UNIT 1: INTRODUCTION TO GROUPS

UNIT STRUCTURE

1.1 Learning objectives

1.2 Introduction

1.3 Group

1.4 Properties of group

1.5 Subgroup

1.6 Cyclic Subgroup

1.7 Let us Sum Up

1.8 Answers to Check Your Progress

1.9 Further Readings

1.10 Model Questions

1.1 LEARNING OBJECTIVES

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

- define groups
- know properties of group.
- subgroups
- cyclic groups

1.2 INTRODUCTION

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.

1.3 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.

×	–1	1
–1	1	–1
1	–1	1

Table 1.1

$\therefore$ G is a group under multiplication.

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

$\therefore$ G is an Abelian group.

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. ($n \in$ IN)

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

$\therefore z_1^n=1, z_2^n=1$

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

$\therefore$ 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

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

$\therefore$1 is the identity element.

(iv) Let $z \in G$. $\therefore z^n = 1$

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 $z \frac{1}{z}=1=\frac{1}{z} z$

$\therefore \frac{1}{z}$ is the inverse of z.

$\therefore$ G is a group under multiplication of complex numbers.

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

$\therefore$ 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 $a, b \in Z$

$\therefore a+b \in Z, \ \forall \ a, b \in Z$

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 $a+0 = a = 0+a$, $\forall\, a \in Z$

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

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

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 $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

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

(ii) $*$ is associative on G

(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.

$\therefore$ G is an Abelian group.

1.4 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-1

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).

1.5 SUBGROUP

Let us consider the set Z of integers.

We know that Z is a group under addition.

Let 2Z = {0, $\pm$2, $\pm$4, ...} be the set of even integers.

Clearly 2Z is a non-empty subset of Z.

Moreover, 2Z is also a group under addition.

In this case, 2Z is said to be a subgroup of Z.

Definition : A non-empty subset H of a group G is a subgroup of G if H is also a group under the same binary operation of G. Symbolically, we write H$\leq$ G.

Note : (1) If e is the identity of G, {e} is also a subgroup of G, called the trivial subgroup of G. All other subgroups are nontrivial.

(2) G itself is a subgroup of G, called the improper subgroup of G. All other subgroups are proper. [John B. Fraleigh, A First Course in Abstract Algebra (First Indian Reprint, 2003)]

Example 1: Let us consider G = {–1, 1, –i, i}, i = $\sqrt{-1}$

We know that G is a group under multiplication,

Let H = {–1, 1}.

We have H $\subseteq$ G.

Also H is group under multiplication

$\therefore$ H $\leq$ G.It is a proper subgroup of G.

Note : The set of real numbers IR is a group under addition. The set IR_+ of positive real numbers is a group under multiplication. IR_+ is a subset of IR, but not a subgroup of IR. Binary operations are different.

Theorem 3: Let H be a subgroup of a group G. Then

(i) the identity element of H is the identity element of G;

(ii) the inverse of any element of H is the same as the inverse of the element of G.

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

(i) If possible, let e be the identity of G, and f be the identity of H.

Let a $\in$ H.

$\therefore$ af = a = fa [$\because$ f is the identity of H]

Again a $\in$ H $\Rightarrow$ a $\in$ G.

$\therefore$ ae = a = ea [$\because$ e is the identity of G]

$\therefore$ af = ae

$\Rightarrow$ f = e [by left cancellation law]

(ii) Let e be the identity of G

$\therefore$ e is also the identity of H.

Let a $\in$ H.

If possible, let b be the inverse of a in H, and c be the inverse of a in G.

$\therefore$ ab = e = ba

ac = e = ca

$\therefore$ ab = ac$\Rightarrow$ b = c [by left cancellation law]

Note : If H, K are two subgroups of a group G and e is the identity of G, then e is also the identity of H as well as of K. So, H and K have at least one common element, viz., the identity element. Thus, we can conclude that there cannot be two disjoint subgroups of a group.

