Coset:

Prepared By Dr. A. K. Maiti

Semester – II (UG)
Paper – C201
Course – Mathematics (H).

Coset

Def^n: Let G be a group and H be a subgroup of G.
Let a be an element of G. For all h in H, $ah \in G$.

Thus, the subset $\{ah : h \in H\}$ is called a left coset of H in G. and is denoted by aH.

Similarly, the subset $\{ha : h \in H\}$ is called the right coset of H in G.

- For different elements $b, c, \ldots$ in G, the left cosets of H are $bH, cH, \ldots$;
Similarly, the right cosets are $Hb, Hc, \ldots$ etc. for elements $b, c, \ldots$ in G.

In a additive group G, the left and right cosets of H are $a+H$ and $H+a$ respectively.

Example: (1) Let $G = (\mathbb{Z}, +)$, $H = (3\mathbb{Z}, +)$. V.H-2010.

The left coset $0 + H = \{3n : n \in \mathbb{Z}\} = H$

The left coset $1 + H = \{3n+1 : n \in \mathbb{Z}\}$

The left coset $2 + H = \{3n+2 : n \in \mathbb{Z}\}$.

There are three distinct left cosets of H.
They are H, $1+H$, $2+H$.

(2) Let $G = S_3$ and $H = \{\rho_0, \rho_3\}$.

Here $S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$ where

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Then $\rho_0 H = \{\rho_0, \rho_3\} = H$

$\rho_1 H = \{\rho_1, \rho_5\}$
$\rho_2 H = \{\rho_2, \rho_4\}$.
$\rho_3 H = \{\rho_0, \rho_3\} = H$
$\rho_4 H = \{\rho_2, \rho_4\} = \rho_2 H$
$\rho_5 H = \{\rho_1, \rho_5\} = \rho_1 H$.

There are three distinct left cosets of H. They are H, $\rho_1 H$, and $\rho_2 H$.

Theorem-1: If H is any subgroup of a group G and $h \in H$.
then $Hh = H = hH$. V.H-2010

Proof: Let h' be any arbitrary element of H. Then $h'h$ is an arbitray element of Hh.

Since H is a subgroup, we have $h' \in H, h \in H \Rightarrow h'h \in H$

Thus $h'h \in Hh \Rightarrow h'h \in H$.

ie every element of Hh is also an element of H.

$\therefore Hh \subseteq H$ —(i)

Again, $h' = h'(h^{-1}h)$ $[h^{-1}h = e]$

$= (h'h^{-1})h \in Hh$

[$\because h \in H \Rightarrow h^{-1} \in H$.
and $h' \in H, h^{-1} \in H \Rightarrow h'h^{-1} \in H$.
$\Rightarrow$ H is a subgroup of G]

$\therefore h' \in H \Rightarrow h' \in Hh$

ie every element of H is also an element of Hh.

$\therefore H \subseteq Hh$ —(ii).

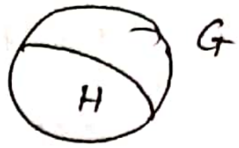
$\therefore$ From (i) and (ii), $Hh = H$.

Similarly, $hH = H$

Thus, $Hh = H = hH$. (Proved).

Theorem-2: If a, b are any two elements of a group G and H is any subgroup of G then

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \text{ and } aH = bH \Leftrightarrow a^{-1}b \in H.$$



Proof: Since a is an element of Ha.

Therefore, $Ha = Hb$

$\Rightarrow a \in Ha \Rightarrow a \in Hb$

$\Rightarrow ab^{-1} \in (Hb)b^{-1}$

$\Rightarrow ab^{-1} \in H \quad [\because bb^{-1} = e]$

Conversely, $ab^{-1} \in H$

$\Rightarrow Hab^{-1} = H \quad [\because h \in H \Rightarrow hH = H]$

$\Rightarrow Hab^{-1}b = Hb$

$\Rightarrow Ha = Hb.$

Similarly, we can prove that $aH = bH \Leftrightarrow a^{-1}b \in H$.

Hence the theorem.

