

Chapter - 7 (Cosets and Lagrange's Theorem)

Coset of a subset in a Group

Let G be a group and H be a subset of G .

For any element $a \in G$,

the set $aH = \{ah \mid h \in H\}$ is called the left coset of H in G containing a .

Similarly, the set $Ha = \{ha \mid h \in H\}$ is called the right coset of H in G containing a .

Note: $|aH| = \text{no of elements in } aH$
 $|Ha| = \text{no of elements in } Ha$

Example 2 $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ $H = \{0, 1\}$

$0 \in \mathbb{Z}_4$.

aH
 $= a * H$

~~$0/H$~~

$$0 +_4 H = \{0 +_4 h \mid h \in H\} \\ = \{0, 1\} = H$$

$$1 +_4 H = \{1 +_4 h \mid h \in H\} = \{1, 2\}$$

$$2 +_4 H = \{2 +_4 h \mid h \in H\} = \{2, 3\}$$

$$3 +_4 H = \{3 +_4 h \mid h \in H\} = \{3, 0\} = \{0, 3\}$$

Coset of subgroup H in Group G

For any $a \in G$,

... , we have

the set $aH = \{ah \mid h \in H\}$ is called the

left coset of subgroup H in G containing a .

and the set $Ha = \{ha \mid h \in H\}$ is called the right coset of subgroup H in G containing a .

Example: $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$
 $H = \{(1), (12)\}$

find all left cosets of H in G .

$$(12) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad (132) = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

$(1) \in G \Rightarrow$

① $(1)H = \{(1)\phi \mid \phi \in H\} = \{(1), (12)\} = H.$

② $(12)H = \{(12)\phi \mid \phi \in H\} = \{(12)(1), (12)(12)\} = \{(12), (1)\} = H.$

③ $(13)H = \{(13)\phi \mid \phi \in H\} = \{(13)(1), (13)(12)\} = \{(13), (123)\}$

④ $(23)H = \{(23)\phi \mid \phi \in H\} = \{(23)(1), (23)(12)\} = \{(23), (132)\}$

⑤ $(123)H = \{(123)\phi \mid \phi \in H\} = \{(123)(1), (123)(12)\} = \{(123), (13)\} = \{(13), (123)\}$

$(23)(12) = (23)(21) = (213) = (132) = (321)$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

or $(132)H$

$$\textcircled{8} (132)H$$

$$= \{ (23), (132) \}$$

$$\begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

$aH = Ha$ may or may not equal.

$$H(132) = \{ \phi(132) \mid \phi \in H \}$$

$$= \{ (1)(132), (12)(132) \}$$

$$= \{ (132), (13) \}$$

$$\therefore (132)H \neq H(132)$$

Properties of Cosets:

Let H be a subgroup of G and let $a, b \in G$

Then, (i) $a \in aH$

(ii) $aH = H$ iff $a \in H$

(iii) $aH = bH$ or $aH \cap bH = \emptyset$

(iv) $aH = bH$ iff $a^{-1}b \in H$

(v) $|aH| = |bH|$

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

(vii) aH is a subgroup of G if and only if $a \in H$

Proof:

(i) $\underline{\underline{\text{If}}} \ a \in aH$

$\therefore H$ is a subgroup

$\therefore e \in H$

Now $aH = \{ah \mid h \in H\}$

$\therefore e \in H \Rightarrow ae \in aH$
 $\Rightarrow a \in aH$.

(ii) First let $aH = H$.

$\therefore a \in aH$ (from part (i))

$\Rightarrow a \in H$ ($\because aH = H$)

conversely ($\Leftarrow$) let $a \in H$.

IS $aH = H$

we will show that $aH \subseteq H$ & $H \subseteq aH$.

$aH = \{ah \mid h \in H\}$

$\therefore H$ is a subgroup

$\therefore ah \in H \forall a, h \in H$ (closure)

$\therefore aH = \{ah \mid h \in H\} \subseteq H$

$\Rightarrow aH \subseteq H$ ——— ①

let $h \in H$ be an arbitrary element of H .

$\therefore a \in H, h \in H \Rightarrow a^{-1}h \in H$ ($\because H$ is a subgroup)

Now $h = eh = a a^{-1}h = a(a^{-1}h)$

$\Rightarrow h \in aH$

$\therefore H \subseteq aH$ ——— ②

from eq ① & ②, $aH = H$.

$$\boxed{\begin{array}{l} h \in H \Rightarrow h \in aH \\ \Rightarrow H \subseteq aH \end{array} \quad \begin{array}{l} h = ah \\ h \in H \end{array}}$$

$$\boxed{H \subseteq aH}$$

$$(iii) \quad aH = bH \text{ or } aH \cap bH = \emptyset$$

$$\text{suppose } aH \cap bH \neq \emptyset$$

$$\text{let } x \in aH \cap bH.$$

$$\Rightarrow x \in aH \text{ and } x \in bH.$$

$$\Rightarrow x = ah_1 \text{ and } x = bh_2 \text{ where } h_1, h_2 \in H.$$

$$\text{Now, } a = xh_1^{-1} = bh_2h_1^{-1}$$

$$\text{and } aH = bh_2h_1^{-1}H.$$

$$\Rightarrow aH = bH.$$

$$\left. \begin{array}{l} \because h_2h_1^{-1} \in H \\ \text{and using part (ii)} \\ a \in H \Rightarrow aH = H. \end{array} \right\}$$

$$(iv) \quad aH = bH \text{ iff } a^{-1}b \in H.$$

$$\text{first let } a^{-1}b \in H$$

$$\Rightarrow (a^{-1}b)H = H$$

(from property (ii))

$$\Rightarrow a^{-1}bH = H$$

$$\Rightarrow a(a^{-1}bH) = aH$$

$$\Rightarrow (aa^{-1})bH = aH \Rightarrow (e)bH = aH.$$

$$\Rightarrow bH = aH \Rightarrow aH = bH$$

$$\text{Conversely (} \Leftarrow \text{) let } aH = bH.$$

$$\Rightarrow a^{-1}(aH) = a^{-1}bH$$

$$\Rightarrow H = (a^{-1}b)H.$$

$$\Rightarrow (a^{-1}b)H = H.$$

$$\Rightarrow a^{-1}b \in H.$$

(property (ii))

