CYCLIC SUBGROUP

Let $(G, *)$ be a group and $a \in G$. Then $H = \{a^n \mid n \in Z\}$ is a subgroup of G. H is called the cyclic subgroup of G generated by a and it is denoted by (a) or $\langle a \rangle$.

In the group $(Z_{12}, +_{12})$, $\{[0], [3], [6], [9]\}$ is the cyclic subgroup generated by $[3]$, since $2[3] = 6$, $3[3] = 9$, $4[3] = 12] = [0]$.

CYCLIC GROUP.

A Group $(G, *)$ is said to be a cyclic group if there exists an element $a \in G$ such that every element $x \in G$ is of the form a^n for some integer n. The element a is called a generator of G and is written as $G = (a)$ or $\langle a \rangle$. It is read as G is cyclic group generated by a.

For eg,

The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic group generated by i, since $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.

It can be seen easily that $-i$ is another generator

1\. **Theorem 9:** Any cyclic group is abelian.

Proof: Let G be a cyclic group generated by 'a'.

Then $G = \{a^n \mid n \in Z\}$

Let $x, y \in G$ be any 2 elements then $x = a^m$, $y = a^n$ for some integers m and n

Now $x * y = a^m * a^n = a^{m+n}$

$y * x = a^n * a^m = a^{n+m}$

$x * y = y * x \quad \forall x, y \in G$

Hence G is abelian.

Note: The converse is not true (i,e) abelian group is not acyclic. Eg: $(Q, +)$ is abelian but not cyclic

2\. **Theorem 10:** Every subgroup of cyclic group is cyclic

Proof: Let $(G, *)$ be cyclic group generated by a

Then $G = \{a^n \mid n \in Z\} = \langle a \rangle$

Let H be a subgroup of G

Since H is subset of G, every element of H is of the form a^r for some $r \in Z$

Since H is a group if $a^r \in H$, then its inverse $(a)^{r-1} = a^{-r} \in H$. So either r or $-r$ is +ve integer. Hence H contains positive integer powers of a.

Let m be a least +ve integer such that $a^m \in H$. We shall prove a^m is generator of H. Let $x \in H$ be any element, then $x = a^n$ for some $n \in Z$.

For integers 'n', 'm' by Eucledian ~~distance~~ division algorithm, we can find integers 'q' and 'r' such that $n = mq + r$, $0 \le r < m$.

Then, $x = a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r$

$\Rightarrow (a^m)^{-q} * x = (a^m)^{-q} * (a^m)^q * a^r$

$= e * a^r$

$= a^r$

$\therefore a^r = (a^m)^{-q} * x = a^{-mq} * x$.

Now $a^m \in H \Rightarrow (a^m)^q \in H$, by closure

$\Rightarrow a^{mq} \in H$

$\Rightarrow a^{-mq} \in H$, since H is group

$\therefore a^{-mn} \in H$, by closure

$\Rightarrow a^r \in H$, where $r < m$

If $r \neq 0$, then $a^r \in H$ is a contradiction to the fact that 'm' is the least positive integer such that $a^m \in H$

Hence $r = 0$

$n = mq \Rightarrow x = (a^m)^q$

Thus any element of H is integral power of a^m.

So H is acyclic group generated by a^m

(i.e) $H = \langle a^m \rangle$

Theorem 11 : If $(G, *)$ is cyclic group generate by 'a', then prove a^{-1} is also generator.

Proof: ~~G = Given G = $\langle a \rangle$~~ Given $G = \langle a \rangle$

So any element $x \in G$ is $x = a^n$ for some integer n.

Now $x = a^n = (a^{-1})^{-n}$

Thus 'x' is integral ~~part~~ power of a^{-1} and

So a^{-1} is also a generator.

Order of element:

Definition: Let $(G, *)$ be a group and let $a \in G$. The order of 'a' is least positive integer 'm' such that $a^m = e$.

The order of 'a' is denoted by $O(a)$ and we write $O(a) = m$

If no such integer exist, then we say that 'a' is of infinite order.