Theorem-3: If a, b are any two elements of a group G and H is any subgroup of G. then

$$a \in Hb \Leftrightarrow Ha = Hb \text{ and } a \in bH \Leftrightarrow aH = bH.$$

Proof: We have, $a \in Hb$

$\Rightarrow ab^{-1} \in Hbb^{-1}$

$\Rightarrow ab^{-1} \in He \Rightarrow ab^{-1} \in H.$

$\Rightarrow Hab^{-1} = H \quad [\because h \in H \Rightarrow Hh = H]$

$\Rightarrow Hab^{-1}b = Hb$

$\Rightarrow Ha = Hb.$

Conversely, $Ha = Hb \Rightarrow ab^{-1} \in H$ [Proved previously]

Theorem: Any two right (left) cosets of a subgroup are either disjoint or identical. V.H–2010

Proof: Suppose H is a subgroup of a group G and let Ha and Hb are two right cosets of H in G. Suppose Ha and Hb are not disjoint. Then there exists at least one element c (say) such that $c \in Ha$ and $c \in Hb$.

Let $c = h_1 a$ for $h_1 \in H$

and $c = h_2 b$ for $h_2 \in H$.

Then $h_1 a = h_2 b$

$\Rightarrow h_1^{-1}(h_1 a) = h_1^{-1} h_2 b$

$\Rightarrow e a = (h_1^{-1} h_2) b \quad [h_1^{-1} h_1 = e]$

$\Rightarrow a = (h_1^{-1} h_2) b. \quad [\because a \cdot e = a]$

Since H is a subgroup, therefore $h_1^{-1} h_2 \in H$.

Let $h_1^{-1} h_2 = h_3$.

Now, $Ha = H h_3 b = (H h_3) b = Hb \quad \left[\because h_3 \in H \Rightarrow H h_3 = H\right]$

$\therefore$ Therefore, the two right cosets are identical if they are not disjoint.

Thus, either $Ha \cap Hb = \phi$ or $Ha = Hb$.

Lagrange theorem:

Statement: The order of every subgroup of a finite group G is a divisor of the order of G.

Proof: Let G be a group of finite order n. Let H be a subgroup of G. and let $O(H) = m$, $O(G) = n$.

Suppose $h_1, h_2, \ldots h_m$ are the m distinct members of H.

Let $a \in G$. Then Ha is a right coset of H in G. and

We have $Ha = \{h_1a, h_2a, \ldots, h_ma\}$.

Ha has m distinct members, since $h_ia = h_ja$, $i \neq j$

$\Rightarrow h_i = h_j$ [cancellation law]

Which is not true.

Therefore each right coset of H in G has m distinct members.

Since G is a finite group, the number of distinct right cosets of H in G will be finite say k.

The union of these k-distinct right cosets of H in G is equal to G. Thus if $Ha_1, Ha_2, \ldots, Ha_k$ are k distinct right cosets of H in G then $G = Ha_1 \cup Ha_2 \cup Ha_3 \ldots \cup Ha_k$.

$\Rightarrow$ The no. of elements in G = The no. of elements in Ha_1 + ... + The no. of elements in Ha_k.

$$\Rightarrow O(G) = O(Ha_1) + O(Ha_2) + \ldots + O(Ha_k).$$

$$\Rightarrow n = m + m + \ldots + m \ (k \text{ times})$$

$$\Rightarrow n = mk$$

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

Hence $O(H)$ is a divisor of $O(G)$.

Hence the theorem.

Note: The converse of Lagrange's theorem is not true.

For ex: The alternating group A_4 of degree 4 is of order 12. It can be seen that there is no subgroup of A_4 of order 6 though 6 is a divisor of 12.

Index: If G be a group and H be a subgroup of G then the number of distinct left cosets of H

in G is called the index of H in G and denoted by $[G:H]$. Lagrange's theorem say that $[G:H] = \frac{O(G)}{O(H)}$.

Theorem: Every group of prime order is cyclic.

Proof: Let G be a group of prime order p. Since p is prime, $O(G)>1$. Let a be a non-identity element of G and H be a cyclic subgroup generated by a., $a \neq e$

Therefore $O(H)>1$.

Since H is a subgroup of G, by Lagrange's theorem, $O(H)$ is a divisor of p. Since p is prime, then only divisors of p are 1 and p.

