UNIT 3: GROUP

UNIT STRUCTURE

3.1 Learning objectives

3.2 Introduction

3.3 Group

3.4 Properties of group

3.5 Let us Sum Up

3.6 Answers to Check Your Progress

3.7 Further Readings

3.8 Model Questions

3.1 LEARNING OBJECTIVES

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

- define groups
- know properties of group.

3.2 INTRODUCTION

In unit-2, we have studied binary operation in a set. In this unit we will introduce the notion of groups. Group is an algebraic structure, i.e, a non-empty set equipped with a binary operation satisfying certain postulates. Group theory occupies an important position in the study of abstract algebra.

3.3 GROUP

A non-empty set G, equipped with a binary operation $*$ is called a group if the following postulates are satisfied.

(i) Associativity

$(a * b) * c = a * (b * c), \forall a, b, c \in G$

(ii) Existence of Identity

There exists $e \in G$ such that

$a * e = a = e * a, \forall a \in G$.

e is called identity.

(iii) Existence of Inverse

For every $a \in G$, there exists $b \in G$ such that

$a * b = e = b * a$

b is called inverse of a and it is denoted by a^{-1}.

Furthermore, if $*$ is commutative, G is called an Abelian group, after the name of the celebrated Norwegian mathematician Niels Henrik Abel (1802–1829).

Note : 1. In order to be a group, there must be a non-empty set equipped with a binary operation satisfying the postulates mentioned above. Later on, we will simply write 'Let G be a group'. It should be borne in mind that there is a binary operation on G.

2. We will drop the binary operation symbol and simply write ab. It should be borne in mind that this is not our usual multiplication.

3. A non-empty set G equipped with a binary operation is called a semigroup if the binary operation is associative.

Finite and Infinite Groups

A group G is finite if the set G is finite; otherwise it is infinite group.

Order of a group

The number of elements of a finite group G is called the order of G. Symbolically it is denoted by 0(G) or |G|.

Example 1 : Let G = {1}

Clearly multiplication is a binary operation on G.

Moreover, all the postulates for a group are satisfied.

$\therefore$G is a group under multiplication.

Furthermore, G is an Abelian group.

Example 2: Let G = {–1, 1}, the set consisting of the square roots of unity.

(i) From the table, we see that multiplication is a binary operation on G.

(ii) We know that multiplication of real numbers is associative.

(iii) 1 is the identity under multiplication.

(iv) Every element G possesses inverse in G.

1 is the inverse of 1,

–1 is the inverse of –1.

∴ G is a group under multiplication.

(v) Moreover, multiplication of real numbers is commutative.

∴ G is an Abelian group.

×	–1	1
–1	1	–1
1	–1	1

Table 3.1

Example 3: Let G = {z : z is complex and z^n=1}, i.e. G is the set consisting of the n the roots of unity. (n∈ IN)

(i) Let $z_1, z_2 \in G$

∴ $z_1^n=1, z_2^n=1$

Now $(z_1 z_2)^n = 1$ ∴ $z_1 z_2 \in G$

∴ multiplication is a binary operation on G.

(ii) We know that multiplication of complex numbers is associative.

(iii) There exists $1 \in G$ such that

$1z = z = z1, \forall z \in G$

∴1 is the identity element.

(iv) Let $z \in G$. ∴$z^n = 1$

Now $\frac{1}{z}$ is a complex number and $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$

$\therefore \frac{1}{z} \in G$

Thus, for every $z \in G$, there exists $\frac{1}{z} \in G$ such that $z \frac{1}{z}=1=\frac{1}{z} z$

∴ $\frac{1}{z}$ is the inverse of z.

∴ G is a group under multiplication of complex numbers.

(v) Moreover, multiplication of complex numbers is commutative.

∴ G is an Abelian group.

Note : We have seen that, for every positive integer n, there exists an Abelian group of order n.

Example 4: Let Z be the set of integers

(i) Let $a, b \in Z$

∴ $a+b \in Z, \forall\ a, b \in Z$

i.e. addition is a binary operation on Z.

(ii) We know that multiplication of integers is associative.

(iii) We have $0 \in Z$ and $a+0 = a = 0+a, \forall a \in Z$

∴ 0 is the identity.

(iv) For every a $\in$ Z, there exists –a $\in$ Z such that a+(–a) = 0 = (–a) +a.

