U. P. Rajarshi Tandon
Open University

Master of Science

PGMM -106/MAMM-106
Advanced Algebra

Course Design Committee

Prof. Ashutosh Gupta, **Chairman**
Director, School of Sciences, UPRTOU, Prayagraj

Prof. A. K. Malik **Coordinator**
School of Sciences, UPRTOU, Prayagraj

Prof. Mukesh Kumar **Member**
Department of Mathematics, MNNIT, Prayagraj

Prof. A. K. Pandey **Member**
Department of Mathematics, ECC, Prayagraj

Dr. Raghvendra Singh **Invited Member/Secretary**
Assistant Professor, Mathematics, School of Sciences, UPRTOU, Prayagraj

Course Preparation Committee

Dr. Mahesh Kumar Jayaswal **Author (Unit 1-3)**
Department of Mathematics, Maharaja Surajmal Brij University, Bharatpur

Dr. Varsha Parihar **Author (Unit 4-6)**
Dept. of Mathematics, Lachoo Memorial College of Science & Technology, Jodhpur

Dr. Chandrapal Singh Chouhan **Author (Unit 7 - 8)**
Department of Mathematics and Statistics
Faculty of Science, Bhupal Nobels' University, Udaipur

Dr. Preeti Mehta **Author (Unit 9 - 11)**
Department of Mathematics and Statistics
Faculty of Science, Bhupal Nobels' University, Udaipur

Dr. Raghvendra Singh **Author (Unit 12)**
Assistant Professor, Mathematics, School of Sciences, UPRTOU, Prayagraj

Dr. P. N. Pathak **Author (Unit 13 - 14)**
Assistant Professor, Mathematics, CSJM University, Kanpur

Prof. A. K. Malik **Editor (Unit 4 - 6)**
School of Sciences, UPRTOU, Prayagraj

Prof. Satish Kumar **Editor (Unit 1-3, 7 - 14)**
Department of Mathematics, D N College Meerut, UP

Prof. A. K. Malik **Program Coordinator**
School of Sciences, UPRTOU, Prayagraj

Dr. Raghvendra Singh **Course Coordinator/Invited Member/Secretary**
Assistant Professor, Mathematics, School of Sciences, UPRTOU, Prayagraj

© UPRTOU, Prayagraj- 2025
PGMM –106: ADVANCED ALGEBRA
ISBN:- 978-81-992992-8-3

©All Rights are reserved. No part of this work may be reproduced in any form, by mimeograph or any other means, without permission in writing from the Uttar Pradesh Rajarshi Tondon Open University, Prayagraj.
Printed and Published by Vinay Kumar Singh, Registrar, Uttar Pradesh Rajarshi Tandon Open University, 2025.

Printed By : Chandrakala Universal Pvt. 42/7 Jawahar Lal Neharu Road, Prayagraj.

Syllabus

PGMM-106/MAMM-106: Advanced Algebra

Block-1: Introduction to Group Theory

Unit-1: Basic Set Theory

Introduction, Representation of sets, types of sets, subset, universal set, Venn diagram, operations on sets, and algebra of sets.

Unit-2: Relations and Functions

Introduction, relations, equivalence relation, and partial order relation, functions.

Unit-3: Introduction of Group Theory

Introduction, algebraic structure, group, Abelian group, finite and infinite group, composition tables for finite sets.

Block-2: Group Theory

Unit-4: Permutations Groups

Introduction, permutations, groups of permutations, cyclic permutations, even and odd permutations, order of an element of a group, isomorphism on groups.

Unit-5: Order of an element of a group and Isomorphism on Groups

Introduction, order of an element of a group, isomorphism on groups.

Unit-6: Subgroup and Cosets

Introduction, complexes and subgroups of a group, intersection of subgroups, cosets, Lagrange's theorem, Fermat's theorem, Cayley's theorem.

Block-3: Advanced Group Theory

Unit-7: Cyclic Group

Introduction, Cyclic groups, subgroup generated by a subset of a group, generating system of a group.

Unit-8: Normal Subgroup

Introduction to Normal subgroup, simple group, conjugate element, centre of a group, conjugate subgroup and quotient groups.

Unit-9: Homomorphism

Homomorphism on groups, Kernel of a homomorphism, fundamental theorem on homomorphism of groups, automorphisms and inner automorphisms, Maximal subgroup, Composition series of a group, Jordon Holder's theorem, Solvable groups, Direct products, Sylow's theorem.

Block-4: Rings and Field Theory

Unit-10: Rings

Introduction, Rings, elementary properties of a ring, ring with or without zero divisors, integral domain, field, subrings and subfields.

Unit-11: Ideals

Introduction, ideals, principal ideal, divisibility in an integral domain, greatest common divisor, polynomials rings, unique factorization domain and reminder theorem. Quotient rings, homomorphism on rings, kernel of a ring homomorphism, maximal ideals, prime ideals and Euclidean rings.

Block-5: Extension Fields and Galois Theory

Unit-12: Extension Fields

Introduction, field extensions, field adjunctions, simple and algebraic field extensions, separable extension and perfect field.

Unit-13: Galois Theory-I

The elements from Galois theory, fixed field, normal extension.

Unit-14: Galois Theory-II

Galois group, fundamental theorem of Galois theory.

U. P. Rajarshi Tandon
Open University

Master of Science

PGMM -106/MAMM-106
Advanced Algebra

Block

1 Introduction to Group Theory

Unit- 1 **Basic Set Theory**
Unit- 2 **Relations and Functions**
Unit- 3 **Introduction of Group Theory**

Block-1

Introduction to Group Theory

Set theory and group theory are two fundamental branches of mathematics. Set theory, developed by Georg Cantor in the late 19th century, provides a formal way to study collections of objects and serves as the foundation for modern mathematics, including logic, number theory, topology, and analysis. Group theory focuses on symmetry and patterns in numbers, shapes, and equations. It began in the 18th century with Lagrange, while Galois introduced the idea of groups to solve polynomial equations. In the 19th century, mathematicians like Cauchy, Jordan, Cayley, and Klein expanded the field by defining groups and applying them to geometry. In the 20th century, group theory became essential in physics, chemistry, cryptography, and computer science, helping to explain atomic structures, quantum mechanics, and algebraic systems.

Today, both set theory and group theory play a crucial role in pure and applied mathematics. In the first unit, we shall discuss about the introduction about set theory, representation of sets, types of sets, subset, universal set, Venn diagram, operations on sets, and algebra of sets. Relations, equivalence relation, partial order relation and functions are also discussed in details in unit two. Third unit introduced the group theory, algebraic structure, group, Abelian group, finite and infinite group, composition tables for finite sets.

UNIT-1: Basic Set Theory

Structure

1.1 Introduction

Georg Cantor, a German mathematician, introduced the concept of set theory, defining a set as a collection or aggregate of definite and distinguishable objects selected by means of some rules or description. Set theory is a fundamental foundation of mathematics, with nearly every mathematical object of interest being a set of some kind. In this unit, our goals are to learn how to describe and

manipulate sets and to develop techniques for constructing new sets from existing ones.

Also we deals with representation of sets: roster method or tabular form and rule method or set builder form, different types of sets, venn diagram, operations of sets, union and intersection of two sets, difference and complement of sets. Some examples of sets include the set of natural numbers, the set of fractions, and the set of all capital cities in India.

1.2 Objectives

After reading this unit the learner should be able to understand about the:

- Basic concepts, terminology and notationon of set
- representation of sets: roster method or tabular form and rule method or set builder form
- different types of sets, venn diagram
- operations of sets, union and intersection of two sets,
- difference and complement of sets

1.3 Set

A set is any well- defined collections of objects, called the elements or members of the sets. These elements may be anything as numbers, points in geometry, letters of alphabets, etc. The examples of sets given below :

(1) A battalion of soldiers (2) Bunches of Grapes (3) The vowels of alphabets.

Capital letters A, B, C…….. are ordinarily used to denote sets lower case letters a, b, c,….. to denotes elements of sets. Well- defined means it is possible to decide if a given element belongs to the collections or not. The statement ‘x is an element of A’ or equivalently ‘x belongs to A’ is written as $x \in A$. The statements ‘x is not an elements of A’ is written as $x \notin A$.

1.4 Representation of Sets

Sets can be represented in two ways:

(i) Roster Method or Tabular form (ii) Rule method or Set Builder Form.

Roster Method or Tabular Form

In roster form, all the elements of the set are listed, the elements being separated by commas and enclosed between curly braces.

Examples

Example 1: Given below are set representation in roaster form:

(i) The sets of binary digits, i.e., A = {0, 1}.

(ii) The set of vowels in the English alphabets, i.e., B = {a, e, i, o, u}.

Example 2: If the set $A = \{x: x \in Z, x^2 < 17\}$ then find out its roster form.

Solution: We find that the squares of integers $0, \pm1, \pm2, \pm3, \pm4$ are less than 17 then the roster form of this set, $A = \{-4, -3, -2, -1, 0, +1, +2, +3, +4\}$.

Rule Method or Set Builder Form

In set builder form, a set is defined by specifying a property that elements of the set have a common. The set is then described as follows: A={ x: p (x) }

A vertical bar is also used in place of colon (:)

Examples

Example.3: Given below are set representation in set builder form-

(i) The set A consisting of element a, e, i, o, u can be written as A = {x: x is a vowel in the English alphabets}.

(ii) The set B = {1, 4, 9, 16, 25, 36} can be written as B = {x: x = n^2 where n is a natural number ≤ 6}.

(iii) The set C = {2, 4, 6, 8} can be written as C = {x: x is an even integer between 1 and 8}.

Some sets are represented by special symbols. In particular, the set of natural numbers is denoted by N, the set of integers represented by Z, the set of rational number represented by Q and the set of real numbers represented by R.

i. e. N = {x: x is a natural number}

Z = {x: x is an integer}

Q = {x: x is a rational number}

R = {x: x is a real number}

Example 4: Write the set A $= \{1, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \frac{1}{25} \ldots \ldots \ldots \ldots\}$ in the set builder form.

Solution: We analyze that; each members of the given set are the reciprocals of the squares of all naturals**.** The set builder form of the given set is, A $= \left\{\frac{1}{n^2} : n \in N\right\}$.

1.5 Different Types of Sets

The sets are divided into various types, based on elements or types of elements. These various types of sets given below:

Finite set

An finite set is a set which contains finite number of elements then the set is called finite sets.

Examples of finite set are

(a) The set of months of a year;

(b) The set of vowels in English alphabets;

(c) The set of students in a class;

Infinite set

An infinite set is a set which contains infinite number of elements then the set is called infinite Set.

Examples of infinite set are:

(a) A= a set of integers {0, 1, 2, …….. }.

(b) B= {1, 1/3, 1/9, 1/27, ……. }.

Empty set

A set which has no elements at all, is known as empty set or null set and it is represented by ϕ or **{}.**

The following sets are empty set:

(a) A = {x: x^2+4=0, x is a real number}

(b) B = {x is multiple of 4, x is a odd number}

Singleton set

A set which has only one element is called singleton set.

For example: (a) : {1} is a singleton set.

(b) : {x: x-5=0, x $\in$N } is a singleton set.

Equal set

Two sets A and B are said to be equal iff every element of A is an element of B and consequently every element of B is an element of A;

i.e., A $\subseteq$ B and B $\subseteq$ A and It is written as A = B.

i.e., A = B if x $\in$ A and x $\in$ B.

For example: If A $= \left\{1, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \frac{1}{25} \ldots \ldots \ldots \ldots \right\}$ and B $= \left\{1, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \frac{1}{25} \ldots \ldots \ldots \ldots \right\}$, then A and B are equal sets.

Equivalent set

Two sets A and B are equivalent if they have same number of elements.

For example: $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ are the examples of the equivalent set because A and B have same number of elements.

Power set

Power set is the collection of all possible subset of a set and it is represented by $P(A)$ where A is any set.

Suppose that $A = \{1,2, 3\}$ then its Power set

$P(A) = \{\Phi, \{1\}, \{2\}, \{3\}, \{2, 3\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$.

Universal set

In the given consideration, if all the sets are a subset of a definite, then this definite set is called universal set and is denoted by U.

For example:

1. The set of all integers is the universal set for the set of positive integers or negative integers.

2. The set of English alphabet is the universal set for the set of vowel.

Note: Every set is a subset of the universal set.

Subset

Let A and B are two sets if every element of set A are also element of set B, then A is said to be a subset of B and it is represented by $A \subseteq B$. When at least one element of the set A does not belong to the set B, then the set A is not a subset of the set B.

For examples:

1. If A = {1, 2, 3} and B = {1, 2, 3, 4, 5}, then $A \subseteq B$ and $B \subseteq A$.

Note: (i) Every set A is a subset of itself, i.e. $A \subseteq A$.

(ii) The null set Φ is considered as a subset of any set A, i.e. $\Phi \subseteq A$.

Check your progress report

Q. 1. What do you means by set?

Q.2. Explain the concept of representation of sets.

Q.3. If A = {a, b, c, d} and B = {b, c, d, a}, then $A \subseteq B$ and $B \subseteq A$.

Q.4. Define finite and infinite sets with examples.

Q.5 If $A = \{1,2,3,4,5\}$ then itwrite the power set of A.

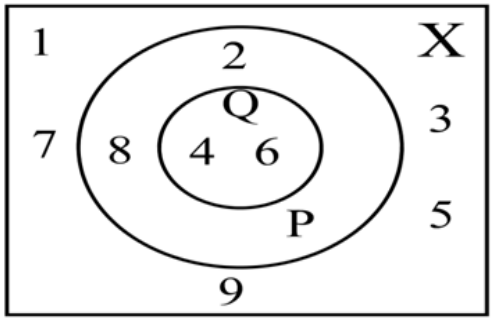
Q.6. Give two examples of empty set.

Q.7. Explain the universal set.

1.6 Venn Diagram

The idea of sets can also show by means of figures/ diagrams. These representations of sets are called Venn Diagrams named after British logician John Venn (1834-1883 A.D.).

In Venn diagram, the universal set represented by a rectangle and the subsets of this universal set are represented by the circles.



Example: In the figure X represent universal set. P = {2, 4, 6, 8} and Q = {4, 6} are the subset of universal set X.

1.7 Operations on Sets

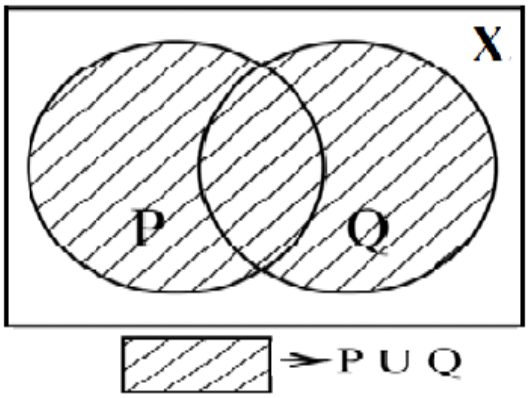
The basic operations in the set theory are union, intersection, difference, complement etc**.** By using of these operation sets are included to make new sets.

Here we can define fixed operations on the sets and explain their properties.

1.8 Union of two Sets

The union of two sets P and Q is the set which consists of all those elements which are either in P or in Q or in both P and Q. The union of two sets P and Q can be represented by $P \cup Q$ and mathematically can be defined as

$P \cup Q = \{x: x \in P \text{ or } x \in Q\}$ and read as P union Q.



Examples- If $P = \{1,2,3,4,5\}$ and $Q = \{6,7,8,9\}$ then, $P \cup Q = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Union of more than two sets

If $A_1, A_2, A_3, \ldots\ldots, A_n$ is a family of finite number of sets, then

$\bigcup_{i=1}^{n} A_i$ *or* $A_1 \cup A_2 \cup A_3 \cup \ldots\ldots \cup A_n$ represents the union of the given sets.

Properties of the Union of sets

(A). Idempotent Law: For any set A

$A \cup A = A$.

