UNIT-III

COSETS & NORMAL SUBGROUPS

Outline of Presentation

- Definition & Examples of Cosets
- Properties of Cosets
- Index of a Subgroup
- Order of an element
- Normal Subgroup
- Quotient Group

Definition: Let H be a subgroup of a group (G,o). If $a \in G$ then the subset aoH of G defined by

aoH = { aoh : $h \in H$ }

is called a **left coset of H** in G determined by element $a \in G$.

Similarly, the subset Hoa of G defined by

Hoa = { hoa : $h \in H$ }

is called a **right coset of H** in G determined by element $a \in G$.

Note that (i) Cosets are not subgroups in general!

(ii) If e is the identity of (G,.) and H is subgroup of G then H itself is a left as well as right coset.

(iii) If (G, +) is a group under addition and H is a subgroup of G.

For $a \in G$

$$a + H = \{ a + h : h \in H \}$$

$$H + a = \{ h + a : h \in H \}$$

are left coset and right coset respectively.

(iv) If (G,o) is an Abelian group then left coset of G is same as right coset of G, i.e., aoH = Hoa

Examples:

1. Suppose G= {1, -1, i, -i}is a group under operation multiplication, where $i^2 = -1$.

   H = { 1, -1 } is a subgroup of G.

   The right coset of H in G are H.1, H.(-1), H(i), H(-i), where

   H.1 = { 1.1, (-1).1 } = H

   H.(-1) = { 1.(-1), (-1)(-1) } = { -1, 1 }= H

   H. i = { 1.i, (-1).i } = { i, -i }

   H.(-i) = {1.(-i), (-1)(-i)} = {-i, i }

2. Suppose G = Z, the set of integers is a group under addition.

H = 2Z, the set of even integers is a subgroup of Z

$H = \{ 0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots \ldots \}$

$H + 0 = \{ h + 0 : h \in H \} = \{h : h \in H \} = H$

$H + 1 = \{ h + 1 : h \in H \} = \{ \pm 1, \pm 3, \pm 5, \ldots \}$

$H + 2 = \{ h + 2 : h \in H \} = \{ 0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots \ldots \}$

$H + 3 = \{ h + 3 : h \in H \} = \{ \pm 1, \pm 3, \pm 5, \ldots \}$

Hence, the only distinct right cosets of H in G are H and H + 1.

Properties of Cosets:

1.Theorem: If G is an abelian group and $a \in G$ then aH = Ha.

Proof: Let $x \in Ha$. Then x = ha for some $h \in H$.

As $h \in H \Rightarrow h \in G$. Again, $a \in G$ and G is abelian, ha = ah

$\Rightarrow$ x = ah for some $h \in H$.

$\Rightarrow x \in a\,H$.

Thus, Ha $\subseteq aH$

Similarly, if $x \in aH$. Then x = ah for some $h \in H$.

As $h \in H \Rightarrow h \in G$. Again, $a \in G$ and G is abelian,

we have, ah = ha $\Rightarrow$ x = ha for some $h \in H$.

$\Rightarrow x \in Ha$. Thus, aH $\subseteq Ha$. Hence, a H = Ha.

2.Theorem: If H is a subgroup of G and a, b $\in G$, then

(i) Ha = H if and only if a $\in H$

(ii) aH = H if and only if a $\in H$

(iii) Ha = Hb if only if $ab^{-1} \in H$

(iv) aH = bH if and only if $a^{-1}b \in H$.

Proof: (i) Firstly, suppose Ha = H.

As H is subgroup of G, so $e \in H$

Thus, $ea \in Ha \Rightarrow a \in Ha \Rightarrow a \in H$.

Hence, Ha = H $\Rightarrow a \in H$.

Conversely, suppose $a \in H$. To prove Ha = H.

Let $x \in Ha \Rightarrow x = ha$ $for\ some\ h \in H$.

Now, $h, a \in H \Rightarrow ha \in H \Rightarrow x \in H$.

This shows that $x \in Ha \Rightarrow x \in H$

$\Rightarrow Ha \subseteq H$. ……….(eq. 1)

Now, take $x \in H$. $Given\ a \in H \Rightarrow xa^{-1} \in H$.

$$\Rightarrow (xa^{-1})a \in Ha \Rightarrow x(a^{-1}a) \in Ha$$

$$\Rightarrow x.e \in Ha \Rightarrow x \in Ha$$

This proves that if $x \in H \Rightarrow x \in Ha \Rightarrow H \subseteq Ha$. ……..(eq. 2)

From eq. (1) & (2), we have Ha = H.