$\therefore$ Z is a group under addition.

(v) Moreover, addition of real numbers is commutative.

$\therefore$ Z is an Abelian group under addition.

Note : Z is an infinite group.

Some other examples are the following.

- Q is an Abelian group under addition.
- IR is an Abelian group under addition.
- Q_0, the set of non-zero rational numbers is an Abelian group under multiplication.
- IR_0, the set of non-zero real numbers is an Abelian group under multiplication.
- C is an Abelian group under addition.
- C_0, the set of non-zero complex numbers is an Abelian group under multiplication.

Example 5: Let G = $\left\{\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix} : \alpha \in IR\right\}$

(i) Let $A_\alpha = \begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix} \in G,$

$$A_\beta = \begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix} \in G;\ \ \alpha, \beta \in IR$$

Now $A_\alpha A_\beta$ = $\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix}$

$$= \begin{pmatrix}\cos(\alpha+\beta) & -\sin(\alpha+\beta)\\ \sin(\alpha+\beta) & \cos(\alpha+\beta)\end{pmatrix} = A_{\alpha+\beta} \in G$$

i.e. matrix multiplication is a binary operation on G.

(ii) We know that matrix multiplication is associative.

(iii) We have $\mathrm{I} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

$$= \begin{pmatrix}\cos 0 & -\sin 0\\ \sin 0 & \cos 0\end{pmatrix} \in G$$

and $A_\alpha I = A_\alpha = IA_\alpha, \forall A_\alpha \in G$.

$\therefore$ I is the identity element

(iv) We have $|A_\alpha| = \begin{vmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{vmatrix}$

$= \cos^2\alpha + \sin^2\alpha = 1 \neq 0$

$\therefore A_\alpha^{-1}$ exists.

$\therefore \text{adj} A_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$

$\therefore A_\alpha^{-1} = \frac{1}{|A_\alpha|} adj\ A_\alpha$

$= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \in G$

$\therefore$G is a group under matrix multiplication.

(v) Moreover, $A_\alpha A_\beta = A_{\alpha+\beta} = A_{\beta+\alpha} = A_\beta A_\alpha$

$\therefore$ G is an Abelian group.

Example 6: Let G = $\left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in IR,\ x \neq 0 \right\}$

(i) Let $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G,\ \begin{pmatrix} y & y \\ y & y \end{pmatrix} \in G$

x, y $\in$ IR, $x \neq 0,\ y \neq 0$

Now $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G$, xy $\in$ IR, xy $\neq 0$

(ii) We know that matrix multiplication is associative.

(iii) We have $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \in G$

and $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \\ \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\therefore \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ is the identity element

(iv) For every $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G$ we have $\begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} \in G$

such that $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\therefore \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}$ is the inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$.

$\therefore$ G is a group under matrix multiplication.

(v) Moreover, $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix}$

$$= \begin{pmatrix} 2yx & 2yx \\ 2yx & 2yx \end{pmatrix}$$

$$= \begin{pmatrix} y & y \\ y & y \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$\therefore$ G is an Abelian group.

Note : In the above example, the identity element is $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$.

Example 7: Let G be the set of rational numbers excluding 1. We define $*$ on G as follows.

$$a * b = a+b-ab, \ \forall \ a, b \in G$$

(i) $*$ is a binary operation on G

[Ref : Example 10 in [unit 2]

(ii) $*$ is associative on G

[Ref : Example 10 in [unit 2]

(iii) We have $0 \in$ G and

$a * 0 = a + 0 - a0 = a$

$0 * a = 0 + a - 0a = a$

$\therefore$ 0 is the identity under $*$.

(iv) For every $a \in G$, there exists $\frac{a}{a-1} \in G$ such that.

$$a * \frac{a}{a-1} = 0 = \frac{a}{a-1} * a$$

$\therefore \frac{a}{a-1}$ is the inverse of a under $*$.

$\therefore$ G is a group commutative.

[Ref : Example 10 in [unit 2]

$\therefore$ G is an Abelian group.

