GMA S2 01

Abstract Algebra and Discrete Mathematics

SEMESTER - II

Mathematics

BLOCK - 1

KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Subject Experts

Prof. N. R. Das, Dept of Mathematics, Gauhati University

Dr. Dillip Kumar Sarma, Former Head, Cotton College

Course Coordinator : Harekrishna Deka, Academic consultant, KKHSOU

SLM Preparation Team

UNITS	CONTRIBUTORS
1, 2, 3, 4, 5, 6, 7, 8	Dr Dilip Kumar Sarma Cotton College, Guwahati

Editorial Team

Content : Prof. Biswajit Bhagawati,Former Head, ,Cotton college

Structure & Format : Harekrishna Deka, KKHSOU

January, 2018, Review: (if any)

© Krishna Kanta Handiqui State Open University.

This Self Learning Material (SLM) of the Krishna Kanta Handiqui State Open University is made available under a Creative Commons Attribution-NonCommercial-ShareAlike4.0 License (international): http://creativecommons.org/licenses/by-nc-sa/4.0/

For the avoidance of doubt, by applying this license KKHSOU does not waive any privileges or immunities from claims that it may be entitled to assert, nor does KKHSOU submit to the jurisdiction, courts, legal processes or laws of any jurisdiction.

Printed and published by Registrar on behalf of the Krishna Kanta Handiqui State Open University.

Headquarters : Patgaon, Rani Gate, Guwahati - 781017

City Office : Housefed Complex, Dispur, Guwahati-781006; Web: www.kkhsou.in

COURSE INTRODUCTION

'Abstract Algebra and Discrete Mathematics' is the second course of the programme B. A Mathematics (pass). The course is divided into two block. The first block consists of eight units and second block consists of six units.

Block 1 deals with the concept of relation and function. Theory and different types of groups are introduced in this block. Concepts of Homomorphism of groups are also covered in this block.

Block 2 deals with the theory of Rings, Integral domain and Field. Concept of Vector space is also introduced in this block. Concept of Combinaorics are also covered in this block. The Notion of Mathematical logic are introduced in this block. Theory of Boolean Algebra is also been introduced in this Block.

BLOCK INTRODUCTION

This is the first block of the course : “Abstract Algebra and Discrete Mathematics”. The block consists of eight units. The first unit deals with relations and functions. After going through this unit, you will be able to know various types of relations and function.

In second unit, we will discuss binary operation and its different types.

In third unit, we will discuss group and its properties.

The fourth unit deals with subgroups and cyclic groups. In this unit, we will also discuss properties of subgroup.

The fifth unit consists of group of permutation. In this unit, we define permutation and different type of permutations. Concept of permutation groups will also be discussed in this unit.

In sixth unit, we will discuss subgroup of a group and Lagrange’s subgroup order theorem.

In seventh unit, concept of normal subgroup and quotient group will be discussed.

The eight unit deals with the concept of homomorphism types of groups. In this unit, we will discuss different types of homomorphisms and properties of homomorphisms.

While going through a unit, you will notics some along boxes. which have been included to help you know some of the difficult, unseen terms. At the end of each section, you will get “CHECK YOUR PROGRESS” questions. These have been designed to self-check your progress of study. It will be better if you solve the problems put in these boxes immediately after you go through the section of the unit and then match your answer “ANSWERS TO CHECK YOUR PROGRESS” given at the end of each unit.

CONTENTS

UNIT 1: Relations and functions **Page : 7-30**

Relations and Types of relations, equivalence relation, function and types of function.

UNIT 2: Binary operations **Page : 31-40**

Binary Operation, Commutative Binary Operation, Associative Binary Operation, Identity Element, Inverse of an Element.

UNIT 3: Group **Page : 41-51**

Definitions and Examples of groups, Properties of groups.

UNIT 4: Subgroup **Page : 52-61**

Subgroups, cyclic groups.

UNIT 5: Groups of permutation **Page : 62-83**

Definition of Permutation, Examples, Multiplication of Permutation, Different Kinds of Permutation, Permutation Group.

UNIT 6: Cosets **Page : 84-90**

Coset, Lagrange's Subgroup order theorem.

UNIT 7: Normal subgroup & Quetion Group **Page : 91-97**

Normal subgroups, Quotient groups.

UNIT 8: Homomorphism of group **Page : 98-115**

Definition and examples, Types of Homomorphism, Properties of Homomorphism.

UNIT1: RELATIONS AND FUNCTIONS

UNIT STRUCTURE

1.1 Learning objectives

1.2 Introduction

1.3 Concept of Relation

1.3.1 Identity Relation

1.3.2 Inverse Relation

1.4 Types of Relation

1.5 Equivalence Relations

1.5.1 Equivalence Class

1.6 Concept of Function

1.6.1 Identity Function

1.6.2 Constant Function

1.7 Types of Function

1.8 Let us Sum Up

1.9 Answers to Check Your Progress

1.10 Further Readings

1.11 Model Questions

1.1 LEARNING OBJECTIVES

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

- the concept of a relation
- different types of relation
- equivalence relation, equivalence class
- the concept of a function
- different types of function.

1.2 INTRODUCTION

Set theory may be called the language of modern mathematics. We know that a set is a well-defined collection of objects. Also we know the notion of subset of a set. If every element of a set B is in set A, then B

is a subset of A. Symbolically we denote it by $B \subseteq A$.

Also we note that if A is a finite set having n elements, the number of subsets of A is 2^n.

Again if A, B are two non-empty sets, the cartesian product of A and B is denoted by A x B and is defined by $A \times B = \{(a, b) : a \in A, b \in B\}$

(a, b) is called an ordered pair.

Let $a \in A$, $c \in A$; $b \in B$, $d \in B$.

$\therefore$ $(a, b) \in A \times B$, $(c, d) \in A \times B$

We know that $(a, b) = (c, d) \Leftrightarrow a=c, b=d$.

Also we know that if A, B are finite and n(A)=x, n(B)= y, then

$$n(AxB) = n(BxA)=xy$$

[Here n(A) denotes the number of elements of A]

If one of the sets A and B is infinite, then A x B and B x A are infinite.

In this unit we will study relations and functions which are subsets of cartesian product of two sets.

We will denote the set of natural numbers by IN, the set of integers by Z, the set of rational numbers by Q, the set of real numbers by IR, the set of complex numbers by C.

1.3 CONCEPT OF RELATION

Let us consider the following sentences.

(1) 11 is greater than 10.

(2) 35 is divisible by 7.

(3) New Delhi is the capital of India.

In each of the sentences there is a relation between two 'objects'.

Now let us see what is meant by relation in set theory.

Definition Let A and B be two non-empty sets. A subset R of A x B is said to be a **relation** from A to B.

If A=B, then any subset of A x A is said to be a relation on A.

If $R \subseteq A \times B$, and $(a, b) \in R$; $a \in A$, $b \in B$, it is also written as aRb and is read as 'a is R related to b'.

Note 1. The set of the first components of the ordered pairs of R is called the domain and the set of the second components of the ordered

pairs of R is called the range of R.

2. If A, B are finite sets and n(A)=x, n(B)=y; then n(AxB)=xy. So, the number of subsets of AxB is 2^{xy}.

Therefore, the number of relations from A to B is 2^{xy}.

Example 1: Let A ={1, 2, 3},

B={8, 9}

$\therefore$ A x B ={(1, 8), (1, 9), (2, 8), (2, 9), (3, 8), (3, 9)}

Let R = {(1, 8), (2, 9), (3, 9)}

Clearly R$\subseteq$ AxB

$\therefore$ R is a relation from A to B.

Here 1R8, 2R9, 3R9

Domain of R = {1, 2, 3}

Range of R = {8, 9}

Example 2 : Let IR be the set of real numbers.

Let R = {(x, y) : x, y $\in$IR, x<y} $\subseteq$IR x IR

$\therefore$ R is a relation on IR.

$\because$ 3<5, $\therefore$ (3, 5)$\in$R i.e. 3R5

19<27, $\therefore$ (19, 27)$\in$R i.e. 19R27

But 5>3, $\therefore$ (5, 3)$\notin$ R, i.e. 5 $\not\mathbb{R}$ 3.

Example 3: Let X be the set of odd integers.

Let R = {(x, y) : x, y $\in$ X and x+y is odd}

We know that the sum of two odd integers is an even integer.

$\therefore$ if x, y are odd, then x+y cannot be odd.

$\therefore$ R = $\phi \subseteq$ X x X

In this case R is called a null relation on X.

Example 4: Let E be the set of even integers.

Let R = {(x, y) : x, y $\in$ E and x+y is even}

We know that the sum of the even integers is an even integer.

$\therefore$ if x, y are even, then x+y is always even.

$\therefore$ R = E x E $\subseteq$ E x E

In this case R is called a universal relation on E.

1.3.1 Identity Relation

Let A be a non-empty set.

$I_A = \{(a, a) : a \in A\} \subseteq A \times A$

I_A is called the identity relation on A.

Example 5: Let A = {1, 2, 3, 4}

Then $I_A = \{(1, 1), (2, 2), (3, 3), (4, 4)\} \subseteq A \times A$.

Clearly I_A is the identity relation on A.

1.3.2 Inverse Relation

Let A, B be two non-empty sets. Let R be a relation from A to B, i.e. $R \subseteq A \times B$. The inverse relation of R is denoted by R^{-1}, and is defined by $R^{-1} = \{(b, a) : (a, b) \in R\} \subseteq B \times A$

Clearly, domain of R^{-1} = range of R

range of R^{-1} = domain of R

Example 6: Let A = {1, 2, 3}

B = {5, 6}

$R = \{(1, 5), (2, 6), (3, 5)\} \subseteq A \times B$

$R^{-1} = \{(5, 1), (6, 2), (5, 3)\} \subseteq B \times A$.



CHECK YOUR PROGRESS 1

Q 1: Let A, B be two finite sets, and n(A)=4, n(B)=3. How many relations are there from A to B?

Q 2: Let A be a finite set such that n(A) =5. Write down the number of relations on A.

Q 3: Let IN be the set of natural numbers.

Let $R = \{(x, y) : x, y \in IN, x>y\}$.

Examine if the following ordered pairs belong to R.

(7, 4), (23, 32), (5, 5), (72, 27), (18, 19).

Q 4: Let E be the set of even integers.

Let $R = \{(x, y) : x, y \in E$ and x+y is odd$\}$

Is R a null relation on E ? Justify your answer.

Q 5: Let A = {1, 2, 3, 4, 5}

Write down the identity relation on A.

Q 6: Let A = {4, 5, 6}, B = {7, 8, 9}

Let R = {(4, 7), (5, 8), (6, 7), (6, 8), (6, 9)}

Write down R^{-1}.

1.4 TYPES OF RELATION

Let A be a non-empty set, and R be a relation on A, i.e. $R \subseteq A \times A$.

1. R is called reflexive if $(a, a) \in R$, i.e; aRa, for all $a \in A$.
2. R is called symmetric if whenever $(a, b) \in R$, then $(b, a) \in R$, i.e, if whenever aRb, then bRa; $a, b \in A$.
3. R is called anti-symmetric if $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$, i.e., if aRb, bRa $\Rightarrow$ a=b; $a, b \in A$.
4. R is called transitive if whenever (a, b), $(b, c) \in R$, then $(a, c) \in R$, i.e., if whenever aRb, bRc, then aRc; $a, b, c \in A$.

Example 7: Let A = {1, 2, 3}

R = (1, 1), (2, 2), (1, 2), (2, 1)}

Examine if R is reflexive, symmetric,anti-symmetric, transitive.

Solution: Here $(1, 1) \in R$, $(2, 2) \in R$; but $(3, 3) \notin R$.

$\therefore$ R is not reflexive.

Again, $(a, b) \in R \Rightarrow (b, a) \in R$

$\therefore$ R is symmetric.

Again, $(1, 2) \in R$, $(2, 1) \in R$, but $1 \neq 2$

$\therefore$ R is not anti-symmetric.

Again, if $(a, b) \in R$, $(b, c) \in R$, then $(a, c) \in R$

$\therefore$ R is transitive.

Example 8: Let Z be the set of integers, and $R = \{(x, y) : x, y \in Z, x \leq y\}$

Examine if R is reflexive, symmetric, anti-symmetric and transitive.

Solution : We have $a \leq a$, $\forall\ a \in Z$

i.e, $(a, a) \in R$, $\forall\, a \in Z$

$\therefore$ R is reflexive.

Again, if $a \leq b$, $b \not\leq a$

i.e; $(a, b) \in R \not\Rightarrow (b, a) \in R$

$\therefore$ R is not symmetric.

Again, $a \leq b$, $b \leq a \Rightarrow a = b$

i.e. $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$

$\therefore$ R is anti-symmetric.

Again $a \leq b$, $b \leq c \Rightarrow a \leq c$

i.e. $(a, b), (b, c), \in R \Rightarrow (a, c) \in R$

$\therefore$ R is transitive.

Example 9: Give an example of a relation which is transitive, but neither reflexive nor symmetric.

Solution : Let A = {1, 2}

Let $R = \{(1, 1), (1, 2)\} \subseteq A \times A$

Clearly R is a relation on A.

Here $(2, 2) \notin R$.

$\therefore$ R is not reflexive.

Again $(1, 2) \in R$, but $(2, 1) \notin R$

$\therefore$ R is not symmetric.

But R is transitive.



CHECK YOUR PROGRESS 2

Q 1: Let A = {1, 2, 3) and R be a reflexive relation on A having minimum number of ordered pairs. Write down R.

Q 2: Define a relation on the set

A = {1, 2, 3, 4} which is

(i) symmetric, but neither reflexive nor transitive;

(ii) reflexive and transitive, but not symmetric;

(iii) reflexive and symmetric, but not transitive.

1.5 EQUIVALENCE RELATION

Let A be a non-empty set. A relation R on A is called an equivalence relation if it is reflexive, symmetric and transitive.

Example 10: Let Z be the set of integers and

$R = \{(x, y) : x, y \in Z \text{ and } x+y \text{ is even}\}$

Examine if R is an equivalence relation on Z.

Solution : Let $x \in Z$

$\therefore$ x+x is even

$\Rightarrow (x, x) \in R, \forall\ x \in Z$

$\therefore$ R is reflexive.

$(x, y) \in R \Rightarrow$ x+y is even

$\Rightarrow$ y+x is even

$\Rightarrow (y, x) \in R.$

$\therefore$ R is symmetric.

$(x, y) \in R, (y, z) \in R$

$\Rightarrow$ x+y is even, y+z is even

$\Rightarrow$ (x+y)+(y+z) is even

$\Rightarrow$ (x+z)+2y is even

$\Rightarrow$ x+z is even

$(x, z) \in R$

$\therefore$ R is transitive

$\therefore$ R is an equivalence relation on Z.

Example 11: Let A be the set of all straight lines in a plane.

Let $R = \{(x, y) : x, y \in A \text{ and } x \perp y\}$

Examine if R is reflexive, symmetric and transitive.

