Theorem: If H is any subgroup of G, then G is equal to the union of all right cosets of H in G.

(i.e., $G = Ha \cup Hb \cup \cdots \cup H_t \cup \cdots$, where $a, b, \cdots \in G$)

Proof: Since each right coset is a subset of G, the union of all right cosets is a subset of G.

i.e., $\bigcup_{a \in G} Ha \subseteq G$ — ①

$Ha = \{ea, \cdots$

Now, for any $a \in G$

$$a = ea \in Ha$$

$$a \in Ha \cup Hb \cup \cdots \cup H_t \cup \cdots.$$

$$a \in \bigcup_{a \in G} Ha$$

$$\Rightarrow G \subseteq \bigcup_{a \in G} Ha \qquad \text{— ②}$$

From (1) & (2), $G = \bigcup_{a \in G} Ha$

* If $(G, *)$ is a group, the number of elements in the set G is said to be the **order** of G and is denoted by $|G|$ or $O(G)$.

Order of an element:

Let G be a group and let $a \in G$.

The smallest +ve integer 'n' such that $a^n = e$, is called the **order** of element 'a' and is denoted by $O(a)$.

$a^{n} = e$

Example ①: $G = \{1, -1, i, -i\}$, $(G, \cdot)$ is a group.

$a = -1$

Here $e = 1$

$1^{1} = 1$

$o(a) = o(1) = 1$

$O(a) = n \rightarrow a^n = e$

$(-1)^2 = 1 = e$, $O(-1) = 2$

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

$(i)^4 = 1$, $O(i) = 4$

$(-i)^4 = 1$, $O(-i) = 4$

Example (2): $G = \{1, \omega, \omega^2\}$, $(G, \cdot)$ is a group

Here $e = 1$

$O(\omega) = 3 \quad \because \omega^3 = 1$

$O(\omega^2) = 3 \quad \because (\omega^2) = 1$

Example (3): Group $Z_5 = \{0, 1, 2, 3, 4\}$ under addition modulo 5, then $O(2) = ?$

Here $e = 0$, $a^n = e = 0$

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

$\oplus_5$	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

$1^2 = 1 \oplus_5 1 = 2$

$1^3 = 1 \oplus_5 1 \oplus_5 1 = 3$

$1^4 = 1 \oplus_5 1 \oplus_5 1 \oplus_5 1 = 4$

$1^5 = 1 \oplus_5 1 \oplus_5 1 \oplus_5 1 \oplus_5 1 = 0$

$O(1) = 5$

$a^2 = a \oplus_5 a$ $\quad a^2 = a * a$

$a^3 = a * a * a$

$2^2 = 2 \oplus_5 2 = 4$

$2^3 = 2 \oplus_5 2 \oplus_5 2 = 1$

$2^4 = 3$

$2^5 = 0$

$O(2) = 5$

Lagrange's theorem:

Let G be a finite group and 'H' a subgroup of G.
Then the order of H divides the order of G.

i.e $O(H) \mid O(G)$

i.e, $O(G) = m\, O(H)$

Proof: Since G is a finite group,

the number of left cosets of H in G is finite.

Let $a_1H, a_2H, \ldots, a_kH$ be all distinct left cosets of H in G.

i.e, $G = a_1H \cup a_2H \cup \cdots \cup a_kH$.

And the set $\{a_iH\}$ are mutually disjoint.

$$O(G) = O(a_1H) + O(a_2H) + \cdots + O(a_kH) \quad \text{— (1)}$$

Since any two left cosets of H in G have the same number of elements, any two a_iH have the same number of elements.

i.e, it is equal to the number of elements in H = no. of elements in a_iH.

$$(1) \Rightarrow O(G) = O(H) + O(H) + \cdots + O(H)$$

$$O(G) = k\, O(H)$$

$$\Rightarrow O(H) \mid O(G)$$

Cyclic Subgroups:

Let G be a group and 'a' be any element of G.

