Unit - 4 Group theory

Definition, properties of groups, sub groups, cyclic groups. (1)

Groups:- A non empty set G with a binary operation $*$ is said to be a group. If the following axioms are satisfied.

$G_1 \Rightarrow$ Closure law:-

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

$G_2 \Rightarrow$ Associative law:-

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

$G_3 \Rightarrow$ Existence of identity

For every element $a \in G\ \exists$ an element $e \in G$ then,

$a * e = e * a = a$

Here $e =$ identity of G.

$G_4 \Rightarrow$ Existence of inverse :-

For every element $a \in G\ \exists$ an element $a^{-1} \in G$

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

Here a^{-1} is called the inverse of a.

$G_5 \Rightarrow$ Commutative law:-

$\forall\ a, b \in G$ then $a * b = b * a$

$\therefore$ G is called an abelian group.

Eg:- $(Z, +)$ $(R, +)$, $(C, +)$. . .

1) The set $G = \{1, -1, i, -i\}$ i.e, the fourth root of unity I.6 of. group with usual multiplication. where $i^4 = 1$ & $i^2 = -1$

Soln:- Given, $G = \{1, -1, i, -i\}$ with multiplication.

The operation table for the 4th root unity with usual (x) plication

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

$i \cdot i = i^2 = -1$

$i \cdot -i = -i^2 = 1$

$G_1 \Rightarrow$ Closure law:-

$\forall\ 1, i \in G$ then $1 \cdot i = i \in G$

$G_2 \Rightarrow$ Associative law:-

$\forall\ -1, i, -i \in G$

then $(-1 \times i) \times (-i) = -i \times -i = i^2 = -1$ — (1)

$-1 \times (i \times -i) = -1 \times (-i^2) = i^2 = -1$ — (2)

$G_3 \Rightarrow$ Existence of identity:-

Since multiplication is the binary composition $1 \in G$ then for every $i \in G$ we have

$1 \cdot i = i \cdot 1 = i \in G$

$G_4 \Rightarrow$ Existence of inverse:-

For every $i \in G$ $\exists$ $-i$ such that $i \times (-i) = -i^2 = 1$

$\therefore$ For i, $-i$ is the inverse.

Illy For -1, -1 is itself is the inverse.

$G_5 \Rightarrow$ Commutative law:-

$\forall\ i, -i \in G$ then $i \times (-i) = -i \times i = -i^2 = 1$

$\therefore$ The group G is an abelian group.

$\therefore$ The set fourth root of unity is an abelian group with respect to multiplication.

cenity

$Z_6 = \{0,1,2,3,4,5\}$ write the operation table for addition modulo 6.

Soln:

$+_6$	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

Theorem:-

1) In a group, $\exists$ only one identity element.

[i.e, The identity element in a group is unique.]

Proof:- In a group G,

Let $a \in G$, if possible let us consider e_1 and e_2 are the two identities of G,

then $a * e_1 = e_1 * a = a$ —— (1)

$a * e_2 = e_2 * a = a$ —— (2)

$\therefore$ (1) = (2)

$\therefore a * e_1 = a * e_2$

$\Rightarrow ae_1 = ae_2$

$\Rightarrow e_1 = e_2$

$\therefore$ The identity element is unique.

Theorem-2

* In a group G, every element has only one inverse
[i.e, Every element has a unique inverse in G.]

Proof:- In a group G,

for every element $a \in G$,

~~let us~~ suppose that b and c are the two inverse

such that $a \times b = b \times a = e$ — ①

$a \times c = c \times a = e$ — ②

① = ②

$\Rightarrow a \times b = a \times c$

$\Rightarrow ab = ac$

$\Rightarrow b = c$

a' & a'' are inverse of an element $a \in G$

$\therefore a' = a'e$

$= a'(a a'')$

$= (a' a) a''$

$= e a''$

$a' = a''$

$\Rightarrow$ The inverse element of 'a' which are b and c is unique.

Order of a group:

The no of elements in a group G is called the order of the group and is denoted by order of G or $O(G)$.

Order of an element:

Let G be a group and let 'a' be an element of G. The order of an element $a(G)$ is defined as, let 'n' be the least +ve integer such that $a^n = e$ & it is denoted as $O(a)$.

Que) Find order of element $\{0,1,2,3,4,5\}$ w.r.t $\oplus_6$

Soln:- Since '0' is the identity element.