Solution : A line cannot be perpendicular to itself, i.e. $x \not\perp x$

$\therefore (x, x) \notin R$

$\therefore$ R is not reflexive

If a line x is perpendicular to another line y, then y is perpendicular to x, i.e. $x \perp y \Rightarrow y \perp x$

$\therefore (x, y) \in R \Rightarrow (y, x) \in R$

$\therefore$ R is symmetric.

If $x \perp y$, $y \perp z$, then $x \not\perp z$

$\therefore (x, y), (y, z) \in R \not\Rightarrow (x, z) \in R$

If x is perpendicular to y, y is perpendicular to z, then x is parallel to z.

$\therefore$ R is not transitive.

Example 12: Let A be the set of all straight lines in a plane.

Let $R = \{(x, y) : x, y \in A \text{ and } x||y\}$

Examine if R is an equivalence relation on A.

Solution : A line is parallel to itself, i.e. $x||x \ \forall \ x \in A$

$\therefore (x, x) \in R, \forall x \in A$

$\therefore$ R is reflexive.

$x||y \Rightarrow y||x$

$\therefore (x, y) \in R \Rightarrow (y, x) \in R$

$\therefore$ R is symmetric.

$x||y, y||z \Rightarrow x||z$

$\therefore (x, y), (y, z) \in R \Rightarrow (x, z) \in R.$

$\therefore$ R is transitive

Thus, R is an equivalence relation on A.

Example 13: Let IN be the set of natural numbers. Let a relation R be defined on IN x IN by (a, b) R (c, d) if and only if ad = bc

Show that R is an equivalence relation on IN x IN.

Solution : We have ab = ba

$\therefore$ (a, b) R (a, b)

$\therefore$ R is reflexive

(a, b) R (c, d) $\Rightarrow$ ad = bc; a, b, c, d, $\in$ IN

$\Rightarrow$ cb = da

$\Rightarrow$ (c, d) R (a, b)

$\therefore$ R is symmetric

(a, b) R (c, d) and (c, d) R (e, f); a, b, c, d, e, f, $\in$ IN

$\Rightarrow$ ad = bc and cf = de

$\Rightarrow$ adcf = bcde

$\Rightarrow$ af = be

$\Rightarrow$ (a, b) R (e, f)

$\therefore$ R is transitive.

Thus, R is an equivalence relation on IN x IN.

Example 14: (Congruence modulo n)

Let Z be the set of integers, and n be any fixed positive integer.

Let a, b $\in$ Z

a is said to be congruent to b modulo n if and only if a–b is divisible by n. Symbolically, we write.

a $\equiv$ b (mod n)

Show that the relation 'congruence modulo n' is an equivalence relation on Z.

Solution : We know that a–a is divisible by n, i.e., a $\equiv$ a (mod n)

$\therefore$ the relation is reflexive.

Let a $\equiv$ b (mod n)

$\Rightarrow$ a–b is divisible by n.

$\Rightarrow$ b–a is divisible by n.

$\Rightarrow$ b $\equiv$ a (mod n)

$\therefore$ the relation is symmetric.

Let a $\equiv$ b (mod n), b $\equiv$ c (mod n)

$\Rightarrow$ a–b is divisible by n, b–c is divisible by n

$\Rightarrow$ a–b+b–c is divisible by n

$\Rightarrow$ a–c is divisible by n

$\Rightarrow$ a $\equiv$ c (mod n)

$\therefore$ the relation is transitive.

Thus, the relation 'congruence modulo n' is an equivalence relation on Z.

We know that 15-3 is divisible by 4.

$\therefore$15 is congruent to 3 modulo 4 i.e.

15 $\equiv$ 3 (mod 4)

15–3 is not divisible by 7

$\therefore$15 is not congruent to 3 modulo 7

i.e. 15 $\not\equiv$ 3 (mod 7)

Example 15: Let Z be the set of integers.

Let R = {(a, b) : a, b $\in$ Z, ab $\geq$ 0}

Examine if R is an equivalence relation on Z.

Solution : We have aa $\geq$ 0

$\therefore (a, a) \in R, \forall a \in Z$

$\therefore R$ is reflexive

Let $(a, b) \in R$

$\therefore ab \geq 0$

$\Rightarrow ba \geq 0$

$\Rightarrow (b, a) \in R$

$\therefore$ R is symmetric.

We have

$(-2) \times 0 = 0, 0 \times 2 = 0$

$\therefore (-2, 0), (0, 2) \in R$

But $(-2) \times 2 = -4 < 0$

$\therefore (-2, 2) \notin R$

$\therefore$ R is not transitive.

Thus, R is not an equivalence relation.

Theorem 1: The inverse of an equivalence relation is also an equivalence relation.

Proof. Let A be a non-empty set. Let R be an equivalence relation on A

R is reflexive.

$\therefore (x, x) \in R, \forall x \in A$

$\Rightarrow (x, x) \in R^{-1}, \forall x \in A$

$\therefore R^{-1}$ is reflexive.

Let $(x, y) \in R^{-1}$

This $\Rightarrow (y, x) \in R$ [by def^n of R^{-1}]

$\Rightarrow (x, y) \in R$ [$\therefore R$ is symmetric]

$\Rightarrow (y, x) \in R^{-1}$

$\therefore R^{-1}$ is symmetric.

Let $(x, y), (y, z) \in R^{-1}$

$\Rightarrow (y, x), (z, y) \in R$ [by def^n of R^{-1}]

$\Rightarrow (z, y), (y, x) \in R$

$\Rightarrow (z, x) \in R$ [$\therefore R$ is transitive]

$\Rightarrow (x, z) \in R^{-1}$

$\therefore R^{-1}$ is transitive

Thus, R^{-1} is an equivalence relation.

Theorem 2: The intersection of two equivalence relations is also an equivalence relation.

Proof. Let A be a non-empty set.

Let R and S be two equivalence relations on A.

R and S are reflexive

$\therefore (x, x) \in R$ and $(x, x) \in S$, $\forall\, x \in A$

$\Rightarrow (x, x) \in R \cap S$, $\forall\, x \in A$

$\therefore R \cap S$ is reflexive.

Let $(x, y) \in R \cap S$

This $\Rightarrow (x, y) \in R$ and $(x, y) \in S$

$\Rightarrow (y, x) \in R$ and $(y, x) \in S$ [$\therefore$ R, S are symmetric]

$\Rightarrow (y, x) \in R \cap S$

$\therefore R \cap S$ is symmetric.

Let $(x, y) \in R \cap S$, $(y, z) \in R \cap S$

$\Rightarrow (x, y) \in R$ and $(x, y) \in S$, $(y, z) \in R$ and $(y, z) \in S$

$\Rightarrow (x, z) \in R$ and $(x, z) \in S$ [$\therefore$ R, S are transitive]

$\Rightarrow (x, z) \in R \cap S$

$\therefore R \cap S$ is transitive.

Thus, $R \cap S$ is an equivalence relation.

Remarks : The union of two equivalence relations is not necessarily an equivalence relation.

Let us consider A = {1, 2, 3}

Now, R = {(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)}

S = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)}

are two equivalence relations on A.

$R \cup S$ = {(1, 1), (2, 2), (3, 3), (1, 3), (3, 1), (1, 2), (2, 1)}

$(2, 1) \in R \cup S$, $(1, 3) \in R \cup S$)

But $(2, 3) \notin R \cup S$

$\therefore$ $R \cup S$ is not transitive

$\therefore$ $R \cup S$ is not an equivalence relation.

1.5.1 Equivalence Class

Let us consider the set Z of integers

Let R = {(a, b) : a, b $\in$ Z, a–b is divisible by 3}

i.e. R = {(a, b) : a, b$\in$Z, a $\equiv$b (mod 3)}

Clearly R is reflexive, symmetric and transitive.

$\therefore$ R is an equivalence relation on Z.

Let [0] denote the set of integers congruent to 0 modulo 3. Then

[0] = {...., –9, –6, –3, 0, 3, 6, 9, ...}

Let [1] denote the set of integers congruent to 1 modulo 3. Then

[1] = {..., –8, –5, –2, 1, 4, 7, 10, ...}

Let [2] denote the set of integers congruent to 2 modulo 3. Then

[2] = {...., –7, – 4, –1, 2, 5, 8, 11, ...}

We see that

..... = [0] = [3] = [6] =.....

..... = [1] = [4] = [7] =.....

..... = [2] = [5] = [8] =.....

Each of [0], [1], [2] is called an equivalence class. [0] is the equivalence class of 0, [1] is the equivalence class of 1, [2] is the equivalence class of 2.

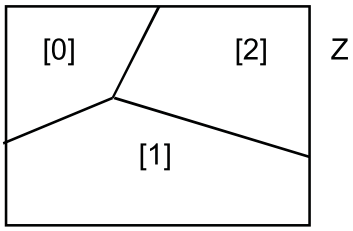
We see that there are 3 distinct equivalence classes, viz, [0], [1], [2].

Also we note that

[0] U [1] U [2] = Z

[0] $\cap$ [1] = ϕ , [1] $\cap$ [2] = ϕ [2]$\cap$[0] = ϕ

The set {[0], [1], [2]} is called a partition of Z.



Definition : Let A be a non-empty set and R be a relation on A.

For any a$\in$ A, the equivalence class [a] of a is defined by

$[a] = \{x \in A : xRa\}$

i.e. the equivalence class [a] of a is the collection of all those elements of A which are related to a under the relation R.



If A, B are two non-empty sets, then either $A \cap B \neq \phi$ or $A \cap B = \phi$

Note : $[a] \neq \phi$, $\because$ aRa

Definition : Let A be a non-empty set.

The set P of non-empty subsets of A is called a partition of A if

(i) A is the union of all members of P,

(ii) any two distinct members of P are disjoint.

Theorem 3 : Let A be a non-empty set and R be an equivalence relation of A. Let $a, b \in A$. Then [a] = [b] if and only if $(a, b) \in R$.

Proof. Let [a] = [b]

$\because$ R is reflexive, $\therefore$ aRa

$\therefore a \in [a]$

$\Rightarrow a \in [b]$ [$\because$ [a]=[b]]

$\Rightarrow$ aRb

$\Rightarrow (a, b) \in R$

Conversely : Let $(a, b) \in R$. $\therefore$ aRb

Let $x \in [a]$. $\therefore$ xRa

Now, xRa and aRb

$\therefore$ xRb [$\because$ R is transitive]

$\Rightarrow x \in [b]$

Thus, $x \in [a] \Rightarrow x \in [b]$

$\therefore [a] \subseteq [b]$ ... (1)

Again, let $y \in [b]$ $\therefore$ yRb

Now, yRb and bRa [$\because$ R is symmetric, aRb $\Rightarrow$ bRa]

$\therefore$ yRa [$\because$ R is transitive]

$\Rightarrow y \in [a]$

Thus, $y \in [b] \Rightarrow y \in [a]$

$\therefore [b] \subseteq [a]$ ... (2)

From (1) and (2), [a] = [b]

Theorem 4 : Two equivalence classes are either equal or disjoint.

Proof. Let A be a non-empty set. Let R be an equivalence relation on A.

Let a, b$\in$A.

Then [a], [b] are either not disjoint or disjoint.

Let [a], [b] be not disjoint,

i.e. [a] $\cap$[b] $\neq \phi$.

Let x $\in$ [a] $\cap$[b]

$\Rightarrow$ x$\in$ [a] and x$\in$[b]

$\Rightarrow$ xRa and xRb

$\Rightarrow$ aRx and xRb [$\because$ R is symmetric, xRa $\Rightarrow$aRx]

$\Rightarrow$ aRb [$\because$ R is transitive]

Let y$\in$[a]

$\Rightarrow$ yRa

Now yRa and aRb

$\therefore$ yRb [$\because$ R is transitive]

$\Rightarrow$ y $\in$ [b]

Thus, y$\in$[a] $\Rightarrow$ y$\in$[b]

$\therefore$ [a] $\subseteq$ [b]

Similarly, [b] $\subseteq$[a]

$\therefore$[a] = [b]

So, if [a], [b] are not disjoint, they are equal.

$\therefore$ [a], [b] are either equal or disjoint.



CHECK YOUR PROGRESS 3

Q 1: What is the name of the relation on a set . which is reflexive, symmetric and transitive?

Q 2: Is the relation "<" on the set of narural nimbers IN an equivalence relation? Justify your answer.

Q 3: Let Z be the set of integers.

Let R = {(a, b) : a, b $\in$ Z, a–b is divisible by 5}

Examine if R is an equivalence relation on Z ?

Q 4: Let A be the set of all triangles in a plane.

Let R = {(x, y) : x, y $\in$ A., x is similar to y}

Examine if R is an equivalence relation on A.

Q 5: let Z be the set of integers.

Let R = {(x, y) : x, y $\in$ Z, x–y is even}

Is R an equivalence relation on Z ?

Justify your answer.

1.6 CONCEPT OF FUNCTION

Let A and B be two non-empty sets, and f $\subseteq$ A xB such that

(i) (x, y) $\in$ f, $\forall$ x$\in$A and any y$\in$B

(ii) (x, y) $\in$ f and (x, y$'$)$\in$ f $\Rightarrow$ y=y$'$.

In this case f is said to be a function (or a mapping) from the set A to the set B. Symbolically we write it as f : A $\rightarrow$ B.

Here A is called the domain and B is called the codomain of f.

Example 16 : Let A = {1, 2}, B = {7, 8, 9}

f = {(1, 8), (2, 7)} $\subseteq$ A x B.

Here, each element of A appears as the first component exactly in one of the ordered pairs of f.

$\therefore$f is a function from A to B.

Example 17 : Let A = {1, 2}, B = {7, 8, 9}

g = {(1, 7), (1, 9)} $\subseteq$ A x B

Here, two distinct ordered pairs have the same first component.

$\therefore$ f is not a function from A to B.

Example 18 : Let A = {1, 2, 3, 4}, B = {x, y, z, w}

Are the following relations from be functions A to B ?

(i) f_1 = {(1, x), (1, w), (2, x), (2, z), (4, w)}

(ii) f_2 = {(1, y), (2, z), (3, x), (4, w)}

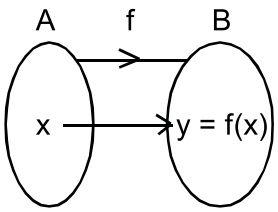
Solution : (i) No. Here two distinct ordered pairs (1, x), (1, w) have the same first component.

(ii) Yes.

Here, each element of A appears as the first component exactly in one of the ordered pairs of f_2.

Thus we see that.

Every function is a relation, but every relation is not a function.



We observe that if A and B are two non-empty sets and if each element of A is associated with a unique element of B, then the rule by which this association is made, is called a function from the set A to the set B. The rules are denoted by f, g etc. The sets A, B may be the same.

Let f be a function from A to B i.e. $f : A \to B$. The unique element y of B that is associated with x of A is called the image of x under f. Symbolically we write it as y = f(x). x is called the pre-image of y. The set of all the images under f is called the range of f.