Example: In group $G = \{1, -1, i, -i\}$ under usual multiplication, $O(i) = 4$, $O(-i) = 4$ and $O(-1) = 2$

Ans: Since $i^2 = -1$

$i^4 = (-1)^2 = 1$ and $(-1)^2 = 1$

Theorem 12: Let $(G, *)$ be finite cyclic group generated by an element $a \in G$. If $O(G) = n$, then $a^n = e$ and so $G = \{a, a^2, a^3, a^{n-1}, a^n = e\}$. Further $O(a) = n$

That is 'n' is least positive integer such that $a^n = e$

Proof: Given $(G, *)$ is finite cyclic group generated by 'a'.

First we shall prove that $a^m = e$ is not possible for $m < n$.

Assume it is possible (i,e) $a^m = e$, $m < n$

Since G is cyclic group generated by 'a' by any element $x \in G$ is integral power of 'a'. (i,e) $x = a^k$ for some integers k.

Now for integers m, k by Eucledian division, we can find integers q & r such that $k = mq + r$, $0 \leq r < m$.

$$\therefore x = a^k = a^{mq+r} = a^{mq} * a^r = e * a^r = a^r$$

Thus any element of G is a^r for $r < m$. This means the no: of elements of G is atmost 'm'. (i,e) $O(G) = m < n$, which contradics the hypothesis $O(G) = n$.

Hence $a^m = e$ is not possible for $m < n$

$$\therefore a^n = e$$

Next we shall prove that elements $a, a^2, a^3 \ldots a^n$ are all distinct.

Suppose it is not true, then there are repititions.

Let $a^s = a^r$, $0 < r < s \leq n$

$\Rightarrow a^s * a^{-r} = a^r * a^{-r}$

$\Rightarrow a^{s-r} = a^0 = e$, $0 < s-r < n$

This is again a contradiction by 1st part,

$\therefore$ all elements are distinct

$\therefore a, a^2 \ldots a^n = e$ are all distinct

Since $O(G) = n$, it follows $G = \{a, a^2 \ldots a^n = e\}$ and $a^n = e$. So $O(a) = n$.

Cycles and transpositions

Def: Let $S = \{a_1, a_2 \ldots a_n\}$ and σ be permutation on S. σ is called cycle of length r if there exist r elements $a_1, a_2 \ldots a_r$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3 \ldots \sigma(a_{r-1}) = a_r$ and $\sigma(a_r) = a_1$

This cycle is represented by symbol $(a_1, a_2 \ldots a_r)$ or $(a_1\ a_2 \ldots a_r)$

Def: Two cycles are said to be disjoint if they have no elements in common

eg: (1 2 3), (4 5) disjoint cycles.

Def: A cycle of length 2 is transposition

Def: If a permutation σ is a product of even number of transposition, then σ is even transposition.

If a permutation σ is pdt of odd no: of transposition, then σ is odd transposition

Example sum

1. Compute pdt (1 2) (2 4) (3 6) as permutation on {1, 2, 3, 4, 5, 6}. Find (i) even/odd (ii) order

ANSWER:

Let $\sigma = (1\ 2)(2\ 4)(3\ 6)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 4 & 5 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$$

We shall write σ as pdt of disjoint cycles

$\sigma = (1\ 4\ 2)(3\ 6)$ $\quad 1 \to 4 \to 2 \to 1$ cycles

$3 \to 6 \to 3$

Order of cycle $(1\ 4\ 2)$ is 3 and the order of cycle $(3\ 6)$ is 2

$\therefore$ Order of $\sigma = \text{lcm}\{3,2\} = 6$

Now to decide σ is odd or even, we shall write σ as product of transposition

$$\sigma = (1\ 4)\ (1\ 2)\ (3\ 6)$$

σ is pdt of 3 transposition.

$\boxed{\therefore \sigma \text{ is odd permutation}}$

Examples 2:

Express $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$ in S_9 as a pdt of disjoint cycles. Decide its order and test it is odd or even.

ANSWER:

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$$

we see $1 \to 2 \to 3 \to 4 \to 5 \to 1$

So one cycle is $(1\ 2\ 3\ 4\ 5)$

6 and 7 are left fixed.