Proof: Let $x \in A \cup A$

$\Rightarrow$ $x \in A$ or $x \in A$

$\Rightarrow$ $x \in A$

$\therefore$ $A \cup A \subseteq A$ …(1)

Again, Let $y \in A$

$\Rightarrow$ $y \in A$ or $y \in A$

$\Rightarrow$ $y \in A \cup A$

$\therefore$ $A \subseteq A \cup A$ …(2)

From equations (1) and (2), we get

$A \cup A = A$.

(B). Commutative Law: For any two sets A and B

$$A \cup B = B \cup A$$

Proof: Let $x \in A \cup B$

$\Rightarrow$ $x \in A$ or $x \in B$

$\Rightarrow$ $x \in B$ or $x \in A$

$\Rightarrow$ $x \in B \cup A$

$\therefore$ $A \cup B \subseteq B \cup A$ … (1)

Again, Let $y \in B \cup A$

$\Rightarrow$ $y \in A$ or $y \in B$

$\Rightarrow$ $y \in A \cup B$

$\therefore$ $B \cup A \subseteq A \cup B$ …(2)

From equations (1) and (2), we get

$A \cup B = B \cup A$.

(C). Associative Law: For any three sets A, B, C

$$(A \cup B) \cup C = A \cup (B \cup C)$$

Proof: Let $x \in (A \cup B) \cup C$

$\Rightarrow$ $x \in (A \cup B)$ or $x \in C$

$\Rightarrow$ $(x \in A$ or $x \in B)$ or $x \in C$

$\Rightarrow$ $x \in A$ or $(x \in B$ or $x \in C)$

$\Rightarrow$ $x \in A \cup (B \cup C)$

$\therefore$ $(A \cup B) \cup C \subseteq A \cup (B \cup C)$ …(1) Similarly,

$A \cup (B \cup C) \subseteq (A \cup B) \cup C$ …(2)

From equations (1) and (2), we get

$(A \cup B) \cup C = A \cup (B \cup C)$.

(D). Law of identity element:

(1) For any set A,

$A \cup \emptyset = A$, where $\emptyset$,is the identity element of $(\cup)$

(2) For any set A,

$A \cup U = U$, where U = universal set.

Proof: (1) : Let $x \in A \cup \emptyset$

$\Rightarrow$ $x \in A$ or $x \in \emptyset$

$\Rightarrow$ $x \in A$

$\therefore \quad A \cup \emptyset \subseteq A \quad \ldots(1)$

But, $A \subseteq A \cup \emptyset \quad (\therefore A \subseteq A \cup B) \quad \ldots(2)$

From equations (1) and (2), we get $A \cup \emptyset = A$

(2) We know that

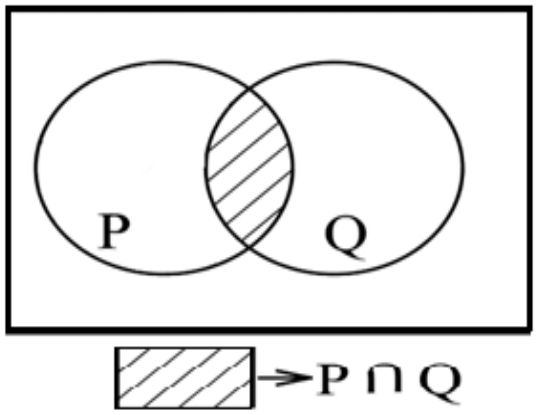
$A \cup U \subseteq U$ and $U \subseteq A \cup U$

Hence $\therefore A \cup U = U.$

1.9 Intersection of two Sets

The intersection of two sets P and Q is the set of common elements of set A and set B. The intersection of two sets P and Q can be represented by $P \cap Q$ and mathematically can be defined as

$P \cap Q = \{x: x \in P \text{ and } x \in Q\}$ and read as P intersection Q.



For examples: If $P = \{1, 2, 3\}$ and $Q = \{3, 4, 8, 9\}$ then $P \cap Q = \{3\}$.

Remarks: For any two sets A and B

i. $A \subseteq A \cup B$

ii. $B \subseteq A \cup B$

iii. $A \cap B \subseteq A$

iv. $A \cap B \subseteq B$

Properties of the Intersection of sets:

(A). Idempotent Law: For any set A

$A \cap A = A$

Proof: Let $x \in A \cap A$

$\Rightarrow \quad x \in A$ and $x \in A$

$\Rightarrow \quad x \in A$

$\therefore \quad A \cap A \subseteq A \qquad \ldots(1)$

Again, Let $y \in A$

$\Rightarrow \quad y \in A$ and $y \in A$

$\Rightarrow \quad y \in A \cap A$

$\therefore \quad A \subseteq A \cap A \qquad \ldots(2)$

From equations (1) and (2), we get

$A \cap A = A$

(B). Commutative Law: For any two sets A and B

$A \cap B = B \cap A$

Proof: Let $x \in A \cap B$

$\Rightarrow \quad x \in A$ and $x \in B$

$\Rightarrow \quad x \in B$ and $x \in A$

$\Rightarrow \quad x \in B \cap A$

$\therefore \quad A \cap B \subseteq B \cap A \quad \ldots(1)$

Similarly, $B \cap A \subseteq A \cap B \quad \ldots(2)$

From equations (1) and (2), we get

$A \cap B = B \cap A.$

(C). Associative Law: For any three sets A, B, C

$$(A \cap B) \cap C = A \cap (B \cap C)$$

Proof: Let $x \in (A \cap B) \cap C$

$\Rightarrow \quad x \in (A \cap B)$ and $x \in C$

$\Rightarrow \quad (x \in A$ and $x \in B)$ and $x \in C$

$\Rightarrow \quad x \in A$ and $(x \in B$ and $x \in C)$

$\Rightarrow \quad x \in A$ and $x \in (B \cap C)$

$\Rightarrow \quad x \in A \cap (B \cup C)$

$\therefore \quad (A \cap B) \cap C \subseteq A \cap (B \cap C) \quad \ldots(1)$ Similarly,

$A \cap (B \cap C) \subseteq (A \cap B) \cap C \quad \ldots(2)$

From equations (1) and (2), we get

$(A \cap B) \cap C = A \cap (B \cap C).$

(D). Law of identity element:

(1) For any set A, we have

$$A \cap \emptyset = \emptyset,$$

(2) For any set A and universal set

$$A \cap U = A$$

Therefore, U is the identity element for intersection (∩).

Proof: (1). $A \cap \emptyset \subseteq \emptyset$ ... . (1) ($\therefore A \cap B \subseteq B$)

We know that the empty set is a subset of every set.

$\therefore \quad \emptyset \subseteq A \cap \emptyset$ …(2)

From equations (1) and (2), we get

$$A \cap \emptyset = \emptyset$$

(2) From $A \cap B \subseteq A$

$A \cap U \subseteq A$ …(1)

Let $x \in A$,

$\Rightarrow \quad x \in A$ and $x \in U$

$\Rightarrow \quad x \in A \cap U$ …(2)

$\therefore \quad A \subseteq A \cap U$

From equations (1) and (2), we get

$$A \cap U = A$$

(E). Distributive Law:

For any three sets A, B and C:

(1) Intersection distributive over union

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

(2) Union distributive over intersection.

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof: (1). Let $x \in A \cap (B \cup C)$

$\Rightarrow$ $x \in A$ and $x \in (B \cup C)$

$\Rightarrow$ $x \in A$ and ($x \in B$ or $x \in C$)

$\Rightarrow$ ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$)

$\Rightarrow$ $x \in A \cap B$ or $x \in A \cap C$

$\Rightarrow$ $x \in (A \cap B) \cup (A \cap C)$

$\therefore$ $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ …(1) Similarly, we have

$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ …(2)

From equations (1) and (2), we get

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

(2). Let $x \in A \cup (B \cap C)$

$\Rightarrow$ $x \in A$ or $x \in (B \cap C)$

$\Rightarrow$ $x \in A$ or ($x \in B$ and $x \in C$)

$\Rightarrow$ ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$)

$\Rightarrow$ $x \in A \cup B$ and $x \in A \cup C$

$\Rightarrow \quad x \in (A \cup B) \cap (A \cup C)$

$\therefore \quad A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ (1)

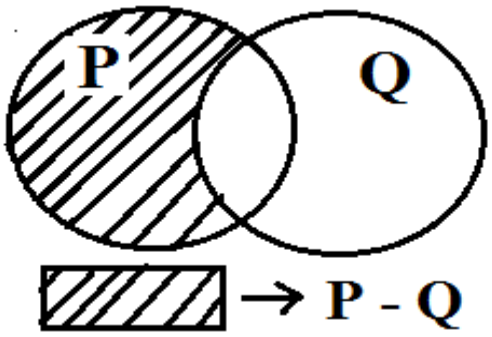
Similarly, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ (2)

From equations (1) and (2)

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

1.10 Difference of Sets

The difference of sets P and Q, is the set of all those elements of P which are not in Q and it is represented by $(P - Q)$.



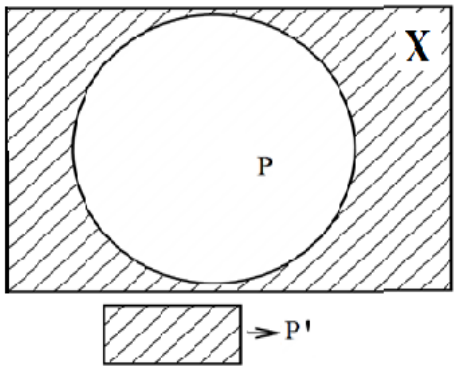
Mathematically can be defined as

$P - Q = \{x: x \in P \text{ and } x \notin Q\}$ and read as P difference Q.

For examples, if $P = \{1, 2, 3\}$ and $Q = \{3, 4, 8, 9\}$ then $P - Q = \{1, 2\}$.

1.11 Complement of Sets

Complement of a set P is the set of all those elements of the universal set which are not in P and it is represented by P'or P^c.



Example- Let us suppose that X is the universal set and $X = \{1,2,3,4,5,6,7,8\}$ and $P = \{1,2,3\}$ then complement of P can be find $P' = \{x: x \in X \text{and } x \notin P\}$ i.e. $P' = \{4,5,6,7,8\}$

(A). Involution Law: For any set A, $(A`)` = A$

Proof: Let $x \in (A`)`$

$\Rightarrow x \notin A`$

$\Rightarrow x \in A$

$\therefore (A`)` \subseteq A$ …(1)

Again, Let $y \in A$

$\Rightarrow y \notin A`$

$\Rightarrow y \in (A`)`$

$\therefore A \subseteq (A`)`$ …(2)

From equations (1) and (2), we have

$$(A`)` = A$$

(B). De-Morgan`s Law:

If A and B are two sets, then

1. $(A \cup B)` = A` \cap B`$

2. $(A \cap B)` = A` \cup B`$

Proof:

1. Let $x \in (A \cup B)`$

$\Rightarrow$ $x \notin A \cup B$

$\Rightarrow$ $x \notin A$ and $x \notin B$

$\Rightarrow$ $x \in A`$ and $x \in B`$

$\Rightarrow$ $x \in A` \cap B`$

$\therefore$ $(A \cup B)` \subseteq A` \cap B`$ (1)

Again, Let $y \in A` \cap B`$

$\Rightarrow$ $y \in A`$ and $y \in B`$

$\Rightarrow$ $y \notin A$ and $y \notin B$

$\Rightarrow$ $y \notin A \cup B$

$\Rightarrow$ $y \in (A \cup B)`$

$\therefore$ $A` \cap B` \subseteq (A \cup B)`$ (2)

From equations (1) and (2), we have

$(A \cup B)` = A` \cap B`$

(2) Let $x \in (A \cap B)`$

$\Rightarrow \quad x \notin A \cap B$

$\Rightarrow \quad x \notin A \text{ or } x \notin B$

$\Rightarrow \quad x \in A` \text{ or } x \in B`$

$\Rightarrow \quad x \in A` \cup B`$

$\therefore \quad (A \cap B)` \subseteq A` \cup B` \qquad (1)$

Again, Let $y \in A` \cup B`$

$\Rightarrow y \in A` \text{ or } y \in B`$

$\Rightarrow y \notin A \text{ or } y \notin B$

$\Rightarrow y \notin A \cap B$

$\Rightarrow y \in (A \cap B)`$

$\therefore A` \cup B` \subseteq (A \cap B)` \qquad (2)$

From equations (1) and (2), we have $(A \cap B)` = A` \cup B`$.

1.12 Summary

Set theory and group theory are two key branches of mathematics. Set theory, introduced by Georg Cantor in the late 19th century, studies collections of objects and forms the foundation of modern mathematics, including logic, number theory, topology, and analysis. Cantor defined a set as a well-defined collection of objects and developed methods for describing and manipulating sets, such as the roster method and set-builder form. This unit focuses on understanding sets and their properties. The goals include learning how to describe, manipulate, and construct sets from existing ones. It covers different ways to represent sets, such as the roster method (tabular form) and the set-builder form (rule method). Key topics include types of sets, Venn diagrams, set operations (union, intersection, difference, complement). Examples of sets include the set of natural numbers, the set of fractions, and the set of all capital cities in India.

1.13 Terminal Questions

Q.1 . If $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $A = \{3, 4, 5, 6\}$ and $B = \{1, 3, 5, 7\}$, Then find each of the following:

1. $A` \cup B`$

2. $A` \cap B`$

3. $(A \cup B)`$

4. $A` - B`$

Q.2. For any three set A, B and C, prove that

1. $A - (B \cup C) = (A - B) \cap (A - C)$.

2. $A - (B \cap C) = (A - B) \cup (A - C)$.

Q.3. If A and B are two sets such that n(A) = 17, n(B) = 23 and $n(A \cup B) = 38$, then determine $n(A \cap B)$.

Q.4. Prove that (i) $A - B \subseteq B'$

(ii) $B - A \subseteq A'$.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Malik, A.K., Singh, S. R. (2020). Topology, Dreamtech Press.

5. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

UNIT-2: Relations and Functions

Structure

2.1 Introduction

The ideas of relations and functions have developed over many centuries, becoming fundamental to modern mathematics. Early studies by ancient Indian and Greek mathematicians explored numerical and geometric relationships, setting the stage for later advancements. The formal notion of a function began in the 17th century, when Leibniz used the term to describe quantities related to curves. In the 18th century, Euler introduced the notation $f(x)$ and treated functions as expressions involving variables and constants.

During the 19th century, Georg Cantor's work on set theory provided a solid foundation, defining a relation as a subset of the Cartesian product of two sets, and a function as a relation where each input corresponds to exactly one output. Today, relations express connections between elements of sets, while functions play a central role in fields like algebra, calculus, differential equations, computer science, and machine learning.

2.2 Objectives

After reading this unit the learner should be able to understand about the:

- Basic concepts, terminology and notationon of relations
- different types of relations
- functions and its types

2.3 Relations

We have study about the ordered pairs, Cartesian product of sets, domain, co-domain and range of a relation, function as a special type of relation and various types of real valued function. In this unit we extend our ideas to relation on a set and function. We shall also discuss composite and inverse of a function. And also we study a particular class of relations called functions. Function plays an important role in mathematics, Computer Science and many applications. We are primarily concerned with discrete which transform a finite set into another finite set . We discuss here the basic properties of functions, several types and their applications.

2.4 Recapitulation of Relations

Ordered Pair: An ordered pair is a pair of entries whose components occur in a specific order. Two ordered pairs are equal if their corresponding elements are equal.

Example:1. Find the value of x and y if $(x + 2, 4) = (5, 2x + y)$.

Solution: By the definition of ordered pair we can write

$x + 2 = 5$ and $2x + y = 4$ after solving of these equations we got $x = 3$ and $y = -2$.

Cartesian Product:

It is defined as the set of all ordered pair (p, q) of two non- empty sets P and Q where $p \in P, q \in Q$ and

it is represented by P × Q.

We can write symbolically it;P × Q = {(p, q): p ∈ P and q ∈ Q}.

Example:2. Find the Cartesian product of P and Q, if P = {1, 2, 3} and Q = {a, b, c}.

Solution: Given here P = {1, 2, 3} and Q = {a, b, c}

So,P × Q = {(1, a),(1, b),(1, c),(2, a),(2, b),(2, c),(3, a),(3, b),(3, c)}

And Q × P = {(a, 1),(a, 2),(a, 3),(b, 1),(b, 2),(b, 3),(c, 1),(c, 2),(c, 3)}.