Example 19 : Let IN be the set of natural members, and Z be the set of integer and $f : IN \to Z$, $f(x) = (-1)^x$; $x \in IN$

Clearly, domain of f = IN

codomain of f = Z

Now $f(1) = (-1)^1 = -1$, $f(2) = (-1)^2 = 1$, $f(3) = (-1)^3 = -1$ and so on.

$\therefore$ range of f = {–1, 1}

1.6.1 Identity Function

Let A be a non-empty set and $i : A \to A$, $i(x) = x$, $\forall x \in A$

i is called the identity function.

Note : In case of identity function, domain and codomain are the same.

1.6.2 Constant Function

Let A, B be two non-empty sets and $f : A \to B$ be a function such that $f(x) = k$, $\forall x \in A$

f is called a constant function.

Note : The range of a constant function is a singleton set.

1.7 TYPES OF FUNCTION

Let A, B be two non-empty sets and $f : A \to B$ be a function.

1. If there is at least one element in B which is not the image of any

element in A, then f is called an "into" function.

2. If each element in B is the image of at least one element in A, then f is called an "onto" function (or a surjective function or a surjection).

Note : In case of an onto function, range of f = codomain of f.

3. If different elements in A have different images in B, then f is called a one-one function (or an injective function or an injection).

4. If two (or more) different elements in A have the same image in B, then f is called a many-one function.

5. A function is said to be bijective if it is one-one (injective) and onto (surjective).

Note : Identity function is a bijective function.

How to prove that f is one-one?

Let $x_1, x_2, \in A$

If $f(x) = f(x_2) \Rightarrow x_1 = x_2$, then f is one-one.

or,

If $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, then f is one-one.

How to prove that f is onto?

Let $y \in B$ (codomain)

Let y = f(x)

We find x in terms of y

If $x \in A$, then f is onto; otherwise not.

Example 20: Let IN be the set of natural numbers,

Let $f : IN \to IN$, $f(x) = 3x+7$

Examine if f is a bijective function.

Solution : Let $x_1, x_2 \in IN$ (domain)

Now $f(x_1) = f(x_2)$

$\Rightarrow 3x_1+7=3x_2+7$

$\Rightarrow x_1 = x_2$

$\therefore$f is one-one (injection).

Let $y \in IN$ (codomain)

Let y = f(x)

$\Rightarrow y = 3x + 7$

$\Rightarrow x = \frac{y-7}{3}$

If y = 1, $x = \frac{1-7}{3} = -2 \notin N$

$\therefore$ f is not onto

$\therefore$ f is not a bijection.

Example 21: Let X be the set of real numbers excluding 1. Show that the function f : X→X, $f(x)=\frac{x+1}{x-1}$ is one-one and onto.

Solution: Let $x_1, x_2 \in$ X(domain)

Let $f(x_1) = f(x_2)$

$\Rightarrow \frac{x_1+1}{x_1-1} = \frac{x_2+1}{x_2-1}$

$\Rightarrow \frac{(x_1+1)+(x_1-1)}{(x_1+1)-(x_1-1)} = \frac{(x_2+1)+(x_2-1)}{(x_2-1)-(x_2-1)}$ (by componendo and dividendo)

$\Rightarrow \frac{2x_1}{2} = \frac{2x_2}{2}$

$\Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

Let y $\in$ X (codomain)

Let y = f(x)

$\Rightarrow y = \frac{x+1}{x-1}$

$\Rightarrow$ y(x–1) = x+1

$\Rightarrow$ yx–y = x+1

$\Rightarrow$ yx – x = y+1

$\Rightarrow$ x(y–1) = y+1

$\Rightarrow x = \frac{y+1}{y-1} \in$ X (domain)

$\therefore$ f is onto.

Example 22: Let A = {1, 2, 3,}. Write down all the bijective function from A to itself.

Solution :

i : A→ A, i(1) = 1, i(2) = 2, i(3) = 3

f_1 : A→ A, $f_1(1) = 1$, $f_1(2) = 3$, $f_1(3) = 2$

f_2 : A→ A, $f_2(1) = 2$, $f_2(2) = 1$, $f_2(3) = 3$

$f_3 : A \to A$, $f_3(1) = 3$, $f_3(2) = 2$, $f_3(3) = 1$

$f_4 : A \to A$, $f_4(1) = 2$, $f_4(2) = 3$, $f_4(3) = 1$

$f_5 : A \to A$, $f_5(1) = 3$, $f_5(2) = 1$, $f_5(3) = 2$

Note. There are 6 =3! bijective functions from A = {1, 2, 3} to itself.

If A has n elements, there are n! bijective functions from A to itself.

Theorem 5 : Let A be a finite set, and $f : A \to A$ be onto. Then f is one-one.

Proof. Let A be a finite set having n elements.

Let $A = \{a_1, a_2, ..., a_n\}$, where a_i' s are distinct.

Let $f : A \to A$ be onto.

Now, range of f

$= \{f(a_1), f(a_2), ..., f(a_n)\}$

$\therefore$ f is onto, range of f = codomain of f = A.

$\therefore A = \{f(a_1), f(a_2), ..., f(a_n)\}$

$\therefore$ A has n elements,

$\therefore f(a_1), f(a_2), ..., f(a_n)$ are distinct.

Thus, distinct elements in A (domain) have distinct images in A (codomain).

$\therefore$ f is one-one.

Note : The result does not hold good if A is an infinite set.

Let IN be the set of natural numbers.

Let $f : IN \to IN$, $f(x) = 1$, if $x = 1$ and $x = 2$,

$= x-1$, if $x \geq 3$

Clearly, f is onto, but not one-one.

Theorem 6 : Let A be a finite set, and $f:A \to A$ be one-one. Then f is onto.

Proof : Let A be a finite set having n elements.

Let $A = \{a_1, a_2, ..., a_n\}$, where a_i's are distinct.

Let $f : A \to A$ be one-one.

$\therefore f(a_1), f(a_2), ..., f(a_n)$ are n distinct elements of A (codomain).

Let $u \in A$ (codomain).

Let $u = f(a_i)$, $1 \leq i \leq n$

$\therefore$ there exists $a_i \in A$ (domain) such that $f(a_i) = u$.

$\therefore$ f is onto.

Note : The result does not hold good if A is an infinite set.

Let IN be the set of natural numbers.

Let f : IN $\rightarrow$IN, f(x) = 5x

Clearly, f is one-one, but not onto.



CHECK YOUR PROGRESS 4

Q 1: Let IN be the set of natural numbers.

Let f : IN $\rightarrow$IN, $f(x) = x^2+1$

Examine if f is (i) one-one, (ii) onto.

Q 2: Let IR be the set of real numbers and

f : IR$\rightarrow$IR be defined by

$$f(x) = \begin{cases} 1, & \text{if } x > 0 \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x < 0 \end{cases}$$

Examine if f is (i) one-one, (ii) onto

Q 3: Let f : IR$\rightarrow$IR be defined by f (x) =|x|

Examine if f is (i) one-one, (ii) onto

$$\left[f(x) = |x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases} \right]$$

Q 4: If A = {1, 2}, write down all the bijective functions from A to itself.

Q 5: Write down the condition such that a constant function is onto.

Q 6: Write down the condition such that a constant function is one-one.



1.8 LET US SUM UP

- If A, B are two non-empty sets, a subset of A x B in said to be a relation from A to B.
- If A, B are two finite sets and n(A) = x, n(B) = y, the number of relations from A to B is 2^{xy}.
- If A is a non-empty set, $I_A = \{(a, a) : a \in A\}$ is called the identity relation on A.

- If A, B are two non-empty sets and R is a relation from A to B, the inverse relation R^{-1} is defined by
  $R^{-1} = \{(b, a) : (a, b) \in R\}$, which is a relation from B to A.
- A relation R on a non-empty set A is called.
  (i) reflexive if $(a, a) \in R$, for all $a \in A$;
  (ii) symmetric if whenever $(a, b) \in R$, $(b, a) \in R$;
  (iii) anti-symmetric if $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$;
  (iv) transitive if whenever $(a, b), (b, c) \in R$, then $(a, c) \in R$.
- A relation R on a non-empty set A is called an equivalence relation if it is reflexive, symmetric and transitive.
- The inverse of an equivalence relation is also an equivalence relation.
- The intersection of two equivalence relations is also an equivalence relation.
- If R is a relation on a non-empty set A, then for any $a \in A$; the equivalence class [a] of a is the collection of all those elements of A which are related to a under the relation R.
- Two equivalence classes are either equal or disjoint.
- If A and B are two non-empty sets and if each element of A is associated with a unique element of B, then the rule by which this association is made, is called a function from A to B.
- Every function is a relation, but every relation is not a function.
- If different elements in domain have different images in codomain, then the function is one-one (injective).
- If each element in codomain is the image of at least one element in domain then the function is onto (surjective).
- A function is bijective if it is injective and surjective.
- If A is a finite set and $f : A \to A$ is onto, then f is one-one.
- If A is a finite set and $f : A \to A$ is one-one, then f is onto.



1.9 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

Ans to Q No 1: 2^{12}

Ans to Q No 2: 2^{25}

Ans to Q No 3: (7, 4), (72, 27) belong to R.

Ans to Q No 4: Yes. The sum of two even integers cannot be odd.

Ans to Q No 5: $I_A = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}$

Ans to Q No 6: $R^{-1} = \{(7, 4), (8, 5), (7, 6), (8, 6), (9, 6)\}$

CHECK YOUR PROGRESS – 2

Ans to Q No 1: $R = \{(1, 1), (2, 2), (3, 3)\}$

CHECK YOUR PROGRESS – 3

Ans to Q No 1: Equivalence relation.

Ans to Q No 2: No. Not reflexive and symmetric.

Ans to Q No 3: Equivalence relation.

Ans to Q No 4: Equivalence relation.

Ans to Q No 5: Yes.

CHECK YOUR PROGRESS – 4

Ans to Q No 1: One-one, but not onto.

Ans to Q No 2: Neither one-one nor onto.

Ans to Q No 3: Neither one-one nor onto

Ans to Q No 4: $i : A \to A$, $i(1) = 1$, $i(2) = 2$

$f : A \to A$, $f(1) = 2$, $f(2) = 1$

Ans to Q No 5: Codomain is a singleton set.

Ans to Q No 6: Domain is a singleton set.



1.10 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.



1.11 MODEL QUESTION

Q 1: Let A = {1, 2, 3}, B = {3, 4, 5}.
How many relations are there from A to B ? Write down any four relations from A to B.

Q 2: Let A = {3, 4, 5}, B = {5, 6, 7}
Which of the following relations are functions from A to B ? If it is a function, determine whether it is one-one and whether it is onto ?
(i) {(3, 5), (4, 5), (5, 7)}
(ii) {(3, 7), (4, 5), (5, 6)}
(iii) {(3, 6), (4, 6), (5, 6)}
(iv) {(3, 6), (4, 7), (5, 5)}

Q 3: Let Q be the set of rational numbers and f : Q$\rightarrow$Q be a function defined f(x) = 4x+5. Examine if f is bijective

Q 4: Let A be the set of all triangles in a plane.
Let R = {(x, y) : x, y $\in$ A and x is congruent to y}
Examine if R is an equivalence relation on A.

Q 5: Let IN be the set of natural numbers. A relation R is defined on IN x IN by (a, b) R (c, d) if and only if a+d = b+c.
Show that R is an equivalence relation on IN x IN.

Q 6: Let A = {1, 2, 3}

R = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)}

Show that R is reflexive but neither symmetric nor transitive.

Q 7: Let C be the set of complex numbers and IR be the set of real numbers. Let $f : C \to IR$, $f(z) = |z|$, $z \in C$.

Examine if f is (1) one-one, (ii) onto.

Q 8: Let A, B be two non-empty sets.

Let $f : A \times B \to B \times A$, $f(a, b) = (b, a)$; $(a, b) \in A \times B$

Show that f is bijective.

Q 9: Let $f : IN \times IN$, $f(a, b) = 3^a 4^b$, $(a, b) \in IN \times IN$

Examine if f is (i) one-one, (ii) onto.

Q 10: Let $f : Z \times Z \to Z$, $f(a, b) = ab$, $(a, b) \in Z \times Z$

Examine if f is (i) injective, (ii) surjective.

*** ***** ***

UNIT 2: BINARY OPERATION

UNIT STRUCTURE

2.1 Learning objectives
2.2 Introduction
2.3 Binary Operation
  2.3.1 Commutative Binary Operation
  2.3.2 Associative Binary Operation
  2.3.3 Identity Element
  2.3.4 Inverse of an Element
2.4 Let Us Sum Up
2.5 Answers to Check Your Progress
2.6 Further Readings
2.7 Model Questions

2.1 LEARNING OBJECTIVES

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

- binary operation on a set

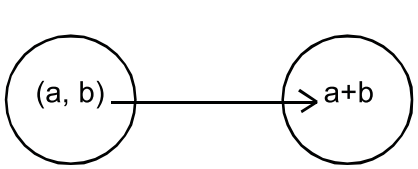
2.2 INTRODUCTION

We have studied relations and functions. In this unit, we will introduce the notion of binary operations and its types.

2.3 BINARY OPERATION

Let us consider the set IN of natural numbers.

For every ordered pair (a, b) $\in$ IN x IN, we get a unique a+b $\in$ IN. So we can define a funtion f : IN x IN $\rightarrow$ IN, f(a, b) = a+b.

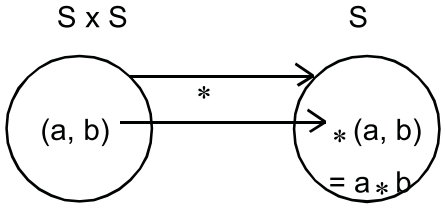


This function is known as a binary operation on IN. Thus, addition is a binary operation on IN.

Similarly, multiplication is a binary operation on IN; for every ordered pair (a, b) $\in$ IN x IN. We get a unique ab $\in$ IN. But subtraction is not a binary operation on IN; for every ordered pair (a, b) $\in$ IN x IN, we do not get a–b $\in$ IN. We have (2, 3) $\in$ IN x IN, but 2–3 = -1 $\notin$ IN.

Definition: A binary operation $*$ on a non-empty set S is a function from S x S to S, i.e.

$* : S \times S \to S$



Here the image of (a, b) $\in$ S x S under the function $*$, i.e $*$ (a, b) is denoted by a $*$ b.

Thus, $*$ is a binary operation on S if a $*$ b $\in$ S, for all a, b $\in$ S.

Definition: Let $*$ be a binary operation on a non-empty set S and H be a subset of S. H is said to be closed under $*$ if for all a, b $\in$ H, we have a $*$ b $\in$ H.In particular,if a $*$ b $\in$ A $\forall$ a, b $\in$ A,then A is said to be closed under the operation $*$.

Number of Binary operations on a finite set

Let A, B be two finite sets, and n (A) = m and n (B) = n.