$8 \to 9 \to 8$. So another cycle $(8\ 9)$

$$\theta = (1\ 2\ 3\ 4\ 5)\ (8\ 9)$$

Order of $(1\ 2\ 3\ 4\ 5)$ is 5 and order of $(8\ 9)$ is 2.

$\therefore$ order of $\theta = \text{lcm}(5,2) = 10$.

Further $\theta = (1\ 2)(1\ 3)(1\ 4)(1\ 5)(8\ 9)$ is a pdt 5 transposition.

$\boxed{\therefore \theta \text{ is odd permutation}}$

Cosets & Legrange's theorem

Cosets: Let $(H, *)$ be a subgroup of $(G, *)$. Let $a \in G$ be any element. Then set $aH = \{a * h \mid h \in H\}$ is called left coset of H in G determined by 'a'.

Sometimes aH is written as $a * H$

The set $Ha = \{h * a \mid h \in H\}$ is called right coset of H in G determined by 'a'.

Theorem 13: Let $(H, *)$ be a subgroup of $(G, *)$ Then the set of all left cosets of H in G form partition of G. That is every element of G belongs to only one left coset of H in G.

Proof: Let aH and bH be any 2 left coset.
We shall prove either $aH = bH$ or $aH \cap bH = \phi$

Suppose $aH \cap bH \neq \phi$ then there exist an element $x \in aH \cap bH$

$\Rightarrow x \in aH$ and $x \in bH$

$\Rightarrow x = a * h_1$ and $x = b * h_2$, for some $h_1, h_2 \in H$

$\therefore a * h_1 = b * h_2$

$\Rightarrow (a * h_1) * h_1^{-1} = (b * h_2) * h_1^{-1}$

$\Rightarrow a * (h_1 * h_1^{-1}) = b * (h_2 * h_1^{-1})$

$\Rightarrow a * e = b * (h_2 * h_1^{-1})$

$\Rightarrow a = b * (h_2 * h_1^{-1})$

If 'x' is any element in aH, then

$x = a * h$

$x = b * (h_2 * h_1^{-1}) * h$

$= b * (h_2 * h_1^{-1} * h) \in bH$

$x \in aH \Rightarrow x \in bH$

$\therefore aH \subseteq bH \rightarrow (2)$

Similarly we can prove $bH \subseteq aH \rightarrow (3)$

From (2) & (3), $\boxed{aH = bH}$

Thus any 2 cosets are either equal or disjoint

Further $\bigcup_{a \in G} aH \subseteq G$. since union of subset is Subset.

If 'x' is any element in G, then

$x = x * e \in xH$

$\therefore x$ is in left coset and hence $x \in \bigcup_{a \in G} aH$

Hence

$x \in G \Rightarrow x \in \bigcup_{a \in G} aH$

$\Rightarrow G \subseteq \bigcup_{a \in G} aH$ $\boxed{\therefore G = \bigcup_{a \in G} aH}$

This is all left coset partition G.

Theorem 14: There is one to one correspondance between any 2 left cosets of H in G

Proof: Let $(H, *)$ be subgroup of $(G, *)$

Let aH be any left coset of H in G. we know H itself is left coset. So its enough to prove that there is 1 to 1 correspondence between H and aH

Let $f : H \rightarrow aH$ be defined by $f(h) = a * h$ $\forall h \in H$

The maping is 1 to 1.

For any $h_1, h_2 \in H$ if $f(h_1) = f(h_2)$

then $a * h_1 = a * h_2$

$\Rightarrow h_1 = h_2$ (left cancelation law)

Now we prove f is onto

Let $x \in aH$ be any element, then $x = a * h$ for some $h \in H$. For this h we have $f(h) = a * h = x$.

So, f is onto.

Hence 'f' is bijective function of H onto aH

$\therefore$ f set up a 1 to 1 corresponce between H and aH

Note: (1) If H is finite, H and aH have same no: of elements

$$\therefore O(H) = O(aH)$$

(2) 13 and 14 theorem are true for right coset also.

Theorem 15: Legrange Theorem.

The order of a subgroup H of finite group G divides the order of group. That is of Order H divides order of G.

Proof: Let $(G, *)$ be a group of order 'n' and $(H, *)$ be a subgroup of order m.