Note:

1. $P \times Q = \emptyset \iff P = \emptyset \text{ or } Q = \emptyset$

2. $P \times Q \neq \emptyset \text{ iff } P \neq \emptyset \text{ and } Q \neq \emptyset$

3. In general, $P \times Q \neq Q \times P$

4. $P \times Q = Q \times P \iff P = Q$

5. If either P or Q is an infinite set then $P \times Q$ is an infinite set.

6. $P \times P$ can be represented by P^2.

Working Rule: To write down P × Q, take first element a_1 of P and then write all ordered pairs having first component a_1 and second component, the elements of Q. Again take second element a_2 of P and write all ordered pairs having first element a_2 and second components, the elements of Q. In similar way write all the ordered pairs.

Relation: Let P and Q be two non – empty sets. Then a Relation R from a set P to Q is a of $P \times Q$, i.e., $R \subseteq P \times Q$

or R = {(x, y): x∈ $P, y \in Q$}.

Working Rule: Let P and Q be two non empty sets. A set R of order pairs will be a relation from P to Q if first component of each element of R belongs to P and second component belongs to Q.

Example:3. If A = {1, 2, 3} and B = {4, 5, 6} then which of the following is a relation from set A to set B? Give reason:

a. $R_1 = \{(1, 5), (2, 4), (3, 5)\}$

b. $R_2 = \{(4, 1), (2, 6), (5, 1), (2, 4)\}$

Solution: $A \times B = \{1,2,3\} \times \{4,5,6\}$

$= \{(1, 4),(1, 5),(1, 6),(2, 4),(2, 5),(2, 6),(3, 4),(3, 5),(3, 6)\}$

a. Here $R_1 \subseteq A \times B$ because first element of each ordered pair is the element of set A and second element of each ordered pair is the element of set B. Hence, R_1 is a relation from set A to set B.

b. Here R_2 is not a relation from set A to set B because ordered pair (4, 1), (5, 1) does not belongs to set $A \times B$.

Number of Relations:

Let A and B are two non – empty sets and they have m and n elements respectively.

No. of elements in $A \times B = mn$

$\Rightarrow$ No. of subsets in $A \times B = 2^{mn}$

$\therefore$ No. of relations from A to B = 2^{mn}

Domain, Co-domain and Range of a Relation:

Domain: Let R be a relation from set P to set Q, then domain of R is the set of all those element $p \in P$ such that $(p, q) \in R$. it is denoted by Dom. (R).

Symbolically: Dom. (R) = $\{p \in P: (p, q) \in R\}$.

Range: Let R be a relation from set P to set Q, then range of R is the set of all those element $q \in Q$ such that $(p, q) \in R$. it is denoted by Range (R).

Symbolically: Range (R) = $\{q \in Q: (p, q) \in R\}$.

Co-domain: Let R is a relation from set P to set Q, then set Q is called the co-domain of R.

In general, if $(p, q) \in R$, then p is called the domain of R and q is called range of R.

i.e. Dom. (R) ⊆ P and Range (R) ⊆ Q.

Working Rule: To find the domain or range of a relation, we proceed as follows:

Step 1: Write R as a set of ordered pair.

Step 2: Dom. (R) = set of first coordinates of all ordered pairs element of R.

Step 3: Range (R) = set of second coordinates of all ordered pairs element of R.

Example:4. Let A = {1, 2, 3, 7} and B = {3, 6}. Defined a relation on set A to set B such that a < b where a ∈ A and b ∈ B. Find domain, co-domain and range of relation R.

Solution: The element of relation R = {(1, 3), (1, 6), (2, 3), (2, 6), (3, 6)}

So, Dom. (R) = {1, 2, 3}

Range (R) = {3, 6}

Co-domain (R) = {3, 6}

Note: 1. Domain R contains only those elements of P which are related to Q by the relation R. Similarly, Range of R consist of those element of Q which are related to P by the relation R. Therefore,

Dom. (R) ⊆ P and Range (R) ⊆ Q.

2. Relation can be written as the subset of ordered pairs.

2.5 Types of Relations

1. Reflexive Relation: A relation R defined in the set P is called the Reflexive Relation if

$(a, a) \in R, \forall\, a \in P\ i.e.\ aRa, \forall\, a \in P$. i.e., if P = {a, b}, then the reflexive relation in P is the set $\{(a, a), (b, b)\}$.

Example:

1. The relation “Equal to” is a reflexive because all numbers are equal to them self.

2. The relation “Parallel to” in the set of straight lines in a plane is a reflexive relation, i.e. the relation ${}_xR_y$ defined by x ⫴ y is a reflexive relation because all lines parallel to them self.

2. Symmetric Relation: A relation R defined in the set P is called Symmetric Relation if$(a, b) \in R \Rightarrow (b, a) \in R$.

i.e. if P= {a, b}, then the Symmetric Relation in P is the set $\{(a, b), (b, a)\}$.

Example:

1. The relation “Equal to” is symmetric because if x = y, then y = x.

2. The relation “Parallel to” in the set of straight lines in a plane is a symmetric relation, i.e. the relation ${}_xR_y$ defined by x ⫴ y is symmetric relation because first line is parallel to second line then second line will also parallel to first.

3. The relation “perpendicular to” in the set of straight lines in a plane is a symmetric relation, because first line is perpendicular to second line then second line will also perpendicular to first line.

3. Anti-Symmetric Relation: A relation R defined in the set P is called Symmetric Relation if $(a, b) \in R$ and $(b, a) \in R \Rightarrow a = b \ \forall\, a, b \in P$.

Example:

1. R_1 = {(1, 2), (2, 2), (2, 3)} on P = {1, 2, 3} is an anti-symmetric relation.

2. R_2 = {(x, y) ∈ R: x ≤ y} is an anti-symmetric relation on R since x ≤ y and y ≤ x ⇒ x = y, then

(x, y)∈ R and (y, x) ∈ R ⇒ x = y.

4. Transitive Relation: A relation R defined in the set P is called transitive if$(a, b), (b, c) \in R \Rightarrow (a, c) \in R$. i.e., if P = {3, 5, 8}, then the transitive relation in P is the set $\{(3,5), (5,8), (3,8), (5,5)\}$.

Example:

1. The relation "Equal to" is transitive because if $x = y$ and $y = z$, then $x = z$.

2. The relation "Parallel to" in the set of straight lines in a plane is a transitive relation, i.e. the relation ${}_xR_y$ defined by x ⫴ y is transitive relation because first line is parallel to second line and second line is parallel to third line then first line will also parallel to third line.

3. The relation "perpendicular to" in the set of straight lines in a plane is a symmetric relation, because first line is perpendicular to second line and second line is perpendicular to third line then first line will also perpendicular to third line.

Equivalence Relation:

A relation R defined in the set P is called equivalence if R is reflexive, symmetric and transitive.

i.e. R is an equivalence relation on P if it has the following three properties:

i. ${}_xR_x \; \forall \; x \in P$ (Reflexive).

ii. ${}_xR_y \Rightarrow {}_yR_x \forall \; x, y \in P$ (Symmetric).

iii. ${}_xR_y, {}_yR_z \Rightarrow {}_xR_z \; \forall \; x, y, z \in P$ (Transitive).

Example:5. Let R is a relation on Z, defined by R = {(x, y): x-y is an even number}. Prove that R is an equivalence relation.

Solution: (1) Let x∈ Z, then

x – x = 0

‘0’ is even number.

⇒ R ∀ x ∈ Z

⇒ R is Reflexive …(1)

(**2**) Let (x, y) ∈ R, ∀ x, y ∈ Z

⇒ x – y is even

⇒ -(x – y) is even

⇒ y – x is even

⇒ (y, x) ∈ R

⇒ R is symmetric …..(2)

(3) Let(x, y), (y, z)∈ R, ∀ x, y, z ∈ Z

⇒ (x - y) and (y - z) are even number

⇒ [(x - y) + (y - z)] is an even number

⇒ (x - z) is an even number

⇒ (x, z) ∈ R

⇒ R is transitive …(3)

Hence from (1), (2) and (3) R is an equivalence relation.

Identity Relation:

A relation R defined in the set P is called identity relation if

$$R = \{(p, p): p \in P\}.$$

Example: P ={a, b, c}, then the identity relation in P is the set$\{(a, a), (b, b), (c, c)\}$.

Empty Relation:

A relation R defined in the set P is called Empty relation or Void relation if $R = \emptyset$.

For example, let, $P = \{2, 3, 5, 7, 10\}$ and let R be a relation defined as "is cube of" is void relation and we can see that $R = \emptyset \subseteq P \times P$.

Partial Order Relation:

A Relation R defined in the set P is called partial order if R is reflexive, anti - symmetric and transitive.

Example: Let $P = \{1,2,3\}$ then we define relation $R = \{(1,1), (2,2), (3,3), (1,2)(2,3), (1,3)\}$ is a partial order relation because it is reflexive, anti - symmetric and transitive.

Partial Order Set:

The set P, with the partial order relation R is called partial order set.

Example: in the set of real numbers, the relation of "less than or equal to" is a partial order relation. So, $(R, \leq)$ is a partial order set.

Total Order Relation:

A partial order relation R in the set P is called total order relation if for every element $p_1, p_2 \in P$ s.t. either $p_1 R p_2$ or $p_2 R p_1$ *or* $p_1 = p_2$.

To Set:

A set with total order relation is called To Set.

Example: the set of integers with "less than or equal to" is To Set.

SOLVED EXAMPLES

Example.6: - Let P = {2, 3, 4} and Q = {3, 4, 5}. List the element of each relation R defined below and find the domain and range of R:

i. p ∈ P is related to q ∈ Q i.e. ${}_pR_q$ iff p < q.

ii. p ∈ P is related to q ∈ Q i.e. ${}_pR_q$ if p and q are both odd numbers.

Solution: i. 2∈ P is less than 3 ∈ Q, then ${}_2R_3$.

Similarly, ${}_2R_4$, ${}_2R_5$, ${}_3R_5$, ${}_4R_5$.

Therefore,

R = {(2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)}

Domain (R) = {2, 3, 4}

Range (R) = {3, 4, 5}

ii. Since 3 ∈ P and 3 ∈ Q both are odd then ${}_3R_3$. Similarly, ${}_3R_5$ therefore

R = {(3, 3), (3, 5)}

Domain (R) = {3}

Range (R) = {3, 5}

Example.7: If R be a relation in the set of integers Z, defined by

R = {(a, b): a∈ Z, b ∈ Z, (a - b) is divisible by 6}, then prove that R is an equivalence relation.

Solution: (1) Let a∈ Z, then

a – a = 0

‘0’ is divisible by 6.

$\Rightarrow R\ \forall\ a \in Z$

$\Rightarrow$ R is Reflexive …(1)

(**2**) Let $(a, b) \in R, \forall\ a, b \in Z$

$\Rightarrow a - b$ is divisible by 6

$\Rightarrow$ - (a - b) is divisible by 6

$\Rightarrow b - a$ is divisible by 6

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

$\Rightarrow$ R is symmetric. …(2)

(3) Let $(a, b), (b, c) \in R, \forall a, b, c \in Z$

$\Rightarrow$ (a - b) and (b - c) are divisible by 6

$\Rightarrow$ [(a - b) + (b - c)] are divisible by 6

$\Rightarrow$ (a - c) are divisible by 6

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

$\Rightarrow$ R is transitive …(3)

Hence from (1), (2) and (3) R is an equivalence relation.

Example.8: Let R_1 and R_2 be two equivalences on A. Show that $R_1 \cap R_2$ is also an equivalence relation

on A.

Solution: Let R_1 and R_2 be two equivalence relations on A.

Then $R_1 \subseteq A \times A$, $R_2 \subseteq A \times A \Rightarrow R_1 \cap R_2 \subseteq A \times A$

$\Rightarrow R_1 \cap R_2$ is a relation on A

i. Reflexivity: Given R_1 and R_2 are reflexive

$\Rightarrow (a, a) \in R_1$ and $(a, a) \in R_2 \quad \forall\, a \in A,$ (R_1 and R_2 are reflexive)

$\Rightarrow (a, a) \in R_1 \cap R_2 \forall a \in A$

$\Rightarrow R_1 \cap R_2$ is reflexive on A (1)

ii. Symmetricity:

Let $(a, b) \in R_1 \cap R_2$ be arbitrary

$\Rightarrow (a, b) \in R_1$ and $(a, b) \in R_2$

$\Rightarrow (b, a) \in R_1$ and $(b, a) \in R_2$ (R_1 and R_2 are symmetric)

$\Rightarrow (b, a) \in R_1 \cap R_2$

$\Rightarrow R_1 \cap R_2$ is symmetric

$R_1 \cap R_2$ is symmetric on A (2)

iii.Transitivity:

Let $(a, b) \in R_1 \cap R_2$ and $(b, c) \in R_1 \cap R_2$

Then $(a, b), (b, c) \in R_1$ and $(a, b), (b, c) \in R_2$

$\Rightarrow$ (a, c) $\in R_1$ and (a, c) $\in R_2$ (R_1 and R_2 are transitive)

$\Rightarrow$ (a, c) $\in R_1 \cap R_2$

$\Rightarrow R_1 \cap R_2$ is transitive on A (3)

Hence from (1), (2) and (3) $R_1 \cap R_2$ is an equivalence relation on A.

Check your progress report

Q.1. Define relations with examples.

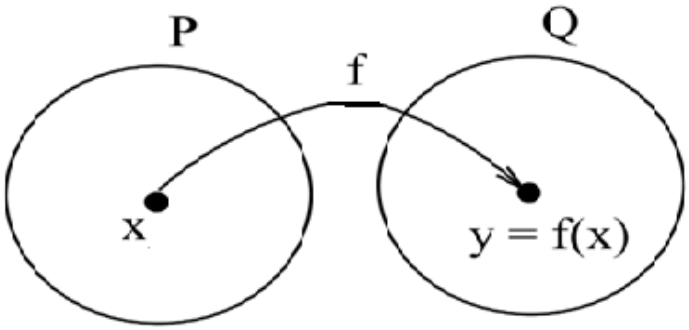
Q.2. What do you mean by partial order relation?

Q.3. Explain the concept of equivalence relation.

Q.4. Define domain, co-domain and range of a relation.

2.6 Function or Mapping

Let P and Q be non-empty sets, then a rule correspondence, which associates each element of set P to a unique element of set Q, is called Function or Mapping from P to Q. If **f** is a function from set P to set Q; then we write $\boldsymbol{f}: \boldsymbol{P} \rightarrow \boldsymbol{Q}$ and read as **f** is a function from P to Q or **f** maps P to Q.



It should be noted that, if **f** associates $x \in P \; to \; y \in Q$, then y is called the image of element x under the mapping **f,** denoted by f(x). Similarly, element x is called the Pre-image of x under mapping **f.**

i.e. $x = f^{-1}(y)$

Thus, we conclude that for a function **f** from P to Q, we get

1. Both set P and Q should be non – empty.

2. Each element of P should have an image in Q.

3. No any elements of P have more than one image in Q.

Remarks:

a) Every function should be a relation but converse need not be true.

b) A relation will be a function only when for each $x \in P$ there exist one and only one element in Q.

c) Sometimes a mapping $\boldsymbol{f}: \boldsymbol{P} \rightarrow \boldsymbol{Q}$ can be written as **y = f(x)** and read **y** is function of x.

d) If mapping $\boldsymbol{f}: \boldsymbol{P} \rightarrow \boldsymbol{Q}$**,** then a single element in P can`t have more than one image in Q, however two or more element in P may have same image in Q.

e) Every element in P have its image in Q, but every element in Q may not have its pre image in P.

f) To each element x in P there exist a unique element in Q, such that y = f(x). This unique element y called the value of **f** at x (the image of x under **f**).

Working Rule:

Let $\boldsymbol{f}: \boldsymbol{P} \rightarrow \boldsymbol{Q}$ be a function such that y = f(x), $\forall\ x \in P\ and\ \forall\ y \in Q$, then following statement are equivalent:

Step 1: f is function of x on y.