Then the number of functions from A to B is n^m. [The first element of A can be associated in n ways, the second element in n ways and lastly, the m th element can be associated in n ways.

$\therefore$ the number of functions

= n. n ... ... n (m factors) = n^m]

We know that n (A x A) = mm = m^2

$\therefore$ number of binary operations on A

= number of functions from A x A to A

= m^{m^2}

Examples

1. Addition is a binary operation on IN.
2. Subtraction is not a binary operation on IN.

3. Multiplication is a binary operation on IN.
4. Addition is a binary operation on Z.
5. Addition is not a binary operation on the set S = Z – {0} of non–zero integers, for $3 \in S$, $-3 \in S$, but $3+(-3) = 0 \notin S$.
6. Subtraction is a binary operation on Z.
7. Let S be the collection of all real matrices. Matrix addition is not a binary operation on S. We cannot find the sum of a 2 x 3 matrix and a 3 x 4 matrix.
8. Let M_{mxn} be the collection of all m x n real matrices. Matrix addition is a binary operation on M_{mxn}.
9. Let M_{nxn} be the collection of all nxn real matrices. Matrix multiplication is a binary operation on M_{nxn}.
10. Addition (also multiplication) is a binary operation on the set C of complex numbers.

Example 1: Is $*$ defined by $a * b = a-b+10$ a binary operation on Z ?

Solution: Let $a, b \in Z$

Clearly $a-b+10 \in Z, \forall\ a, b \in Z$

i.e., $a * b \in Z, \forall\ a, b \in Z$

$\therefore *$ is a binary operation on Z

Example 2: Is $*$ defined by $a * b = \frac{ab}{5}$ a binary operation on Q ?

Solution: Let $a, b \in Q$

$\therefore ab \in Q$ (the product of two rational numbers is a rational number)

$\therefore \frac{ab}{5} \in Q$

i.e. $a * b \in Q, \forall\ a, b \in Q$

$\therefore *$ is a binary operation on Q

Example 3: Let P be the set of all subsets of a non-empty set S. Show that union and intersection are two binary operations on P.

Solution: Let $A, B \in P$ i.e. $A \subseteq S, B \subseteq S$

$\therefore A \cup B \subseteq S$ i.e $A \cup B \in P$

$\therefore \cup$ is a binary operation on P.

Similarly, $A \cap B \in P, \forall\ A, B \in P$

$\therefore \cap$ is a binary operation on P.

Operation (or composition) Table

Let S be a finite set and the number of elements of S be small. We can construct a table, known as the operation (or composition) table, as follows.

Let $A = \{a_1, a_2, a_3\}$.

We write the elements a_1, a_2, a_3 in a horizontal row as well as in a vertical column and write the binary operation $*$ in the top left corner. Now we enter each of the 9($= 3^2$) entries a_i x a_j (i = 1, 2, 3; j = 1, 2, 3) in the (i, j) th cell as shown in Table 2.1. Each of the 9 entries belongs to A, since $*$ is a binary operation on A.

$*$	a_1	a_2	a_3
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$

Table 2.1

Example 4: Is multiplication a binary operation on {–1, 0, 1} ?

Solution: Each of the 9 entries belongs to A

$\therefore$ multiplication is a binary operation on {–1, 0, 1}.

x	–1	0	1
–1	1	0	–1
0	0	0	0
1	–1	0	1

Table 2.2

Example 5: Is addition a binary operation on {–1, 0, 1} ?

Solution: $-2 \notin \{-1, 0, 1\}$

$2 \notin \{-1, 0, 1\}$

$\therefore$ addition is not a binary operation on {–1, 0, 1}.

+	–1	0	1
–1	–2	–1	0
0	–1	0	1
1	0	1	2

Table 2.3

Example 6: Is $*$ defined by $a * b=|a-b|$ a binary operation on {0, 1, 2} ?

Solution: $0 * 0 = |0-0|=0$,

$0 * 1 = |0-1|=1$,

$0 * 2 = |0-2|=2$;

$1 * 0 = |1-0|=1$, $1 * 1 = |1-1|=0$,

$1 * 2 = |1-2|=1$;

$2 * 0 = |2-0|=2$, $2 * 1 = |2-1|=1$, $2 * 2 = |2-2|=0$,

From the table we see that $*$ is a binary operation on {0, 1, 2}.

$*$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

Table 2.4

2.3.1 Commutative Binary Operation

A binary operation $*$ on a non-empty set S is commutative if $a * b = b * a$, $\forall a, b \in S$.

Note : For a finite set, a binary operation is commutative if and only if the entries in the operation table are symmetric with respect to the principal diagonal.

For example, the entries in Table 2.3 are symmetric with respect to the principal diagonal 0, 0, 0. Therefore, $*$, defined in Example 6, is commutative on {0, 1, 2}.

Example 7: Is the binary operation $*$ defined by $a * b = a-b+5$ commutative on Z ?

Solution: We have $a * b = a-b+5$

$b * a = b-a+5$, $\forall a, b \in Z$

Clearly $a * b \neq b * a$

$\therefore *$ is not commutative on Z.

Example 8: Let Q be the set of rational numbers. Let $*$ be a binary operation on Q defined by $a * b = ab^2$, $\forall a, b \in Q$. Is $*$ commutative?

Solution: $a * b = ab^2$, $b * a = ba^2$, $\forall a, b \in Q$

$\therefore a * b \neq b * a$

$\therefore *$ is not commutative.

2.3.2 Associative Binary Operation

A binary operation $*$ on a non-empty set S is associative if $(a * b) * c = a * (b * c)$, $\forall$ a, b, c $\in$ S.

Example 9: Is the binary operation $*$ defined by $a * b = a–b+5$ associative on Z ?

Solution: Let a, b, c $\in$ Z.

$(a * b) * c = (a–b+5) * c$

$= (a–b+5) – c+5$

$= a–b–c+10$

$a * (b * c) = a * (b–c+5)$

$= a – (b–c+5)+ 5$

$= a – b + c – 5 + 5$

$= a – b + c$

$\therefore (a * b) * c \neq a * (b * c)$

$\therefore *$ is not associative.

Example 10: Let X be the set of rational numbers excluding 1. We define $*$ on X as follows.

$a * b = a + b – ab$, $\forall$ a, b $\in$ X.

Show that $*$ is a binary operation on X. Examine if $*$ is (i) commutative, (ii) associative.

Solution: Let a, b $\in$ X

$\therefore$ a, b are two rational numbers and $a \neq 1$, $b \neq 1$.

Now a + b – ab is a rational number and $a+b–ab \neq 1$, for if $a+b–ab=1$, then

$a+b–ab–1=0$

i.e. $(a–1)–b(a–1)=0$

i.e. $(a–1)(1–b)=0$

i.e. $a–1=0$ or $1–b=0$

i.e. a = 1 or b = 1, which is a contradiction.

$\therefore a+b–ab \in X$

i.e $a * b \in X$, $\forall$ a, b $\in$ X

$\therefore *$ is a binary operation on X

Second Part

$a * b = a+b-ab$

$= b+a-ba$

$= b * a$

$\therefore *$ is commutative on X.

Again $(a * b) * c$

$= (a+b-ab) * c$

$= (a+b-ab) + c - (a+b-ab)c$

$= a+b-ab+c - ac-bc+abc$

$= a+b+c-ab-bc-ca+abc$

$a * (b * c) = a * (b+c-bc)$

$= a+(b+c-bc) - a(b+c-bc)$

$= a+b+c-ab-bc-ca+abc$

$\therefore (a * b) * c = a * (b * c)$

$\therefore *$ is associative.

2.3.3 Identity Element

Let S be a non-empty set equipped with a binary operation $*$. An element $e \in S$ is called an identity element for $*$ if

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

Note: Identity element for a binary operation if it exists, is unique.

Examples

1. Multiplication is a binary operation on IN. There exists $1 \in$ IN such that

$$a \ 1 = a = 1 \ a, \forall \ a \in \text{IN}$$

$\therefore$ 1 is the identity for multiplication in IN.

2. Addition is a binary operation on Z.

There exists $0 \in Z$ such that

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

$\therefore$ 0 is the identity for addition in Z.We say that 0 is the additive identity in Z.

3. Addition is a binary operation on IN. But there does not exist

identity element for addition in IN.

4. Matrix addition is a binary operation on M_{mxn}, the set of all m x n real matrices. The m x n null matrix 0 is the identity for matrix addition in M_{mxn}.

2.3.4 Inverse of an Element

Let S be a non-empty set equipped with a binary operation $*$, and with identity element e. An element $b \in S$ is called inverse of a under $*$ if

$$a * b = e = b * a$$

Note : 1. Inverse of an element under a binary operation, if it exists, is unique.

2. Generally inverse of a is denoted by a^{-1}. In case of real numbers, inverse of a under addition (i. e. additive inverse) is denoted by –a, whereas inverse of a ($a \neq 0$) under multiplication (i.e. multiplicative inverse) is denoted by $\frac{1}{a}$.

Examples

1. Multiplication is a binary operation on IN and $1 \in$ IN is the identity for multiplication. But no element of IN, except 1, possesses inverse under multiplication in IN.
2. Addition is a binary operation on Z and $0 \in Z$ is the identity for addition. For every $a \in Z$, there exists $-a \in Z$ such that $a+(-a) = 0=(-a) + a$.
   $\therefore$ –a is the inverse of a under addition.



CHECK YOUR PROGRESS

Q 1: Let A be a finite set having 4 elements. What is the number of binary operations on A?

Q 2: Is $*$ defined by $a * b = \frac{a}{b}$, a binary operation on IR ?

Q 3: Is multiplication a binary operation on {–1, 1, i, –i} ? where $i = \sqrt{-1}$.

Q 4: Let Q be the set of rational numbers. Show that $*$ defined by

$a * b = a + ab$, is a binary operation on Q.

Examine if $*$ is (i) commutative, (ii) associative.



2.4 LET US SUM UP

- A binary operation $*$ on a non-empty set S is a function from S x S to S.
- If S is a finite set having m elements, the number of binary operations on S is m^{m^2}.
- A binary operation $*$ on a non-empty set S is commutative if $a * b = b * a$, $\forall$ a, b$\in$S.
- A binary operation $*$ on a non-empty set S is associative if $(a * b) * c = a * (b * c)$, $\forall$ a, b, c $\in$ S
- An element e in a non-empty set S equipped with a binary operation $*$ is called an identity element for x if $a * e = a = e * a$, $\forall$ a $\in$ S.
- An element b in a non-empty set S equipped with a binary operation $*$ is called an inverse element of a $\in$ S if $a * b = e = b * a$.



2.5 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

Ans to Q No 1: $4^{4^2} = 4^{16}$

Ans to Q No 2: No.

Ans to Q No 3: Yes

Ans to Q No 4: Not commutative, not associative.



2.6 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.



2.7 MODEL QUESTION

Q 1: Let IR be the set of real numbers. Examine if the binary operation $*$ defined by $a * b = a+5b$; $a, b \in IR$ is (i) commutative, (ii) associative.

Q 2: Let S be a set having 3 elements. How many binary operations can be defined on S?

*** ***** ***

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∈ G such that

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

∴1 is the identity element.

(iv) Let z∈ 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∈ 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 ∈ Z

∴ a+b ∈ Z, ∀ a, b ∈ Z

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

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

(iii) We have 0∈ Z and a+0 = a = 0+a, ∀ a∈ 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 $a, b \in G$.

*** ***** ***

UNIT 4: SUBGROUP

UNIT STRUCTURE

4.1 Learning objectives

4.2 Introduction

4.3 Sub group

4.4 Cyclic Group

4.5 Let us Sum Up

4.6 Answers to Check Your Progress

4.7 Further Readings

4.8 Model Questions

4.1 LEARNING OBJECTIVES

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

- subgroups
- cyclic groups

4.2 INTRODUCTION

In unit 3,we discussed the concept of group and its properties.In this unit,we will discuss subgroup and its properties.In this unit, We will also discuss cyclic group.

4.3 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;

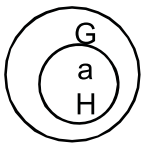
(ii) the inverse of any element of H is the same as the inverse of the element of G.

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

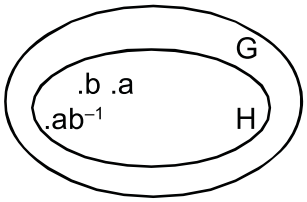
$\therefore$ $ab^{-1} \in$ H

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 $a \in K$

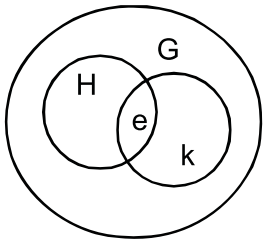
$b \in H \cap K \Rightarrow b \in H$ and $b \in K$

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 $2Z \cup 3Z$.

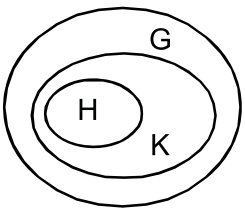
$\therefore 2Z \cup 3Z$ cannot be a group.

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 1

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.

$mZ = \{0, \pm m, \pm 2m, \pm 3m, ...\}$ 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.

4.4 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 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

●	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Table 4.1

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 2

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



4.5 LET US SUM UP

- 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



4.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

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 – 2

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



4.7 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.



4.8 MODEL QUESTION

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

Q 2: Show that a group of order 4 is always Abelian.

Q 3: 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 $a, b \in G$.

*** ***** ***

UNIT 5 : GROUP OF PERMUTATIONS

UNIT STRUCTURE

5.1 Learning Objectives

5.2 Introduction

5.3 Definition of Permutation, Examples

5.4 Multiplication of Permutation

5.5 Different Kinds of Permutation

5.6 Permutation Group

5.7 Let Us Sum Up

5.8 Answers To Check Your Progress

5.9 Further Readings

5.10 Model Questions

5.1 LEARNING OBJECTIVES

After going through this unit, you will able to know -

- permutation and its examples
- multiplication of permutations
- different kinds of permutation
- permutation group

5.2 INTRODUCTION

The word permutation is used in two different ways. Firstly, it is an ordered arrangement of the elements of a finite set of distinct elements. Secondly, a permutation is a one-one and onto mapping from a non-empty set to itself. In Group theory, permutation is taken as a one-one and onto mapping from a non-empty set to itself. In this unit, we will define a permutation, give examples and obtain the number of permutations from a finite set to itself. We will prove that the collection of permutations on a finite set is a group under multiplication of permutations. This group is called permutation group (or symmetric group).

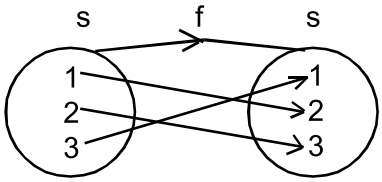
5.3 DEFINITION OF PERMUTATION, EXAMPLES

A bijective mapping (i.e. a one-one and onto mapping) from a non-empty set to itself is called a permutation on the set.