Since G is finite group, the no: of left coset of H in G is finite

Let 'r' be no: of cosets of H in G

Let 'r' cosets be $a_1H, a_2H \ldots\ldots a_rH$

we know that left coset of G form partition of G. [by theorem-13]

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

$$\therefore O(G) = O(a_1H \cup a_2H \ldots \cup a_rH)$$

$$= O(a_1H) + O(a_2H) \ldots + O(a_rH)$$

But $O(a_iH) = O(H)$ (theorem-14)

$\therefore O(G) = O(H) + O(H) + \cdots O(H)$, r times

$\Rightarrow O(G) = r\, O(H)$

$\Rightarrow \dfrac{O(G)}{O(H)} = r$

Thus $O(H)$ divides $O(G)$.

Index of H in G

Def: Let $(H, *)$ be subgroup of $(G, *)$. Then the no: of different left (right) cosets of H in G is called index of H in G and is denoted by [G : H] or $i_G H$

Note: * In case of finite group $i_G(H) = \frac{O(G)}{O(H)}$

* It is quite possible in an infinite group there is a subgroup of finite index.

Corollary 1: The order of any element of finite group G divides O(G)

Proof: Let G be finite group of order 'n'.

Let $a \in G$ be element & $O(a) = m$.

Then cyclic group $\langle a \rangle$ is of order m.

By Lagrange theorem,

$$\boxed{O(\langle a \rangle) \mid O(G) \Rightarrow m \mid n}$$

$\therefore$ order of element divides O(G)

Corollary 2: Any group of prime order is ~~spe~~ cyclic

Proof: Let 'G' be a group of order P, where P is a prime number

Let $a \in G$, $a \neq e$. Let $H = \langle a \rangle$

Since $a \neq e$, $O(H) \neq 1$ $\therefore O(H) \geq 2$

By legrange theorem, $O(H) \mid O(G)$

$\Rightarrow O(H) \mid P \Rightarrow O(H) = P$ (Since P is prime ≥ 2)

$= O(G)$

Hence $G = H = \langle a \rangle$. G is cyclic.

$\therefore$ Any group of prime order is cyclic.

Note: * If $O(G) = P$, then every element other than identity e is generator of group.

* If G is cyclic group of order P, a prime then G has no proper subgroup

Normal Subgrps & Quotient groups.

Normal Subgroups: In general, $Ha \neq aH$. The subgroup H of G for which $Ha = aH$ $\forall a \in G$ is a special class of subgroups called normal subgroups.

Def: A subgroup $(H, *)$ of $(G, *)$ is called normal subgroups of G if $aH = Ha$ $\forall a \in G$

Examples 1: Every group of an abelian group is normal

Sol: Let $(G, *)$ be an abelian group and $(H, *)$ be a subgroup of G

Let $a \in G$ be any element

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

$= \{h * a \mid h \in H\}$ [$\because G$ is abelian]

$= Ha$

Since 'a' is arbitary, $aH = Ha \ \forall a \in G$

$\therefore H$ is normal subgroup of G

Note: Since $H_n = n\mathbb{Z}$ is subset of $\mathbb{Z}$ and $(\mathbb{Z}, +)$ is an abelian group, subgroup $(H_n, +)$ is a normal subgroup of $\mathbb{Z}$

Examples: Prove that intersection of two normal subgroup of $(G, *)$ is a normal subgroup of $(G, *)$

Sol: Let $(N_1, *)$ and $(N_2, *)$ be 2 normal subgroup of $(G, *)$.

~~Since~~ To prove $(N_1 \cap N_2, *)$ is normal subgroup of $(G, *)$

Since N_1, N_2 are normal subgroup of G, they are basically subgroups. We know $N_1 \cap N_2$ is subgroup of G. Now we shall prove it is a normal subgroup of G.

Let $n \in N_1 \cap N_2$ be any element and $a \in G$ be any element.

Then $n \in N_1$ and $n \in N_2$.

Since N_1, N_2 are normal, $a n a^{-1} \in N_1$ and $a n a^{-1} \in N_2$

$\therefore a n a^{-1} \in N_1 \cap N_2$.