$0^1 = 0 \Rightarrow O(0) = 1$

$1^1 = 1$

$1^2 = 1 \oplus_6 1 = 2$

$1^3 = 1 \oplus_6 1 \oplus_6 1 = 3$

$1^4 = 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$

$1^5 = 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 5$

$1^6 = 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 6-6 = 0$

$\therefore O(1) = 6$

$2^1 = 2$

$2^2 = 2 \oplus_6 2 = 4$

$2^3 = 2 \oplus_6 2 \oplus_6 2 = 6-6 = 0$

$\therefore O(2) = 3$

$3^1 = 3$

$3^2 = 3 \oplus_6 3 = 6-6 = 0$

$\therefore O(3) = 2$

$4^1 = 4$

$4^2 = 4 \oplus_6 4 = 8-6 = 2$

$4^3 = 4 \oplus_6 4 \oplus_6 4 = 12-6 = 6-6 = 0$

$\therefore O(4) = 3$

$5^1 = 5$

$5^2 = 5 \oplus_6 5 = 10-6 = 4$

$5^3 = 5 \oplus_6 5 \oplus_6 5 = 15-6 = 9-6$
$= 3$

$5^4 = 5 \oplus_6 5 \oplus_6 5 \oplus 5 = 20-6$
$= 14-6$
$= 8-6 = 2$

$5^5 = 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5$
$= 25-6 = 19-6 = 13-6$
$= 7-6 = 1$

$5^6 = 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5$
$= 30-6 = 24-6 = 18-6$
$= 12-6 = 6-6 = 0$

$\therefore O(5) = 6$

Problems:-

1) The set of all integers defined by $a*b = a+b+1 \ \forall a,b$ is a group.

Soln:- Given $(Z,*) = \{a*b = a+b+1 / a,b \in Z\}$

$G_1 \Rightarrow$ Closure law:-

$\forall a,b \in (Z,*)$

then consider $a*b = a+b+1 \in Z$

$G_2 \Rightarrow$ Associative law:-

$\forall a,b,c \in (Z,*)$

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

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

$= a+b+c+2$ —①

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

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

$= a+b+c+2$ —②

$\therefore$ ① = ②

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

$G_3 \Rightarrow$ Existence of Identity:-

For every $a \in (Z,*)$

then $\exists \ e \in (Z,*)$ such that $a*e = a$

$\Rightarrow a+e+1 = a$

$\Rightarrow e+1 = 0$

$\Rightarrow e = -1$

$\therefore e = -1$ is the identity of $(Z,*)$

$G_4 \Rightarrow$ Existence of Inverse:-

$\forall\ a, b \in (z, *)\ \exists\ a^{-1} \in (z, *)$

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

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

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

$\Rightarrow a + a^{-1} + 1 = -1 \quad \Rightarrow a^{-1} = -1 - 1 - a$

$\Rightarrow a^{-1} = -(a+2)$ or $-a-2$

$\therefore \forall\ a \in (z, *)$ its inverse $a^{-1} = -(a+2) \in (z, *)$.

$\therefore (Z, *)$ is a group.

Q) The set of all +ve rational no. forms an abelian group under the composition defined by $a * b = ab/2$

Soln :-

Given, $G = \{a * b = ab/2 \mid (a, b) \in Q\}$

$G_1 \Rightarrow$ closure law:-

$\forall\ (a, b) \in Q$ then by defination $a * b = ab/2 \in Q$

$G_2 \Rightarrow$ Associative law:-

For every $(a, b) \in Q$,

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

$$= \frac{\frac{ab}{2} * c}{2} = \frac{abc}{4} \quad \text{--- (1)}$$

Again consider $a * (b * c) = a * \frac{bc}{2}$

$$= \frac{a * \frac{bc}{2}}{2} = \frac{abc}{4} \quad \text{--- (2)}$$

$\therefore (1) = (2)$

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

$G_3 \Rightarrow$ Existence of Identity:-

$\forall\ a \in G\ \exists$ an element $e \in G$

such that $a * e = e * a = a$

$\Rightarrow a * e = a$

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

$\Rightarrow \frac{e}{2} = 1$

$\Rightarrow e = 2$ is the identity of G.