(ii) Proof is similar to (i).

(iii) Firstly, suppose Ha = Hb.

Now $e \in H$, as H is a subgroup of G $\Rightarrow ea \in Ha, \; a \in Ha$

$$\Rightarrow a \in Hb, \text{ since Ha = Hb}$$

$$\Rightarrow a = hb \quad for \quad h \in H$$

$$\Rightarrow ab^{-1} = (hb)b^{-1} = h(bb^{-1}) = h\,e = h$$

Thus, $ab^{-1} \in H$.

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

Therefore, $ab^{-1} = h \;\; for\ some\ h \in H$.

$$\Rightarrow \; (ab^{-1})b = hb \;\; \Rightarrow a(b^{-1}b) = h\,b \Rightarrow a = hb.$$

Thus, Ha = H (hb) = (Hh)b = Hb.

(iv) Proof is similar to (iii).

3. Theorem: If H is a subgroup of G and a, b $\in G$, then

(i) $a \in H$b if and only if Ha = Hb

(ii) $a \in bH$ if and only if aH = bH.

Proof: (i) Suppose $a \in H$b.

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

$\Rightarrow a\, b^{-1} \in H(\mathrm{b}b^{-1})$

$\Rightarrow \mathrm{a}b^{-1} \in He = H$

$\Rightarrow \mathrm{Ha}b^{-1} = H$

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

$\Rightarrow Ha\,(b^{-1}b) = Hb$

$$\Rightarrow Hae = Hb \;\Rightarrow Ha = Hb.$$

Conversely, let Ha = Hb. Now $e \in$ H, as H is a subgroup of G.

$$\Rightarrow ea \in Ha \;\Rightarrow a \in Ha\,,$$

$$But\ Ha = Hb \;\Rightarrow a \in Hb.$$

(ii) Proof is similar to (i)

4. Theorem: Prove that any two right(left) cosets of a subgroup are either disjoint or identical.

Proof: Let H be a subgroup of a group G and $a, b \in G$.

Let Ha and Hb be two right cosets of H in G.

We have to show that either Ha = Hb or $\boldsymbol{Ha \cap Hb = \emptyset}$.

Case 1: If $Ha \cap Hb = \emptyset$, then nothing to prove.

Case 2: Let $Ha \cap Hb \neq \emptyset$. We have to show that Ha = Hb.

Since $Ha \cap Hb \neq \emptyset$, so there exist atleast one element

$$x \in Ha \cap Hb$$

$$\Rightarrow x \in Ha \quad \& \quad x \in Hb$$

$$\Rightarrow x = h_1 a \text{ for some } h_1 \in H \quad \& \quad x = h_2 b \text{ for some } h_2 \in H$$

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

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

$$\Rightarrow ea = h_3 b, \; where \; h_3 = (h_1^{-1} h_2) \in H$$

$$\Rightarrow a = h_3 b \quad \Rightarrow Ha = H(h_3 b) = (Hh_3) b = Hb$$

$since \; Hh_3 = H.$

Hence, Ha = Hb.

Thus, if $Ha \cap Hb \neq \emptyset,$ then Ha = Hb.

So, either Ha = Hb or $Ha \cap Hb = \emptyset$.

5.Theorem : The group G is equal to the union of all right cosets of H in G.

Proof: Let e,a,b,c,……be elements of G and H=He, Ha, Hb, Hc, …… are right cosets of H in G. We have to show that

$$\mathrm{G} = \mathrm{H} \cup \mathrm{Ha} \cup \mathrm{Hb} \cup \mathrm{Hc} \cup \ldots\ldots\ldots$$

Let $x \in G$ and xH be a right coset of H in G.

Now $ex \in Hx$, (since $e \in G$ and H is a subgroup of G).

Thus, $x \in Hx \Rightarrow x \in \mathrm{H} \cup \mathrm{Ha} \cup \mathrm{Hb} \cup \mathrm{Hc} \cup \ldots . \cup \mathrm{Hx} \cup \ldots\ldots\ldots$

Therefore,

$$\mathrm{G} \subset \mathrm{H} \cup \mathrm{Ha} \cup \mathrm{Hb} \cup \mathrm{Hc} \cup \ldots\ldots\ldots (1)$$

Conversely, suppose Ha is any right coset of H in G, where $a \in G$.

Let $x \in Ha \Rightarrow x = ha$ for some $h \in H$. As $H \subset G \Rightarrow h \in G$.