Example 1 : Let us consider the set S = {1, 2, 3}. Let f ; S $\rightarrow$ S be a mapping such that f(1) = 2, f(2) = 3, f(3) = 1

Clearly, f is a one-one and onto mapping from S to itself.

$\therefore$ f is a permutation on S.



Notation for permutation

Let us consider the permutation given above.

S = {1, 2, 3}

f : S $\rightarrow$ S, f(1) = 2, f(2) = 3, f(3) = 1

The above permutation is, generally, written as

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

We write the elements of the set S in the first row. In the second row, we write their respective images. The image of 1 under f is 2. We write 2 just below 1. Similarly the image of 2 is 3. We write 3 just below 2. Similarly, we write 1 just below 3. In this way, a permutation is written.

Number of permutations on S = {1, 2, 3}.

Here S has 3 distinct elements.

Now 1 can be associated in 3 ways. It can be associated with 1 or with 2 or with 3.

2 can be associated in 2 ways.

3 can be associated in 1 way.

$\therefore$ the number of permutations = $3 \times 2 \times 1 = 3!$

Number of permutations on a finite set having n elements

Let us consider a set S having n distinct elements.

The first element can be associated in a ways.

The second element can be associated in (n-1) ways.

The third element can be associated in (n-2) ways.

In this way (n-1)th element can be associated in 2 ways, and the nth element can be associated in 1 way.

$\therefore$ the number of permutations

= n(n-1)(n-2) . . . . . 2.1 = n!

Example 2 : Let S = {1, 2}. Write down all the permutations on S.

Solution : The number of elements of S is 2.

$\therefore$ there are 2!, i.e. 2 permutations on S. They are

$$i = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \qquad f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Note : The permutation i is called the identity permutation. Here the image of 1 is 1, the image of 2 is 2.

Example 3 : Let S = {1, 2, 3}. Write down all the permutations on S.

Solution : The number of elements of S is 3.

$\therefore$ there are 3!, i.e. 6 permutations on S.

They are

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Note : In this case $i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

is the identity permutation.

Identity permutation

Let S = {a_1, a_2, ..., a_n} where all the a_i's are distinct.

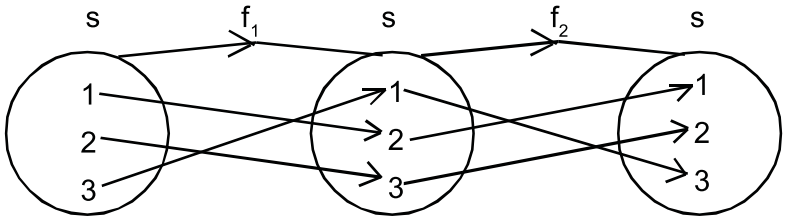
The identity permutation i on S is defined by

$$i = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ a_1 & a_2 & a_3 .....a_n \end{pmatrix}$$

5.4 MULTIPLICATION OF PERMUTATION

Let S = {1, 2, 3}. Let us consider the following two permutations on S

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



Then we get the composite mapping

$f_2of_1 : S \to S$, such that

$(f_2of_1)(1) = f_2(f_1(1)) = f_2(2) = 1$

$(f_2of_1)(2) = f_2(f_1(2)) = f_2(3) = 2$

$(f_2of_1)(3) = f_2(f_1(3)) = f_2(1) = 3$

Clearly, f_2of_1 is a permulation on S, and $f_2of_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Similarly f_1of_2 is also a permutation on S.

The product f_2f_1 of permutations is defined by the composite mapping f_2of_1. Thus

$$f_2 f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Note : 1. We know that the composite mapping of two one-one and onto functions is also a one-one and onto function. Therefore, the product of two permutations is always a permutation.

2. We know that the composition of mappings is associative. Therefore, the multiplication of permutations is associative.

3. We know that the composition of mappings is not, in general, commutative. Therefore, the multiplication of permutations is not, in general, commutative.

Let $$f = \begin{pmatrix} a_1 & a_2 & a_3 & .....a_n \\ f(a_1) & f(a_2) & f(a_3).....f(a_n) \end{pmatrix}$$

$$g = \begin{pmatrix} a_1 & a_2 & a_3 & .....a_n \\ g(a_1) & g(a_2) & g(a_3).....g(a_n) \end{pmatrix}$$

be two permutations on S.

Then $$fg = \begin{pmatrix} a_1 & a_2 & a_3 & ..... a_n \\ f(g(a_1)) & f(g(a_2)) & f(g(a_3)).....f(g(a_n)) \end{pmatrix}$$

Similarly

$$gf = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots\ldots\ldots\ldots & a_n \\ g(f(a_1)) & g(f(a_2)) & g(f(a_3)) & \ldots\ldots & g(f(a_n)) \end{pmatrix}$$

Example 4 : Let S ={1, 2, 3, 4}. Consider the following permutations f and g on S.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},\ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

Find fg and gf

Solution : $fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(g(1) & f(g(2) & f(g(3) & f(g(4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(4) & f(2) & f(1) & f(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ g(f(1) & g(f(2) & g(f(3) & g(f(4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ g(2) & g(3) & g(4) & g(1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Clearly fg $\neq$ gf [Recall the definition of equality of two functions.]

Example 5 : Let S= {1, 2, 3, 4}. Consider the following permutations on S.

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},\ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Find $\phi\psi$ and $\psi\phi$

Solution : $\phi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\psi\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

In this case $\phi\psi = \psi\phi$

Example 6: Let S = {1, 2, 3, 4}. Consider the following permutations on S.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},\ h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Find fh and hf

Solution : $fh = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = i$$

$$hf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = i$$

Here fh = hf = i

Note : In the above example fh=hf = i, the identity permutation f is called the inverse of h, and vice versa, h is the inverse of f. We write $f = h^{-1}$ or $h = f^{-1}$

Inverse of a permutation

Let S = {a_1, a_2, ... , a_n} where the a_i's are distinct.

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 & ..... & a_n \\ f(a_1) & f(a_2) & f(a_3) ..... & & f(a_n) \end{pmatrix}$ be a permutation on f.

Then the inverse of f, denoted by f^{-1}, is given by

$$f^{-1} = \begin{pmatrix} f(a_1) & f(a_2) & f(a_2) ..... & f(a_n) \\ a_1 & a_2 & a_3 & ..... & a_n \end{pmatrix}$$

We note that $ff^{-1} = f^{-1}f = i$



CHECK YOUR PROGRESS

Q 1: Let S = {a_1, a_2, a_3}, where all the a_i's are distinct. How many permutations are there on S? Write down all the permutations on S.

Q 2: Let S = {1, 2, 3, 4}. How many permutations are there on S ? Write down any five permutations on S.

Q 3: Let S = {1, 2, 3, 4, 5}. Consider the following permutations on S.

$$f=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix},\quad g=\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}$$

$$\phi=\begin{pmatrix}1&2&3&4&5\\1&2&5&4&3\end{pmatrix},\quad \psi=\begin{pmatrix}1&2&3&4&5\\5&3&4&2&1\end{pmatrix}$$

(i) Find $fg,\ f\phi,\ f\psi,\ g\psi$

(ii) Find $g\phi,\ \phi g$. Are they equal ?

(iii) Find $\phi\psi,\ \psi\phi$. Are they equal?

Q 4: Let S = {1, 2, 3, 4, 5, 6, 7}. Write down the inverse of each of the following permutations on S.

(i) $f=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&4&5&6&7&1\end{pmatrix}$

(ii) $g=\begin{pmatrix}1&2&3&4&5&6&7\\7&6&5&4&3&2&1\end{pmatrix}$

(iii) $h=\begin{pmatrix}1&2&3&4&5&6&7\\3&4&5&6&7&2&1\end{pmatrix}$

5.5 DIFFERENT KINDS OF PERMUTATION

Cyclic Permutation

Let S be a finite set. Let f be a permutation on S. f is called a cyclic permutation if there exist elements a_1, a_2, a_3, ..., a_{n-1}, a_n in S such that $f(a_1) = a_2$, $f(a_2) = a_3$, $f(a_3)=a_4$, ..., $f(a_{n-1}) = a_n$, $f(a_n) = a_1$, and all other elements, if any, remain fixed under f, i.e., f(a) = a, for all other $a \in S$.

In this case we denote f by (a_1, a_2, a_3 . . . . a_n).

f is called a cyclic permutation of length n.

Note : A cyclic permutation is also called a cycle. A cyclic permutation of length n is called an n-cycle.

Transposition

A cyclic permutation of length 2 is called a transposition.

Example 7: Let S ={1, 2, 3}

Let $f=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ be a permutation on S.

Here f(1) = 2, f(2) = 3, f(3) = 1

$1\to 2\to 3\to 1$

Thus, $f=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=(1 \quad 2 \quad 3)$

f is a cyclic permutation of length 3 or a 3-cycle.

Example 8 : Let S = {1, 2, 3, 4, 5}. Let

$f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 2 & 5\end{pmatrix}$ be a permutation on S.

Here f(2) = 3, f(3) = 4, f(4) = 2

$2\to 3\to 4\to 2$

And f(1) = 1, f(5) = 5

i.e, 1, 5 remain fixed under f, i.e. f(1) = 1, f(5) = 5

Thus, $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 2 & 5\end{pmatrix}=(2 \quad 3 \quad 4)$

f is a cyclic permutation of length 3 or a 3-cycle.

Example 9 : Let S = {1, 2, 3, 4}. Let

$f=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{pmatrix}$ be a permutation on S

Here f(2) = 3, f(3) = 2

$2\to 3\to 2$

And f(1) = 1, f(4) = 4

Thus, $f=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{pmatrix}=(2 \quad 3)$

f is a cyclic permutation of length 2, i.e. f is a transposition.

Note : Let S = {1, 2, 3}

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) \qquad (1)$$

is a cyclic permutation on S = (1, 2, 3}.

Now, we consider

S = {1, 2, 3, 4, 5}

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1 \quad 2 \quad 3) \qquad (2)$$

is a cyclic permutation on S = {1, 2, 3, 4, 5}.

We note that (1) and (2) are different permutations. In (2), (1 2 3) means the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

Cycles of a permutations

Let S = {1, 2, 3}

Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3)$

be a permutation of S = {1, 2, 3}

Now $(1 \quad 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $(1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$$(1 \quad 3)(1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3)$$

Thus, we see that

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) = (1 \quad 3)(1 \quad 2)$$

Again, we consider S = {1, 2, 3, 4, 5}

Let $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4 \quad 5)$

be a permutation on S = {1, 2, 3, 4, 5}

Now, it can be shown that

$g = (1 \quad 2 \quad 3 \quad 4 \quad 5)$

$= (1 \quad 5)(1 \quad 4)(1 \quad 3)(1 \quad 2)$

Again, we consider S = {1, 2, 3, 4, 5, 6}

Let $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}$

be a permutation on S = {1, 2, 3, 4, 5, 6}

Now h can be expressed as

$h = (1 \quad 2 \quad 3)(4 \quad 5 \quad 6)$

Here $(1 \quad 2 \quad 3), (4 \quad 5 \quad 6)$ are called the cycles of the permutation h. Here $(1 \quad 2 \quad 3)$ and $(4 \quad 5 \quad 6)$ have no common elements. They are called disjoint cycles.

Disjoint Permutations

Let S = {1, 2, 3, 4, 5, 6}

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$

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

and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}$

$= (4 \quad 5 \quad 6)$

be two permutations on S = {1, 2, 3, 4, 5, 6}

We note that $(1, \quad 2, \quad 3)$, and $(4, \quad 5, \quad 6)$ have no common elements. In this case, the permutations f, and g are said to be disjoint.

Again, consider the permutations

$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4)$

$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix} = (3 \quad 4 \quad 5 \quad 6)$

on S = {1, 2, 3, 4, 5, 6}

Here $(1 \quad 2 \quad 3 \quad 4)$ and $(3 \quad 4 \quad 5 \quad 6)$ have common elements. So, the permutations ϕ and ψ are not disjoint.

Thus, we define disjoint permutations as follows.

Two permutations f and g on a finite set S are said to be disjoint if

(i) $f(a) \neq a \Rightarrow g(a) = a$, for any $a \in S$.

and (ii) $g(a) \neq a \Rightarrow f(a) = a$, for any $a \in S$.

It can be proved that multiplication of two disjoint cycles, as well as of two disjoint permutations is commutative.

Even and odd permutations

Let S = {1, 2, 3}

$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ is a permutation on S = {1, 2, 3}

Again $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) = (1 \quad 3) = (1 \quad 2)$

Again, consider the set S = {1, 2, 3, 4}

Let $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ be a permutation on S = {1, 2, 3, 4}

Now $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4) = (1 \quad 4)(1 \quad 3)(1 \quad 2)$

Thus, we see that f has been expressed as the product of even number of transpositions (two), whereas g has been expressed as the product of odd number of transpositions (three).

If a permutation can be expressed as the product of even number of transpositions, then it is said to be even. On the other hand, if a permutation can be expressed as the product of odd number of transpositions, then it is said to be odd.

The permutation f, given above, is even, whereas the permutation g is odd.

We note the following results without proof.

1. The product of two even permutations is an even permutation.
2. The product of two odd permutation is an even permutation.
3. The product of an even permutation and an odd permutation is an odd permutation.
4. Identity permutation is an even permutation.
5. The inverse of an even permutation is even.
6. The inverse of an odd permutation is odd.



CHECK YOUR PROGRESS

Q 5: Write down all the permutations on the set S = {1, 2, 3}, and pick out the even permutations and the odd permutations.

Q 6: Let S = {1, 2, 3, 4, 5, 6}. Determine whether the following permutations on S are even or odd.

(i) $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix}$

(ii) $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix}$

(iii) $f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

(iv) $f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix}$

(v) $f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 3 & 6 \end{pmatrix}$

Number of even permutations and odd permutations on S = {1, 2, 3, . . . , n}, $n \geq 2$

Let S = {1, 2, 3, ..., n}

Let S_n be the set of all permutations on S. Then number of elements of S_n is n!. Of these n! permutations, some are even and some are odd.

Let the number of even permutations be m, and the number of odd permutations be k.

Clearly, m+k = n!

Let the even permutations be $e_1, e_2, \ldots, e_m$; where the e_i's are distinct.

Let f be any transposition

Then $fe_1, fe_2, \ldots, fe_m$ are odd permutations, and are distinct, for if $fe_i = fe_j$, then $e_i = e_j$, which is a contradiction.

Since the number of odd permutations is k,

$\therefore\ m \leq k$

Interchanging the roles of m, k, we get

$k \le m$

$\therefore \ m = k$

$\because \ m + k = n!, \quad \therefore \ m = k = \frac{n!}{2}$

$\therefore$ Number of even permutations on $S = \frac{n!}{2}$, and number of odd permutations on $S = \frac{n!}{2}$, where S = {1, 2, 3, ..., n}, $m \ge 2$.

5.6 PERMUTATION GROUP

Let S = {1, 2, 3, 4, ... , n}, and let S_n be the set of all permutations on S.

