So, there exist a one to one correspondence between sets aH and bH.

$\therefore |aH| = |bH|$.

$\boxed{\text{(8) \& (9) try yourself.}}$

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

First let $aH = Ha$

$\Rightarrow aHa^{-1} = Haa^{-1}$

$\Rightarrow aHa^{-1} = He \Rightarrow \boxed{H = aHa^{-1}}$

Conversely ($\Leftarrow$) let $H = aHa^{-1}$

$\Rightarrow Ha = aHa^{-1}a$

$\Rightarrow Ha = aHe$

$\Rightarrow Ha = aH$

(9) aH is a subgroup of G iff $a \in H$

First let $a \in H$.

Property (2).

First let $a \in H$.

$a \in H \Rightarrow aH = H$

$\Rightarrow aH$ is a subgroup of G.

Property ②. $aH = H \Leftrightarrow a \in H$.

Conversely ($\Leftarrow$) let aH is a subgroup of G.

$\therefore e \in aH$ and $e \in eH$ $eH = H$.

$\Rightarrow aH \cap eH \neq \phi$

$\Rightarrow aH = eH$ Property ⑤

$\Rightarrow aH = H$

$\Rightarrow a \in H$ Property ②

Lagrange's Theorem ($|H|$ divides $|G|$)

Let G be a finite group and H be a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (or right) cosets of H in G is $|G|/|H|$.

Proof: let aH ...

Proof: Let $a_1H, a_2H, \ldots, a_rH$ denote the distinct left cosets of H in G.

Then, for each $a \in G$, we have $aH = a_iH$ for some $1 \le i \le r$.

$\because a \in aH \quad \forall a \in G$. $\quad (\because e \in H$ & $a = ae)$

$\therefore$ each element of G belongs to one of the cosets a_iH, where $1 \le i \le r$.

Thus, $G = a_1H \cup a_2H \cup \cdots \cup a_rH$.

$\Rightarrow |G| = |a_1H| + |a_2H| + \cdots + |a_rH|$ $\quad (\because$ all cosets a_iH are distinct$)$

$\Rightarrow |G| = |H| + |H| + \cdots + |H|$ $\quad (\because |a_iH| = |H| \; \forall 1 \le i \le r)$

$\Rightarrow |G| = r|H|$ ____ (1)

$\Rightarrow |H|$ divides $|G|$.

Now, from eq^n (1), $r = \dfrac{|G|}{|H|}$

Thus, Number of distinct left cosets of H in G is $|G|/|H|$.

Note: ① A group of order 10 may have subgroup of order 1, 2, 5 and 10. (No others).

② Converse of Lagrange theorem need not be true.

$A_4 \to$ Alternating Group of degree 4

$$|A_4| = \frac{4!}{2} = 12$$

$6 \mid 12$ but A_4 has no subgroup of order 6.

Corollary 1: $|a|$ divides $|G|$

In a finite group, the order of each element of the group divides the order of the group.

Proof: Let G be a group & $a \in G$.

Proof: Let G be a group & $a \in G$.

TS $|a|$ divides $|G|$.

- Clearly $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

By Lagrange's theorem $|\langle a \rangle|$ divides $|G|$.

$\Rightarrow |a|$ divides $|G|$ $\left(\because |\langle a \rangle| = |a|\right)$.

Corollary 2:

A group of prime order is cyclic.

Proof: Suppose that G is the group of prime order p (say).

TS G is cyclic.

Let $a \in G$ and $a \neq e$.

Then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

$\Rightarrow |\langle a \rangle|$ divides $|G|$