Also $a \in G \Rightarrow ha \in G \Rightarrow x \in G$.

Therefore, $x \in Ha \Rightarrow x \in G$.

Hence,

$$Ha \subset G \Rightarrow \bigcup_{a \in G} Ha \subset G.$$

$$\Rightarrow \mathrm{H} \cup \mathrm{Ha} \cup \mathrm{Hb} \cup \mathrm{Hc} \cup \ldots. \subset \mathrm{G} \qquad \ldots\ldots(2)$$

From (1) & (2), we have

$$\mathrm{G} = \mathrm{H} \cup \mathrm{Ha} \cup \mathrm{Hb} \cup \mathrm{Hc} \cup \ldots\ldots\ldots$$

6.Theorem: There is one-to-one correspondence between any two left cosets of H in G.

Proof: Let aH and bH be two left cosets of H in G for $a, b \in H$.

Define a map f: aH $\rightarrow$ bH by f(ah) = bh $\forall ah \in aH$.

<u>f is one-to-one map</u>: Let $x, y \in aH$ such that f(x) = f(y).

Since $x, y \in aH \Rightarrow x = ah_1, y = ah_2$ $for\ some\ h_1 h_2 \in H$.

Thus, $f(x) = f(y) \Rightarrow f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2$

$\Rightarrow bh_1 = bh_2 \Rightarrow h_1 = h_2$ by left cancellation laws.

$\Rightarrow ah_1 = ah_2 \Rightarrow x = y \Rightarrow f$ is one-to-one.

<u>f is onto map</u>: Let $y \in bH \Rightarrow y = bh$ for some $h \in H$.

Suppose x = ah. Since $h \in H \Rightarrow ah \in aH \Rightarrow x \in aH$

where $x = ah \in aH$. Thus, f is onto map.

Therefore, f is one-to-one and onto map.

Hence, aH and bH are in one-one correspondence.

7.Theorem: There is one-to-one correspondence between any two right cosets of H in G.

Proof: Same as in theorem 6 by using right cosets in place of left cosets.

8.Theorem: There is one-to-one correspondence between the set of all left cosets of H in G and the set of right cosets of H in G.

Proof: Let $\mathrm{L} = \{\mathrm{aH}: \mathrm{a} \in \mathrm{G}\}$ and $M = \{ Ha : a \in G\}$

Define a map $\mathrm{f} : \mathrm{L} \rightarrow \mathrm{M}$ by $f\,(aH) = Ha^{-1}\, \forall a \in G$.

If $a \in G$ then $a^{-1} \in G$ and hence $Ha^{-1} \in M$, so f is a map from L to M.

<u>f is well-defined</u>: Let $a, b \in G$ such that aH = bH

$$\Leftrightarrow a^{-1}b \in H \Leftrightarrow Ha^{-1}b = H \Leftrightarrow (Ha^{-1}b)b^{-1} = Hb^{-1}$$

$$\Leftrightarrow Ha^{-1}(bb^{-1}) = Hb^{-1} \Leftrightarrow Ha^{-1}e = Hb^{-1}$$

$\Leftrightarrow Ha^{-1} = Hb^{-1} \Leftrightarrow f(aH) = f(bH)$.

Thus, f is well-defined.

<u>f is one-one map</u>: The proof follows from reverse steps of f is well-defined.

<u>f is onto map</u>: Let $Ha \in M$ be arbitrarily.

As $a \in G \Rightarrow a^{-1} \in G \Rightarrow a^{-1}H \in L$ such that

$f(a^{-1}H) = H(a^{-1})^{-1} = Ha$. Thus, f is onto map.

Hence, f : L $\rightarrow$ M is one-to-one and onto map.

Definition: (Index of Subgroup)

The number of distinct left or right cosets of a subgroup H in group G is called the **index of H in G** and is denoted by [G:H]

Definition: (Order of an element)

Let a be an element of a group G. If there exists a positive integer such that $a^n = e$, then a is said to have finite order and the smallest such positive n such that $a^n = e$ is called the **order of a** and is denoted by O(a).

If there does not exist a positive integer n such that $a^n = e$, then a is said to have **infinite order or the order does not exist**.

If (G, +) is an additive group and a is an element of G then n is called order of an element a if n is a smallest +ve integer such that

$$na = a + a + a + \cdots (n - times) + a = 0$$

Example: In group $(G, +_6)$, the order of each element exists.

Here G = {0, 1, 2, 3, 4, 5}.