(i) Let $f, g \in S_n$.

We know that the product fg is defined by the composite mapping fog.

Also we know that the composite mapping of two one-one and onto function is also one-one and onto.

Therefore, the product of two permutations is always a permutation .

$\therefore \ fg \in S_n$

(ii) We know that the composition of mappings is associative. Therefore, the multiplication of permutations is associative.

(iii) The identity permutation

$$i = \begin{pmatrix} 1 & 2 & 3 & ..... & n \\ 1 & 2 & 3 & ..... & n \end{pmatrix} \in S_n$$

Also if = f = fi, $\forall f \in S_n$

i is the identity element of S_n.

(iv) Let $f = \begin{pmatrix} 1 & 2 & 3 & ..... & n \\ f(1) & f(2) & f(3) & ..... & f(n) \end{pmatrix} \in S_n$

Now $g = \begin{pmatrix} f(1) & f(2) & f(3) & ..... & f(n) \\ 1 & 2 & 3 & ..... & n \end{pmatrix} \in S_n$

and fg = i = gf

g is the inverse of f.

We denote g by f^{-1}

i.e., $ff^{-1} = i = f^{-1}f$.

Thus S_n is a group under multiplication of permutations, called the permutation group (or symmetric group) of degree n.

Note : 1) The group S_n is not Abelian, since in general, non commutative.

2) The number of elements of S_n is n!, i.e, the order of S_n is n! .

Example 10 : Let S = {1, 2, 3}. Let S_3 be the set of all permutations on S. Show that S_3 is a group under product of permutations. Is the group Abelian?

Solution : Let $S_n = \{i, f_1, f_2, f_3, f_4, f_5\}$, where

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3)$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \quad 3 \quad 2), \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \quad 3)$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \quad 3), \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \quad 2)$$

We construct the operation table as follows :

	i	f_1	f_2	f_3	f_4	f_5
i	i	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	i	f_5	f_3	f_4
f_2	f_2	i	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	i	f_1	f_2
f_4	f_4	f_5	f_3	f_2	i	f_1
f_5	f_5	f_3	f_4	f_1	f_2	i

(i) From the table we see that S_3 is closed under multiplication of permutations.

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

(iii) The identity permutations $i \in S_3$, and if = f = fi, $\forall f \in S_3$

(iv) Every element of S_3 possesses inverse in S_3.

The inverse of i is i.

The inverse of f_1 is f_2.

The inverse of f_2 is f_1.

The inverse of f_3 is f_3.

The inverse of f_4 is f_4.

The inverse of f_5 is f_5.

Thus, S_3 is a group under multiplication of permutations.

2nd Part : The group S_3 is not Abelian.

$$f_2 f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4$$

$$f_3 f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_5$$

$\therefore \; f_2 f_3 \neq f_3 f_2$

Alternating Group

Let S = {1, 2, 3, ..., n}

Let A_n be the set of all even permutation on S. Then A_n is a group under multiplication of permutations, called the **alternating group** of degree n.

Number of elements of A_n is $\frac{n!}{2}$,i.e order of A_n is $\frac{n!}{2}$.

Clearly A_n is a subgroup of S_n.

Example 11 : Let S = {1, 2, 3}. Let A_3 be the set of all even permutations on S. Show that A_3 is a group under multiplication of permutations. Is the group Abelian ?

Solution : Let S = {1, 2, 3}.

Let A_3 be the set of all even permutations.

Let $A_3 = \{i, f_1, f_2\}$, where

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \;\; 3 \;\; 2) = (1 \;\; 3)(1 \;\; 2)$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \;\; 3 \;\; 2) = (1 \;\; 2)(1 \;\; 3)$$

i, f_1, f_2 are even permutations.

We construct the operation table as follows.

(i) From the table, we see that A_3, is closed under multiplication of

permutations.

(ii) We know that multiplications of permutations is associative.

(iii) The identity permutation $i \in A_3$, and if = f = fi, $\forall f \in A_3$

(iv) Every element of A_3 possesses inverse in A_3.

Th inverse of i is i.

The inverse of f_1 is f_2.

The inverse of f_2 is f_1.

Thus, A_3 is a group under multiplication of permutations.

2nd Part : From the table we see that multiplication is commutative.

$\therefore$ A_3 is an Abelian group

Note : We have seen that S_3 is a non-Abelian group, whereas A_3 is an Abelian group.

Moreover, A_3 is a subgroup of S_3.

Thus, we can conclude that a non-Abelian group can have an Abelian subgroup.

CHECK YOUR PROGRESS



Q 7: Let S = {1, 2, 3, ..., n}. Is the set of all odd permutations on S a group? Justify.

Q 8: Let S = {1, 2, 3, 4}

Let V = {1, f_1, f_2, f_3}, where

$$i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Show that V is group under multiplication of permutations. Is the group Abelion ?

Q 9: Give an example of a finite non-Abelian group.



5.7 LET US SUM UP

- A bijiective mapping (i. e., a one-one and onto mapping) from a non-empty set to itself is called a permutation on the set.
- The number of permutations on a finite set S having n elements is n!.
- Let S be a finite set. Let f be a permutation on S. f is said to be a cyclic permutation of length n if there exist elements $a_1, a_2, a_3, \ldots . a_{n-1}, a_n$ in S such that $f(a_1) = a_2$, $f(a_2) = a_3$, ..., $f(a_{n-1}) = a_n$, $f(a_n) = a_1$, and all other elements, if any, remain fixed under f, i.e., f(a) = a, for all $a \in S$. In this case f is denoted by $(a_1\ a_2\ a_3 \ldots . a_n)$.
- A cyclic permutation of length 2 is called a transposition.
- If a permutation can be expressed as the product of even number of transpositions, then it is said to be even.
- If a permutation can be expressed as the product of odd number of transpositions, then it is said to be odd.
- Let S = {1, 2, 3, ..., n}, and let S_n be the set of all permutations on S. S_n is a group under multiplications of permutations called the permutation group (or symmetric group) of degree n, and of order n!. If A_n is the set of all even permutations on S, then A_n is a group under multiplications of permutations, called the alternating group of degree and of order $\frac{n!}{2}$.



5.8 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Here S = $(a_1, a_2, a_3\}$, where all the a_i1s are distinct.

$\therefore$ there are 3!, i.e., $3 \times 2 \times 1$, i.e. 6 permutations on S. These are

$$i = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix}, f_1 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}$$

$$f_2 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \end{pmatrix}, f_3 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix}, f_5 = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}$$

Ans to Q No 2: S = {1, 2, 3, 4}

The number of permutations on S is 4!, i.e., $4 \times 3 \times 2 \times 1$, i.e., 24.

Any five permutations on S :

$$i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Ans to Q No 3: (i) $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

$$f\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$f\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$$

$$g\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$$

(ii) $g\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

$$\phi g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

Clearly $g\phi = \phi g$

(iii) $\phi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

$\psi\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$$

Clearly $\phi\psi \neq \psi\phi$

Ans to Q No 4: (i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$

$\therefore f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

$\therefore g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}$

$\therefore h^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

Ans to Q No 5: Here S = {1, 2, 3}

The permutations on S are

$i\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) = (1 \quad 3)(1 \quad 2)$

$f_2\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \quad 3 \quad 2) = (1 \quad 2)(1 \quad 3)$

$f_3\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \quad 3)$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \quad 3)$$

$$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \end{pmatrix} 3 = (1 \quad 2)$$

Even permutations : i, f_1, f_2

Odd permutations : f_3, f_4, f_5.

Ans to Q No 6: S = {1, 2, 3, 4, 5, 6}

(i) $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix}$

$$= (1 \quad 3 \quad 4 \quad 5 \quad 6) = (1 \quad 6)(1 \quad 5)(1 \quad 4)(1 \quad 3)$$

$\therefore$ f_1 is an even permutations.

(ii) $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix}$

$$= (1 \quad 2 \quad 3 \quad 5)(4 \quad 6)$$

$$= (1 \quad 5)(1 \quad 3)(1 \quad 2)(4 \quad 6)$$

$\therefore$ f_2 is an even permutation.

(iii) $f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

$$= (1 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2)$$

$$= (1 \quad 2)(1 \quad 3)(1 \quad 4)(1 \quad 5)(1 \quad 6)$$

$\therefore$ f_3 is an odd permutation.

(iv) $f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix}$

$$= (3 \quad 4 \quad 5 \quad 6) = (3 \quad 6)(3 \quad 5)(3 \quad 4)$$

$\therefore$ f_4 is an odd permutation.

(v) $f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 3 & 6 \end{pmatrix}$

$$= (2 \quad 5 \quad 3 \quad 4) = (2 \quad 4)(2 \quad 3)(2 \quad 5)$$

$\therefore$ f_5 is an odd permutation.

Ans to Q No 7: Here S = {1, 2, 3, ..., n}

Let O_n be the set of odd permutations on S.

Let f. g $\in O_n$

We know that the product of two odd permutations is an even permutation.

$\therefore fg \notin O_n$

$\therefore$ O_n cannot be a group.

Ans to Q No 8: Here S = {1, 2, 3, 4}

V = {i, f_1, f_2, f_3}, where

$i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

(i) From the table we see that V is closed under multiplication of permutations.

(ii) We know that multiplications of permutations is associative.

(iii) We have $i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in V$

and if = f = f_1, $\forall f \in V$.

$\therefore$ i is the identity

(iv) Every element of V has inverse in V.

i is the inverse of i.

f_1 is the inverse of f_1.

f_2 is the inverse of f_2.

f_3 is the inverse of f_3.

[Here every element is its own inverse]

$\therefore$ V is a group under multiplication of permutations.

2nd Part: From the table we see that multiplication is commutative.

$\therefore$ V is an Abelian group

Ans to Q No 9: Let S = {1, 2, 3}

Let S_3 be the set of all permutations on S. Then S_3 is a group under multiplication of permutations.

Clearly S_3 is a finite group of order 3! i.e. 6.

S_3 is not an Abelian group.



5.9 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.



5.10 MODEL QUESTIONS

Q 1: Let S = {1, 2, 3}. Show that the set S_2 of all permutations on S is an Abelian group under multiplication of permutations.

Q 2: Let S = {1, 2, 3, 4, 5, 6, 7, 8}.
Express the following permutations on S as product of trenspositions.

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 2 & 4 & 3 & 1 & 7 & 8 \end{pmatrix}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$

Q 3: Let S = {1, 2, 3, 4}
Let V = {1, f_1, f_2, f_3}, where

$$i = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad f_1 = (1 \quad 2)(3 \quad 4)$$

$$f_2 = (1 \quad 3)(2 \quad 4), \quad f_3 = (1 \quad 4)(2 \quad 3)$$

are permutations on V.
Examine if V is an Abelian group under multiplication of permutations.

Q 4: Prove that the set S_n of all permutations on S = {1, 2, 3, 4, ..., n} is a group under multiplication of permutations.

*** ***** ***

UNIT 6: COSETS

UNIT STRUCTURE

6.1 Learning objectives

6.2 Introduction

6.3 Coset

6.4 Lagrange's Subgroup order theorem

6.5 Let us Sum Up

6.6 Answers to Check Your Progress

6.7 Further Reading

6.8 Model Questions

6.1 LEARNING OBJECTIVES

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

- cosets of a subgroup
- Lagrange's subgroup order theorem

6.2 INTRODUCTION

We have already discussed group ,subgroup and their properties in unit 3 and unit 4.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.

6.3 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 $2Z = \{0, \pm 2, \pm 4, \pm 6, ...\} \leq Z$

We have

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

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

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

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

$\Rightarrow ae \in H$ [$\because$ 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, $x \in aH \quad \Rightarrow x \in H$

$\therefore aH \subseteq H$ ...(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, $y \in H \Rightarrow y \in aH$

$\therefore H \subseteq aH$ ...(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 $h_3 \in H$

$= bh_2h_1^{-1}h_3$

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

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

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

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

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

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

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

6.4 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

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

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



6.5 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.



6.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

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



6.7 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.



6.8 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 $[G : H] = \frac{o(G)}{o(H)}$.

*** ***** ***

UNIT 7: NORMAL SUBGROUP& QUOTIENT GROUP

UNIT STRUCTURE

7.1 Learning objectives

7.2 Introduction

7.3 Normal Subgroup

7.4 Quotient Group

7.5 Let us Sum Up

7.6 Answers to Check Your Progress

7.7 Further Readings

7.8 Model Questions

7.1 LEARNING OBJECTIVES

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

- normal subgroups
- quotient groups.

7.2 INTRODUCTION

We have already discussed group ,subgroup and their properties in unit 3 and unit 4.In this unit,we will discuss normal subgroup of a group.In this unit,we will also discuss quotient group.

7.3 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 $a \in G$

$\therefore H \Delta G$.

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.

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

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

$= b^{-1}h_1d$

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

$= h_2h_1 \in H$

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

$\Rightarrow abH = cdH$

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)]

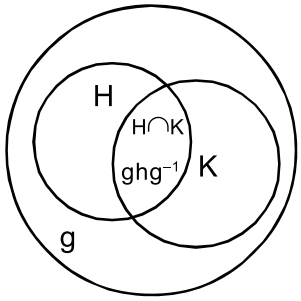
$= (aH)((bc)H)$

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

$\therefore$ 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 $xH = a^m H$

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

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

$= (aH)^m$

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

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



CHECK YOUR PROGRESS

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, ω , ω^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 $Z/3Z$.



7.5 LET US SUM UP

- 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).



7.6 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS

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.



7.7 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.



7.8 MODEL QUESTIONS

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.

*** ***** ***

UNIT 8 : HOMOMORPHISM OF GROUPS

UNIT STRUCTURE

8.1 Learning Objectives
8.2 Introduction
8.3 Homomorphism of Groups : Definition and examples
8.4 Types of Homomorphism
8.5 Properties of Homomorphism
8.6 Let Us Sum Up
8.7 Answers To Check Your Progress
8.8 Further Readings
8.9 Model Questions

8.1 LEARNING OBJECTIVES

After going through this unit, you will able to know-

- the concept of homomorphism of groups
- different types of homomorphism
- properties of homomorphism, and related theorems.

8.2 INTRODUCTION

The word homomorphism has been derived from two Greek words homos (meaning 'same') and morphe (meaning 'form' or 'shape'). Thus, homomorphism means 'of the same form or shape'.

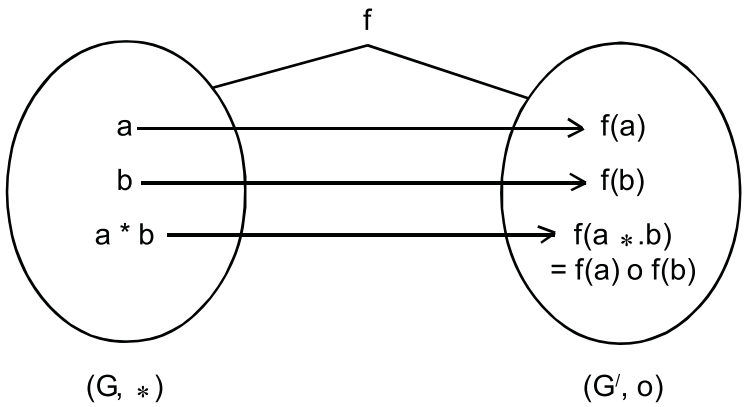
A homomorphism is a structure-preserving mapping between two algebraic structures. Thus, a group homomorphism is a homomorphism that preserves the group structure.