3.4 PROPERTIES OF GROUP

Theorem 1: Let G be a group. Then

(i) identity element is unique;

(ii) inverse of each element in G is unique;

(iii) $(a^{-1})^{-1} = a$, for all $a \in G$, where a^{-1} denotes the inverse of a,

(iv) $(ab)^{-1} = b^{-1}a^{-1}$, for all $a, b \in G$

(v) $ab = ac \Rightarrow b = c$, (left cancellation law)

$ba = ca \Rightarrow b = c$, (right cancellation law) for all $a, b, c \in G$.

Proof (i) If possible, let e, f be two identities of G.

$\therefore ef = e = fe$ [$\because$ f is identity]

Again $ef = f = fe$ [$\because$ e is identity]

$\therefore e = f$

Thus, identity element is unique.

Note : In view of the above theorem, we write the identity, not 'an identity'.

(ii) Let $a \in G$ and e be the identity of G.

If possible, let b and c be two inverses of a.

$\therefore ab = e = ba$ [$\because$ b is inverse of a]

$ac = e = ca$ [$\because$ c is inverse of a]

Now $b = be$ [$\because$ e is the identity}

$= b(ac)$ [$\because e = ac$]

$= (ba)c$ [by associativity]

$= ec$ [$\because$ e is the identity]

$= c$

Thus, inverse of a is unique.

Note : In view of the above theorem, we write 'the inverse of a', not ' an inverse of a'.

(iii) We have $aa^{-1} = e = a^{-1}a$

$\therefore$ a^{-1} is the inverse of a, and vice versa, a is the inverse of a^{-1} i.e. $(a^{-1})^{-1} = a$

(iv) Let e be the identity of G and a, $b \in G$

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

$= a\ e\ a^{-1}$

$= aa^{-1}$

$= e$

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

$= b^{-1}\ eb$

$= b^{-1}\ b$

$= e$

$\therefore$ $b^{-1}a^{-1}$ is the inverse of ab, i.e. $(ab)^{-1} = b^{-1}a^{-1}$

(v) We have $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b=(a^{-1}a)c$, [by associativity]

$\Rightarrow eb = ec$

$\Rightarrow b = c$, [$\because$ e is the identity]

Again $ba = ca$

$\Rightarrow (ba)a^{-1} = (ca)\ a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$ [by associativity]

$\Rightarrow be = ce$

$\Rightarrow b = c$ [$\because$ e is the identity]

Example 8: If, in a group G, every element is its own inverse, prove that G is Abelian.

Solution: Let G be a group. Let a, $b \in G$

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

Now ab = $(ab)^{-1} = b^{-1}a^{-1}$ =ba [Theorem 1 (iv)]

$\therefore$ G is Abelian

Example 9: Prove that a group G is Abelian if and only if $(ab)^2 = a^2b^2$, for all a, b $\in$ G.

Solution: $(ab)^2 = a^2 b^2$

$\Leftrightarrow$ (ab) (ab) = (aa) (bb)

$\Leftrightarrow$ a(ba)b = a(ab)b

$\Leftrightarrow$ (ba)b = (ab)b, [by left cancellation law]

$\Leftrightarrow$ ba = ab, [by right cancellation law]

$\Leftrightarrow$ G is Abelian.



CHECK YOUR PROGRESS

Q 1: Show that the set G = {1, ω, ω^2} consisting of the cube roots of unity is a group under usual multiplication. (ω is a complex cube root of unity).

Q 2: Show that the set G consisting of all 2 x 2 non-singular matrices over reals is a group under matrix multiplication.

Q 3: Let G = $\left\{\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in IR,\ x \neq 0\right\}$

Show that G is an Abelian group under matrix multiplication.

Q 4: If for every element a in a group G, a^2 = e; prove that G is Abelian. (e is the identity of G).



3.5 LET US SUM UP

- A group is an algebraic structure i.e., a non-empty set equipped with a binary operation satisfying certain postulates.
- Elementary Properties of a group are discussed



3.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

Ans to Q No 1: Left as an exercise

Ans to Q No 2: Left as an exercise

Ans to Q No 3: Left as an exercise

Ans to Q No 4: Left as an exercise



3.7 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.



3.8 MODEL QUESTION

Q 1: Let G be the set of odd integers. A binary operation $*$ on G is defined as follows $a * b = a+b-1$; $a, b \in G$.
Show that G is an Abelian group under $*$.

Q 2: Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$, for all $a, b \in G$.

*** ***** ***