The Cyclic subgroup of G generated by 'a' is denoted by $H = (a)$ or $H = \langle a \rangle$ and is defined to be,

$$H = (a) = \{a^n / n \in \mathbb{Z}\}$$

i.e., (a) is a subset containing all powers (+ve, -ve or zero) of 'a'.

To prove $H = (a)$ is a subgroup of G –

$a^0 = e \in H$, $H \neq \phi$

Let $x, y \in H$, then $x = a^m$, $y = a^n$, $m, n \in \mathbb{Z}$

$x y^{-1} = a^m (a^n)^{-1} = a^{m-n} \in H$, $m-n \in \mathbb{Z}$

$\Rightarrow H$ is a subgroup of G.

Cyclic group:

A group G is said to be cyclic if there exist an element $a \in G$ such that every element of G can be written as a power of 'a'.

Then 'a' is called the generator of G.

$G = (a)$.

Example: $G = \{1, -1, i, -i\}$, $(G, \cdot)$ is a group. a^n

Here $G = (i)$ $\quad i^1 = 1 \quad i^3 = -1$

~~$1^1 = 1$~~ $\quad i^2 = -1 \quad i^4 = 1$

~~$G = (1)$??~~ ~~$1^2 = 1$~~

$G = \{1, w, w^2\}$ $\quad G = (w)$, $G = (w^2)$

cyclic group w.r.to addition defined by,

$G = (a) = \{ an \mid n \in Z \}$

Eg: The group $(Z, +)$ is cyclic with $Z = \overset{a}{(1)}$, $Z = \overset{a}{(-1)}$

$1 = 1(1)$ $\quad$ $3 = -1(-3)$

$2 = 1(2)$ $n \in Z$

$3 = 1(3)$

Eg: Show that $Z_5 = \{0, 1, 2, 3, 4\}$ forms a cyclic group under operation of addition modulo 5.

$\oplus_5$	0	1	2	3	4
$\boxed{0}$	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

→ In this table, all the elements are in G

i.e $a \oplus_5 b \in G$, $\forall a, b \in G$

→ closure satisfies.

→ $|||^{ly}$ associative law satisfies.

i.e, $\forall a, b, c \in G$, $(a \oplus_5 b) \oplus_5 c = a \oplus_5 (b \oplus_5 c)$

→ Identity element is '0'

→ Inverse law, $0^{-1} = 0$, $1^{-1} = 4$

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

$4^{-1} = 1$

∴ Therefore $(G, \oplus_5)$ is a group

$G = (a) = \{an \mid n \in Z\}$

$$\begin{array}{ll}
(1) = 1(\overset{n}{\downarrow}{0}) = 0 & (2) = 2(0) = 0 \\
(1) = 1(1) = 1 & (2) = 2(1) = 2 \\
(1) = 1(2) = 2 & (2) = 2(2) = 4 \\
(1) = 1(3) = 3 & (2) = 2(3) = 1 \\
(1) = 1(4) = 4 & (2) = 2(4) = 3
\end{array}$$

$$\begin{array}{ll}
(3) = 3(0) = 0 & (4) = 4(0) = 0 \\
(3) = 3(1) = 3 & (4) = 4(1) = 4 \\
(3) = 3(2) = 1 & (4) = 4(2) = 3 \\
(3) = 3(3) = 4 & (4) = 4(3) = 2 \\
(3) = 3(4) = 2 & (4) = 4(4) = 1
\end{array}$$

$\therefore Z_5$ is cyclic group with generators (1), (2), (3), (4)

(except the identity elt 0)

Result: If G is cyclic group with generator (a), then

$O(a) = O(G)$.

Q: Show that a cyclic group is always abelian.

Ans: Let G be a cyclic group.

then there is an element $a \in G$ such that $G = (a)$

Let $x, y \in G$ then $x = a^m$, $y = a^n$ for some $m, n \in Z$

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$$

$\rightarrow$ commutative law holds

$\Rightarrow G$ is abelian.