UNIT 2: LAGRANGE'S THEOREM, NORMAL GROUPS AND QUOTIENT GROUPS

UNIT STRUCTURE

2.1 Learning objectives

2.2 Introduction

2.3 Coset

2.4 Lagrange's Subgroup order theorem

2.5 Normal subgroup

2.6 Quotient Groups

2.7 Let us Sum Up

2.8 Answers to Check Your Progress

2.9 Further Readings

2.10 Model Questions

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to know :

- cosets of a subgroup
- lagrange's subgroup order theorem
- normal subgroups
- quotient groups.

2.2 INTRODUCTION

We have already discussed group ,subgroup and their properties in unit 1. In this unit,we will discuss cosets of a subgroup of a group.

We will also discuss Lagrange's subgroup order theorem in this unit.In this unit,we will discuss normal subgroup of a group.In this unit,we will also discuss quotient group.

2.3 COSET

Let G be a group and $H \leq G$

Let $a \in G$

The set Ha = {ha : h $\in$ H} is called a right coset of H in G.

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

Note : (1) Right (or left) coset cannot be empty ,we have e$\in$H

$\therefore$ ea = a $\in$ H a $\quad\quad$ $\therefore$ Ha $\neq \phi$

Similarly ae = a $\in$ aH $\therefore$ aH $\neq \phi$

(2) H $\leq$ G, but Ha or aH is not necessarily a subgroup of G.

(3) If H is a subgroup of the additive group G and a $\in$ G, the right coset of H in G is given by H+a = {h+a : h $\in$ H}

Similarly, the left coset of H in G is given by a+H={a+h : h$\in$ H}

(4) If G is abelian,then every left coset is a right coset.

Example : Let us consider the additive group of integers Z.

We know that 2 Z = {0, $\pm$2, $\pm$4, $\pm$6,.....} $\leq$ Z

We have

0+2 Z = {0, $\pm$2, $\pm$4, $\pm$6,.....} = 2 Z

1+2Z = {$\pm$1, $\pm$3, $\pm$5, $\pm$7, ...}

2+2Z = {0, $\pm$2, $\pm$4, $\pm$6, ...}

3+2Z = {$\pm$1, $\pm$3, $\pm$5, $\pm$7, ...} and so on.

Thus, we see that

2Z = 2+2Z = 4+2Z = ...

1+2Z = 3+2Z = 5+2Z = ...

$\therefore$ 2Z has two distinct left cosets viz. 2Z and 1+2Z such that

$$2Z \cup (1+2Z) = Z$$

$$2Z \cap (1+2Z) = \phi$$

Similarly, 2Z has two distinct right cosets 2Z and 2Z + 1 such that

$$2Z \cup (2Z+1) = Z$$

$$2Z \cap (2Z+1) = \phi$$

Theorem 1 : Let G be a group and H $\leq$ G. Then

(i) aH = H $\Leftrightarrow$ a $\in$ H; Ha = H $\Leftrightarrow$ a $\in$ H

(ii) aH = bH $\Leftrightarrow$ $a^{-1}b \in H$; Ha = Hb $\Leftrightarrow$ $ab^{-1} \in H$, where a, b$\in$ G

Proof : (i) Let aH = H

We have ae$\in$ aH, e is the identity of G

$\Rightarrow$ ae$\in$ H $\quad$ [$\because$ aH = H]

$\Rightarrow$ a $\in$ H

Conversely, let $a \in H$

Let $x \in aH$

This $\Rightarrow x = ah$, for some $h \in H$

Now $a \in H, h \in H \quad \therefore ah \in H \Rightarrow x \in H$

Thus, $x \in aH \quad \Rightarrow x \in H$

$\therefore aH \subseteq H \quad ...(1)$

Again, let $y \in H$

$\therefore a \in H, \therefore a^{-1} \in H$

$\therefore a^{-1}y \in H$

$\Rightarrow a^{-1}y = h_1$, for some $h_1 \in H$

$\Rightarrow a(a^{-1}y) = ah_1$

$\Rightarrow (aa^{-1})y = ah_1$

$\Rightarrow ey = ah_1$

$\Rightarrow y = ah_1 \in aH$

Thus, $y \in H \Rightarrow y \in aH$

$\therefore H \subseteq aH \quad ...(2)$

From (1) and (2), $aH = H$

Similarly $Ha = H \Leftrightarrow a \in H$.

