# 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 $O(a) = n$ & $O(a^{-1}) = m$

Now $O(a) = n$

$\Rightarrow a^n = e$

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

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

$\therefore O(a^{-1}) = n$ — (1)

$m = n$

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

$\boxed{(a^{-1})^m = e}$ 2nd way

Taking inverse both sides

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

$(a)^m = e$

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

$\Rightarrow (a^m)^{-1} = e$ $\quad \left(\because \begin{array}{l} b.b^{-1} = e \\ b = e,\ b^{-1} = e \end{array}\right)$

$a^m = e$

$\therefore O(a) = m$ — (2)

$n = m.$

From (1) & (2). $m = n$.

Theorem: Every cyclic group is an abelian group. $(G, \cdot)$

PROOF: Let 'G' is a group generated by 'a' such that $\langle a \rangle$ and $a \in G$.

Let $x, y \in G$ then there exist integers $r$ and $s$ such that $x = a^r$, $y = a^s$

Now for commutative property

$$x \cdot y = a^r \cdot a^s$$
$$= a^{r+s} \quad \text{--- (1)}$$

also $$y \cdot x = a^s \cdot a^r$$
$$= a^{s+r} \quad \text{--- (2)}$$

from (1) & (2) they are equal

$xy = yx$ for $\forall x, y \in G$.

Thus G is an abelian grp.

Q) Prove that every subgrp of abelian grp is normal subgroup.

$\underline{\text{Sol}^n}$ Let 'G' be an abelian grp and 'H' is normal subgrp of G.

then let $x \in G$ and $h \in H$.

Consider $x \cdot h x^{-1}$ ($\in H$).

$\underbrace{x \cdot x^{-1}}\cdot h$

$e \cdot h$

$\Rightarrow h$

$\Rightarrow h \in H$.

Q) a) Show that $(Z_6, +_6)$ is abelian grp.

b) obtain left cosets of $\{[0], [3]\}$ in $(Z_6, +)$

$\underline{\text{Sol}^n}$ $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$e = 0$.

Inverses. $0 - 0$

$1 = 5$

$2 = 4$

$3 = 3$.

$4 = 2$.

(b) $H = \{0, 3\}$.

$0 +_6 H = \{0, 3\}$

$1 +_6 H = \{1, 4\}$

$2 +_6 H = \{2, 5\}$

$3 +_6 H = \{3, 0\} = H$

$4 +_6 H = \{4, 1\}$

$5 +_6 H = \{5, 2\}$.

# LAGRANGE'S THEOREM :-

The order of each subgrp of a finite grp is a divisor of order of the grp $\left(\frac{O(G)}{O(H)} = K.\right)$

PROOF

Let the order of 'G' is 'n' i.e G contains 'n' elements.
Also, let subgrp 'H' of G contains 'm' elements.

$$O(H) = m, \quad O(G) = n.$$

Let $a \in G$. but $a \notin H$.

$$H = \{h_1, h_2, h_3 \ldots h_m\}$$

The left cosets of H will be given as :-

$$aH = \{ah_1, ah_2, \ldots ah_m\}$$

Now, set aH has m distinct elements and set 'H' also has m distinct elements
i.e if $ah_i = ah_j$ then $h_i = h_j$. (LEFT CANCELLATION)

Now for some value i & j let

$$ah_i = h_j \quad \text{(multiply } h_i^{-1} \text{ both sides)}$$

$$ah_i . h_i^{-1} = h_j h_i^{-1} \in H$$

$$ae = h_j h_i^{-1} \in H$$

$\because$ we got $\boxed{a \in H}$ which is again a contradiction

$\therefore$ $ah_i \neq h_j$

Now, we know union of all left & right coset of H in G is equal to the group
i.e,

$$G = a_1H \cup a_2H \cup \ldots a_nH$$

$$a_1H = \{a_1h_1, a_1h_2, \ldots a_1h_m\}$$

$$a_2H = \{a_2h_1, a_2h_2 \ldots a_2h_m\}$$

$\vdots$

$$a_nH = \{a_nh_1, a_nh_2 \ldots a_nh_m\}$$

Lagrange continue :-

$\therefore$ no. of elements in $G$ is equal to no of elements in $a_1H$ + no of elements in $a_2H$ ---- + $a_mH$.

$$n = \underbrace{m + m + \cdots\cdots}_{km} \text{ k times}$$

$$n = km$$

$$\frac{n}{m} = k.$$

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

The order of H divides order of G.