The order of 0, O(0)= 1, O(1) = 6,

O(2) = 3,O(3) = 2, O(4) = 3, O(5) = 6

Lagrange's Theorem:

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

Proof: Let G be a group of finite order n. Let H be a subgroup of G and let O(H) = m. Suppose $h_1, h_2, h_3, h_4, \ldots\ldots h_m$ be m distinct elements of H. Suppose $a \in G$, Ha is a right coset of H in G and we have

$$Ha = \{ h_1a, h_2a, h_3a, \ldots\ldots h_ma\}$$

Ha has m distinct elements, (since if

$$h_ia = h_ja, \qquad 1 \leq i, j \leq m, i \neq j$$

By using right cancellation laws, $h_i = h_j$, a contradiction.)

Hence, each right coset of H in G has m distinct members. Any two distinct right cosets of H in G are disjoint. Since G is a finite group, the number of distinct right cosets of H in G will be finite, say equal to k. The union of these k distinct right cosets of H in G is equal to G.

Thus, if $Ha_1, Ha_2, Ha_3, \ldots\ldots Ha_k$ are distinct right cosets of H in G, then

$$G = Ha_1 \cup Ha_2 \cup Ha_3 \cup \ldots\ldots \cup Ha_k$$

Therefore, Number of elements in G

= the number of elements in Ha_1 + number of elements in Ha_2 + …….+ the number of elements in Ha_k

(since two distinct right cosets are mutually disjoint)

This implies that $O(G) = km \Rightarrow n = km \Rightarrow k = \frac{n}{m}$

Thus, m is a divisor of n.

This shows that O(H) is a divisor of o(G).

Hence, the theorem.

Converse of the Lagrange's theorem is not true.

e.g. The alternating group A_4 of degree 4 is of order 12. But there is no subgroup of A_4 of order 6, although 6 is a divisor of 12.

Definition (Normal Subgroups)

A subgroup H of G is called a **normal subgroup** of G if every left coset of H in G is equal to the corresponding right coset of h in G.

i.e., aH = Ha, for all $a \in G$.

Note that (i) If (G,+) is an additive group and H is called normal subgroup of G iff a + H = H + a for all $a \in G$.

(ii) If G is an Abelian group then every subgroup H of G is a normal subgroup.

(iii) The subgroups {e} and G of any group G are always normal subgroups of G. These are called trivial normal subgroups.

Theorem: A subgroup H of G is a normal subgroup of G if and only if $ghg^{-1} \in H \ \forall\, h \in H, g \in G$.

Proof: Firstly, suppose H is a normal subgroup of G.

Therefore, $gH = Hg \ \forall\, g \in G$.

Let $h \in H, g \in G$. Then $gh \in gH = Hg \Rightarrow gH \in Hg$.

This implies that $gh = h_1 g$ for some $h_1 \in H$

$\Rightarrow ghg^{-1} = h_1 \in H \Rightarrow ghg^{-1} \in H$.

Conversely, suppose H is a subgroup of G such that

$ghg^{-1} \in H \ \forall\, h \in H, g \in G$.

We have to show that H is a normal subgroup,

i.e., $a H = Ha \ \forall\, a \in G$.

Let $a \in G$. Then by given condition

$$aha^{-1} \in H \quad \forall\, h \in H.$$

Suppose $ah \in aH$. Then

$$aH = (aHa^{-1})a \in Ha \Rightarrow ah \in Ha \Rightarrow aH \subset Ha \ldots .(1)$$

Again, let $b = a^{-1} \in G$.

Then by given condition $bhb^{-1} \in H$.

But $bhb^{-1} = a^{-1}h(a^{-1})^{-1} = a^{-1}ha \in H$.

Let $ha \in Ha$. Then

$$ha = (aa^{-1})ha = a(a^{-1}ha) \in a\,H$$

$$\Rightarrow ha \in a\,H \Rightarrow Ha \subset a\,H \ldots\ldots.(2)$$

From (1) and (2), we get $aH = Ha \quad \forall\, a \in G$

Hence, H is a normal subgroup of G.