(ii) $aH = bH$

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

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

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

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

$\Leftrightarrow a^{-1}b \in H$ (using (1)

Similarly, $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Theorem 2 : (i) Any two left (or right) cosets of a subgroup are either disjoint or identical.

(ii) A group G is union of all its right (or left) cosets of a subgroup H of G.

Proof :(i) Let G be a group and $H \leq G$.

Let $a, b \in G$.

Then aH, bH are two left cosets of H in G.

Clearly aH, bH are either disjoint or not disjoint.

Let aH, bH be not disjoint, i.e, $aH \cap bH \neq \phi$.

Let $x \in aH \cap bH$

$\Rightarrow x \in aH$ and $x \in bH$

Now $x \in aH \Rightarrow x = ah_1$ for some $h_1 \in H$

$x \in bH \Rightarrow x = bh_2$ for some $h_2 \in H$

$\therefore ah_1 = bh_2$

$\Rightarrow (ah_1)h_1^{-1} = (bh_2)h_1^{-1}$

$\Rightarrow a\, h_1h_1^{-1} = b\, h_2h_1^{-1}$

$\Rightarrow ae = bh_2h_1^{-1}$, where e is the identity of G

$\Rightarrow a = bh_2h_1^{-1}$

Similarly $b = ah_1h_2^{-1}$

Let $p \in aH \Rightarrow p = ah_3$ for some $h_3 \in H$

$= bh_2h_1^{-1}h_3$

$\in bH, \because h_2h_1^{-1}h_3 \in H$

Thus, $p \in aH \Rightarrow p \in bH$ $\therefore aH \subseteq bH$ (1)

Again, let $q \in bH \Rightarrow q = bh_4$ for some $h_4 \in H$

$\Rightarrow q = ah_1h_2^{-1}h_4$

$\in aH,$ $\because h_1h_2^{-1}h_4 \in H$

Thus $q \in bH \Rightarrow q \in aH$ $\therefore bH \subseteq aH$ (2)

From (1) and (2), aH = bH

Thus, aH, bH are either disjoint or identical.

(ii) Let $G = \{a_1, a_2, \cdots, a_n, \cdots\}$ be a group and let $H = \{h_1, h_2, \cdots, h_m, \cdots\}$ be a subgroup of G.Let $B = \cup(a_kH), a_k \in G$

Clearly $B \subseteq G$ ... (1)

Also $x \in G \Rightarrow x \in xH \subseteq B$

$\Rightarrow x \in B$

$\therefore G \subseteq B$ ... (2)

From (1) and (2),we get $G = B$

or $G = \underset{a_k \in G}{\cup}(a_kH)$

2.4 LAGRANGE'S SUBGROUP ORDER THEOREM

Theorem 3 : (Lagrange's subgroup Order Theorem) The order of a subgroup of a finite group divides the order of the group.

Proof : Let G be a finite group, and let O(G) = n

and $H \leq G$.

Let e be the identity of G.

Case 1 : Let H = {e},

There is nothing to prove. O(H) =1, and 1 divides n.

Case 2 : Let H = G. Hence O(H) = O(G).

There is nothing to prove.

Case 3 : Let $H \neq \{e\}$, $H \neq G$.

Let O(H) = m, m < n.

Let $H = \{h_1, h_2, h_3, \ldots h_m\}$, where the h_i's are distinct.

Let $a \in G$, $a \notin H$.

Let us consider the left coset.

$aH = \{ah_1, ah_2, ah_3, \ldots, ah_m\}$

We claim that all the elements in aH are distinct, for if $ah_i = ah_j$, $1 \leq i \leq m$, $1 \leq j \leq m$, $i \neq j$ then $h_i = h_j$, (by left cancellation law), which is a contradiction.

Again, no element of H is equal to any element of aH, for if $h_i = ah_j$, then $h_i h_j^{-1} = a$ i.e. $a = h_i h_j^{-1} \in H$

i.e. $a \in H$, which is a contradiction.