Therefore, $O(H) = p$, since $O(H) \neq 1$.

Therefore $H = G$. and this proves that G is a cyclic group generated by a.

Ex: Prove that every group of order less than 6 is commutative.
V.H -

Ans: A group of order 1 contains the identity element e only. This is a cyclic group generated by e.

Therefore it is a commutative group.

A group of order 2 is cyclic, since 2 is prime. Therefore it is commutative.

A group of order 3 is cyclic, since 3 is prime. Therefore it is commutative.

Let us consider a group of order 4. Then order of every element of G is a divisor of $O(G)$. The divisors are 1, 2 and 4.

Case-I: If there exists an element of order 4 in G, then the group is cyclic. Therefore it is commutative.

Case-II: If there exists no element of order 4, then each non-identity element of the group is of order 2 and the order of the identity element is 1. Therefore, for every element a in G

$$a \circ a = e$$

$$\Rightarrow a = a^{-1}, \ \forall a \in G.$$

Let $a, b \in G$. Then $a = a^{-1}$, $b = b^{-1}$

Also, $a, b \in G \Rightarrow a \circ b \in G$.

$$\therefore (a \circ b) = (a \circ b)^{-1}$$

$$\Rightarrow a \circ b = b^{-1} \circ a^{-1}$$

$$= b \circ a$$

$\therefore a \circ b = b \circ a \ \forall a, b \in G$, G is commutative.

It follows that a group of order 4 is always commutative.

A group of order 5 is cyclic, since 5 is prime. Therefore it is commutative.

Therefore, every group of order less than 6 is commutative.

Ex: Prove that every proper subgroup of a group of order 6 is cyclic. V.H-'06.

Ans: Let G be a group of order 6 and H be a proper subgroup of G.

By Lagrange's theorem, $O(H)$ is a divisor of 6. The divisors of 6 are 1, 2, 3 and 6. Since H is a proper subgroup of G, $O(H) < 6$.

If $O(H) = 1$ then $H = \{e\} = \langle e \rangle$ and H is cyclic.

If $O(H) = 2$ then H is a group of prime order and so H is cyclic.

If $O(H) = 3$, then also H is a group of prime order and so H is a cyclic.

Thus in any case, H is cyclic.

Note: Every proper subgroup of a symmetric group S_3 is cyclic.
V.I-06.

Theorem: A cyclic group of prime order has no proper non-trivial subgroup.

Proof: Let (G, o) be a cyclic group of prime order p and let $G = \langle a \rangle$. Let (H, o) be a cyclic subgroup generated by a^m, m is the least positive integer.

Since $O(G) = p$, $a^p = e$.

Since $H = \langle a^m \rangle$ and $a^p \in H$, $p = mk$ for some integer k.

Therefore, m is a divisor of p. Since p is prime, m is either 1 or p.

If $m = 1$ then $H = G$

If $m = p$ then $H = \{e\}$.

Therefore (H, o) is either trivial subgroup $\{e\}$ or the improper subgroup G.

Ex: Show that the group of order 2 and 3 are always cyclic but the group of order 4 may or may not be a cyclic.

Ans: We know that every group of prime order is cyclic. Here 2 and 3 are prime. Therefore, the group of order 2 and 3 are always cyclic.

We consider the example, the group of order 2 and 3 are $\{-1, 1\}$ and $\{1, \omega, \omega^2\}$.

Now, $(-1)^1=1$, $(-1)^2=1$, $(-1)^3=-1$, $(-1)^4=1$, ...

Here $\langle -1 \rangle$ is a generator of $\{-1,1\}$.

Thus $\{-1,1\}$ is a cyclic group order 2.

Again, $\omega^1=\omega$ and $(\omega^2)^1=\omega^2$

$\omega^2=\omega^2$ $\quad (\omega^2)^2=\omega$

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

$\omega^4=\omega$ $\quad (\omega^2)^4=\omega^2$

$\omega^5=\omega^2$ $\quad (\omega^2)^5=\omega$

$\omega^6=\omega^3=1$ $\quad$ - - - -

- - -

Here ω and ω^2 are generators of $\{1,\omega,\omega^2\}$.