Hence $N_1 \cap N_2$ is normal, from above example.

Quotient group or factor group:

If $(N, *)$ is a normal subgroup of $(G, *)$ then the group $(G/N, \oplus)$ is called quotient group or factor group of G by N or quotient group modulo N.

Direct product of 2 groups:

Theorem 17: Let $(G, *)$ and (H, Δ) be two groups. Let $G \times H$ be cartesian product of G and H.

If $\cdot$ is the binary operation $G \times H$ gn/. by $(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2)$ for any $(g_1, h_1), (g_2, h_2) \in G \times H$ then $(G \times H, \cdot)$ is group.

Proof: Given $(G, *)$, (H, Δ) are groups, let e_1, e_2 be identities of G and H.

$G \times H = \{(g, h) \mid g \in G, h \in H\}$

$\cdot$ is binary operation componentwise multiplication.

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2) \ \forall (g_1, h_1), (g_2, h_2) \in G \times H$

$g_1 * g_2 \in G$ and $h_1 \Delta h_2 \in H$

$(g_1 * g_2, h_1 \Delta h_2) \in G \times H$

$\Rightarrow (g_1, h_1) \cdot (g_2, h_2) \in G \times H$

So closure is satisfied.

Associativity: Let x, y, z be any 3 elements of $G \times H$.

$\therefore x = (g_1, h_1), y = (g_2, h_2), z = (g_3, h_3)$

for some $g_1, g_2, g_3 \in G$ and $h_1, h_2, h_3 \in H$.

Now $x \cdot (y \cdot z) = (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3))$

$= (g_1, h_1) \cdot (g_2 * g_3, h_2 \Delta h_3)$

$= (g_1 * (g_2 * g_3), h_1 \Delta (h_2 \Delta h_3))$

$= ((g_1 * g_2) * g_3, (h_1 \Delta h_2) \Delta h_3)$

[$\because$ $*$ and Δ are associative]

$= \left((g_1, h_1) \cdot (g_2, h_2) \right) \cdot (g_3, h_3)$

$= (x \cdot y) \cdot z$

$\therefore$ associative axiom is satisfied

Identity: (e_1, e_2) is identity element of $G \times H$, where e_1 is the identity of G and e_2 is identity of H.

For if $(g, h) \in G \times H$ be any element then

$(g, h) \cdot (e_1, e_2) = (g * e_1, h \Delta e_2) = (g, h)$

and $(e_1, e_2) \cdot (g, h) = (e_1 * g, e_2 \Delta h) = (g, h)$

$\therefore (e_1, e_2)$ is identity of $G \times H$

Inverse: Let (g, h) be any element of $G \times H$.

Since $g \in G$, $h \in H$ and so $(g^{-1}, h^{-1}) \in G \times H$

Now $(g, h) \cdot (g^{-1}, h^{-1}) = (g * g^{-1}, h \Delta h^{-1}) = (e_1, e_2)$

$(g^{-1}, h^{-1}) \cdot (g, h) = (g^{-1} * g, h^{-1} \Delta h) = (e_1, e_2)$

$\therefore (g^{-1}, h^{-1})$ is inverse of (g, h)

$\therefore$ Inverse axiom is satisfied.

Hence $(G \times H, \cdot)$ is group.

This group is called direct product of G and H

Group Homomorphism :

Let $(G, *)$ and $(G', \cdot)$ be 2 groups. A mapping $f: G \to G'$ is called group homomorphism if for all $a, b \in G$.

$$f(a * b) = f(a) \cdot f(b)$$

Elementary properties of homomorphism :

Theorem 18 : If f is a homomorphism from group $(G, *)$ into $(G', \cdot)$ then prove that

(i) $f(e) = e'$, where e, e' are identities of G and G' respectively.

(ii) $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$

Proof : (i) Let $a \in G$ be any element.

Then $a * e = a$

$\Rightarrow f(a * e) = f(a)$

$\Rightarrow f(a) \cdot f(e) = f(a)$ [$\because f$ is homomorphism

$\Rightarrow f(a) \cdot f(e) = f(a) \cdot e'$

By left cancellation law in G', we get $f(e) = e'$