Thus, we have listed m+m = 2m elements of G. If this exhausts all the elements of G, then 2m = n. $\therefore$ m divides n.

If not, let $b \in G$, $b \notin H$, $b \notin aH$

Let us consider $bH = \{bh_1, bh_2, \ldots, bh_m\}$

Clearly, all the elements in bH are distinct. No element of H is equal to any element of bH.

Again, no element of aH is equal to any element of bH, for if $ah_i = bh_j$, then $ah_i h_j^{-1} = bh_j h_j^{-1}$ i.e $ah_i h_j^{-1} = b$ i.e $b = ah_i h_j^{-1} \in aH$,

($\because h_i h_j^{-1} \in H$) i.e. $b \in aH$, which is a contradiction.

Thus, we have listed m+m+m = 3m elements of G. If this exhausts all the elements of G, then 3m = n. $\therefore$ m divides n.

If not, we proceed as above. Since G is finite, we must stop somewhere, say, after k times. $\therefore$ mk = n $\Rightarrow$ m divides n.

Note : Joseph Louis Lagrange (1736 – 1813) was a famous mathematician,

''born at Turin of once prosperous parents with French and Italian backgrounds".

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



CHECK YOUR PROGRESS-1

Q 1: Find all cosets of the subgroup 4Z of 2Z.

Q 2: Find all cosets of the subgroup 6Z of 2Z.

2.5 NORMAL SUBGROUP

Definition : A subgroup H of a group G is said to be a normal subgroup of G if aH = Ha, for all a $\in$ G, i.e., if its left and right cosets coincide. Symbolically We write H Δ G.

Note : A group G has at least two normal subgroups, viz., G and {e}. A group, having no normal subgroups other than G and {e}, is called a simple group.

Example : Let G ={ –1, 1, –i, i}

We know that G is a group under multiplication.

Let H = {–1, 1}, and H$\leq$G

Now 1H = {–1, 1} = H1

(–1)H = {1, –1} = H (–1)

iH = {–i, i} = Hi

(–i)H = {i, –i} = H (–i)

Thus, aH = Ha, for all a$\in$ G

$\therefore$ H Δ G.

Note : In the above example, H has two distinct left (or right) cosets, viz H, iH. We note that iH is not a subgroup of G.

Theorem 1 : Every subgroup of an Abelian group is normal.

Proof : Let G be an Abelian group.

Let H $\leq$G.

Let a $\in$ G

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

= {ha : h$\in$ H} [$\because$ G ia Abelian]

$= Ha$

$\therefore H \Delta G.$

Theorem 2 : A subgroup H of a group G is a normal subgroup of G if and only if $ghg^{-1} \in H$, for all $g \in G, h \in H$

Proof : Let $H \Delta G$.

$\therefore aH = Ha$, for all $a \in G$

Let $g \in G, h \in H$

$\therefore gh \in gH$

$\Rightarrow gh \in Hg$ [$\because gH = Hg$, H being normal in G]

$\Rightarrow gh = h_1 g$, for some $h_1 \in H$

$\Rightarrow ghg^{-1} = h_1 gg^{-1}$

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

i.e. $ghg^{-1} \in H$

Conversely, let $H \leq G$ such that $ghg^{-1} \in H$, for all $g \in G, h \in H$.

Let $a \in G$ $\therefore ah \in aH$

$\therefore aha^{-1} \in H$, by the given condition

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

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

$\Rightarrow ah \in Ha$

$\therefore aH \subseteq Ha$ (1)

Now $ha \in Ha$.

We take $a^{-1} = b$.

$\therefore bhb^{-1} \in H$

$\Rightarrow a^{-1}h(a^{-1})^{-1} \in H$

$\Rightarrow a^{-1}ha \in H$

$\Rightarrow a(a^{-1}ha) \in aH$

$\Rightarrow (aa^{-1})ha \in aH$

$\Rightarrow ha \in aH$

$\therefore Ha \subseteq aH$ (2)

From (1) and (2), $aH = Ha$

$\therefore H \Delta G.$

Theorem 3 : The intersection of any two normal subgroup of a group is again a normal subgroup of the group.