Step 2: y is a function of x.

Step 3: y is the image of x under the mapping **f.**

Step 4: x is the pre-image of y under the mapping **f.**

Step 5: $y \in Q$, which is associated to x under the mapping **f** represented by f(x) is the value of **f** at x.

Example: 9. Let $P = \{1, 2, 3\}$ and $Q = \{4,5\}$. Define a function **f** such that

$\boldsymbol{f} = \{(1,4), (1,5), (2,4), (3,5)\}$. $Is\ \boldsymbol{f}\ a\ function$ from P to Q?

Solution: Since two ordered pair pairs $(1,4)\ and\ (1,5)$ in $\boldsymbol{f}$ have the same first component, $\boldsymbol{f}$ is not a function from P to Q.

Example:10. Let $P = \{1,2,3,4\}$ and $Q = \{1,6,8,11,15\}$. Define a function **f** such that

$\mathbf{f} = \{(1,1), (2,6), (3,8), (4,8)\}$. Is **f** a function from P to$Q$?

Solution: Yes, $\boldsymbol{f}$ is a function from P into Q because each element of P there corresponds exactly one element of Q.

Domain, Co-domain and Range of Function:

Let $f: P \to Q$ is a function, then

- Set P is called the domain of function **f.**
- Set Q is called the co-domain of function **f.**
- The set of elements of set Q which are the **f**-images of all the elements of P, is called the range of **f.** It is denoted by f (P).

f (P) = {f (x) $\in Q: x \in P$}

Therefore, f(P) =Q or f(P) $\subseteq$ Q.

Example:11. Let A = {-2, -1, 0, 1, 2} and B the set of whole numbers for every x ∈A and

f(x) ∈ B such that f (x) = x^2, then find domain, co-domain and range of function **f**.

Solution: Here A is the domain and B is co-domain of the function f. The value of **f**(x), x ∈ A is the range of f.

So, when x = -2, f(-2) = $(-2)^2$ = 4

When x = -1, f(-1) = $(-1)^2$ = 1

When x = 0, $f(0) = (0)^2 = 0$

When x = 1, $f(1) = (1)^2 = 1$

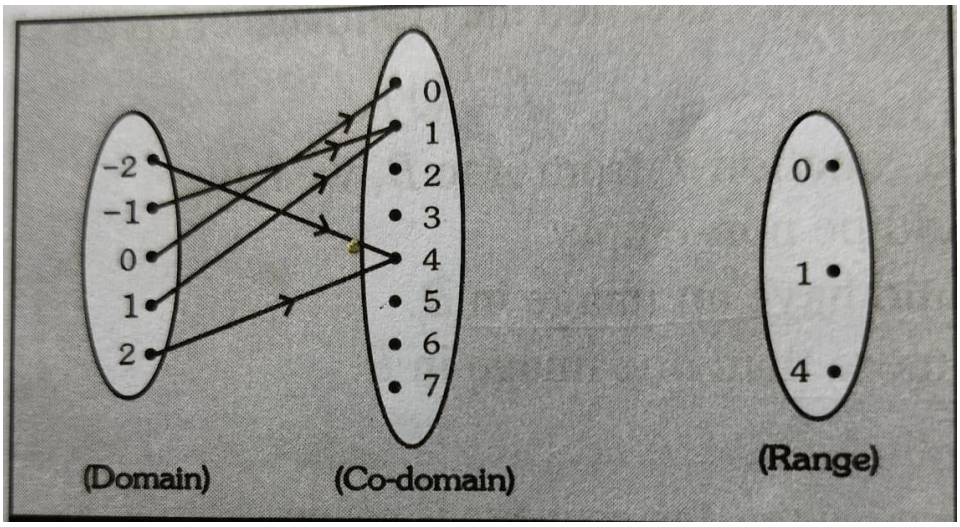
When x = 2, $f(2) = (2)^2 = 4$

Hence,

domain of f = Dom. (f) = {-2, -1, 0, 1, 2} = A

Co-domain of f = {0, 1, 4, …….}

range of f = {0, 1, 4}



Types of Functions:

The functions can be different types. These functions are important in mathematics as well as in many applications of computer science.

1. One – one Function:

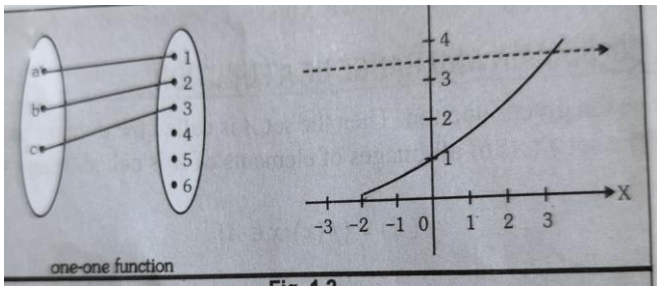
A function **f : P → Q** is said to one – one iff different elements of **A** have different images.

Symbolically**,** a function **f : P→ Q** is said to be one – one if

$f(x_1) = f(x_2)$

$\Rightarrow \quad x_1 = x_2 \quad \forall\, x_1, x_2 \in \mathbf{P}$

i.e. A mapping f : P→ Q is such that each element in P has only one image in Q and every image in Q have only one pre-image in P, then f is called one – one function.



Note- one – one function is also known as injective function.

Example : Let A = {1, 2, 3}, B = {*a*, b, c, d} and let f (1) = *a*, f (2) = b, f (3) = d.

Then f is one – one since the different elements (1, 2, 3) of A are assigned to the different elements (a, b, d) in B respectively.

Example : Let f (x) = 3x-1, then f is one – one because if

$f(x_1) = f(x_2)$

$\Rightarrow \quad 3x_1 - 1 = 3x_2 - 1$

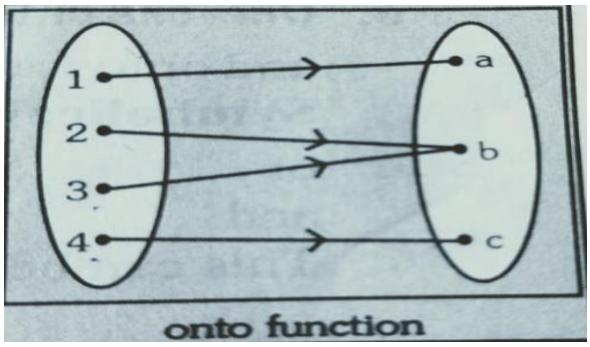
$\Rightarrow \quad x_1 = x_2$

Example : Let f :R→R be defined by f (x) = 2x + 9, $x \in R$, then f is one-one function because every member of R belong in the range of f.

1. Onto function (Surjective Function):

A function, $f: P \to Q$ is said to be an onto function if there is no any element in Q which is not the image of some element of P.

i.e., every element of Q appears as the image of at least one element of P.



Note- The onto function is also known as Surjective function.

Example 12: Let P = {-1, 1, 2}, Q = {1, 16} and f : P→ Q be a function defined by f (x) = x^4. Show that f is onto.

Solution: Given that f: P→ Q and f (x) = x^4

⇒ f (-1)=$(-1)^{4=1}$

⇒ f (1) = $(1)^4$ = 1

⇒ f (2) = $(2)^4$ = 16

Here, it is clear that,

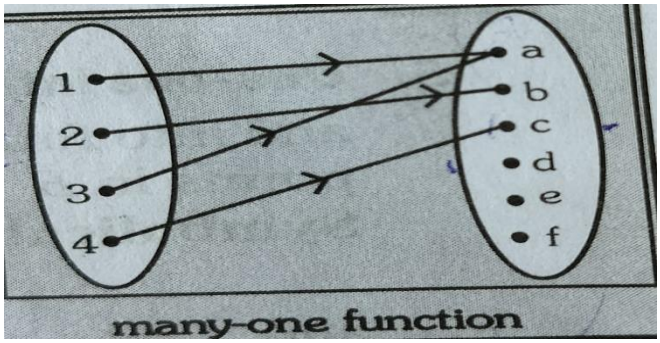
- 1 and -1 are the inverse image of 1
- 2 is inverse image of 16 and there is no element in Q

Which has no pre-image in P.

Hence, f is onto function.

2. Many-one function:

Definition: A function $f: P \rightarrow Q$ is called many one function, if at least one element of co-domain Q has two or more than two pre-images in domain P.



Example:13. Let $f: Z \rightarrow Z$ be defined by $f(x) = x^2, for\ all\ \ x \in Z$ then show that f is many one.

Solution: Given that,$f(x) = x^2, for\ all\ \ x \in Z,$

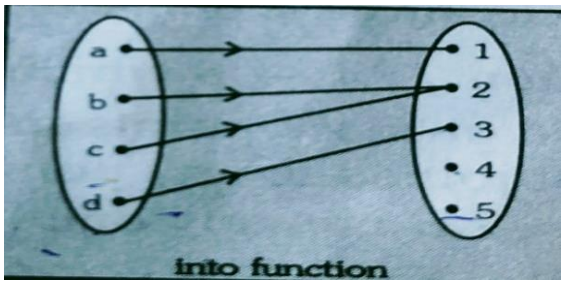
$\Rightarrow$ $f(1) = (1)^2 = 1$

and $f(-1) = (-1)^2 = 1$

Thus we find $f(1) = f(-1) = 1$ which shows that two distinct number -1, 1 are assigned to the same number 1 1 under f, therefore f is many onto function.

3. Into function:

A function $f: P \to Q$ is called into function, if there is at least one element of set Q which has no pre-image in set P.

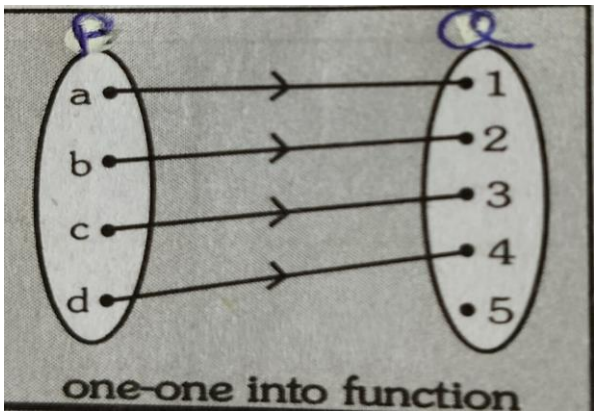


i.e. the range of f is proper subset of co-domain of f.

Symbolically: A function $f: P \to Q$ will be into if f (p) is subset of set q.

4. One – one into function:

A function $f: P \to Q$ is called one – one into function if it is both one – one and into function. i.e. the distinct point in P are joined to distinct point in Q and there are some points in Q which are not joined to any point of P.



i.e. A function $f: P \to Q$ is called one – one into function if

f (P) is subset of Q and $f(x_1) = f(x_2)$

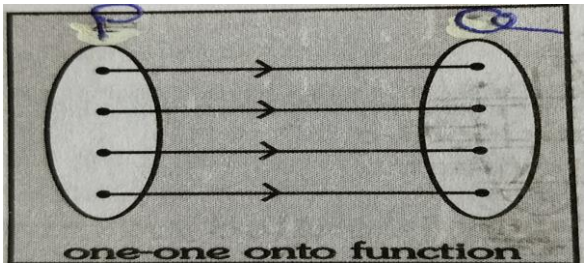
$\Rightarrow x_1 = x_2 \quad \forall\, x_1, x_2 \in P$

and $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \ \forall\ x_1, x_2 \in P$

Note- For one - one into function Range ⊆ co-domain

5. One – one onto function:

A function $f: P \to Q$ is called one – one onto function if it is both one – one and onto function. i.e. the distinct point in P are joined to distinct point in Q and no point in Q is left vacant.



i.e. $f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \quad \forall\ x_1, x_2 \in P$.

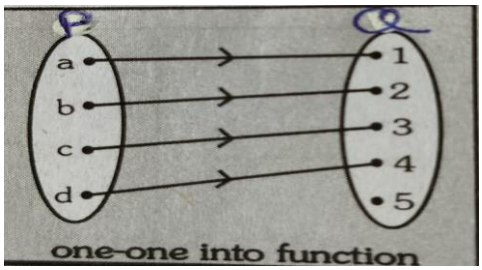
or $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \quad \forall\ x_1, x_2 \in P$

and $f(P) = Q$

Note: One – one onto mapping is also known as bi-jective or one to one mapping\function.

6. Many – one into function:

A function $f: P \to Q$ is called many – one into function if it is both many – one and into function. i.e. two or more points in P are joined to same point in Q and there are some points in set Q which are joined not to any point of set P.



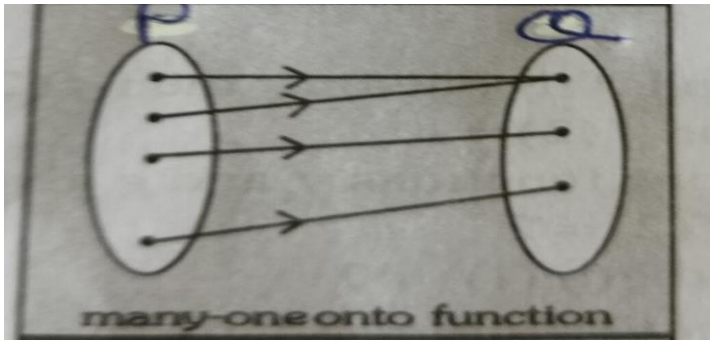
i.e. A function $f: P \to Q$ is called many – one into function if

$f(x_1) = f(x_2) \Rightarrow x_1 \neq x_2 \ \forall\ x_1, x_2 \in P$.

and f (P) is subset of Q.

7. Many – one onto function:

A function $f: P \to Q$ is called many – one into function if it is both many – one and onto function. i.e. in Q one point is assigned to at least one point in P and two more points in P are assigned to the same point Q.



i.e. A function $f: P \to Q$ is called many – one and onto function

if f (x_1) = f (x_2) $\Rightarrow x_1 \neq x_2 \quad \forall \quad x_1, x_2 \in P$

and f (P) = Q.

Working Rule:

1. Checking for injectivity of a function:

Step 1 – Let f (x_1) = f (x_2), $\forall\ x_1, x_2 \in P$.

Step 2 –On solving f (x_1) = f (x_2), if we get $x_1 = x_2$ then function $f: P \to Q$ is one – one.

2. Checking for Surjectivity of a function:

Step 1: Let $y \in Q$.

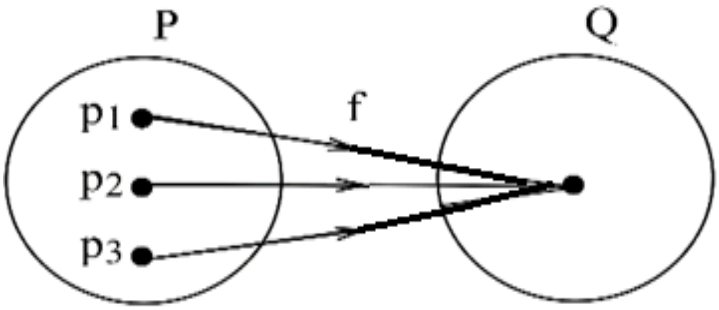
Step 2: Put f (x) = y

Step 3: Solve f (x) = y for x and obtain x in terms of y.

Step 4: Get the equation of the x = g (y). If x = g (y) belongs to domain of f for all values of y, the f is onto.

Constant Function:

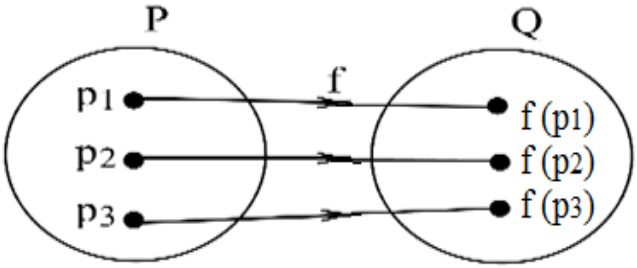
f is said to be constant function if the range of f is singleton set.



Example: Let P = {a, b, c}, Q = {1, 2, 3} and a function $f: P \to Q$ defined by f (x) = 2,$\forall\ x \in P$ is an example of constant function.

