Prop :—

Let $H \leq G$, and $a, b \in G$, then,

i) $a \in aH$

ii) $aH = H$ iff $a \in H$ — $Ha = H$ iff $a \in H$

iii) $aH = bH$ iff $a^{-1}b \in H$ — $\Rightarrow a \notin H \Rightarrow Ha \neq H$

iv) $aH = bH$ or $aH \cap bH = \phi$

v) $|aH| = |bH| = |H|$

vi) $aH = Ha$ iff $H = aHa^{-1}$

vii) aH is a subgp of G iff $a \in H$

Proof :— i) $e \in H$.

$a = a.e \in aH$.

ii) Let $aH = H$

$a = a.e \in aH = H \Rightarrow a \in H$.

conversely, let $a \in H$.

Let $h \in H$, $a.h \in H$ [closure]

$\Rightarrow aH \subseteq H$ —— (1)

Let $h_1 \in H$, $a \in H \Rightarrow a^{-1}h_1 \in H$

$\therefore h_1 = e.h_1 = (aa^{-1})h_1$

$= a(a^{-1}h_1) \in aH$

$\Rightarrow H \subseteq aH$ —— (2)

from (1), (2), $aH = H$.

iii) $aH = bH$ iff $a^{-1}bH = H$

$\Rightarrow a^{-1}b \in H$ [from (ii)]

Another approach :—

Let $aH = bH$

Let $aH = bH$

$ah_1 = bh_2$, for some $h_1, h_2 \in H$

$\Rightarrow a^{-1}b = h_1 h_2^{-1} \in H$

Conversely, Let $a^{-1}b \in H$

$\therefore a^{-1}b = h_3$, for some $h_3 \in H$

$\Rightarrow b = ah_3$

$\Rightarrow bH = ah_3 H = aH$

iv) $aH = bH$ or $aH \cap bH = \phi$.

$aH \cap bH \neq \phi$

Let $x \in aH \cap bH$

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

$\Rightarrow x = ah_1$, $x = bh_2$, $h_1, h_2 \in H$

$a = xh_1^{-1} = bh_2 h_1^{-1} \in bH$

$ah \in bH \Rightarrow aH \subseteq bH$

Similarly, $bH \subseteq aH$

$aH = bH$

Another approach :-

$ah_1 = bh_2$

$\Rightarrow a^{-1}b = h_1 h_2^{-1} \in H$

$\Rightarrow a^{-1}b \in H \Rightarrow aH = bH$ [From (iii)]

v) $|aH| = |bH|$.

Let us define $f : aH \longrightarrow bH$ by

$f(ah) = bh$, $\forall h \in H$

f is a bijection.

$|aH| = |bH| = |H|$

vi) $aHa^{-1} = \{ aha^{-1} : h \in H \}$

To show $= H$ iff $aH = H$

$aH = Ha$ iff $(aH)a^{-1} = (Ha)a^{-1}$

$\Rightarrow aHa^{-1} = H(aa^{-1}) = H$

vii) aH is a subgp of G.

$e \in H$, $e \in aH$

$e \in H \cap aH \Rightarrow aH = H$

$aH = H$ iff $a \in H$

OR Using (ii)

Lagrange's theorem :— $|H| / |G|$

If G is finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left cosets of H in G is $|G|/|H|$

$[G:H] = |G|/|H|$ (Index of H in G)

Ex :— $G = S_3$, $H = \{ I_0, I_3 \}$

H, $I_1 H$, $I_2 H$ three distinct left cosets of H in G.

$|G| = 6$, $|H| = 2$

Index of H in G $= [G:H] = 3$

= The no of distinct left/right

cosets of H in G.

When $[G : H] = 2$, then $aH = Ha, \forall a \in G$.

H, aH $(a \notin H)$ $\quad G = H \cup aH \Rightarrow aH = Ha$

H, Ha $(a \notin H)$ $\quad G = H \cup Ha$

$$G = H \cup a_1 H \cup a_2 H \cup a_3 H$$
$$G = H \cup Ha_1 \cup Ha_2 \cup Hb_3$$

Proof of Lagrange's thm :—→

$$G = a_1 H \cup a_2 H \cup \dots \cup a_k H$$
$$|G| = |a_1 H| + |a_2 H| + \dots + |a_k H|$$
$$= |H| + |H| + \dots + |H|$$
$$= k \cdot |H|$$
$$\Rightarrow |H| \,/\, |G|$$
$$k = |G| / |H| = [G : H].$$