IS

$$(v) \underline{\text{IS}} \quad |aH| = |bH|$$

we need to find a one - one correspondence between sets aH and bH .

$$\phi : aH \rightarrow bH$$

$$\phi(ah) = bh. \quad \forall h \in H.$$

IS ϕ is one-one & onto.

$$(vi) \quad aH = H a \quad \text{iff} \quad H = aH a^{-1}$$

$$aH = H a \quad \Leftrightarrow \quad aH a^{-1} = H a a^{-1}$$

$$\Leftrightarrow \quad aH a^{-1} = H e$$

$$\Leftrightarrow \quad aH a^{-1} = H$$

$$(vii) \quad \underline{\text{IS}} \quad aH \text{ is a subgroup of } G \quad \text{iff} \quad a \in H.$$

let aH be the subgroup of G

$$\underline{\text{IS}} \quad a \in H.$$

aH is the subgroup of $G \Rightarrow e \in aH$
and $e \in eH$.

$$\therefore e \in aH \cap eH \Rightarrow aH \cap eH \neq \emptyset$$

$$\Rightarrow aH = eH$$

$$\Rightarrow aH = H. \quad (\text{by (ii)})$$

$$\Rightarrow a \in H.$$

Conversely ($\Leftarrow$) let $a \in H$.

$$a \in H \Rightarrow aH = H. \\ \Rightarrow aH \text{ is a subgroup of } G.$$

Center of a

$$C(a) = \{x \in G \mid ax = xa\}$$

center

$$Q. 77 \quad Z(G) = \{x \in G \mid ax = xa \forall a \in G\}$$

$$Z(G) = \bigcap C(a)$$

$$x \in Z(G) \Rightarrow x \in \bigcap C(a)$$

$$x \in \bigcap C(a) \Rightarrow x \in Z(G)$$

$$Q. 78 \quad a \neq b \quad \underline{\underline{\nexists}} \quad a^2 \neq b^2 \text{ or } a^3 \neq b^3$$

$$\text{Suppose if, } a^2 = b^2 \text{ and } a^3 = b^3$$

$$\Rightarrow \textcircled{a^2} a = \textcircled{b^2} b \quad (\text{left Cancellation})$$

$$\Rightarrow a = b.$$

$$\rightarrow \leftarrow$$

2) Lagrange's Theorem:

order of a subgroup divides order of group.
or.

If G is a finite group and H is a subgroup of G ,

then $|H|$ divides $|G|$. Moreover, the number of

distinct left (or right) cosets of H in G is $\frac{|G|}{|H|}$.

Proof: $\because G$ is finite group, there are finite no. of left cosets of H in G .

Let $a_1H, a_2H, \dots, a_rH$ be the distinct left cosets of H in G .

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

$\Rightarrow a \in a_iH$ for some $1 \leq i \leq r$.

$$\therefore G \subseteq a_1H \cup a_2H \cup \dots \cup a_rH.$$

————— ①

Now clearly, $a_iH \subseteq G \quad \forall 1 \leq i \leq r$.

$$\therefore a_1H \cup a_2H \cup \dots \cup a_rH \subseteq G$$

————— ②

$$\boxed{\begin{array}{l} a_i \in G, H \text{ subgroup} \\ a_iH = \{a_ih \mid h \in H\} \\ \subseteq G. \end{array}} \quad \begin{array}{l} h \in G \\ h \in H \end{array}$$

from eqn ① & ②,

$$G = a_1H \cup a_2H \cup \dots \cup a_rH \quad \text{————— ③}$$

Now $a_1H, a_2H, \dots, a_rH$ are distinct left cosets of H in G .

$$\therefore a_iH \cap a_jH = \emptyset \quad \forall 1 \leq i, j \leq r.$$

$$\text{Thus, } |G| = |a_1H| + |a_2H| + \dots + |a_rH|.$$

$$\Rightarrow |G| = \underbrace{|H| + |H| + \dots + |H|}_{r \text{ times}} \quad \left[\begin{array}{l} \because |a_iH| = |H| \\ |a_iH| = |G|/r \\ \Rightarrow |a_iH| = |G|/r \end{array} \right]$$

← 2 times →

$$\begin{aligned} |aH| &= |bH| \\ \Rightarrow |aH| &= |eH| = |H| \end{aligned}$$

$$\Rightarrow |G| = 2 |H|$$

$$\Rightarrow |H| \text{ divides } |G|$$

and $2 = |G| / |H|$

$\Rightarrow$ No. of distinct left cosets of H in G

$$\text{are } |G| / |H|$$

① G is a Group of order 6.

then G can have subgroups of order 1, 2, 3 and 6.

G can have proper subgroups of order 2 and 3.

Q. If $a \in G$, then $\langle a \rangle$ divides $|G|$.

Solⁿ $\because a \in G \Rightarrow a^2 \in G, a^3 \in G, \dots$

$$\therefore \langle a \rangle \subseteq G \text{ and } \langle a \rangle \text{ is a subgroup of } G.$$

$$\Rightarrow |\langle a \rangle| \text{ divides } |G|$$

$$\Rightarrow |a| \text{ divides } |G|.$$