(Ex) Find the order of each element of the multiplicative group $G = \{1, -1, i, -i\}$.

Sol^n $(-1)^2 = 1$ $\boxed{(o(-1)) = 2}$

$(1)^1 = 1$ $\boxed{o(1) = 1}$

$(i)^4 = 1$ $\boxed{o(i) = 4}$

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

$$\boxed{o(-i) = 4}$$

Theorem: The order of an element $a \in G$. $(G, \cdot)$ is same as the order of a^{-1} i.e $O(a) = O(a^{-1})$

Proof: Let n and m be orders of a and a^{-1} i.e $O(a) = n$ and $O(a^{-1}) = m$.

(i) $O(a) = n \Rightarrow a^n = e$

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

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

$\therefore O(\bar{a}) = n$

Also (ii) $O(\bar{a}) = m$

$(\bar{a})^m = e$ $(\because e^{-1} = e)$

$(a^m)^{-1} = e \Rightarrow (a^m) = e$ because $b^{-1} = e \Rightarrow b$

Q) Let G is a group and $x^2 = 1$, $x \in G$. $(G, \cdot)$ Show that G is Abelian

Sol: Let a & $b \in G$,

then $a \cdot b \in G$ } closure prop.

Now $\because ab \in G$ then

$(ab)^2 = 1$

opening this, $(ab) \cdot (ab) = 1$

multiply (ba) both sides

$ab \cdot (ba)\, ab = ba$.

$\Rightarrow ab(a \cdot b^2 \cdot a) = ba$ } Associative law.

$ab(a^2) = ba$

$ab = ba$ $\therefore G$ is commutative

SUBGROUP :-

Let G be group then any non-empty subset H of G is called complex of group G. A non-empty H of group $(G, *)$ is said to be a subgroup if $(H, *)$ is also a group i.e $(G, *)$ is a group then the complex which satisfy all the axioms of group is said to be sub-group i.e all subgroups are complexes but all complexes are not subgroups.

⇒ If e is the identity element of G, then the subset of G containing only identity element is called as improper or trivial subgroups, others are proper or non-trivial subgroups.

Theorem (1) The identity element of subgroup is same as that of the group.

Proof Let H be the subgroup of G and suppose e, e' be its element (identity)

$e \in G$, $e' \in H$.

Now - if $a \in H$ then $a \in G$ and

$$ae = a \quad (\because e \in G)$$

again, $a \in H$ then $\quad (\because e' \in H)$

$$ae' = a$$

Thus $ae' = ae \Rightarrow e = e'$.

orem II: A non empty subset H of a group G is a subgroup of G, if and only if :—

(i) $a \in H \quad b \in H \Rightarrow a * b \in H$.

(ii) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G.

PROOF: NECESSARY CONDITION :-

Let $H \subseteq G$. 'H' is subgroup of 'G' then H must be closed with * i.e $a \in H, b \in H$

$\Rightarrow a * b \in H$.

Let $a \in H$; a^{-1} be inverse of a in G, then, a^{-1} is also the inverse of a in H.

Each element of H must possess inverse since H itself a group.

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

Theorem III: The necessary and sufficient condition for a non-empty subset H of group $(G, *)$ to be subgroup is $a \in H, b \in H \Rightarrow$

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

where b^{-1} is the inverse of b in G.

Proof: Let H is subgroup and $a \in H$, $b \in H$ since H is a subgroup and $b \in H$, so, 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.

To prove this condition is also sufficient we assume that.

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

we have to prove that H is subgroup of G.

① identity :-

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

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

$e \in H$

② inverse :-

Let $a \in H$ then

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

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

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

Thus each element of H possesses inverse.

③ CLOSORE :- $a, b \in H$ then.

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

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

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

This law satisfies in H because,

$\forall a, b, c \in H \Rightarrow a, b, c \in G$.

$(ab)c = a(bc)$ (By associative law)

$\therefore (ab)c = a(bc) \ \forall \ a, b, c \in H$.

$\therefore$ H is a subgroup of G.

Theorem The intersection of any subgroups of group $(G, *)$ is again a subgroup of $(G, *)$

PROOF Let H_1 and H_2 forms any two subgroups of $(G, *)$. We have $H_1 \cap H_2 \neq \phi$ as identity element is common to both H_1 and H_2

Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$.

Now, $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$.

Since H_1 & H_2 from subgroups under $(G, *)$

then $a \in H_1, b \in H_1 \Rightarrow a * b^{-1} \in H_1$

$a \in H_2, b \in H_2 \Rightarrow a * b^{-1} \in H_2$.

Finally, $ab^{-1} \in H_1$, $ab^{-1} \in H_2$

mf

$\therefore \quad a * b^{-1} \in H_1 \cap H_2$.

Thus, $a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow$

$a * b^{-1} \in H_1 \cap H_2$.

$\therefore (H_1 \cap H_2)$ forms a subgroup under $(G, *)$

Theorem Union of two subgroups is not necessarily a subgroup.

Proof Suppose G be additive group of integers then

$H_1 = \{0, \pm 2, \pm 4, \pm 6 \cdots\}$

$H_2 = \{0, \pm 3, \pm 6, \pm 9 \cdots\}$

are both subgroups of G.