Thus $\{1,\omega,\omega^2\}$ is a cyclic group of order 3.

Again, 4 is not a prime number, therefore 4 may or may not be cyclic. We consider the example, $\{1,-1,i,-i\}$ is a group of order 4. Also, $\{1,-1,i,-i\}$ is also a cyclic group generated by i and $-i$.

But the Klein's 4-group $\{e,a,b,c\}$ of order 4 is not cyclic group.

(Ex): Find the right cosets of the subgroup $\{-1,1\}$ of the multiplicative group of all nonzero reals that contains 5.

Ans: Let $H=\{1,-1\}$. ~~$G=\{x : x\in R\}$~~

$G=\{R-\{0\},\cdot\}$

Then $H\circ 5=\{-5,5\}$ is the right coset of H.

Again $H\circ x=\{-x,x\}$ is the rights of H where $x(\neq 0)\in R$.

(Ex) In the symmetric group S_3, find two subgroups A and B such that $A\cup B$ is not a subgroup of S_3. C.H-01

$\therefore$ ρ_3 and ρ_4 does not belong to $A \cup B$.

<u>Ans</u>: Let 1, 2, 3 be the elements of a set and then six Permutations are $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$,

$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

ρ_0 is the identity element.

The set $S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$ is a group with respect to permutation multiplication.

In that case composition table of S_3 is

	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_0	ρ_4	ρ_5	ρ_2	ρ_3
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	ρ_5	ρ_4
ρ_3	ρ_3	ρ_2	ρ_5	ρ_4	ρ_0	ρ_1
ρ_4	ρ_4	ρ_5	ρ_1	ρ_0	ρ_3	ρ_2
ρ_5	ρ_5	ρ_4	ρ_3	ρ_2	ρ_1	ρ_0

The subsets $\{\rho_0, \rho_1\}$, $\{\rho_0, \rho_2\}$ and $\{\rho_0, \rho_5\}$ are subgroups of S_3 with ρ_0 as the identity. These are groups of order 2.

Again $\{\rho_0, \rho_3, \rho_4\}$ is the only subgroup of S_3 of order 3.

$\{\rho_0\}$ ~~and ρ_3 it~~ is a subgroup of order one.

and S_3 it self is a subgroup of S_3 of order 6.

$\{\rho_0\}$ and S_3 are improper subgroups. The other are proper subgroups. The orders of the subgroups are namely, 1, 2, 3, 6, are factors of 6 [By Lagrange's theorem].

Here, we take $A = \{\rho_0, \rho_1\}$, $B = \{\rho_0, \rho_5\}$ be two subgroups of the symmetric ~~sets~~ group S_3. Now $A \cup B = \{\rho_0, \rho_1, \rho_5\}$ is not a subgroup, since $\rho_1 \cdot \rho_5 = \rho_3$, $\rho_5 \cdot \rho_1 = \rho_4$

i.e. ρ_3 and ρ_4 does not belong to $A \cup B$.

So, $A \cup B = \{\rho_0, \rho_1, \rho_5\}$ is not a subgroup of S_3.

<u>Theorem</u>: Let G be group and H be a subgroup of G. Let $a \in G-H$. Then $aH \cap H = \varphi$.

<u>Ans</u>: If possible, let $p \in aH \cap H \Rightarrow p \in aH$ and $p \in H$

Hence $p = ah_1$ for some h_1 in H and $p = h_2$ for some $h_2 \in H$.

This implies $h_2 = ah_1 \Rightarrow a = h_2 h_1^{-1} \in H$, H is a subgroup.

This contradicts that $a \in G-H$.

So, $aH \cap H = \varphi$.

<u>Theorem</u>: The order of each element in a finite group G is a divisor of $o(G)$.

<u>Proof</u>: Let G be a finite group and $a \in G$. The cyclic group $\langle a \rangle$ is a subgroup of G. By Lagrange's theorem, $o(\langle a \rangle)$ is a divisor of $o(G)$.

But $o(a) = o(\langle a \rangle)$.

$\therefore$ $o(a)$ is a divisor of $o(G)$.