Theorem 1 : A non-empty subset H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof : Let $H \leq G$ and $a, b \in H$.

$b \in H \Rightarrow b^{-1} \in H$ [$\because$ H is a group]

Now $a \in H, b^{-1} \in H$

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

Conversely, let $H \subseteq G$ such that $a, b \in H \Rightarrow ab^{-1} \in H$

(i) Now $a, a \in H \Rightarrow aa^{-1} \in H$ (by the given condition)

$\Rightarrow e \in H$,

where e is the identity of G.

(ii) $e \in H, a \in H \Rightarrow ea^{-1} \in H$

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

$\therefore$ every element of H has inverse in H.

(iii) $b \in H \Rightarrow b^{-1} \in H$ by (ii)

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

$\Rightarrow ab \in H$

(iv) The binary operation is associative in H as it is associative in G.

$\therefore$ H is a group under the same binary operation in G. Also $H \subseteq G$.

$\therefore H \leq G$.

Note : If G is an additive group, i.e., if G is a group under addition, then a non-empty subset H of G is a subgroup of G if and only if $a, b \in H \Rightarrow a - b \in H$.

Theorem 2 : The intersection of two subgroups of a group is again a subgroup of the group.

Proof : Let G be a group and e be the identity of G.

Let $H \leq G, K \leq G$.

We note that $H \cap K \neq \phi$,

for at least the identity element $e \in H \cap K$

Let $a, b \in H \cap K$

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

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

Now $a, b \in H$ and $H \leq G$. $\therefore ab^{-1} \in H$

$a, b \in K$ and $K \leq G$. $\therefore ab^{-1} \in K$

$ab^{-1} \in H$ and $ab^{-1} \in K \Rightarrow ab^{-1} \in H \cap K$

$\therefore H \cap K \leq G$

Note : The union of two subgroups is not necessarity a subgroup.

Let $Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ be the additive group of integers.

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

$3Z = \{0, \pm 3, \pm 6, \pm 9, ...\}$

Clearly $2Z \leq Z$, $3Z \leq Z$

Now $2 \in 2Z \cup 3Z$, $3 \in 2Z \cup 3Z$

But $2+3 = 5 \notin 2Z \cup 3Z$

$\therefore$ addition is not a binary operation on $2Z \cup 3Z$.

$\therefore 2Z \cup 3Z$ cannot be a group.

Theorem 4 : The union of two subgroups is a subgroup if and only if one of them is contained in the other.

Proof : Let G be a group and $H \leq G$, $K \leq G$.

Let $H \subseteq K$. Then $H \cup K = K$.

$\because K \leq G, \therefore H \cup K \leq G$

Conversely, let $H \leq G, K \leq G$ such that $H \cup K \leq G$.

Let e be the identity of G.

We are to prove that either $H \subseteq K$ or $K \subseteq H$

If possible, let it not be true.

$\therefore H \not\subseteq K$ and $K \not\subseteq H$

$\therefore$ there exists $a \in H$ such that $a \notin K$

Also, there exists $b \in K$ such that $b \notin H$

Now $a \in H \Rightarrow a \in H \cup K$

$b \in K \Rightarrow b \in H \cup K$

$\because H \cup K \leq G, \therefore ab \in H \cup K$

This $\Rightarrow ab \in H$ or $ab \in K$

If $ab \in H$, then $a \in H$, $ab \in H \Rightarrow a^{-1}(ab) \in H$

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

$\Rightarrow$ eb $\in$ H

$\Rightarrow$ b $\in$ H,

which is a contradiction.

Similarly, if ab $\in$ K, then ab $\in$ K, b $\in$ K $\Rightarrow$ (ab)$b^{-1} \in$ K

$\Rightarrow$ a(bb^{-1}) $\in$ K

$\Rightarrow$ ae $\in$ K

$\Rightarrow$ a $\in$ K

which is a contradiction.

So, our assumption is wrong.

$\therefore$ either H $\subseteq$ K or K $\subseteq$ H.