Proof : Let G be a group, an $H \Delta$ G, $K \Delta$ G.

$\therefore$ $H \leq G$, $K \leq G$ and so $H \cap K \leq G$.

Let $g \in G$, $h \in H \cap K$

$h \in H \cap K \Rightarrow h \in H$ and $h \in K$

Now $g \in G$, $h \in H$ and $H \Delta G$

$\therefore$ $ghg^{-1} \in H$

Again $g \in G$, $h \in K$ and $K \Delta G$

$\therefore$ $ghg^{-1} \in K$

Thus, $ghg^{-1} \in H$ and $ghg^{-1} \in K$.

$\therefore ghg^{-1} \in H \cap K$

$\therefore$ $H \cap K \Delta G$.

Note : The union of two normal subgroups is not necessarily a normal subgroup.For example $2Z \Delta Z, 3Z \Delta Z$. But $2Z \cup 3Z \not\subset Z$ and so not a normal subgroup of Z.

2.6 QUOTIENT GROUPS

Let G be a group and H be a normal subgroup G.

$\because$ H is normal in G, therefore, there is no distinction between a left coset and its corresponding right coset. So, by a coset we mean left coset (or right coset).

Let G/H denote the collection of all cosets of H in G.

Let $a, b \in G$ $\therefore$ $aH, bH \in G/H$.

We define a binary operation in G/H by the rule $(aH)(bH) = abH$, $ab \in G$.

We show that the binary operation is well defined.

Let $aH = cH$,

$bH = dH$; $a, b, c, d \in H$.

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

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

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

$\Rightarrow a^{-1}c \in H$ [Theorem 6 (i)]

$\Rightarrow a^{-1}c = h_1$, for some $h_1 \in H$

Similarly $bH = dH \Rightarrow b^{-1}d \in H$ $\Rightarrow b^{-1}d = h_2$, for some $h_2 \in H$.

Now $(ab)^{-1}(cd) = (b^{-1}a^{-1})(cd)$

$= b^{-1}(a^{-1}c)d$

$= b^{-1}h_1 d$

$= b^{-1}dh_1$ [$\because$ dH = Hd]

$= h_2h_1 \in H$

$\therefore (ab)^{-1}(cd)H = H$

$\Rightarrow abH = cdH$

Thus, $\left.\begin{matrix} aH = cH \\ bH = dH \end{matrix}\right\} \Rightarrow abH = cdH$

$\therefore$ the binary operation defined above is well defined.

Theorem : Let G be a group and H be a normal subgroup G. The set G/H consisting of all the cosets of H in G is a group under the binary operation defined by

$(aH)(bH) = abH$; $a, b \in G$.

Proof : (i) It is given that the binary operation is $(aH)(bH) = abH$; $a, b \in G$

(ii) Let $a, b, c \in G$

$\therefore aH, bH, cH \in G/H$

Now $((aH)(bH))(cH) = (abH)(cH)$

$= (ab)c\,H$

$= a(bc)H$ [$\because$G is a group, (ab)c = a(bc)]

$= (aH)((bc)H)$

$= (aH)((bH)(cH))$

$\therefore$ the binary operation is associative.

(iii) let e be the identity of G.

$\therefore eH = H \in G/H$

Now $(aH)H = (aH)(eH) = aeH = aH$

$H(aH) = (eH)(aH) = eaH = aH.$

$\therefore$ H is the identity.

(iv) $a \in G \Rightarrow a^{-1} \in G$

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

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

$\therefore a^{-1}H$ is the inverse of aH.

$\therefore$ G/H is a group under the binary operation defined above.

Note : This group is known as the quotient group (or factor group) of G by H.

Theorem 5 : Every quotient group of an Abelian group is Abelian.

Proof : Let G be an Abelian group, and $H \leq G$.

$\therefore$ G is Abelian, $\therefore$ H is normal in G.

So, we can construct the quotient group G/H.

Let $a, b \in G$. $\therefore aH, bH \in G/H$.