Identity Function:

A function, $f: P \to P$ is said to be identity function if there exits an element $p \in P$ such that $f(p) = p$ for $p \in P$. Here, domain of f is P and range of the function of f is Q.



Absolute value function:

A function, $f: R \to R$ is said to be **Absolute value** function if it is defined as

$f(p) = |p| = \begin{cases} p \geq 0 \\ -p < 0 \end{cases}$. Here, domain of$f$ is R and range of the function f is the set of all none negative function.

Equal Function:

Let f: X→ Y and g: X → Y are two maps. Then the mappings f and g are said to be equal iff

f (x) = g(x) $\qquad\qquad \forall\ x\ \in X$

and this relationship is expressed by writing f = g. In case of equal maps, the domains of mapping are the same.

Invertible Function:

Let f: P→Q is a one – one onto function. Then f^{-1}: Q → P is called the inverse mapping or inverse function of 'f'.

Symbolically: If f: P → Q is a mapping such that

f (P) = Q

then f^{-1}: Q → P is given by f^{-1} (Q) = P

In the form of ordered pair, it can be defined as follows;

If f = {(x, y): x ∈ P, y ∈ Q}

Then f^{-1} = {(y, x): x ∈ P, y ∈ Q }.

Theorem 1: If f: A → B is one – one and onto then f is invertible.

Proof: Let f: A → B is a one – one onto mapping and y ∈ B then ∃ a unique x ∈ A such that

y = f (x) (since f is one – one onto)

define g: B → A such that g (y) = x

then gof[x] = g [f(x)] =g (y)

= x= I_A(x) (since f (x) = y)

⇒ gof = I_A

Similarly, (fog)[y] = f[g(y)] = f (x) (since g (y) = x)

= y= I_B(y)

fog = I_B

Hence, f is invertible and f^{-1} = g

Theorem: Every invertible function has a unique inverse.

Proof: Let f: A → B is an invertible function i.e., f is one – one and onto mapping.

Let if possible there exists two inverse g_1 and g_2 of f.

Then $(fog_1) = I_B$ and $(fog_2) = I_B$

$\Rightarrow (fog_1)(y) = (fog_2)(y) = I_B(y)$

$\Rightarrow f\{g_1(y)\} = f\{g_2(y)\}$

$\Rightarrow g_1(y) = g_2(y)$

$\Rightarrow g_1 = g_2$ ($\therefore$ f is one one)

Hence, inverse of f is always unique.

Example:14. If the function f: R → R, defined by $f(x) = x^2$, then find $f^{-1}(9)$ and $f^{-1}(-9)$.

Solution: Given that $f(x) = x^2$ and function f is R → R

$\Rightarrow f^{-1}(9) = \{x \in R: f(x) = 9\}$

$\Rightarrow = \{x \in R: x^2 = 9\}$

$\Rightarrow = \{x \in R: x = \pm 3\}$

$\Rightarrow = \{+3, -3\}$

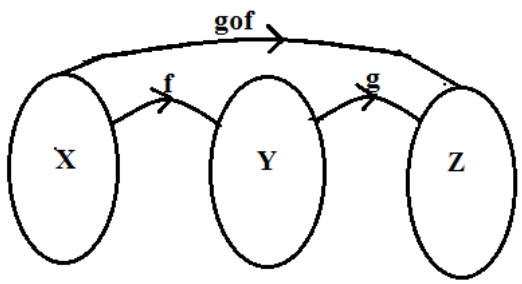
And $f^{-1}(-9) = \{x \in R: f(x) = -9\}$

$\Rightarrow = \{x \in R: x^2 = -9\}$

$\Rightarrow = \{x \in R: x = \pm 3\sqrt{-1} = \emptyset\}$ ($\pm 3\sqrt{-1}$ is not a real number)

Finally, $f^{-1}(9) = \{3, -3\}$ and $f^{-1}(-9) = \emptyset$.

Composite Function or Product of Function:

Let f : X → Y and g : Y → Z are any two maps. Then we define a map gof : X → Z by the formula $(gof)(x) = g[f(x)] \ \forall \ x \in X$	

Example 15: Let the two maps f : R → R and g : R → R, defined by fog(x) = $sinx^2$ and

gof(x) = $\sin x^2$.

Find the value of $f(x)$ and $g(x)$

Solution: We have

$(fog)(x) = sinx^2$ ⇒ $f\big(g(x)\big) = \sin x^2$.

And gof(x) = $\sin x^2$. ⇒ $g\big(f(x)\big) = (sinx)^2$

From above , it is clear that

f(x)=sin x and $g(x) = x^2$

It is clear that these values of f(x) and g(x) satisfies (1) and (2).

Example.16: Let $f: R \to R$ and $g: R \to R$ be defined by $f(x) = x^2 + 3x + 1$, $g(x) = 2x - 3$. Find fog and gof.

Solution: We can find

$(fog)(x) = f\big(g(x)\big) = f(2x-3) = (2x-3)^2 + 3(2x-3) + 1 = 4x^2 - 6x + 1$

and $(gof)(x) = g\big(f(x)\big) = g(x^2 + 3x + 1) = 2(x^2 + 3x + 1) - 3 = 2x^2 + 6x - 1.$

Solved examples

Example.17: Let $f: R \to R$ be defined by $f(x) = 3x + 4$. Show that f is invertible and find the $f^{-1}: R \to R$.

Solution: we have given that, $f(x) = 3x + 4, x \in R$. $\boldsymbol{f(x)}$ **is one-one**, then we can write, $f(x_1) = f(x_2)$, $\Rightarrow 3x_1 + 4 = 3x_2 + 4 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2$

Which reflect that f is one-one.$f(x)$ is onto: $k \in R, f(x) = k \Rightarrow 3x + 4 = k$

$$\Rightarrow x = \frac{(k-4)}{3} \in R$$

We have, $f\left(\frac{(k-4)}{3}\right) = k$, hence $f(x)$ is an onto function and so $f(x)$ is an invertible function, then we can find out the inverse of the function. We can easily see that,

$f\left(\frac{(k-4)}{3}\right) = k, k \in R$

$= f^{-1}(k) = \left(\frac{(k-4)}{3}\right)$, for every $k \in R$

For every $x \in R$, $f^{-1}(x) = \left(\frac{(x-4)}{3}\right)$

Example.18: In each of the following cases, state whether the function is onto, one- one or bijective. Justify your answer.

(i) $f: R \to R$ defined by $f(x) = 3 - 4x$.

(ii) $f: R \to R$ defined by $f(x) = 1 + x^2$.

(iii) $f: N \to N$ defined by $f(x) = \begin{cases} \frac{n+1}{2} if\ n\ is\ odd \\ \frac{n}{2} if\ n\ is\ even \end{cases}$

Solution: (i) First, we will prove that, $f: R \to R$ is one-one function, for this $f(x) = f(y) \Rightarrow 3 - 4x = 3 - 4y \Rightarrow x = y$. It means that f is one –one and given that $y \in R, \frac{3-y}{4} \in R$

Such that, $f\left(\frac{3-y}{4}\right) = y \Rightarrow f$ is onto function and it is also bijective function.

(ii) It is given that $f: R \to R$ defined by $f(x) = 1 + x^2$ and if we take by $1, -1 \in R$, then$f(1) = f(-1) = 2$, so$f$ is not one-one and so f is not onto function similarly f is not bijective function.

(iii) If we choose, $3,4 \in N$ and obviously $3 \neq 4$ but $f(3) = f(4) = 2$. So f is not one-one. Therefore f is not bijective.

Example.19: Let $A = \{1,2\}$. Find all one - one function from $A\ to\ A$.

Solution: We suppose that, $f: A \to A$ is one to one function and $f(1)$ has two choices namely, 1 or 2. Therefore $f(1) = 1\ or\ f(1) = 2$.

Condition 1: When $f(1) = 1$. As $f: A \to A$ is one-one. Therefore, $f(2) = 2$. Thus $f(1) = 1$ or $f(1) = 2$.

Condition 2: When $f(1) = 2$. Since $f: A \to A$ is one-one. Therefore, $f(2) = 1$. Thus $f(1) = 1$ and $f(2) = 1$. So there are two one-one functions say f and g from $A\ to\ A$ given by

$f(1) = 1, f(2) = 2$ and $g(1) = 2$ and $f(2) = 1$.

Example.20: Show that the function $f: A \to A$ given by $f(x) = ax + b$, where $a, b \in R, a \neq 0$ is a bijection.

Solution: First, we will prove that, $f: R \to R$ is one-one function, for this $f(x) = f(y) \Rightarrow ax + b = ax + b \Rightarrow x = y$. So $f: A \to A$ is an injective function.

Subjectivity: If we choose, $y \in R$, then $f(x) = y$ thus, $ax + b = y \Rightarrow x = \frac{y-b}{a} \in R(Domain)$for all $y \in R(Co - domain)$ such that

$f(x) = f\left(\frac{y-b}{a}\right) = a\left(\frac{y-b}{a}\right) + b = y$. So $f(x)$ is surjective

Example.21: Show that $f: N \to N$ defined by

$f(x) = \begin{cases} \frac{n+1}{2} if\ n\ is\ odd \\ \frac{n}{2} if\ n\ is\ even \end{cases}$ is a many –one onto function.

Solution: We see that, $f(1) = \frac{1+1}{2}$=1 and $f(2) = 1$.

Here, we can see that if we choose, $1,2 \in N$ and obviously $1 \neq 2$ but $f(1) = f(2) = 1$. So f is many one function.

Surjectivity: If n is an odd natural number, then $(2n-1)$is also odd natural number such that

$\boldsymbol{f(2n-1) = \frac{2n-1+1}{2} = n.}$

If n is an even natural number, then $(2n)$is also even natural number such that

$\mathbf{f(2n) = \frac{2n}{2} = n.}$

Thus, every element $n \in N$(whatever even or odd) there exits its pre –image in N. So**f** is a surjective. Hence f is many –one onto function**.**

Example.22: Let $f = \left\{\left(x, \frac{x^2}{1+x^2}\right) : x \in R\right\}$ be a function from R to R. Determine the range of f.

Solution: it is given that,$f: R \to R$ is a function, such that $f(x) = \frac{x^2}{1+x^2}$

We Suppose that, $f(x) = y$, then $x^2 = y(1+x^2)$

$$x = \pm\sqrt{\frac{y}{1-y}}$$

Since, $x \in R$, $\frac{y}{1-y} \geq 0$ and $(1-y) \neq 0$. We find that $y \geq 0$, $y \neq 1$ and$(1-y) > 0$. Therefore, $0 \leq$

$y < 1$ and the range of f is $y \in [0,1)$.

2.7 Summary

This units includes concepts like relations, partial order relations, equivalence relation, and functions. Group theory, which focuses on symmetry and patterns, originated in the 18th century with Lagrange, while Galois introduced groups to solve polynomial equations. In the 19th century, Cauchy, Jordan, Cayley, and Klein further developed the field by applying groups to geometry. By the 20th century, group theory became essential in physics, chemistry, cryptography, and computer science, helping explain atomic structures, quantum mechanics, and algebraic systems.

Set theory provides the foundation for most mathematical structures, while group theory plays a crucial role in understanding symmetry and transformations. Key topics include relations, types of relations, and functions, types of functions.

2.8 Terminal Questions

1. Let $f: A \to B$ and $g: B \to C$ be two functions such that $gof: A \to C$. Show that If gof is onto, then g is onto.

2. Show that the function Let $f: N \to N$ defined by $f(x) = x^2 + x + 1, x \in N$ is not invertible.

3. Let $f: Z \to Z$ defined by $f(x) = x + 1$. Find $g: Z \to Z$ such that $gof = I_z$.

4. If $f: R \to R$ defined by $f(x) = 6x + 1, x \in R$, show that the function f is one-one, onto.

5. Draw the graph of the function

$$f(x)\begin{cases} 1, x > 0 \\ 0, x = 0 \\ -1, x < 0 \end{cases}, x \in R.$$

6. If gof is one-to-one, then f is a one-to-one.

7. If gof is onto and g is one-to one, then f is onto.

8. Let $f: Z \to Z$ defined by $f(x) = 2x$. Find $g: Z \to Z$ such that $fog = I_Z$.

9. Let $A = \{a, b\}$. List all relations on A.

10. Let $A = \{a, b, c\}$ and let $B = \{1,2\}$. Find the number of relations from A to B.

11. Let $A = \{a, b\}$ and let $B = \{1,2,3\}$. Find the number of functions from A to B.

12. Let $A = \{a, b, c\}$ and let $B = \{1,2,3\}$. Find the number of onto functions from A to B.

13. Let $A = \{a, b, c\}$and let $B = \{1,2,3\}$. Find the number of into functions from A to B.

14. Let $A = \{a, b, c\}$ and let $B = \{1,2,3\}$. Find the number of one-one functions from A to B.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Malik, A.K., Singh, S. R. (2020). Topology, Dreamtech Press.

5. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

UNIT- 3: Introduction of Group Theory

Structure

3.1 Introduction

Group theory is one of most important fundamental concepts of modern algebra. Groups arise naturally in various mathematical situations. They have found wide applications in physical sciences and biological

sciences particularly in the study of crystal structure, configuration molecules and structure of human genes. The structure of a group is one of the simplest mathematical structures. Hence, group may be considered as the starting point of the study of various algebraic structures. Group theory is a branch of mathematics that studies patterns and symmetry in numbers, shapes, and equations. It started in the 18th century when Lagrange studied how numbers could be rearranged. Later, Galois introduced the idea of a "group" to help solve equations.In the 19th century, Cauchy, Jordan, and Cayley developed group theory further, and Klein used it to study geometry. In the 20th century, group theory became important in science and technology, helping in physics, chemistry, cryptography, and computers.

Today, group theory is widely used in both mathematics and real-world applications. In this unit, we will discuss the concept of binary operation, algebraic structure, group, abelian group, finite and infinite group and composition tables of finite groups.

3.2 Objectives

After studying this unit, the learner will be able to understand the:

- binary operations
- algebraic structure
- group, abelian group, semi group and monoid
- finite and infinite group
- Composition table of finite group

3.3 Binary Operation

A binary operation (*) on a non - empty set G also called a binary composition in the set G, if $\forall$ a, b ϵ G then a * b $\in$ G.

i.e. G is closed with respect to the operation denoted by (*). Examples are given below:

(i) Addition is a binary operation on the set R of real number as well as N of natural number.

(ii) Subtraction is a binary operation on R, since for difference of two real numbers is also real number.

(iii) Multiplication is a binary operation on the set of real number and natural number both.

Remark: Subtraction and Division may or may not be a binary operation on the set of natural number.

3.4 Algebraic Structure

A non-empty set, $A \neq \Phi$ which has one or more than one binary operation $(*)$ satisfies the closure property then it is called algebraic structure and it is represented by $(A, *)$. In place of *; we can take the symbols as$(A, +)$, $(A, -)$, $(A, \times)$ and $(A, \div)$.

Example 1: Let us suppose that N is a set of natural number then $(N, +)$ is algebraic structure because it is close with respect to addition if we choose any two number from this set and after adding these numbers the resulting number is also belong to the natural number. Numerically it can write, if $\forall\, a, b \in N, \text{then } a + b \in N$is called algebraic structure with respect to addition.

Justification: We take $1, 2 \in N$, then $1 + 2 = 3 \in N$, it means that it is closed with respect to addition, so $(N, +)$ is algebraic structure with respect to addition. In this similar way, $(N, \times)$ is an algebraic structure with respect to multiplication because natural number satisfies the closure property.$(N, -)$ and $(N, \div)$ are not algebraic structure with respect to subtraction and division. If we choose$1, 2 \in N$, then $1 - 2 = -1 \notin N$ it means that it is not close with respect to subtraction. Hence $(N, -q)$ is not algebraic structure with respect to subtraction. Similarly, if we choose$1, 2 \in N$, then $1 \div 2 = \frac{1}{2} \notin N$ it means that it is not close with respect to division. Hence $(N, \div)$ is not algebraic structure with respect to division. We have discussed algebraic structure on some other sets which is given below in the Table 1.