CHECK YOUR PROGRESS-2

Q 1: Is the multiplicative group IR_+ of positive real numbers a subgroup of the additive group IR of real numbers? Justify your answer.

Q 2: Can there be two disjoint subgroups of a group? Justify your answer.

Q 3: Can an Abelian group have a non-Abelian subgroup ?

Q 4: Let Z be the additive group of integers. Let m be a fixed integer. Show that the set.

m Z = {0, $\pm$m, $\pm$2m, $\pm$3m, ...} is a subgroup of Z.

Q 5: Let G be the group consisting of all 2 x 2 non-singular real matrices under matrix multiplication. Let

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in IR \text{ and } ad - bc = 1 \right\}$$

Show that H is a subgroup of G.

Q 6: Give an example to show that a group cannot be expressed as the union of two of its proper subgroups.

1.6 CYCLIC GROUPS

Definition : A group G is said to be cyclic if there exists an element a in G such that every element of G can be expressed in the form a^n, n $\in$ Z. a is said to be a generator of G. Symbolically we write G = <a>, i.e., G is a cyclic group generated by a.We can also write, $G = \{a^n : a \in G, n \in Z\}$

Note : If the group G is additive, every element of G is expressed in the form na.

Examples

(1) We know that G = {–1, 1} is a group under multiplication.

We have $(-1)^1 = -1$, $(-1)^2 = 1$

$\because$ G is a cyclic group generated by –1, i.e. G = <–1>

(2) We know that G = {1, ω, ω^2} is a group under multiplication ; ω is a complex cube root of unity.

We have, $\omega^1 = \omega, \omega^2 = \omega^2, \omega^3 = 1$

.. G is cyclic group generated by ω i.e., G = <ω>

Similarly G = <ω^2>

(3) We know that G = {–1, 1, –i, i} is a group under multiplication.

We have $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

$\therefore$ G is a cyclic group generated by i , i.e. G = < i >

Similarly G = < – i >

(4) Let Z be the additive group of integers.

Let $x \in Z$ Then x = 1x

$\therefore$ G is a cyclic group generated by 1, i.e. G = < 1 >

Similarly G = < –1 >.

Theorem 5 : Every cyclic group is Abelian.

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

Let $x, y \in G$.

Then there exist integers m, n such that $x = a^m$, $y = a^n$

Now $xy = a^m a^n$

$= a^{m+n}$

$= a^{n+m}$

$= a^n a^m$

$= yx$

$\therefore$ G is Abelian.

Theorem 6 : If a is a generator of a cyclic group G, a^{-1} is also a generator of G.

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

Let $x, y \in G$.

Then there exists integer m such that $x = a^m$

$= (a^{-1})^{-m}$

$\therefore G = < a^{-1} >$.

Division Algorithm for Z

If b is a positive integer and a is any integer, then there exist unique integers q and r such that $a = bq+r$, $0 \leq r < b$

Theorem 7 : A subgroup of a cyclic group is cyclic.

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

Let $H \leq G$.

Let e be the identity of G.

Case 1. If H = {e}, there is nothing to prove.

Case 2. If H = G, then also the result is obvious,

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

Each element of H is a power of a.

Let m be the least positive integer such that $a^m \in H$.

Let $x \in H$.

Then $x = a^p$ for some p.

Now, by Division Algerithm, there exist unique integers q and r such that

$p = mq + r$, where $0 \leq r < m$

$\therefore r = p - mq$

$\therefore a^r = a^{p-mq} = a^p (a^m)^{-q} = x(a^m)^{-q}$

Now $x (a^m)^{-q} \in H$. $\therefore a^r \in H$.

But m is the least positive integer such that $a^m \in H$. $\therefore$ r must be 0.

$\therefore p = mq$

$\Rightarrow x = a^p = a^{mq} = (a^m)^q$

$\therefore H = <a^m>$ is a cyclic group.

Theorem 8 : A group of prime order is cyclic.

Proof : Let G be a finite group, and O (G) = p, where p is a prime number.