$G_4 \Rightarrow$ Existence of inverse:-

For every $a \in G$, $\exists\ a^{-1} \in G$

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

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

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

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

$\Rightarrow aa^{-1} = 4$

$\Rightarrow a^{-1} = 4/a$

$\therefore$ The inverse of 'a' is a^{-1} which $= 4/a$

$G_5 \Rightarrow$ Commutative law:-

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

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

$\Rightarrow a * b = b * a$

$\therefore$ The given set G is an abelian group.

) ~~Let G be the set of real no. not equal to -1 and~~

) The set $(G,*) = \{a*b = a+b-ab \mid a,b \in Q\}$ is a group.

Soln:- $(G,*) = \{a*b = a+b-ab \mid a,b \in Q\}$

$G_1 \Rightarrow$ Closure law:-

$\forall\ a,b \in (G,*)$

then consider $a*b = a+b-ab \in G$

$G_2 \Rightarrow$ Associative law:-

$\forall\ a,b,c \in G, \Rightarrow (a*b)*c = (a+b-ab)*c$

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

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

$= a+b+c+abc-ab-ac-bc$ — ①

Again consider,

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

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

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

$= a+b+c+abc-ab-bc-ac$ — ②

① = ②

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

$G_3 \Rightarrow$ Existence of Identity:

For every $a \in (G,*)$ then $\exists\ e \in (G,*)$

such that $a*e = a$

$\Rightarrow a+e-ae = a$

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

$\Rightarrow e = 0$

$G_4 \Rightarrow$ Existence of inverse:-

$\forall\ a \in (G, *)$, $\exists\ a^{-1} \in (G, *)$

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

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

$\Rightarrow a * a^{-1} = 0$

$\Rightarrow a + a^{-1} - aa^{-1} = 0$

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

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

$G_5 \Rightarrow$ Commutative law:-

Let $a, b \in G$ $\exists$ $a * b = b * a$

$a * b = a + b - ab$ — (3)

$b * a = b + a - ba$ — (4)

$\therefore$ (3) & (4) holds good.

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

4) Find the order of group of elements of $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under $\otimes$plication module 15. and construct operation table. Also find inverse of each. Then find all x in $(U_{15}, \otimes_{15})$ such that $x = x^{-1}$

4Soln:- Given: Order of the group $= |U_{15}| = 8$

Here $e = 1$ is the identity element. ($\because$ xplication module)

$1^1 = 1 \Rightarrow O[1] = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 = 16 - 15 = 1 \Rightarrow \therefore O[2] = 4$

$4^1 = 4$

$4^2 = 16 - 15 = 1 \Rightarrow \therefore O[4] = 2$

IIIly $O[7] = 4$

$O[8] = 4$

$O[11] = 2$

$O[13] = 4$

$O[14] = 2$

$\otimes_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

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

$a = 2 \Rightarrow a^{-1} = 8$

$a = 4 \Rightarrow a^{-1} = 4$ - *

$a = 7 \Rightarrow a^{-1} = 13$

$a = 8 \Rightarrow a^{-1} = 2$

$a = 11 \Rightarrow a^{-1} = 11$ - *

$a = 13 \Rightarrow a^{-1} = 7$

$a = 14 \Rightarrow a^{-1} = 14$ - *

$\therefore x = 1, 4, 11, 14$ satisfies $x = x^{-1}$.

Sub
be

Finite Group:- A group G consisting of finite no of elements then it is called finite group.

Eg:- $(Z_6, \oplus_6)$

Infinite Group:- A group G consisting of infinite no of element, then it is called infinite group.

Eg:- $(Z, +)$

Subgroup :- A subset H of a group G is said to be a subgroup. If H itself is a group under the same binary composition defined on G.

Eg :- Consider a multiplicative group, 4^{th} root of unity

$G = \{1, -1, i, -i\}$ under $\otimes$

$\therefore H = \{1, -1\}$ is a subgroup of G.

Cyclic group :-

A group G is said to be cyclic group, generated by the element $a \in G$, if $G = \{a^n / n \in Z\}$

Here 'a' is called the generator of G

Then the cyclic group is denoted by $G = \langle a \rangle$

Eg :- Is the multiplicative group 1, 2, 3, 4, 5, 6 mod 7 is cyclic.