Table 1 - Information about algebraic structure on some operations

Set with operation	**Algebraic structure**
$(Z, +)$	Yes
$(Z, -)$	Yes

$(Z,\times)$	Yes
$(Z,\div)$	No
$(R,+)$	Yes
$(R,-)$	Yes
$(R,\times)$	Yes
$(R,\div)$	No

3.5 Group

Let A be a non-empty set and a binary operation denoted by (*), then the algebraic structure (A,*) is called Group, if the binary operation satisfies the following postulates-

1. **Closure axioms:** Let a, b be the elements of the set A. Then $\forall$ a,b$\in$ A , also a*b $\in$ A

2. **Associative axioms:** Let a, b and c be the elements of the set A. Then

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

3. **Existence of identity:** There exists an element e $\in$ A, called identity such that

$a * e = e * a = a \quad \forall\ a \in A$

4. **Existence of inverse:** For each element 'a' of A, there exists an element 'b' in A, such that

$b * a = e = a * b$

The element 'b' is then called the inverse of 'a'.

i. e. $b = a^{-1}$

or $a^{-1}a = e = aa^{-1}$

3.6 Abelian Group or Commutative Group

A group (A,*) is said to be abelian group if in addition of the above four postulates the following postulate is also satisfied.

5. **Commutative:** Let a and b are the two elements of the set A then

$a * b = b * a \quad \forall\ a, b \in A.$

Examples:

1. (Z, +), (Q, +), (R, +) are all commutative groups w. r. t. addition. Zero (0) is the identity and (- a) is the inverse of 'a' for all mentioned group.

2. $(Q_o,*)$, $(R_o,*)$ are commutative group w. r. t. multiplication 1 is the identity and 1/a (a^{-1}) are the inverse of 'a' in each case.

Note: Q_o is Q – {0} i.e., set of Rational Number excepting zero.

3. The set of all m x n matrices (real or complex) with matrix addition as a binary operation is a commutative group. The zero matrix is the identity element and the inverse of the matrix A is - A.

Note: A group consisting of the identity element alone is called a trivial group, other are called non – trivial groups.

Example 1: Show that the set $G = \{a + b\sqrt{2}: a, b \in Q\}$is a group with respect to addition.

Solution: Closure Property: Let x, y be any two elements of G. Then

$x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, where $a, b, c, d \in Q$

now, $x + y = (a + b\sqrt{2}) + (c + d\sqrt{2})$

$= (a + c) + (b + d)\sqrt{2}$

Since a + c and b + d are elements of Q, therefore $(a + c) + (b + d)\sqrt{2} \in G$.

Thus $x + y \in G \quad \forall\ x, y \in G$. Therefore, G is closed with respect to addition.

Associativity: The elements of G are all real numbers and the addition of real number is associative.

Existence of Left Identity: We have $0 + 0\sqrt{2} \in G$ since $0 \in Q$.

If $a + b\sqrt{2}$ is any element of G, then

$(0 + 0\sqrt{2}) + (a + b\sqrt{2}) = (0 + a) + (0 + b)\sqrt{2}$

$= a + b\sqrt{2}$

Therefore, $0 + 0\sqrt{2}$ is the left identity.

Existence of Left Inverse: We have

$a + b\sqrt{2} \in G \Rightarrow (-a) + (-b)\sqrt{2} \in G$

since $a, b \in Q \Rightarrow -a, b \in Q$.

Now, $[(-a) + (-b)\sqrt{2}] + [a + b\sqrt{2}] = [(-a) + a] + [(-b) + b]\sqrt{2}$

$= 0 + 0\sqrt{2}$

= the left identity.

$\therefore \Rightarrow (-a) + (-b)\sqrt{2}$ is the left inverse of $a + b\sqrt{2}$.

Hence G is a group with respect to addition.

Example 2: Show that the set of matrices

$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$, where α is a real number, forms a group under matrix multiplication.

Solution: Let G denote the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$, where $\alpha \in \mathbf{R}$. Here **R** is a real numbers.

To prove that G is a group with respect to matrix multiplication, we have to prove following axioms-

Closure Property: Let A_α, A_β be any two elements of G where $\alpha, \beta \in \mathbf{R}$. Then

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

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}$$

$= A_{(\alpha+\beta)} \in G$, since $(\alpha + \beta) \in \mathbf{R}$

Therefore, G is closed with respect to matrix multiplication.

Associativity: The elements of G are all real numbers and the multiplication of real number is associative. Hence matrix multiplication is associative.

Existence of Left Identity: Since $0 \in \mathbf{R}$, therefore

$A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} \in G$

If A_0 be any member of G, then

$A_0 A_\alpha = A_{0+\alpha}$

$= A_\alpha.$

Therefore, A_0 is the left identity.

Existence of Left Inverse: Let $A_\alpha \in G$. Then $A_{(-\alpha)} \in G$ because

$\alpha \in \mathbf{R} \Rightarrow -\alpha \in \mathbf{R}$ **.**

Now $A_{(-\alpha)} A_\alpha = A_{(-\alpha)+\alpha}$

$= A_0$

= the left identity.

$\therefore A_{(-\alpha)}$ is the left inverse of A_α.

Thus each element of G possesses left inverse.

Hence G is a group with respect to matrix multiplication.

3.7 Semi Group and Monoid

Semi Group:

Let a non-empty set A, and a binary operation (*), then this algebraic structure (A, *) is called Semi Group if the binary operation is associative.

i. e. $\forall\, a, b, c \in A$, then $(a * b) * c = a * (b * c)$.

Example.1: we have proved $(N, +)$ is algebraic structure. This algebraic structure may or may not be semi group if it holds the associative property then it will be semi group. If $2, 3, 5 \in N$, then $(2 + 3) + 5 = 2 + (3 + 5) = 10$. It means the algebraic structure $(N, +)$ holds the associative property so, $(N, +)$ is a semi group. The algebraic structure $(N, \times)$ is also semi group whereas $(N, \div)$ and $(N, -)$ are not semi group because it is not algebraic structure and also do not satisfy the associative property with

respect to division and subtraction.

Monoid:

Let a non- empty set A, and a binary operation $(*)$then this algebraic structureis called Monoid if it satisfy the identity property.

i. e. $\forall\, a \in A,$ there is an elements e such that $a * e = e * a = a.$

Also, we can say that a semi group satisfies the identity property then it is called Monoid. As we know that $(N,\times)$is a semi group with respect multiplication and also it is monoid because the set of natural number has multiplicative identity which is 1 whereas $(N,+)$ is a semi group with respect to addition but there is no additive identity in this set of natural number so this not monoid.

3.8 Finite and Infinite Group

A group (G,*) is categories as finite of infinite group according as number of distinct elements of G is finite or infinite.

Order of a Group: The number of distinct elements in a finite group (G,*) is called order of the group. An infinite group is said to be of infinite order. The order of a group (G, *) is denoted by O (G).

Example: If G is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2 = e$.

Solution: Suppose G be a group of order 2n, where n is a positive integer. We shall prove that G must have an element $a \neq e$ such that $a^{-1} = a$. We shall prove it by contradiction.

Let G has no element, other than identity element e, which is its own inverse. Now in a group every element possesses a unique inverse. The identity element e is its own inverse. Further if b is the inverse of c, then c is the inverse of b. so excluding the identity element e, the remaining 2n-1 elements of G must be divided into pairs of two such that each pair consists of an element and its inverse. But we cannot do so because the odd integers 2n-1 is not divisible by 2. Hence our initial assumption is wrong.

So in G there is an element $a \neq e$ such that

$$a = a^{-1} \Rightarrow aa = a^{-1}a \Rightarrow a^2 = e$$

Example: Show that the set of Real Number R is a group with respect to the operation of addition of integers.

Solution: Closure property: Since sum of two real numbers also a real number.

i.e., $a + b \in R \; \forall \; a, b \in R$.

Thus R is closed with respect to addition.

Associative Law: Since addition of real number is associative composition.

i.e. $(a + b) + c = a + (b + c) \quad \forall \; a, b, c \in R$

Existence of identity: For the element Zero $\in$ R we have

$0 + a = a + 0 = a \; \forall a \in IR$

Therefore, real number zero (0) is the identity.

Existence of Inverse: If $a \in IR$, then $-a \in IR$ and also, we have $(-a) + a = 0 = a + (-a)$.

Thus, every real number possesses an additive inverse. Thus (R, +) is a group with respect to addition

We have shown the examples of the group in the Table 2.

Table 2 Examples of Group

Set with operation	**Algebraic structure**	**Semi group**	**Monoid**	**Group**
$(N, -)$	No	No	No	No
$(N, \div)$	No	No	No	No
$(Z, +)$	Yes	Yes	Yes	Yes
$(Z, -)$	Yes	No	No	No
$(Z, \times)$	Yes	Yes	Yes	No
$(Z, \div)$	No	No	No	No
$(R, +)$	Yes	Yes	Yes	Yes
$(R, -)$	Yes	No	No	No
$(R, \times)$	Yes	Yes	Yes	No
$(R, \div)$	No	No	No	No

Exercise: - Write which of above Group are abelian group?

Check Your Progress Report

Q.1. State the axioms which a set must obey so that it may form a group.

Q.2. Show that the set Q of all rational numbers form a Group with respect to addition.

Q.3. Is the Set R_o of all non-zero real numbers are group with respect to multiplication?

Q.4. Do the set I of integers, a group: (i) With respect to subtraction? (ii) With respect to multiplication?

Q.5. Do the positive irrational numbers form a group with respect to multiplication operation?

3.9 Composition Table of finite Group

A binary composition in finite set can be represented in a tabular form known as Composition table. Let us suppose that $P = \{p_1, p_2, p_3, \ldots\ldots\ldots p_n,\}$ finite set having n different elements. We manage the elements of the set P in a horizontal row as well as in a vertical column. The element $p_i\ p_j$, connected to the ordered pair$(p_i, p_j,)$ is put at the intersection of the row headed by p_i and the column headed by p_j. The composition table for a finite group contains each member exactly ones in each of its rows and columns.

Example: Show that fourth roots of unity namely $1, -1, i, -i$ form a group with respect to multiplication.

Solution: Let $P = \{1, -1, i, -i\}$. To show that multiplication is a composition in P, we make the composition table

×	1	−1	I	-i
1	1	−1	I	-i
−1	−1	1	−i	I
I	I	−i	−1	1
-i	−i	i	1	-1

From the composition table, we can get some conclusion regarding group.

1. Closure property:

In the composition table, all elements of the set P are present in each rows and in each columns. It means that P is closed under multiplication.

2. Associativity:

The members of P are complex numbers and as we know that the multiplication of complex numbers is associative.

3. Existence of identity:

We have $1 \in P$ and $1\ a = \forall\ a \in P$. It means that 1 is the multiplicative identity of the finite set P.

4. Existence of inverse:

From the composition table, each member of the finite set P has inverse.

The inverse of $1, -1, i, -i$ are 1,-1, $-i$ and i.

The given finite set P satisfied all axiom of group. Hence P is group under multiplication.

Addition modulo $(+_m)$

Let us suppose that a and b are any integers then the addition modulo m can be define and it is represented by $a+_m b$ where m is fixed positive integer. By definition, we have; $a+_m b = s, 0 \leq s < m$ wheres is least none - negative remainder when $a + b$ is divided by m and $a + b$ is ordinary sum of a and b. Example $18+_5 4 = 2$, since $18 + 4 = 22 = 4(5) + 2$ i.e where 2 is least non- negative remainder when $18 + 4$ is divided by 5 and 22 is ordinary sum of 18 and 4. Similarly$-8+_2 4 = -2(2) + 0 = 0. -23+_3 3 = -20 = -3(7) + 1$.

Problem under addition modulo$(+_m)$

Show that set $P = \{0,1,2,3,4,5\}$ is a finite abelian group of order 6 with respect to addition modulo 6.

or

Show that set $P = \{0,1,2,3,4,5 +_6\}$ is a finite abelian group of order 6.

Solution: Given that a $P = \{0,1,2,3,4,5\}$. To show P is abelian group, we form a composition table of a given set under addition modulo 6 which is given below**;**

$+_6$	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**	**0**
2	**2**	**3**	**4**	**5**	**0**	**1**
3	**3**	**4**	**5**	**0**	**1**	**2**
4	**4**	**5**	**0**	**1**	**2**	**3**
5	**5**	**0**	**1**	**2**	**3**	**4**

1. Closure property:

It can be easily seen that all entries in the composition table are the member of the set P. It means that $(P, +_6)$ is closed under addition modulo 6. Hence closure property holds**.**

2. Associativity:

If we choose any three numbers from the set i.e. if $\forall\, a, b, c \in P,$ then$(a +_6 b) +_6 c = a +_6 (b +_6 c) =$ s which is least none-negative remainder when $(a + b) + c$ / $a + (b + c)$ /is divided by 6 . The composition $'+_6'$ is associative. Hence associativity is holds for the given set.

3. Existence of identity:

We have $0 \in P$ and $0 +_6 a = a, \forall\, a \in P$. It means that 0 is the additive identity of the given set P.

4. Existence of inverse:

From the composition table, each member of the finite set P has inverse. The inverse of $0,1, 2, 3,4,5$ are $0, 5, 4, 3, 2$ and 1.

5. Commutative group:

The composition is commutative as the corresponding rows and columns in the composition table are identical and it show the property of commutative.

The given finite set P satisfied all axiom of group. Hence P is group under addition modulo 6and also satisfied the commutative property with respect to addition modulo 6. Hence the given set is abelian group.

Multiplication modulo $(\times_m)$

Let us suppose that a and b are any integers then the multiplication modulo m can be define and it is represented by $a \times_m b$ where m is fixed positive integer. By definition, we have; $a \times_m b = s, 0 \leq s < m$ where s is least none- negative remainder when $a \times b$ is divided by m and $a \times b$ is ordinary multiply of a and b.

Example: $8 \times_5 4 = 2$, since $84 = 32 = 6(5) + 2$ i.e where 2 is least none- negative remainder when 8×4 is divided by 5 and 32 is ordinary multiply of 8 and 4. Similarly $-3 \times_2 4 = -6(2) + 0, -3 \times_3 3 = -20 = -3(3) + 0$.

Problem under multiplication modulo$(\times_m)$

Example: Show that set $P = \{1, 2,3,4,5,6, \times_7\}$ is a finite abelian group of order 7 with respect to multiplication modulo 7.

or

Show that set $P = \{1, 2,3,4,5, 6, \times_7\}$ is a finite abelian group of order 7**.**

Solution: Given that $P = \{1, 2,3,4,5,6, \times_7\}$. To show P is abelian group, we form a composition table of a given set under multiplication modulo 7 which is given below**;**

$\times_7$	**1**	**2**	**3**	**4**	**5**	**6**
1	**1**	**2**	**3**	**4**	**5**	**6**
2	**2**	**4**	**6**	**1**	**3**	**5**
3	**3**	**6**	**2**	**5**	**1**	**4**
4	**4**	**1**	**5**	**2**	**6**	**3**
5	**5**	**3**	**1**	**6**	**4**	**2**
6	**6**	**5**	**4**	**3**	**2**	**1**

1. Closure property:

It can be easily seen that all entries in the composition table are the member of the set P. It means that $(P,\times_7)$ is closed under multiplicative modulo 7. Hence closure property holds**.**

2. Associativity:

If we choose any three numbers from the set i.e. if $\forall\, a, b, c \in P$, then $(a \times_7 b) \times_7 c = a \times_7 (b \times_7 c) =$ swhich is least non-negative remainder when $(a \times_7 b) \times_7 c$ / $a \times_7 (b \times_7 c)$ is divided by 7. The composition $' \times_7 '$ is associative under multiplication modulo 7. Hence associativity is holds for given set.

3. Existence of identity:

We have $1 \in P$ and $1 \times_7 a = a, \forall\, a \in P$. It means that 1 is the multiplicative identity of the given set P.

4. Existence of inverse:

From the composition table, each member of the finite set P has inverse. The inverse of $1, 2, 3,4,5,6$ are 1, 4, 5, 2, 3 and 6 respectively.