Theorem: Let H be subgroup of a group G. Then the following are equivalent:

$$(i)\ \ ghg^{-1} \in H,\ \ \forall\, g \in G, h \in H.$$

$$(ii)\ gHg^{-1} = H,\ \ \forall\, g \in G.$$

$$(iii)\ gH = Hg\ \ \forall\, g \in G.$$

Proof: $(\boldsymbol{i}) \Rightarrow (\boldsymbol{ii})$ Given $ghg^{-1} \in H,\ \forall\, g \in G, h \in H.$

Let $ghg^{-1} = h_1\ \ \forall\, h_1 \in H, \Rightarrow gHg^{-1} = H\ \ \forall\, g \in G.$

$(\boldsymbol{ii}) \Rightarrow (\boldsymbol{iii})$ Given $gHg^{-1} = H,\ \forall\, g \in G$

$$\Rightarrow (gHg^{-1})g = Hg,\ \forall\, g \in G$$

$$\Rightarrow gH(g^{-1}g) = Hg, \ \ \forall\, g \in G$$

$$\Rightarrow gHe = Hg, \ \ \forall\, g \in G$$

$$\Rightarrow gH = Hg, \ \ \forall\, g \in G$$

$(iii) \Rightarrow (i)$ $\quad Given \qquad gH = Hg, \ \ \forall\, g \in G$

$$\Rightarrow g\,h = h_1 g \quad \forall\, h, h_1 \in H$$

$$\Rightarrow g\,hg^{-1} = h_1 \in H$$

$$\Rightarrow g\,hg^{-1} \in H.$$

Hence, the theorem.

Ex: If H is a subgroup of G of index 2 in G then H is normal subgroup of G.

Solu: Let H be a subgroup of G such that [G:H]= 2. Thus, the number of distinct cosets(left or right) of H in G is 2.

We have to show that H is a normal subgroup of G.

It is enough to show that $aH = Ha \; \forall \; a \in G$.

Case I: If $a \in H \Rightarrow \quad aH = H = Ha$. Hence, H is a normal subgroup of G.

Case II: If $a \notin H \Rightarrow aH \neq H, \; Ha \neq H$.

Also, [G:H] = 2, $H \cup aH = G = H \cup Ha$

$$\Rightarrow aH = Ha.$$

From Case(I) and Case (II), we have $aH = Ha \; \forall \; a \in G$.

Hence, H is a normal subgroup of G.

Quotient Group

Definition: Let H be normal subgroup of group G.

Consider the set G/H, where

$$G/H = \{ aH : a \in G\},$$

the set G/H of all the left(right) cosets of H in G. Define an operation of composition as (aH)(bH) = abH.

Then G/H forms a group under the composition and group is known as **Quotient Group.**

Theorem: Let H be normal subgroup of G. Then the set G/H of all the left(right) cosets of H in G forms a group under the composition defined by (aH)(bH) = abH.

Proof: Let H be normal subgroup of group G.

Then the set $G/_H = \{ aH: a \in G\}$

For $aH, bH \in G/_H$ Define the composition in $G/_H$ as

(aH)(bH) = abH

To show that the above composition is well-defined.

Let $a H = cH$ & $bH = dH \;\; \forall c, d \in G$

Now $aH = cH \Rightarrow c^{-1}a \in H \Rightarrow c^{-1}a = h_1 \;\; \forall h_1 \in H$

$$\Rightarrow a = ch_1 \;\; \forall h_1 \in H$$

Thus, $aH = cH \Rightarrow a = ch_1 \ \forall h_1 \in H$.

Similarly, $bH = dH \Rightarrow b = dh_2 \ \forall h_2 \in H$.

Hence, the composition is well-defined if (aH)(bH) = (cH)(dH)

if abH = cdH if $(ab)(cd)^{-1} \in H$.

To show $G/_H$ is a group, let $aH, bH, cH \in G/_H \ \forall a, b, c \in G$.

Closure Property: $aH\ bH = abH \in G/_H$ *since* $ab \in G$.

Associativity:$(aH.bH)cH = (abH)(cH) = (ab)cH = a(bc)H$

(since $a(bc) = (ab)c \ \forall a, b, c \in G$)

$= aH(bcH) = aH(bH.cH)$.

Existence of Identity: Let $e \in G,\ eH \in G/_H$

$(aH)(eH) = aeH = aH = eaH = eHaH$.

Thus, $He = H$ is identity element of G/H

Existence of Inverse: For $aH \in G/H$ we have $a \in G \Rightarrow a^{-1} \in G$

$$\Rightarrow a^{-1}H \in G/H$$

$$(aH)(a^{-1}H) = aa^{-1}H = eH = H = He = a^{-1}aH$$
$$= (a^{-1}H)(aH)$$

Thus, $a^{-1}H$ is the inverse of $aH \in G/H$

Hence, G/H forms a group.

****