8.3 HOMOMORPHISM OF GROUPS

Definition : Let G be a group under the binary operation '$*$' and G' be a group under the binary operation 'o'.

Let $f : G \to G'$ be a mapping. f is said to be a homomorphism if

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



Note : 1. Here a is related to f(a), b is related f(b). Moreover, $a * b$ is related to f(a) o f(b). Thus, the mapping f not only relates two elements of G with two unique elements of G/, but also relates $a * b$ to f(a) of (b) in G/. Thus, the mapping f preserves the algebraic structure of the systems.

2. In our subsequent discussions, we will drop the symbols for binary operations. Simply we will write f(ab) = f(a) f(b).

It should be borne in mind that the binary operations in the two groups are not necessarily the same.

Example 1: Let $\underline{\underline{Z}}$ be the additive group of integers. We define a mapping

$$f : \underline{\underline{Z}} \to \underline{\underline{Z}},\ \ f(x) = -x, \forall x \in \underline{\underline{Z}}$$

Let $a,\ b \in \underline{\underline{Z}}$

Now f(a+b) = –(a+b), by definition of f

= – a – b

= (–a) + (–b)

= f(a) + f(b)

$\therefore$ f is a homomorphism.

Note : In the above example the binary operation is "+". Moreover, both the groups are the same with same binary operation.

Example 2 : Let R be the additive group of real numbers, and R_+ be the multiplicative group of positive real numbers. We define

f: $R \to R_+$, $f(x) = e^x$

We are to examine whether f is a homomorphism or not. Now, the

binary operation in R is " + ", and the binary operation in R_+ is " . ". So, we are to examine if f(a+b) = f(a) f(b), $\forall\ a, b \in R$

Now f(a+b) = e^{a+b}, by definition of f

= $e^a e^b$

= f(a) f(b)

$\therefore$ f is a homomorphism.

Example 3: Let $\underline{\underline{Z}}$ be the additive group of integers. We define

$f : \underline{\underline{Z}} \to \underline{\underline{Z}},\ \ f(x) = x + 5$

Let $a,\ b \in \underline{\underline{Z}}$

Now f(a+b) = (a+b) + 5

f(a) + f(b) = (a+5) + (b+5)

= (a+b) +10

$\therefore$ f(a+b) $\neq$ f(a) + f(b)

$\therefore$ f is not a homomorphism.

Example 4: Let $\underline{\underline{Z}}$ be the additive group of integers. Let G = {–1, 1} be the multiplicative group. We define

$$f(x) = \begin{cases} 1, & if\ x\ is\ even \\ -1, & if\ x\ is odd \end{cases}$$

Let $a,\ b \in \underline{\underline{Z}}$

Case I: Let a be even, b be even.

$\therefore$ f(a) = 1, f(b) = 1

Also, a + b is even

$\therefore$ f (a + b) = 1

= 1 x 1

= f(a) f(b)

Case 2: Let a be odd, b be odd

$\therefore$ f(a) = –1, f(b) = –1

$\therefore$ a, b are odd, $\therefore$ a + b is even

$\therefore$ f (a + b) = 1

= (–1) x (–1)

= f(a) f(b)

Case 3: Let a be even, be be odd $\therefore$ a + b is odd.

$\therefore$ f(a) = 1, f(b) = –1

$\because$ a is even and b is odd, $\therefore$ a + b is odd

$\therefore$ f(a + b) = –1

= 1 x (–1)

= f(a) f(b)

Similarly, if a is odd, and b is even, then f(a + b) = f(a) f(b)

Thus, in all the cases

f(a + b) = f(a) f(b)

$\therefore$ f is a homomorphism.

Example 5: Let G be a group, and e be the identity of G. We define

$f : G \to G$ such that f(x) = e, $\forall\ x \in G$

Let $a,\ b \in G$

$\therefore\ ab \in G$

Now f(a) = e, f(b) = e

Also f(ab) = e

= e e ($\because$ e is the identity)

= f(a) f(b)

$\therefore$ f is a homomorphism



CHECK YOUR PROGRESS

Q 1: Let $\underline{\underline{Z}}$ be the additive group of integers.

Define $f : \underline{\underline{Z}} \to \underline{\underline{Z}},\ f(x) = 5x$

Examine if f is a homomorphism.

Q 2: Let $\underline{\underline{Z}}$ be the additive group of integers.

Define $f : \underline{\underline{Z}} \to \underline{\underline{Z}},\ f(x) = x + 3$

Examine if f is a homomorphism.

Q 3: Let $\underline{\underline{R}}_+$ be the multiplicative group of positive reals. Define

$f : \underline{\underline{R}}_+ \to \underline{\underline{R}}_+,\ f(x) = \frac{1}{x}$

Examine if f is a homomorphism.

Q 4: Let $\underline{\underline{R}}_+$ be the multiplicative group of positive real numbers,

and $\underline{\underline{R}}$ be the additive group of real numbers. Define

$f : \underline{\underline{R}}_+ \to \underline{\underline{R}}$, $f(x) = \log_e x$

Examine if f is a homomorphism.

Q 5: Let S = {1, 2, 3}, and let S_3 be the group of all permutations of S. Let G = {–1, 1} be the multiplicative group. Define

$$f(\alpha)\begin{cases} = 1, \text{ if } \alpha \text{ is an even permutation} \\ = -1, \text{ if } \alpha \text{ is an odd permutation} \end{cases}$$

Examine if f is a homomorphism.

8.4 TYPES OF HOMOMERPHISM

Let f : G $\to$ G/ be a homomorphism from a group G to a group G/.

1. A homomorphism f is said to be a monomorphism if f is one-one (i.e. if f is injective).
2. A homomorphism f is said to be an epimorphism if f is onto (i.e. if f is surjective).
3. A homomorphism from a group to itself is called an endomorphism.
4. A homomorphism f is said to be an isomorphism if f is one-one and onto (i.e. if f is bijective).

   The word 'isomorphism' has also been derived from two Greek words "isos" (meaning "equal"). If there exists an isomorphism between two groups, they can be called "abstractly identical". They can be treated as one group, and not as two different groups.
5. An isomorphism from a group to itself is called an automorphism

Example 6: Let $\underline{\underline{Z}}$ be the additive group of integers. We define a mapping

f : $\underline{\underline{Z}} \to \underline{\underline{Z}}$, f(x) = – x, $\forall\ x \in \underline{\underline{Z}}$

(i) We have proved that f is a homomorphism (Example 1)

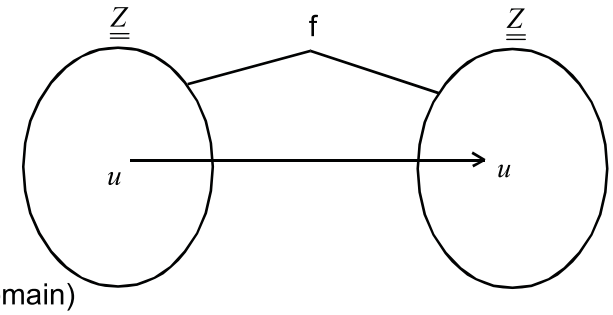
(ii) Let $a, b \in \underline{\underline{Z}}$

f(a) = f(b)

$\Rightarrow$ –a = – b

$\Rightarrow$ a = b

$\therefore$ f is one-one



(iii) Let $u \in \underline{\underline{Z}}$ (codomain)

Then there exists

$-u \in \underline{\underline{Z}}$ (domain) such that

$f(-u) = -(-u) = u$

$\therefore$ f is onto.

Thus, f is a homomorphism, f is one-one, and f is onto.

$\therefore$ f is an isomorphism. Moreover, f is an automorphism, for f is an isomorphism from $\underline{\underline{Z}}$ to itself.

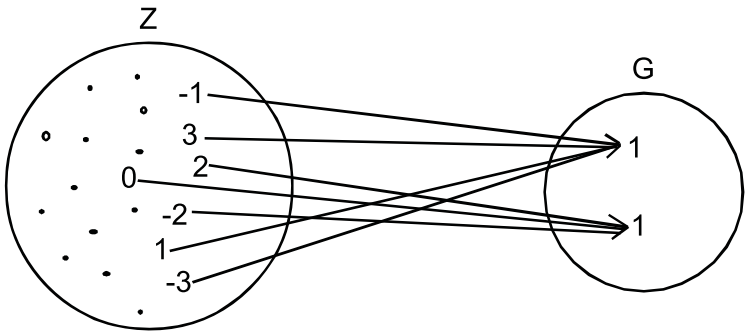
Example 7: Let $\underline{\underline{Z}}$ be the additive group of integers. Let G = {–1, 1} be the multiplicative group. We define

$$f(x)\begin{cases} = 1, \text{ if } x \text{ is even} \\ = -1, \text{ if } x \text{ is odd} \end{cases}$$

(i) We have proved that f is a homomorphism (Example 4).

(ii) Clearly f is not one-one.

(iii) Clearly f is onto.



1 is the image of all even integers, and –1 is the image of all odd integers.

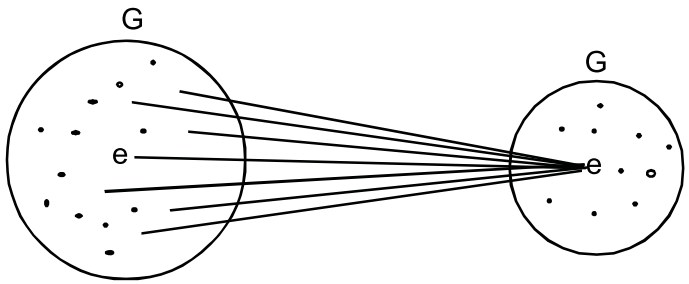
Thus, f is an epimorphism, but not an isomorphism.

Example 8: Let G be a group, and e be the identity of G. We define

$f(x) = e, \ \forall x \in G$

(i) We have proved that f is a homomorphism (Example 5).

(ii) Clearly f is not one-one. All the elements are related to e.



(iii) f is not onto. e is the only image.

$\therefore$ f is not an isomorphism. It is neither a monomorphism nor an epimorphism.

$\because$ f is a homomorphism from G to itself, it is an endomorphism.



CHECK YOUR PROGRESS

Q 6: Let C be the additive group of complex numbers.Define $f : \underline{\underline{C}} \to \underline{\underline{C}},\ f(z) = \bar{z},\ \forall z \in \underline{\underline{C}}$

Examine if f is an automorphism.

Q 7: Let $\underline{\underline{R}}$ be the additive group of real numbers, and $\underline{\underline{R}}_+$ be the multiplicative group of positive real numbers.

Define $f : \underline{\underline{R}} \to \underline{\underline{R}}_+,\ f(x) = e^x$

Examine if f is an isomorphism

Q 8: Let $\underline{\underline{Z}}$ be the additive group of integers, and $\underline{\underline{2Z}}$ be the additive group of even integers. Define $f : \underline{\underline{Z}} \to \underline{\underline{2Z}},\ f(x) = 2x,\ \forall x \in \underline{\underline{Z}}$

Examine if f is an isomorphism.

Q 9: Let $\underline{\underline{2Z}} = \{.....,-8,-6,-4,-2,0,2,4,6,8,....\}$

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

$\underline{\underline{2Z}}$ and $\underline{\underline{3Z}}$ are additive groups.

Define $\underline{\underline{2Z}} \to \underline{\underline{3Z}}$, f(2x)=3x where x is an integer.

Examine if f is an isomorphism.

Q 10: Let $\underline{\underline{R}}_+$ be the multiplicative group of positive real numbers, and $\underline{\underline{R}}$ be the additive group of real numbers. Define

$f : \underline{\underline{R}}_+ \to \underline{\underline{R}},\ f(x) = \log_{10} x$

Examine if f is an isomorphism.

8.5 PROPERTIES OF HOMOMORPHISM

Theorem : Let G, G/ be two groups. Let e, e/ be the identities of G, G/ respectively. Let f : G $\to$ G/ be a homomorphism. Then

(i) f(e) = e/

(ii) $f(x^{-1}) = (f(x))^{-1},\ x \in G$

(iii) $f(x^n) = (f(x))^n$, $x \in G$, n is an integer.

Proof: (i) We have

$e\ e = e$

$\Rightarrow f(e\ e) = f(e)$

$\Rightarrow f(e)\ f(e) = f(e)$, $\because$ f is a homomerphism

$\Rightarrow f(e)\ f(e) = f(e)e'$, $f(e) \in G'$, and e' is the identity of G'

$\Rightarrow f(e) = e'$, by left cancellation.

(ii) We have

$$x x^{-1} = e = x^{-1} x$$

$$\Rightarrow f(x x^{-1}) = f(e) = f(x^{-1} x)$$

$$\Rightarrow f(x) f(x^{-1}) = e' = f(x^{-1}) f(x)$$

This $\Rightarrow f(x^{-1})$ is the inverse of f(x).

i.e. $(f(x))^{-1} = f(x^{-1})$

(iii) Let n be a positive integer :

Then $f(x^n) = f(x x x....x)$

= $f(x) f(x) f(x) f(x)....f(x)$, $\because$ f is a homomorphism

= $(f(x))^n$

Let n = 0 :

Then $x^0 = e$

$\therefore$ $f(x^0) = f(e)$

$= e'$

$= (f(x))^0$

Let n be a negative integer :

Let n = –m, where m is a positive integer.

Now $f(x^n) = f(x^{-m})$

$= f(x^{-1})^m)$

$= ((f(x))^{-1})^m$

$= (f(x))^{-m}$

$= (f(x))^n$

Thus, $f(x^n) = (f(x))^n$, for any integer n.

Theorem : Let $f : G \to G'$ be an epimorphism from a group G to a group G'. If G is Abelian, then G' is also Abelian

Proof : Here f : G $\to$ G/ is an epimorphism.

$\therefore$ f is a homomorphism and f is onto.

Let $u, v \in G'$

$\because$ f is onto, there exist a, b $\in$ G such that f(a) = u, f(b) = v

Now $u\,v$ = f(a) f(b)

= f(ab), $\because$ f is a homomorphism

= f(ba), $\because$ G is Abelion

= f(b) f(a), $\because$ f is a homomorphism

= vu

Thus, $u\,v = vu,\ \forall u, v \in G'$

$\therefore$ G is Abelian

Note : The converse of the above theorem is not true.

Let us consider the group S_3 of all permutntions of S = {1, 2, 3}.

Let G = {–1, 1} be the multiplicative group.