Now $(aH)(bH) = abH$

$= baH$ [$\because$ G ia Abelian, ab = ba]

$= (bH)(aH)$

$\therefore G/H$ is Abelian.

Theorem 7 : Every quotient group of a cyclic group is cyclic.

Proof : Let G = <a> be a cyclic group.

Let $H \leq G$

$\because$ G is cyclic, $\therefore$G is Abelian and, therefore, H is normal in G.

So, we can construct the quotient group G/H.

Let $x \in G$, $\therefore xH \in G/H$.

Now $x = a^m$ for some integer m.

Let $m > 0$

Now $xH = a^mH$

$= (a\ a\ a \ldots\ a)H$

$= (aH)(aH)(aH) \ldots (aH)$

$= (aH)^m$

$\therefore G/H$ is a cyclic group generated by aH.

We can prove the result immediately for $m = 0$ or $m < 0$.



CHECK YOUR PROGRESS-2

Q 1: Can a non-Abelian group be cyclic?

Q 2: Show that a non-Abelian group must contain at least six elements.

Q 3: Let $G = \{1, \omega, \omega^2\}$ be the multiplicative group; ω being a complex cube root of unity. Is the group simple?

Q 4: Can a group of order seven be non-Abelian?

Q 5: Let Z be the additive group of integers. The set 3 Z = {0, $\pm$ 3, $\pm$ 6, ...} is a subgroup of Z. Write down the number of elements of the quotient group $Z/_{3Z}$.



2.7 LET US SUM UP

- If H is a subgroup of a group G, the set Ha = {ha : h $\in$ H}, a $\in$ G, is called a right coset of H in G. Similarly, a left coset is defined.
- Any two left (or right) cosets of a subgroup are either disjoint or identical.
- Lagrange's subgroup Order Theorem state that the order of a subgroup of a finite group divides the order of the group.
- A subgroup H of a group G is a normal subgroup of G if aH = Ha, for all a $\in$ G.
- If G is a group and H is a normal subgroup of G, the set $G/_H$ consisting of all the cosets of H in G is a group, called the quotient group (or the factor group).



2.8 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS-1

Ans to Q No 1: Since 2Z is abelian,the left cosets and the right cosets are the same.The left coset containing the integer 0 is $0+4Z=\{\cdots,-8,-4,0,4,8,\cdots\}$ and left coset containing the integer 2 is $2+4Z=\{\cdots,-6,-2,2,6,10,\cdots\}$.

Ans to Q No 2: Left as an exercise

CHECK YOUR PROGRESS-2

Ans to Q No 1: Every cyclic group is Abelian. Therefore, every non-Abelian group is non-cyclic.

Ans to Q No 3: Yes. It has no normal subgroups other than G, {1}.

Ans to Q No 4: No. Every group of prime order is cyclic and every cyclic group is Abelian.

Ans to Q No 5: Three.



2.9 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.

2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).

3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).

4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.

5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.



2.10 MODEL QUESTION

Q 1: Let G be a group and H be a subgroup of G. Let a, b $\in$ G. Show that the two right cosets Ha, Hb are equal if and only if the two left cosets $a^{-1}H$, $b^{-1}H$ are equal.

Q 2 : Find all cosets of the subgroup 4Z of Z.

Q 3: Index of a subgroup. Let G be a group and H be a subgroup of G. The number of distinct left (or right) cosets of H in G is called the index of H in G. Generally it is denoted by [G : H]

If G is a finite group, show that [G : H] = $\frac{o(G)}{o(H)}$.

Q 1: If $N_1, N_2, \cdots, N_m$ are normal subgroups of a group G, Show that $N_1 \cap N_2 \cap \cdots \cap N_m$ is also a normal subgroup of G.

Q 2: Let G = $\left\{\begin{pmatrix} a & b \\ o & d \end{pmatrix} : a, b, d \in IR \text{ and } ad \neq 0\right\}$

Show that G is a non-Abelian group under matrix multiplication.

Let H = $\left\{\begin{pmatrix} 1 & b \\ o & 1 \end{pmatrix} : b \in IR\right\}$

Show that H is a normal subgroup of G.

Q 3: Show that a group of prime order is simple.

*** ***** ***