Chapter-3
Finite groups; subgroups

Defⁿ :- order of a group :- The number of elements of a group (finite and infinite) is called order. We denote it as $|G|$ or $o(G)$.

Ex ① $U(10) = \{1, 3, 7, 9\}$ is group under multiplication ~~under~~ modulo 10 has order 4

② $Z = \{$ set of integers $\}$ is a group of infinite order.

Defⁿ :- order of an element :-

The order of an element g in a group G is the smallest positive integer n such that $g^n = e$ (~~in addit~~ (in addition, $ng = 0$). If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$ or $o(g)$.

Note :- We need to compute $g, g^2, g^3 \ldots$ until we reach the identity for the first time.

Ex $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15.

$\Rightarrow o(U(15)) =$ order of $U(15) = 8$

Now $7 \in U(15)$

$7^1 \bmod(15) = 7$

$7^2 \bmod(15) = 49 \bmod(15) = 4$

$7^3 \bmod(15) = 243 \bmod 15 = 13$

$7^4 \bmod(15) = 1$

$\Rightarrow |7| = o(7) = 4$

11y order(11) = ?

Ex $Z_{10} = \{0, 1, 2, \ldots, 9\}$

$o(2) = ?$

$2 \cdot 1 \bmod 10 = 2$

$2 \cdot 2 \bmod 10 = 4$

$2 \times 3 \bmod 10 = 6$

$2 \times 4 \bmod 10 = 8$

$2 \times 5 \bmod 10 = 0$

$\Rightarrow o(2) = |2| = 5$

$\Rightarrow o(0) = 1$

$o(7) = 10$

$o(5) = 2$

$o(6) = 5$

Ex Z = set of integer under addition every non-zero element has infinite order

Def^n :- (Subgroup) :- If a subset H of group G is itself a group under the operation of G, we say that H is subgroup of G

we use the notation as $H \leq G$

if H is subgroup but not equal to G then denote it as $H < G$. in this case H is called proper subgroup of G

$\Rightarrow$

→ $\{e\}$ is called the trivial subgroup of G

→ Any subgroup other than $\{e\}$ is called non-trivial subgroup of G

Remark :- Z_n is a group under addition modulo n but it is not subgroup of Z because operation is not same.

Subgroup Test

one-Step Subgroup Test :-

Let G be a group and H a non-empty subset of G. If ab^{-1} is in H whenever a & b are in H, then H is a subgroup of G. (In additive we write $a-b$ is in H whenever a & b are in H Then H is a subgroup of G).

Ex Let G be an Abelian group with identity e. and $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.

$\because e^2 = e$

$\Rightarrow e \in H$

let $a, b \in H$

$\Rightarrow a^2 = e$

$b^2 = e$

To show:- $ab^{-1} \in H$

$(ab^{-1})^2 = abab^{-1} = aab^{-1}b^{-1}$ {$\because$ 'G is an abelian}

$= a^2(b^2)^{-1}$

$= ee^{-1} = e$

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

$\Rightarrow H$ is subgroup of G

Ex:- let G be an Abelian group multiplication with identity e.

let $H = \{x^2 \mid x \in G\}$

$e^2 = e$

$\Rightarrow e \in H$

let $a, b \in G$

$ab^{-1} \in G$

$\Rightarrow (ab^{-1})^2 \in H$

$\Rightarrow H$ is subgroup of G.

Theorem :- Two-step subgroup Test

Let G be a group and let H be a non-empty subset of G. If ab is in H whenever a & b are in H i.e H is closed under the operation and a^{-1} is in H when $a \in H$, then H is a subgroup of G.

Ex :- Let G be an abelian group. Then $H = \{x \in G \mid o(x) = \text{finite}\}$ is subgroup of G

Sol^n :- $\because e^1 = e$,

$\Rightarrow e \in H \Rightarrow H \neq \phi$

Now let $a, b \in H$

and let $o(a) = m$

$o(b) = n$

To show $ab \in H$, $a^{-1} \in H$

$\Rightarrow (ab)^{mn} = a^{mn} b^{mn}$ $\quad$ $\because$ G is abelian $\Rightarrow (ab)^n = a^n b^n$

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

$= e^n \cdot e^m$

$= e$

$\Rightarrow o(ab) =$ finite

Now $(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$

$\Rightarrow$ H is subgroup of G

Ex Let G be a group of real numbers under multiplication.