We define $f : S_3 \to G$ by

$$f(\alpha)\begin{cases} = 1, \text{ if } \alpha \text{ is an even permutation} \\ = -1, \text{ if } \alpha \text{ is an odd permutation} \end{cases}$$

f is a homomorphism. Moreover f is onto, i.e, f is an epimorphism.

Now G is Abelian, but S_3 is not Abelian.

Theorem : Let f : G $\to$ G/ be an epimorphism from a group G to a group G/. If G is cyclic, then G/ is also cyclic.

Proof : Here f : G $\to$ G/ is an epimorphism.

$\therefore$ f is a homomorphism and f is onto. Let the cyclic group G be generated by $a \in G$.

Let $u \in G$

Then there exists $p \in G$ such that

u = f(p)

= $f(a^m)$, $\because$ p = a^m, for some integer m

= $(f(a))^m$

This $\Rightarrow$ G/ is a cyclic group generated by f(a).

Note : The converse of the above theorem is not true.

Let us consider the example given in the previous theorem.

Here G = {–1, 1} is cyclie,

but S_3 is not cyclic.

Theorem : Let f : G $\rightarrow$ G/ be a homomorphism from a group G to a group G/.

(i) If H is a subgroup G, f(H) is a subgroup of G/.

(ii) If K is a subgroup of G/, $f^{-1}(K)$ is a subgroup of G.

[f(H) = {f(h) : h $\in$ H}, called the image of H under f.

$f^{-1}(K) = \{a \in G : f(a) \in K\}$, called the inverse image of K under f.

It should be borne in mind that f^{-1} may not be a homomorphism, though f is a homomorphism]

Proof : Let e be the identity of G, and e/ be the identity of G/.

$\therefore$ f(e) = e/

(i) We have e/ = f(e) $\in$ f(H)

$\therefore\ f(H) \neq \phi$

Let $u, v \in f(H)$

$\therefore$ there exist a, b $\in$ H such that f(a) = u, f(b)= v

Now uv^{-1} = f(a) $(f(b))^{-1}$

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

= $f(ab^{-1})$

$\because$ H is a subgroup of G, $\therefore$ $ab^{-1} \in H$

$\therefore$ $f(ab^{-1}) \in f(H)$

$\therefore\ uv^{-1} \in f(H)$

Thus, $u,\ v \in f(H) \Rightarrow uv^{-1} \in f(H)$

$\therefore$ f(H) is a subgroup of G/

(ii) We have $e^{/} \in K$

$\Rightarrow f(e) \in K$

$\Rightarrow e \in f^{-1}(K)$

$\therefore\ f^{-1}(K) \neq \phi$

Let a, b $\in$ f^{-1}(K)

$\therefore$ f(a) $\in$ K, f(b) $\in$ K

$\Rightarrow$ f(a) $(f(b))^{-1} \in$ K, $\because$ K is a subgroup of G/

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

$\Rightarrow f(ab^{-1}) \in K$

$\Rightarrow ab^{-1} \in f^{-1}(K)$

Thus, $a, b \in f^{-1}(K) \quad \Rightarrow ab^{-1} \in f^{-1}(K)$

$\therefore f^{-1}(K)$ is a subgroup of G'.

Example 9 : Let G be a group. Let the mapping $f : G \to G$, $f(x) = x^{-1}$ be a homomorphism. Show that G is Abelian.

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

Now $f(ab) = f(a)\, f(b)$, $\because$ f is a homomorphism by definition of f

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

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

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

$\Rightarrow ab = ba$

$\therefore$ G is Abelian



CHECK YOUR PROGRESS

Q 11: Let $f : G \to G$, $f(x) = x$ be a mapping from group G to itself. Show that f is an automorphism.

Q 12: Let G be an Abelian group. Show that the mapping.

$f : G \to G$, $f(x) = x^{-1}$ is an automorphism.



8.6 LET US SUM UP

Let G be a group under the binary operation $*$, and G' be a group under the binary operation o. The mapping $f : G \to G'$ is said to be a homomorphism if $f(a * b) = f(a)$ of (b)

- A homomorphism if said to be a monomorphism if it is one-one.
- A homomorphism is said to be an epimorphism if it is onto.
- A homomorphism is said to be an isomorphism if it is one-one and onto.
- A homomorphism from a group to itself is called an endomorphism.
- An isomorphism from a group to itself is called an automorphism.

- Let f : G $\rightarrow$ G/ be a homomorphism from a group G to a grant G/. Let e, e/ be the identities of G, G/ respectively. Then
  (i) f(e) = e/
  (ii) $f(x^{-1}) = (f(x))^{-1}$, $x \in G$
  (iii) $f(x^n) = (f(x))^n$, n is an integer.
- Let f G $\rightarrow$ G/ be an epimorphism from a group G to a group G/.
  (i) If G is Abelian, then G/ is Abelian.
  (ii) If G is cyclic, then G/ is cyclic.
  The converse of each of (i) and (ii) is not true.
- Let f : G $\rightarrow$ G/ be a homomorphism from a group G to a group G/.
  (i) If H is a subgroup of G, f(H) is a subgroup of G/.
  (ii) If K is a subgroup of G/, $f^{-1}(K)$ is a subgroup of G.



8.8 FURTHER READINGS

1) Fraleigh, Johu B : *A First Course in Abetract Algebra* (2003), Pearson Education (Singapure) Pvt. Ltd, Indian Branch, Delhi 110092.
2) Mapa, S.K. : *Higher Algebra* (Abstract and Linear) (1994), Asoke Prakasan, Calcutta 700007.
3) Khanna, V. K. and Bhambri, S. K. : *A Course in Abstract Algebra* (2006), Vikas Publishing House Pvt. Ltd. New Delhi 110014.



8.7 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: $f : \underline{\underline{Z}} \rightarrow \underline{\underline{Z}}$, $f(x) = 5x$

Let $a, b \in \underline{\underline{Z}}$

Now f(a+b) = 5(a+b)

=5a+ 5b

= f(a) + f(b)

$\therefore$ f is a homomorphism.

Ans to Q No 2: $f : \underline{\underline{Z}} \to \underline{\underline{Z}}, \quad f(x) = x + 3$

Let $a, b \in \underline{\underline{Z}}$

f(a+b) = (a+b) + 3 = a+b+3

f(a) +f(b) = (a+3) + (b+3)

= a + b + 6

$\therefore$ f(a+b) $\neq$ f(a) + f(b)

$\therefore$ f is not a homomorphism

Ans to Q No 3: $f : \underline{\underline{R}}_+ \to \underline{\underline{R}}_+, f(x) = \frac{1}{x}$

Let $a, b \in \underline{\underline{R}}_+$

Now $f(ab) = \frac{1}{ab}$

$= \frac{1}{a}\frac{1}{b}$

= f(a)f(b)

$\therefore$ f is a homomerphism.

Ans to Q No 4: $f : \underline{\underline{R}}_+ \to \underline{\underline{R}}, f(x) = \log_e x$

Let $a, b \in \underline{\underline{R}}_+$

Now f(ab) = $\log_e$ ab

= $\log_e$a + $\log_e$b

= f(a) + f(b)

$\therefore$ f is a homomorphism

Ans to Q No 5: f : $S_3 \to$ G = {–1, 1}, where

$$f(\alpha)\begin{cases} = 1, \text{ if } \alpha \text{ is an even permutation} \\ = -1, \text{ if } \alpha \text{ is an odd permutation} \end{cases}$$

Case I : Let α, β be even permutation.

$\therefore f(\alpha) = 1, f(\beta) = 1$

We know that the product of two even permutations is an even permutation.

$\therefore f(\alpha\beta) = 1$

$= 1 \times 1$

$= f(\alpha) f(\beta)$

Case 2: Let α, β be add permutations

$\therefore\ f(\alpha) = -1,\ f(\beta) = -1$

We know that the product of two odd permutations is an even permutation.

$\therefore\ f(\alpha\beta) = 1$

$= (-1) \times (-1)$

$= f(\alpha) f(\beta)$

Case 3 : Let α be an even permutation, and β be an odd permutation.

$\therefore\ f(\alpha) = 1,\ f(\beta) = -1$

We know that the product of an even permutation and an odd permutation is an odd permutation.

$\therefore\ f(\alpha\beta) = -1$

$= 1 \times (-1)$

$= f(\alpha) f(\beta)$

Similarly, if α is an odd permutation and β is an even permutation, then also

$f(\alpha\beta) = f(\alpha) f(\beta)$

Thus, in all the cases,

$f(\alpha\beta) = f(\alpha) f(\beta)$

$\therefore$ f is a homomorphism.

Ans to Q No 6: $f : \underline{\underline{C}} \to \underline{\underline{C}},\ f(z) = \bar{z}$

Let $z, w \in \underline{\underline{C}}$

Now $f(z + w) = \overline{z + w}$

$= \bar{z} + \overline{w}$

$= f(z) + f(w)$

$\therefore$ f is a homomorphism.

Let f(z) = f(w)

$\Rightarrow \bar{z} = \overline{w}$

$\Rightarrow z = w$

$\therefore$ f is one-one.

Let $\Rightarrow z \in \underline{\underline{C}}$ (codomain)

Then, there exists $\bar{z} \in \underline{\underline{C}}$ (domain) such that

$f(\bar{z}) = (\bar{\bar{z}}) = z$

$\therefore$ f is onto.

$\therefore$ f is an isomorphism.

$\because$ f is an isomorphism from $\underline{\underline{C}}$ to itself,

$\therefore$ f is an automorphism.

Ans to Q No 7: $f : \underline{\underline{R}} \to \underline{\underline{R}}_+$, $f(x) = e^x$

Let $a, b \in \underline{\underline{R}}$

Now f(a+b) = e^{a+b}

= e^a e^b

= f(a) f(b)

Let f(a) = f(b)

$\Rightarrow$ $e^a = e^b$

$\Rightarrow$ a = b

$\therefore$ f is one-one

Let $u \in \underline{\underline{R}}_+$ such that f(c) = u

$\therefore$ e^c = u

$\therefore$ e = $\log_e u \in \underline{\underline{R}}$

Thus, corresponding to every $u \in \underline{\underline{R}}_+$, there exists $\log_e u$ in $\underline{\underline{R}}$ such that

f($\log_e u$) = u

$\therefore$ f is onto.

$\therefore$ f is an isomorphism.

Ans to Q No 8: $f : \underline{\underline{Z}} \to 2\underline{\underline{Z}}$, $f(x) = 2x$

Let $a, b \in \underline{\underline{Z}}$

Now f(a+b) = 2(a+b)

= 2a + 2b

= f(a) + f(b)

$\therefore$ f is a homomorphism.

Let f(a) = f(b)

$\Rightarrow$ 2a = 2b

$\Rightarrow$ a = b

$\therefore$ f is one-one

Let $u \in 2\underline{\underline{Z}}$

Then there exists $\frac{u}{2} \in \underline{\underline{Z}}$ such that $f\left(\frac{u}{2}\right) = 2\frac{u}{2} = u$

$\therefore$ f is onto.

$\therefore$ f is an isomorphism.

Ans to Q No 9: $f : 2\underline{\underline{Z}} \to 3\underline{\underline{Z}},\ f(2x) = 3x$, where x is an integer.

Let a, b be integers.

$\therefore$ 2a, 2b $\in 2Z$

Now f (2a+2b) = f(2(a+b))

= 3(a+b)

= 3a + 3b

= f(2a)+ f(2b)

$\therefore$ f is a homomorphism.

Let f(2a) = f(2b)

$\Rightarrow$ 3a = 3b

$\Rightarrow$ a = b

$\Rightarrow$ 2a = 2b

$\therefore$ f is one-one

Let $3u \in 3\underline{\underline{Z}}$, where u is an integer.

Then, there exists $2u \in 2Z$ such that f (2u) = 3u

$\therefore$ f is onto

$\therefore$ f is an isomorphism

Ans to Q No 10: $f : \underline{\underline{R}}_{+} \to \underline{\underline{R}},\ f(x) = \log_{10} x$

Let $a, b \in \underline{\underline{R}}_{+}$

Now f(ab) = $\log_{10}$ ab

= $\log_{10}$a + $\log_{10}$b

= f(a) + f(b)

$\therefore$ f is a homomorphism

Let f(a) = f(b)

$\Rightarrow$ $\log_{10}$a = $\log_{10}$b

$\Rightarrow$ a = b

$\therefore$ f is one-one

Let $u \in \underline{\underline{R}}$

Then there exists $10^u \in \underline{\underline{R}}_+$ such that

$$f(10^u) = \log_{10}{}^{10^u}$$
$$= u \log_{10}{}^{10}$$
$$= u$$

$\therefore$ f is onto.

$\therefore$ f is an isomorphism.

Ans to Q No 11: $f : G \to G, \quad f(x) = x$

Let $a, b \in G$

Now f(ab) = ab

= f(a) f(b)

$\therefore$ f is a homomorphism

f(a) = f(b)

$\Rightarrow$ a = b

$\therefore$ f is one-one

For every $a \in G$, f(a) = a

$\therefore$ f is onto

$\therefore$ f is an isomorphism from G to itself

$\therefore$ f is an authomorphism.

Ans to Q No 12: $f : G \to G, \quad f(x) = x^{-1}$

Let $a, b \in G$

Now f(ab) = $(ab)^{-1}$

= $b^{-1} a^{-1}$

= $a^{-1}b^{-1}$, $\because$ G is Abelion

= f(a) f(b)

$\therefore$ f is a homomorphism

Let f(a) = f(b)

$\Rightarrow$ a = b

$\therefore$ f is one-one

Let $u \in G$,

Then there exists $u^{-1} \in G$ such that

$f(u^{-1}) = (u^{-1})^{-1}$

$= u$

$\therefore$ f is onto

$\therefore$ f is an isomorphism from G to itself.

$\therefore$ f is an automorphism.



8.9 MODEL QUESTIONS

Q 1: Let $\underline{\underline{R}}$ be the additive group of real numbers. Let

$f : \underline{\underline{R}} \to \underline{\underline{R}}$, $f(x) = 5x$ be a mapping.

Examine if f is a homomorphism.

Q 2: Let $3\underline{\underline{Z}}$ ={. . ., –9, –6, –3, 0, 3, 6, 9, ...}

$5\underline{\underline{Z}}$ ={. . ., –20, –15, –10, –5, 0, 5, 10, 15, 20, ...}

$3\underline{\underline{Z}}$, and $5\underline{\underline{Z}}$ are additive groups.

Let $f : 3\underline{\underline{Z}} \to \underline{\underline{Z}}$, $f(3x) = 5x$, where x is an integer.

Examine if f is a homomorphism.

Q 3: Give an example of a homomorphism from an infinite group to a finite group.

Q 4: Let $f : G \to G'$ be an isomorphism from a group G to a group G/. If G/ is Abelian, prove that G is also Abelian.

Q 5: Let $f : G \to G'$ be an isomorphism from a group G to a group G/. If G/ is cyclic, prove that G is also cyclic.

*** ***** ***