5. Commutative group:

The composition is commutative as the corresponding rows and columns in the composition table are identical and it show the property of commutative. The given finite set P satisfied all axiom of group. Hence P is group under multiplicative modulo 7 and also satisfied the commutative property with respect to multiplicative modulo 7. Hence the given set is abelian group.

Check your progress report

Q.1. Show that the set $G = \{\ldots, 3^{-4}, 3^{-3}, 3^{-2}, 3^{-1}, 1, 3, 3^2, 3^3, \ldots\}$ forms an infinite abelian group with respect to multiplication Groups.

Q.2. Show that set of all possible rational numbers (real numbers forms an abelian group with respect to multiplication of numbers.

Q.3. Show that set $G = \{1, -1\}$ is a finite abelian group of order 2 under multiplication ascomposition.

Some elementary properties of group:

Let us considered that $' * '$ is a binary operation defined on a group P.

Theorem 1: To prove that $(ab)^{-1} = b^{-1}a^{-1} \ \forall\, a, b \in G$ i.e. the inverse of the product of two element of G is the product of the inverses taken in the reverse order.

Proof: Let a, b ∈ G. If a^{-1} and b^{-1} are the inverse of a and b respectively, then

$a^{-1}a = e = aa^{-1}$, where e is the identity element and

$b^{-1}b = e = bb^{-1}$

Now $(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1}$ [Compositionis assocative]

$= [a(bb^{-1})]a^{-1}$ [By associativity]

$= (ae)a^{-1}$ $[bb^{-1} = e]$

$= aa^{-1}$ [ae = a]

$= e$ $[aa^{-1} = e]$

Also, $(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)]$ [Compositionis assocative]

$= b^{-1}[(a^{-1}a)b]$

$= b^{-1}(eb)$

$= b^{-1}b$

$= e$

Thus we have $(b^{-1}a^{-1})(ab) = e = (ab)(b^{-1}a^{-1})$

By definition of inverse, we have $(ab)^{-1} = b^{-1}a^{-1} \ \forall\, a, b \in G$

Hence proved.

Note 1: In additive notation the statement of above theorem will b

- (a + b) = (- b) + (- a).

Note 2: The rule given in this theorem is known as the reversal rule. It can be generalized by induction as follows:

If a, b, c, ……, k are in G then

$(a\ b\ c\ \ldots.\ k)^{-1} = k^{-1}\ \ldots.c^{-1}\ b^{-1}\ a^{-1}$.

Theorem 2: $\forall\ x \in P, \text{then}\ x^{-1} * x = e = x * x^{-1}$ i.e. the left inverse of an element is equal to right inverse of an element**.**

Proof: - Let x^{-1} be the left inverse of an element x of a group P, so that

$$x^{-1} * x = e \qquad \text{(e being the identity)} \qquad (1)$$

To prove that x^{-1} is also the right inverse of x, it is enough to show that

$$x * x^{-1} = e \qquad (2)$$

By Associative Law,

$x^{-1} * (x * x^{-1}) = (x^{-1} * x) * x^{-1}$

$= e * x^{-1}$ [by (1)]

$= x^{-1}$

$= x^{-1} * e$

Thus,

$$x^{-1} * (x * x^{-1}) = x^{-1} * e$$

By left cancellation law, this gives

$$x * x^{-1} = e$$

Hence proved

Theorem 3: - If $\forall\ x, y, z \in P, \text{then}\ (x * y) = (x * z) \Rightarrow y = z$ and also known as left cancelation law.

Proof: - Given that$(x * y) = (x * z), \forall\ x, y, z \in P$. As we know that P is group then $x^{-1} \in P$. Multiplying by x^{-1}on left side of the equation $(x * y) = (x * z)$, then we can write

$$x^{-1} * (x * y) = x^{-1} * (x * z)$$

By using of associativity property, we can write

$$(x^{-1} * x) * y = (x^{-1} * x) * z,$$

where $(x^{-1} * x)$ and $(x^{-1} * x)$ are equal to the identity 'e' by using the property of identity.

$(e) * y = (e) * z \Rightarrow y = z.$ By left cancelation law

Hence proved

Theorem 4: If $\forall\, x, y, z \in P,$ then $y * x = z * x \Rightarrow y = z$ and also known as right cancelation law.

Proof: - Given that $y * x = z * x, \forall\, x, y, z \in P.$ As we know that P is group then $x^{-1} \in P.$ Multiplying by x^{-1}on right side of the equation $y * x = z * x$, then we can write

$$(y * x) * x^{-1} *= (z * x) * x^{-1}$$

By using of associativity property, we can write

$$y * (x * x^{-1}) = z * (x * x^{-1})$$

where $(x * x^{-1}) = e$ and $(x * x^{-1}) = e$ from the theorem 2.

$y * (e) = z * (e)$, from the theorem 1, we get

$$y = z\,.$$

Hence proved

Theorem 5: The identity element (e) in a group P is unique**.**

Proof: Let us consider that if possible e and e' be two identity elements of the group P and then as e is an element so we can write it $x * e = x.$

Similarly as e' is an identity element of the group P then we can write $x * e' = x.$

Now, $x * e = x$ and $x * e' = x \Rightarrow x * e = x * e'$

$$\Rightarrow\ e = e' \quad (\text{by cancelation law})$$

It means that identity element in a group is unique.

Theorem 6: The inverse element (x^{-1}) in a group P is unique**.**

Proof: Let us consider that if possible a and b be two inverses of x and then as e is an element so we can write it $a * x = e = x * e.$ Similarly, as b is another inverse of x then we can write $b * x = e = b * x.$

Now, $a * x = e$ and $b * x = e \Rightarrow a * x = b * x$

$$\Rightarrow a = b$$

It means that inverse element in a group is unique and hence proved.

Theorem.7: If $\forall x \in P, \text{then} (x^{-1})^{-1} = x$ i.e the inverse of x^{-1} is x.

Proof: - As per consideration, since x^{-1} is inverse of x

$$x^{-1} * x = e = x^{-1} * x$$

which also implies that x is inverse of x^{-1}

Thus, $(x^{-1})^{-1} = x$

Hence proved.

Solved Example

Problem.1: If P is a group in which $(xy)^n = x^n y^n$ for three consecutive integers n and any x, y in P, then P is abelian.

Solution: Suppose $n, n+1, n+2$ are three consecutive integers and for which the given condition holds, then for any $x, y \in P$.

$(xy)^n = x^n y^n$ …(1)

$(xy)^{n+1} = x^{n+1} y^{n+1}$ …(2)

$(xy)^{n+2} = x^{n+2} y^{n+2}$ …(3)

Now, from the equation (3) we can write

$$(xy)^{n+2} = (xy)^{n+1}(xy)$$

$$x^{n+2} y^{n+2} = (x^{n+1} y^{n+1})(xy)$$

$x\, x^{n+1} y^{n+1} y = x\, x^n y^n y (xy)$

$x^{n+1} y^{n+1} = x^n y^n yx$ [by using of left and right cancellation law]

$$(xy)^{n+1} = (xy)^n yx$$

Further as

$$(xy)^n(xy) = (xy)^n yx$$

$xy = yx$ [by using of left cancellation law]

Hence P is abelian group.

Problem 2: Show that if a, b are any two elements of a group P, then $(a\ b)^2 = a^2\ b^2$ if and only if P is abelian.

Solution: Let P be an abelian group, then

$(a\ b)^2 = (a\ b)(ab)$

$= a\ (b\ a)\ b$

$= a\ (a\ b)\ b$ [since P is abelian]

$= (a\ a)\ (b\ b)$

$= a^2\ b^2$

Conversely: Let a, b be any two elements of P then

$(a\ b)^2 = a^2\ b^2$

$(a\ b)(a\ b) = (a\ a)\ (b\ b)$

$a\ (b\ a)\ b = a\ (a\ b)\ b$

$b\ a = a\ b$ [by using of left and right cancellation law]

Hence P is abelian.

Problem 3: Prove that if for every element a in a group G, $a^2 = e$, then G is an abelian group.

Solution: Let a and b be any element of G. Then ab is also an element of G.

Therefore $(ab)^2 = e$.

Now, $(ab)^2 = e$

$\Rightarrow \quad (ab)(ab) = e$

$\Rightarrow \quad (ab)^{-1} = ab \qquad \Rightarrow \quad b^{-1} a^{-1} = ab.$

But $\quad a^2 = e \qquad \Rightarrow \quad aa = e$

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

Similarly, $b^2 = e \qquad \Rightarrow \quad b^{-1} = b.$

Therefore from above we get

$b\ a = a\ b$

Thus we have $a\ b = b\ a \qquad \forall\ a, b \in G.$

Therefore G is an abelian group.

Problem 4: Given $a\ x\ a = b$ in a group G, Find x.

Solution: We have

$a\ x\ a = b$

$\Rightarrow \quad a^{-1}\ a\ x\ a = a^{-1} b$

$\Rightarrow \quad (a^{-1}\ a)\ x\ a = a^{-1} b$

$\Rightarrow \quad e\ (x\ a) = a^{-1} b$

$\Rightarrow \quad x\ a = a^{-1} b$

$\Rightarrow \quad (x\ a)\ a^{-1} = a^{-1} b\ a^{-1}$

$\Rightarrow \quad x\ (\ a^{-1} a) = a^{-1} b\ a^{-1}$

$\Rightarrow \quad x\ e = a^{-1} b\ a^{-1}$

$\Rightarrow \quad x = a^{-1} b\ a^{-1}.$

3.10 Summary

Group theory is a fundamental concept in modern algebra that appears naturally in many mathematical areas. It has wide applications in physical and biological sciences, including the study of crystal structures, molecular configurations, and human genes. Groups provide a simple mathematical structure and serve as a starting point for studying other algebraic structures. Group theory began in the 18th century with Lagrange, followed by Galois, who introduced the formal idea of groups. In the 19th century, Cauchy, Jordan, Cayley, and Klein further developed the field. By the 20th century, group theory became crucial in physics, chemistry, cryptography, and computing. Today, it is widely used in both mathematics and real-world applications. This unit will cover binary operations, algebraic structures, groups, Abelian groups, finite and infinite groups, and composition tables of finite groups.

3.11 Terminal Questions

Q.1. (i) Distinguish between an abelian and a non - abelian group. Give an example of each.

(ii) In group theory, prove that the left axioms imply the right axioms.

Q.2. Show that the set G of all square matrices $a[i,j]_{m\times n}$ such that det.$a[i,j] = \pm 1$ is a group under matrix multiplication. Show also that those metrices in G for which det. $a[i,j] = 1$ form a group.

Q.3. Show that set of all matrices $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, where a and b are non zero real numbers, is a group under matrix multiplication.

Q.4. Show that set of all matrices $\begin{bmatrix} c^a & b \\ 0 & c^{-a} \end{bmatrix}$, a and b are real numbers not both equal to zero, is a group under matrix multiplication, c being a positive constant.

Q.5. Show that set of all matrices $\begin{bmatrix} a & b \\ -\mathrm{b} & a \end{bmatrix}$, where a and b are real numbers not both equal to zero, is a group under matrix multiplication.

Q.6. Show that the set of matrices $\begin{bmatrix} cos\,\alpha & sin\,\alpha & 0 \\ -sin\,\alpha & cos\,\alpha & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

where α is a real number forms a group under matrix multiplication.

Q.7. Show that the four constants f_1, f_2, f_3, f_4 on set of complex numbers defined by

$$f_1(z) = z, f_2(z) = -z, f_3(z) = \frac{1}{z}, f_4(z) = -\frac{1}{z}$$

forms a finite abelian group with respect to composite composition.

Q.8. Show that the set of complex numbers z with |z| = 1 is not a group under the operation * denoted by $z_1 * z_2 = |z_1|.z_2$

Q.9. Show the four matrices $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}$ form a multiplicative group.

Q.10. Show that the set of numbers forms an abelian all positive rational numbers (real group with respect to multiplication with operation * defined by a * b = a + b + 2.

Q.11. Prove that the set rational numbers of the form $\frac{m}{2^n}, (m, n\ integers)$ is a group under addition.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

U. P. Rajarshi Tandon
Open University

Master of Science

PGMM -106/MAMM-106
Advanced Algebra

Block

2 Group Theory

Unit- 4 **Permutation Groups**
Unit- 5 **Order of an element of a group and Isomorphism on Groups**
Unit- 6 **Subgroup and Cosets**

Block-2

Group Theory

Group theory has an interesting history linked to the study of patterns and equations. It started in the 18th century when Joseph-Louis Lagrange looked at how the roots of equations could be rearranged, called permutations. Later, Évariste Galois introduced the idea of a group to help solve difficult equations, which became the basis of modern group theory. Permutations help us understand how elements in a set can be organized, especially in symmetric groups. Subgroups are smaller groups within a bigger group that follow the same rules, and they help in understanding the overall structure. Group theory, especially through permutations and subgroups, is useful in many areas like solving equations, understanding molecules and crystals, and creating secure codes in cryptography and computer science.

Today, both set theory and group theory are essential in both pure and applied mathematics, forming the foundation for many modern mathematical theories and practical applications. In the fourth unit we shall discuss about the permutations, groups of permutations, cyclic permutations, even and odd permutations. In the fifth unit we shall discuss about the order of an element of a group and some important theorems based on order of an element of a group and isomorphism on groups. In the sixth unit we shall discuss about the complexes and subgroups of a group, intersection of subgroups, cosets, right and left cosets, Lagrange's theorem, Fermat's theorem, Cayley's theorem and Euler's theorem.

UNIT- 4: Permutations Groups

Structure

4.1 Introduction

The concept of permutation groups started in the 18th century when Joseph-Louis Lagrange studied how the roots of equations could be rearranged, which helped develop early ideas about permutations in math. In the 19th century, Augustin-Louis Cauchy made the study of permutations more organized by introducing a way to write them (cycle notation) and studying their structure. Later, in the 1830s, Évariste

Galois made a major discovery by connecting permutation groups with solving equations. His work, known as Galois Theory, showed that whether an equation can be solved depends on the properties of its related permutation group.

In 1854, Arthur Cayley showed that any group can be seen as a permutation group, helping build the basics of modern group theory. Today, permutation groups are an important part of algebra and are used in many fields like coding, science, and computer studies.

4.2 Objectives

After studying this unit the learner will be able to understand the :

- Permutation
- Equality of two permutations
- Identity permutation, product of two permutations
- groups of permutations
- cyclic permutations, even and odd permutations

4.3 Permutations

Let $A = \{a_1, a_2, a_3, ..., a_n\}$ be a finite set having n distinct elements. A permutation is a function which is one one onto. The number of elements in the finite set A is called as the degree of permutation.

Consider $A = \{a_1, a_2, a_3, a_4, a_5, ..., a_{n-1}, a_n\}$ is a finite set having n distinct elements. If $f : A \to A$ and f is one-one onto function, then f is a permutation of degree n.

Suppose $f(a_1)=b_1,\ f(a_2)=b_2,\ f(a_3)=b_3,\ f(a_4)=b_4,\ldots\ldots\ldots,\ f(a_n)=b_n,$ where $\{b_1,b_2,b_3,b_4,\ldots\ldots\ldots,b_{n-1},b_n\}=\{a_1,a_2,a_3,a_4,\ldots\ldots\ldots,a_{n-1},a_n\}$ *i.e.*, $b_1,b_2,b_3,b_4,\ldots\ldots\ldots,b_{n-1},b_n$ is nothing but some arrangement of the n elements of A.

For write this permutation, we have $f=\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots\ldots & \ldots\ldots\ldots & a_n \\ b_1 & b_2 & b_3 & b_4 & \ldots\ldots & \ldots\ldots\ldots & b_n \end{pmatrix}$ *i.e.*, each element in the second row is the f image of the element of the first row.

If $A=\{1,\ 2,\ 3\}$ is a finite set having three elements, then

$$f_1=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ f_2=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ f_3=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\text{etc.}$$

Here all the above permutations $f_1,\ f_2,\ f_3,\ldots\ldots$ are of degree three. So in the permutation f_1 the elements 1, 2, 3 have been replaced respectively by the elements 2, 3, 1. Thus we have

$$f(1)=2,\ f(2)=3,\ f(3)=1.$$

4.4 Equality of Two Permutations

Let f_1 and f_2 are two permutation of degree n. Then f_1 and f_2 are said to be equal permutations if we have $f_1(a)=f_2(a),\ \forall a\in A.$

Note. The interchange of columns will not change the permutations.