Let $H = \{x \in G \mid x = 1 \text{ or irrational}\}$

& $K = \{x \in G \mid x \geq 1\}$

Sol" Let $\sqrt{2}, \sqrt{2} \in H$

$\Rightarrow \sqrt{2} \cdot \sqrt{2} = 2 \notin H$

$\Rightarrow$ H is not subgroup of G

Now Let $2 \geq 1$

$\Rightarrow 2 \in K$

but $2^{-1} = \frac{1}{2} < 1$

$\Rightarrow 2^{-1} \notin K$

$\Rightarrow$ K is not subgroup of G

Theorem 3.3 Finite Subgroup Test

Let H be a non-empty finite subset of a Group G. If H is closed under the operation of G, then H is a subgroup of G.

Theorem (3.9) $\langle a \rangle$ is a subgroup

Let G be a group, and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G.

Proof :- $\langle a \rangle = \{a^0, a, a^2, a^3, \dots\}$

clearly $a \in \langle a \rangle$

$\Rightarrow$ $\langle a \rangle$ is non-empty

let $a^n, a^m \in \langle a \rangle$

$\Rightarrow$ $a^n (a^m)^{-1} = a^{n-m} \in \langle a \rangle$

$\Rightarrow$ by one-step test

$\langle a \rangle$ is a subgroup of G

Note :- The subgroup $\langle a \rangle$ is called the cyclic subgroup of G generated by a.

if $G = \langle a \rangle$ then a is called a cyclic group

Ex :- $U(10) = \{1, 3, 7, 9\}$

$\langle 3 \rangle = \{3, 9, 7, 1\}$

$3^1 = 3$

$3^2 \bmod 10 = 9$

$3^3 \bmod 10 = 7$

$3^4 \bmod 10 = 1$

$\Rightarrow$ $U(10) = \langle 3 \rangle$

$U(10)$ is group

$\Rightarrow$ $\langle 3 \rangle$ is subgroup of $U(10)$

Ex $Z_{10} = \{0, 1, 2, \ldots, 9\}$

$\langle 2 \rangle = \{2, 4, 6, 8, 0\}$

in addition $\langle n \rangle = \{zn\}$

Ex Z,

$\langle -1 \rangle = Z$

$(-1) = \langle \ldots (-3)(-1), (-2)(-1), (-1)(-1), 0(-1), (1)(-1) \ldots \}$

Ex D_n, the dihedral group of order $2n$, let R denote a rotation of $360/n$ degree.

$R^n = R_{360} = e$, $R^{n+1} = R$, $R^{n+2} = R^2$

$R^{n-1} = R^{-1}$, $R^{-2} = \bar{R}^2 \ldots$

$\Rightarrow \langle R \rangle = \{e, R, R^2 \ldots R^{n-1}\}$.

$\langle R \rangle$ is a subgroup of D_n

Remark:- If the group is of finite order then subgroup is also finite.

Ex In Z_{20}

$\langle 8, 14\rangle = \{0, 2, 4, \cdots 18\} = \langle 2\rangle$

in D_4

$\langle H, V\rangle = \{H, H^2, V, HV\}$

$= \{R_0, R_{180}, H, V\}$

$\langle R_{90}, V\rangle = \{R_{90}, R_{90}^2, R_{90}^3, R_{90}^4, V, R_{90}V, R_{90}^2V, R^3V\} = D_4$

in C^* = ~~st~~ group of non zero complex numbers

$\langle 1, i\rangle = \{1, -1, i, -i\} = \langle i\rangle$

Def^n:- Center of a group

The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G,

$$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$$

Theorem :- center is a subgroup

The center of a group G is a subgroup of G.

Proof :- clearly identity element commute with every element in G

$\Rightarrow e \in Z(G)$

$\Rightarrow Z(G)$ is non-empty

Now let $a, b \in Z(G)$

$\Rightarrow ax = xa$ and $bx = xb$ $\forall x \in G$

To show :- $ab \in Z(G)$

i.e To show $(ab)x = x(ab)$ $\forall x \in G$

$(ab)x = a(bx)$ {associativity}

$= a(xb)$

$= (ax)b = (xa)b$

$= x(ab)$

Now

To show $\bar{a}^1 \in Z(G)$

i.e $\bar{a}^1 x = x\bar{a}^1$

$\because ax = xa$

$\Rightarrow \bar{a}^1(ax)\bar{a}^1 = \bar{a}^1(xa)\bar{a}^1$

$\Rightarrow (\bar{a}^1 a)x\bar{a}^1 = \bar{a}^1 x(a\bar{a}^1)$

$\Rightarrow x\bar{a}^1 = \bar{a}^1 x$

Hence $Z(G)$ is a subgroup of G