Now, $H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9\}$

Obviously $H_1 \cup H_2$ is not closed with addition

as $3 + 4 = 7 \notin H_1 \cup H_2$ (Not Closure)

$H_1 \cup H_2$ is not a subgroup of G.

$\therefore$

8) Find the orders of each element of multiplicative group $\{1, \omega, \omega^2\}$

Sol^n $e = 1$.

$a^n = e$.

$a^n = 1$.

① $(1)^1 = 1$

$O(1) = 1$

② $(\omega)^3 = 1$

$O(\omega) = 3$.

③ $(\omega^2)^3 \Rightarrow (\omega^3)^2 = (1)^2 = 1$.

$O(\omega^2) = 3$.

Theorem If H is any subgroup, then $HH = H$.

Proof Let $h_1 h_2$ be any element of HH where $h_1 \in H$ and $h_2 \in H$.

Since H is the subgroup of G. therefore,

$h_1 h_2 \in HH \Rightarrow$

$h_1 h_2 \in H$.

$\therefore \quad HH \subseteq H$

Now, let h be any element of H, then

$h = he$.

$h \in H, e \in H \Rightarrow he \in HH$.

$H \subseteq HH$.

Hence, $H = HH$.

COSETS

Suppose G is a group and H is any subgroup of G let 'a' be any element of G, then the set

$Ha = \{ha : h \in H\}$

is called right coset of H in G generated by 'a'

Similarly, $aH = \{ah : h \in H\}$. — left coset of H in G generated by 'a'.

$\Rightarrow$ If e is the identity element of G, then

$He = H = eH$.

$\therefore$ H itself is a right as well as left coset.

$\Rightarrow$ If the group G is abelian then we have $ah = ha \ \forall \ h \in H$ $\therefore$ right coset Ha will be equal to the corresponding left coset aH.

if the group operation is addition then right coset of H in G generated by 'a' is defined as $\boxed{H+a = \{h+a : h \in H\}}$

and left coset is $\boxed{a+H = \{a+h : h \in H\}}$

→ If H is a subgroup of group G, then the no of distinct left or right cosets of H in G is called index of H in G. and is denoted as $[G:H]$ or by $i_G(H)$.

Ex: If G is an additive group of all integers and H is additive subgroup of all even integers of G, then find all the cosets of H in G.

Sol^n

$$G = \{0, \pm 1, \pm 2, \cdots\}$$
$$H = \{0, \pm 2, \pm 4, \pm 6 \cdots\}.$$

let $0, 1, 2 \cdots \in G$ then.

$$H+0 = \{0, \pm 2, \pm 4, \pm 6 \cdots\}$$
$$H+1 = \{0+1, \pm 2+1, \pm 4+1 \cdots\}$$
$$= \{\cdots 3, -1, 1, 3 \cdots\}$$
$$H+2 = \{0+2, \pm 2+2, \pm 4+2 \cdots\}$$
$$= \{\cdots -4, -2, 0, 2, 4 \cdots\}$$
$$= H.$$

Hence H and $H+1$ are two distinct cosets.

2) Find all left & right cosets of H in G,

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

Sol^n

LEFT COSETS

$aH = \{ah : h \in H\}$.

$1 \times H = \{1\times 1, 1\times -1\} = \{1, -1\} = H$.

$-1 \times H = \{-1\times 1, -1\times -1\} = \{-1, 1\} = H$.

$i \times H = \{i\times 1, i\times -1\} = \{i, -i\} \neq H$.

$-i \times H = \{-i\times 1, -i\times -1\} = \{-i, i\} \neq H$.

RIGHT COSETS:-

$H\times 1 = \{1\times 1, 1\times -1\} = \{1, -1\} = H$.

$H\times -1 = \{-1\times 1, -1\times -1\} = \{-1, 1\} = H$.

$H\times i = \{1\times i, -1\times i\} = \{i, -i\} \neq H$.

$H\times -i = \{1\times -i, -1\times -i\} = \{-i, i\} \neq H$.

NOTE! Ha and aH are subsets of G and they may / may not be equal to H.

CYCLIC GROUPS:-

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

→ Every cyclic group is abelian grp.

multiplicative group $G = \{1, -1, i, -i\}$ is cyclic

$$G = \{i, i^2, i^3, i^4\} \Rightarrow \langle i \rangle$$

⇒ This $-i$ is also the generator as

$$G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$$

$$\langle -i \rangle.$$

→ So there may be more than one generator of a cyclic group.

→ If G is a cyclic group generated by 'a' it is denoted by $G = \langle a \rangle$.

The elements of G are in form.

$$\cdots a^{-2}, a^{-1}, a^0, e, a, a^2 \cdots$$

The group $(G, +_6)$ is cyclic group where

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

Sol^n $1^1 = 1$, $1^2 = 1 +_6 1 = 2$, $1^3 = 1 +_6 1^2 = 3$

$1^4 = 1 +_6 1^3 = 1 +_6 3 = 4$.

$1^5 = 1 +_6 1^4 = 1 + 4 = 5$

$1^6 = 0$.