Let e be the identity of G.

Let $a \in G$ such that $a \neq e$

Let $H = \{a^n : n \text{ is an integer}\}$

Clearly, H is a cyclic subgroup of G.

$\therefore$ by Lagrange's subgroup order theorem, [see unit 6.4]

O (H) divides O (G)

i.e. O(H) divides p

This $\Rightarrow$ O(H) = 1 or p

But O(H) $\neq$1, $\because$ a $\neq$e.

$\therefore$ O (H) = p = O(G)

$\therefore$ H = G

$\therefore$ G is a cyclic group generated by a.

Example 2: Prove that a group of order $\leq$ 5 is Abelian.

Solution: Obviously, a group of order one is Abelian. We know that every group of prime order is cyclic and every cyclic group is Abelian.

$\therefore$ groups of orders 2, 3, 5 are Abelian.

Let us consider group of order 4.

Let G = {e, a, b, c}, where all the elements are distinct, and e is the identity of G.

Clearly, e is its own inverse. Similarly if each of the remaining three elements is its own inverse, then G is Abelian. (Ref. Example 18)

If not, let $b^{-1} = c$, $c^{-1} = b$. Then $a^{-1} = a$

Now let us complete the operation table

$\because$ $a^{-1} = a$ $\therefore$ aa = e

Again, each element of G must appear exactly once in every row or column of the operation table.

$\therefore$ ab = b or ab = c.

Now ab = b $\Rightarrow$ ab = eb $\Rightarrow$ a = e (by right cancellation law), which is a contradiction.

$\therefore$ ab = c, and $\therefore$ ac = b

$\therefore$ b = c^{-1}, $\therefore$ bc = e

$\therefore$ ba = a or ba = c

ba = a $\Rightarrow$ b = e, which is a contradiction

$\therefore$ ba = c, and bb = a

Again, $\because$ c = b^{-1} $\therefore$ cb = e

$\therefore$ ca = a or ca = b

ca = a $\Rightarrow$ c = e, which is a contradiction.

$\therefore$ ca = b, and $\therefore$ cc = a

We see that the operation table is symmetrical about the principal diagonal.

$\therefore$ G is Abelian.



CHECK YOUR PROGRESS-3

Q 1: How many generators are there of the cyclic group G of order 10 ?

Q 2: Which of the following groups are cyclic? For each cyclic group list all the generators of the group.

(a) G = <Z, + >

(b) G = < Q, + >

(c) G = < Q^+, + >

(d) G = {6^n : n $\in$ z} under multiplication.



1.7 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
- A non-empty subset H of a group G is a subgroup of G if H is also a group under the same binary operation of G.
- A group G is said to be cyclic if there exists an element a in G such that every element of G can be expressed in the form a^n; n $\in$ Z



1.8 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS-1

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

CHECK YOUR PROGRESS – 2

Ans to Q No 1: No,Binary operations are different.

Ans to Q No 2: No. Two subgroups of a group have at least one common element, viz., the identity element.

Ans to Q No 3: No.

Ans to Q No 4: Left as an exercise

Ans to Q No 5: Left as an enexise

Ans to Q No 6: $Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ is an additive group.

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

and $3Z = \{0, \pm 3, \pm 6, \pm 9, ...\}$

are two subgroups of Z

$Z \neq 2Z \cup 3Z$.

CHECK YOUR PROGRESS – 3

Ans to Q No 1: Since 1, 3, 7, 9 are relatively prime to 10. Thus, a, a^3, a^7 and a^9 are generators of G.

Ans to Q No 2: Left as an exercise



1.9 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.



1.10 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 $a, b \in G$.

Q 3: Let G be an Abelian group. Prove that the set $H = \{x \in G : x = x^{-1}\}$ is a sub group of G.

Q 4: Show that a group of order 4 is always Abelian.

Q 5: Let g be a group and e be the identity of G. Prove that G is Abelian if $b^{-1}a^{-1}ba = e$, for all $a, b \in G$.

*** ***** ***