Soln :- $G = \{1, 2, 3, 4, 5, 6 \text{ mod } 7\}$ or $G = \{1, 2, 3, 4, 5, 6\} \otimes_7$

$1^1 = 1$	$2^1 = 2$	$3^1 = 3$	$4^1 = 4$	$5^1 = 5$	$6^1 = 6$
$1^2 = 1$	$2^2 = 4$	$3^2 = 9 = 2$	$4^2 = 2$	$5^2 = 4$	$6^2 = 1$
	$2^3 = 8 = 1$	$3^3 = 27 = 6$	$4^3 =$	$5^3 =$	
		$3^4 = 81 = 4$		$5^4 =$	
		$3^5 = 243 = 5$		$5^5 =$	
		$3^6 = 694 = 1$		$5^6 =$	

$\therefore$ The group contains two generators i.e, 3 & 5 $\therefore$ G is cyclic

Theorem :-

* For any elements a,b in a group G, we have

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

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

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

$\forall$ $a \in G$, $\exists$ a^{-1} such that $a \cdot a^{-1} = e$.

$$\Rightarrow a^{-1} \cdot a = e \quad \text{—} \; (1)$$

$\forall$ $a^{-1} \in G$ $\exists$ $(a^{-1})^{-1}$ such that $a^{-1}(a^{-1})^{-1} = e$

$$\Rightarrow (a^{-1})^{-1} \cdot a^{-1} = e \quad \text{—} \; (2)$$

$$(1) = (2)$$

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

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

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

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

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

$\Rightarrow$ For every $ab \in G$, $\exists$ $(ab)^{-1} \in G$

such that $(ab)(ab)^{-1} = (ab)^{-1}(ab) = e$ — (1)

For every ab, let us consider $b^{-1}a^{-1}$ such that

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$$
$$= a(e)a^{-1}$$
$$= aa^{-1}$$
$$= e \quad \text{—— (2)}$$

$$\therefore (ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e \quad \text{—— (3)}$$

(1) = (3)

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

Left cancelling (ab) on b/s.

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

1) Prove that the group $(Z_4, +)$ is cyclic. Find all its generators.

Soln:- It is given that $Z_4 = \{0, 1, 2, 3\}$ under addition modulo 4.

$1^1 = 1$

$1^2 = 1 \oplus_4 1 = 2$

$1^3 = 1 \oplus_4 1 \oplus_4 1 = 3$

$1^4 = 1 \oplus_4 1 \oplus_4 1 \oplus_4 1 = 4-4 = 0$

$2^1 = 2$

$2^2 = 2 \oplus_4 2 = 4-4 = 0$

$3^1 = 3$

$3^2 = 3 \oplus_4 3 = 6-4 = 2$

$3^3 = 3 \oplus_4 3 \oplus_4 3 = 9-4$
$= 5-4 = 1$

$3^4 = 3 \oplus_4 3 \oplus_4 3 \oplus_4 3 = 12-12 = 0$

$\therefore$ 1 & 3 is a generator.

$\therefore (Z_4, +)$ is a cyclic group.

(HW)
2) Prove that $(Z_5, \cdot)$ is a cyclic group. Find all generators. [zero is not included in Z_5 because it is ... under multiplication.]

3) Check whether $U = \{1, 2, 4, 5, 7, 8\}$ under $\otimes_9$ & find its generator.

Then ...

Coset :- 2nd chapter

Let $(G, *)$ be a group and $(H, *)$ be a subgroup.

For any $a \in G$, then $a * H = \{a * h \mid h \in H\}$

$H * a = \{h * a \mid h \in H\}$

Then $a * H$ is called left coset of H in G.

and $H * a$ is called right coset of H in G.

Theorem :- Lagrange's theorem

Statement :- If G is a finite group and H is a subgroup of G, then the order of H divides the order of G i.e, $O(H) / O(G)$.

Proof :- Since G is a finite group.

H is a subgroup of G.

$\therefore$ H is finite

$\therefore$ The no of cosets of H in G is finite.

Let $Ha_1, Ha_2, \ldots Ha_n$ be distinct right coset of H in G

Then by the right coset decomposition of G we have

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_n$$

& So that $O(G) = O(Ha_1) + O(Ha_2) + \dots + O(Ha_n)$

But WKT $O(Ha_1) = \dots = O(Ha_n) = O(H)$

$\therefore O(G) = O(H) + O(H) + \dots + O(H)$ (n-times)

$\therefore O(G) = n\,O(H)$

$$\Rightarrow \frac{O(G)}{O(H)} = n$$

$\therefore$ Thus order of group G divides order of subgroup H.

Hence the proof