For example, If $f_1=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$ and $f_2=\begin{pmatrix} b & d & c & a \\ c & a & d & b \end{pmatrix}$ are two permutations of degree 4, then we have $f_1=f_2$. Here we see that both f_1 and f_2 replace *a* by *b*, *b* by *c*, *c* by *d* and *d* by *a*.

Let $f_1=\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix}$ be a permutation of degree four. Here we can write f_1 it in several ways

as follows: $f_1 = \begin{pmatrix} a_2 & a_1 & a_3 & a_4 \\ b_2 & b_1 & b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_4 & a_1 & a_3 & a_2 \\ b_4 & b_1 & b_3 & b_2 \end{pmatrix} = \begin{pmatrix} a_4 & a_3 & a_2 & a_1 \\ b_4 & b_3 & b_2 & b_1 \end{pmatrix}$ etc.

4.5 Identity Permutation

If I_P is a permutation of degree n such that I_P replaces each element by the element itself, then I_P is called the identity permutation of degree n.

Thus $I_P = \begin{pmatrix} 1 & 2 & 3.....n \\ 1 & 2 & 3.....n \end{pmatrix}$ or $\begin{pmatrix} a_1 & a_2 & a_3.....a_n \\ a_1 & a_2 & a_3.....a_n \end{pmatrix}$ or $\begin{pmatrix} b_1 & b_2 & b_3.....b_n \\ b_1 & b_2 & b_3.....b_n \end{pmatrix}$ is the identity permutation of degree n.

Note: 1. If $A = \{a_1, a_2\}$ is a finite set having two elements, then the identity permutation is defined as

$$I_p = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}.$$

2. If $A = \{1, 2, 3\}$ is a finite set having three elements, then the identity permutation is defined as

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

3. If $A = \{a, b, c, d\}$ is a finite set having four elements, then the identity permutation is defined as

$$I_p = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}.$$

4. If A is a finite set having n distinct elements, then we shall have $n!$ distinct arrangements of the elements of A. If A_n be the set consisting of all permutations of degree n, then the set A_n will have $n!$ distinct elements. The set A_n of all permutations of degree 3 will have 3! *i.e.*, 6 elements. Clearly

$$A_3 = \left\{ \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix}, \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}, \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_3 & a_2 \end{pmatrix}, \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix}, \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}, \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \end{pmatrix} \right\}.$$

4.6 Product of two Permutations

Consider f_1 and f_2 are two permutation of degree n. Then the product f_1 and f_2 is denoted as $f_1 f_2$, is obtained by first carrying out the operation defined by f_1 and then by f_2.

Note: 1. If $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ then the product f_1 and f_2 is denoted as

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

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

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

Here the permutation f_2 has been written in such a way that the first row of f_2 coincides with the second row of f_1.

2. If $f_1 = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$ and $f_2 = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$ then the product f_1 and f_2 is denoted as

$$f_1 f_2 = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

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

3. If $f_1 = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$ and $f_2 = \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}$ then the product f_1 and f_2 is denoted as

$$f_1 f_2 = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}\begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \begin{pmatrix} b & a & d & c \\ b & c & d & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}.$$

4. If $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \ldots\ldots\ldots a_n \\ b_1 & b_2 & b_3 & b_4 \ldots\ldots\ldots b_n \end{pmatrix}$ and $f_2 = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \ldots\ldots\ldots b_n \\ c_1 & c_2 & c_3 & c_4 \ldots\ldots\ldots c_n \end{pmatrix}$ then the product f_1 and f_2 is denoted as

$$f_1 f_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \ldots\ldots\ldots a_n \\ b_1 & b_2 & b_3 & b_4 \ldots\ldots\ldots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \ldots\ldots\ldots b_n \\ c_1 & c_2 & c_3 & c_4 \ldots\ldots\ldots c_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \ldots\ldots\ldots a_n \\ b_1 & b_2 & b_3 & b_4 \ldots\ldots\ldots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \ldots\ldots\ldots b_n \\ c_1 & c_2 & c_3 & c_4 \ldots\ldots\ldots c_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \ldots\ldots\ldots a_n \\ c_1 & c_2 & c_3 & c_4 \ldots\ldots\ldots c_n \end{pmatrix}.$$

For, f_1 replaces a_1 by b_1 and then f_2 replaces b_1 by c_1 so that $f_1 f_2$ replaces a_1 by c_1. Similarly $f_1 f_2$ replaces a_2 by c_2, a_3 by $c_3, \ldots\ldots\ldots, a_n$ by c_n.

Note: If f_1 and f_2 are two permutation of degree n then it is not essential that $f_1 f_2 = f_2 f_1$ as permutation composition is not generally commutative.

4.7 Inverse Permutation

Let $f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots\ldots & a_n \\ b_1 & b_2 & b_3 & b_4 & \ldots\ldots & b_n \end{pmatrix}$ be a permutation of degree n then $f^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 & \ldots\ldots & b_n \\ a_1 & a_2 & a_3 & a_4 & \ldots\ldots & a_n \end{pmatrix}$ is known as the inverse permutation of degree n such that f

$f^{-1} = I_P$.

Since we know that a permutation is one-one onto map and it is invertiable.

Note: 1. If $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ is a permutation of degree three then the inverse of f is $f^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$ such that

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

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

$$= I_P.$$

2. If $f = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$ is a permutation of degree two then the inverse of f is $f^{-1} = \begin{pmatrix} a_2 & a_1 \\ a_1 & a_2 \end{pmatrix}$ such that

$$f\, f^{-1} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & a_1 \\ a_1 & a_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$$

$$= I_P.$$

3. If $f = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$ is a permutation of degree four then the inverse of f is $f^{-1} = \begin{pmatrix} b & a & d & c \\ a & b & c & d \end{pmatrix}$ such that

$$f\,f^{-1} = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}\begin{pmatrix} b & a & d & c \\ a & b & c & d \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}.$$

$$= I_P.$$

4. If $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 .....a_{n-1} & a_n \\ b_1 & b_2 & b_3 .....b_{n-1} & b_n \end{pmatrix}$ be a permutation of degree n, then the inverse of f_1^{-1} i.e., f_1^{-1} is obtained by interchanging the two rows of f_1. Thus we have

$$f_1^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 ..... & b_{n-1} & b_n \\ a_1 & a_2 & a_3 ..... & a_{n-1} & a_n \end{pmatrix}.$$

Solved Examples

Example 1. Let $f_1 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$ and $f_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$ be two permutations of degree three. To show that $f_1 f_2 \neq f_2 f_1$.

Sol. It is given that

$$f_1 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \text{ and } f_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

Then we have

$$f_1 f_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \begin{pmatrix} a & c & b \\ b & a & c \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

and

$$f_2 f_1 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} b & c & a \\ c & b & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}.$$

Hence $f_1 f_2 \neq f_2 f_1$.

Example 2. Let $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ and $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$ be two permutations of degree five. To find $f_1 f_2$.

Sol. It is given that

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \text{ and } f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

Then we have

$$f_1 f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

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

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

Example.3. Let $f_1 = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$ and $f_2 = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$ be two permutations of degree two. To show that $f_1 f_2 = f_2 f_1$.

Sol. It is given that

$f_1 = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$ and $f_2 = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$

Then we have

$$f_1 f_2 = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

and

$$f_2 f_1 = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

Hence $f_1 f_2 = f_2 f_1$.

Check your Progress

Q.1. Define permutation.

Q.2. What is inverse permutation?

Q.3. Explain the identity Permuation.

Q.4. What do you mean by product of two permutations?

4.8 Groups of Permutations

Theorem. The set A_n of all permutations of n symbols is a finite group of order $n!$ with respect to composite of mappings as the operation. For $n \leq 2$, this group is abelian and for $n > 2$ it is always non-abelian.

Proof. Let $A = \{a_1, a_2, a_3, ..., a_n\}$ be a finite set having n distinct elements.

Let $f = \begin{pmatrix} a_1 & a_2 .....a_n \\ b_1 & b_2 .....b_n \end{pmatrix}$ be a permutation of degree n.

Here elements $b_1, b_2, b_3, ..., b_n$ of the second row are simply an arrangement of the n elements

$a_1, a_2, a_3, ..., a_n$ of the set A.

The elements of the set of A can be arranged in n ! different ways. Therefore we shall have n ! distinct permutations of degree n. If A_n be the set of all permutations of degree n, then P_n has n ! distinct elements.

Let $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$ and $f_2 = \begin{pmatrix} b_1 & b_2 & b_3 .....b_n \\ c_1 & c_2 & c_3 .....c_n \end{pmatrix}$ be any two permutations of degree n.

They by definition of product or composite of two permutations, we have

$$f_1 f_2 = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ c_1 & c_2 & c_3 .....c_n \end{pmatrix}$$

Obviously, $f_1 f_2$ is also a permutation of degree n, since $c_1, c_2, c_3, ..., c_n$ is nothing but an arrangement of the same n elements $a_1, a_2, a_3, ..., a_n$ of the set A.

Thus $f_1 f_2 \in A_n \ \forall \ f_1, f_2 \in A_n$.. Therefore A_n is closed with respect to the composition known as product of two permutations.

Associativity. We know that the permutation multiplication is associative.

Consider $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$, $f_2 = \begin{pmatrix} b_1 & b_2 & b_3 .....b_n \\ c_1 & c_2 & c_3 .....c_n \end{pmatrix}$, $f_3 = \begin{pmatrix} c_1 & c_2 & c_3 .....c_n \\ d_1 & d_2 & d_3 .....d_n \end{pmatrix}$ are any three permutations of degree n where $b_1, b_2, b_3, ..., b_n$; $c_1, c_2, c_3, ..., c_n$; $d_1, d_2, d_3, ..., d_n$ are simply different arrangements of the same n elements $a_1, a_2, a_3, ..., a_n$.

Then we have

$$f_1 f_2 = \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots\ldots\ldots a_n \\ b_1 & b_2 & b_3 \ldots\ldots\ldots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots\ldots\ldots b_n \\ c_1 & c_2 & c_3 \ldots\ldots\ldots c_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots\ldots\ldots a_n \\ c_1 & c_2 & c_3 \ldots\ldots\ldots c_n \end{pmatrix}$$

Now

$$(f_1 f_2) f_3 = \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots\ldots\ldots a_n \\ c_1 & c_2 & c_3 \ldots\ldots\ldots c_n \end{pmatrix} \begin{pmatrix} c_1 & c_2 & c_3 \ldots\ldots\ldots c_n \\ d_1 & d_2 & d_3 \ldots\ldots\ldots d_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots\ldots\ldots a_n \\ d_1 & d_2 & d_3 \ldots\ldots\ldots d_n \end{pmatrix}$$

Also $f_2 f_3 = \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots\ldots\ldots b_n \\ c_1 & c_2 & c_3 \ldots\ldots\ldots c_n \end{pmatrix} \begin{pmatrix} c_1 & c_2 & c_3 \ldots\ldots\ldots\ldots c_n \\ d_1 & d_2 & d_3 \ldots\ldots\ldots d_n \end{pmatrix}$

$$= \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots\ldots\ldots b_n \\ d_1 & d_2 & d_3 \ldots\ldots\ldots d_n \end{pmatrix}$$

Now we have

$$f_1 (f_2 f_3) = \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots\ldots\ldots a_n \\ b_1 & b_2 & b_3 \ldots\ldots\ldots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots\ldots b_n \\ d_1 & d_2 & d_3 \ldots\ldots\ldots d_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots\ldots\ldots a_n \\ d_1 & d_2 & d_3 \ldots\ldots\ldots d_n \end{pmatrix}$$

Thus $(f_1 f_2) f_3 = f_1 (f_2 f_3)$.

Existence of identity. Let $I_P = \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots a_n \\ a_1 & a_2 & a_3 \ldots\ldots a_n \end{pmatrix}$ or $I_P = \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots b_n \\ b_1 & b_2 & b_3 \ldots\ldots b_n \end{pmatrix}$ be the identity

permutation of degree n. Then $I_P \in A_n$

If $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$ is any element of A_n, we have

$$f_1 I_P = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 .....b_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$$

$$= f_1$$

Also $$I_P f_1 = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ a_1 & a_2 & a_3 .....a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$$

$$= f_1$$

Hence the identity permutation I_P is the identity element.

Existence of Inverse. Let $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$ be any element of A_n

Then $f_1^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 .....b_n \\ a_1 & a_2 & a_3 .....a_n \end{pmatrix}$ is also an element of A_n since f_1^{-1} is also a permutation of degree n .

We have

$$f_1^{-1} f_1 = \begin{pmatrix} b_1 & b_2 & b_3 .....b_n \\ a_1 & a_2 & a_3 .....a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 .....a_n \\ b_1 & b_2 & b_3 .....b_n \end{pmatrix}$$

$$= \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots\ldots b_n \\ b_1 & b_2 & b_3 \ldots\ldots\ldots b_n \end{pmatrix}$$

$$= I_P$$

Also

$$f_1 f_1^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots\ldots a_n \\ b_1 & b_2 & b_3 \ldots\ldots\ldots b_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots\ldots b_n \\ a_1 & a_2 & a_3 \ldots\ldots\ldots a_n \end{pmatrix}$$

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

$$= I_P$$

Hence the inverse of f_1 is f_1^{-1}.

Hence A_n is a group of order $n!$ with respect to product of permutations as composition.

If $n = 1$, the set A_n has only one element and every group of order 1 is abelian.

If $n = 2$, the set A_n has $2!$ *i.e.*, 2 element and every group of order 2 is again abelian.

Now we shall show that if $n > 2$, A_n is non-abelian.

Consider f_1 and f_2 are two permutation of degree 5 such that

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \text{ and } f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

Then we have

$$f_1 f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

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

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

$$f_2 f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

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

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

Here $f_1 f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$ and $f_2 f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$.

Hence $f_1 f_2 \neq f_2 f_1$.

Therefore A_n is non-abelian if $n > 2$.

Note 1. If $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 \ldots\ldots a_{n-1} & a_n \\ b_1 & b_2 & b_3 \ldots\ldots b_{n-1} & b_n \end{pmatrix}$ be a permutation of degree n, then the inverse of f_1^{-1} i.e., f_1^{-1} is obtained by interchanging the two rows of f_1. Thus we have

$$f_1^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 \ldots\ldots & b_{n-1} & b_n \\ a_1 & a_2 & a_3 \ldots\ldots & a_{n-1} & a_n \end{pmatrix}.$$

4.9 Cyclic Permutation, Transposition and Disjoint Cycles

Cyclic Permutation

A permutation is known as cyclic permutation if objects are replaced cyclically in it.

For example, the permutation $f_1 = \begin{pmatrix} a & b & c & d & e \\ b & c & d & e & a \end{pmatrix}$ is cyclic. It can be represented by the cycle $(a\ b\ c\ d\ e)$ which means that each element in the bracket is replaced by the element following it, the last element is replaced by the first element.

Note:1. The number of objects in a cyclic is called its length.

2. A cycle does not change by changing the place of its elements provided their cyclic order is not changed.

Thus we have $(a\ b\ c\ d) = (b\ c\ d\ a) = (c\ d\ a\ b) = (d\ a\ b\ c)$.

Transposition

A cycle of length two is called a transposition.

For example, If the transposition $(b\ c)$ is a permutation of degree three on three symbols *a*, *b*, *c* then the corresponding permutation will be $\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$.

Note: A cycle of length one represents the identity permutation.

Disjoint Cycles

Two cycles are said to be disjoint if they have no symbols in common.

For example, $(a\ c\ e)$ and $(b\ f\ h\ i)$ are disjoint cycles while $(a\ c\ d)$ and $(b\ c\ e\ f)$ are not disjoint.

Note:1. Every permutation can be expressed as a product of disjoint cycles. For example, let $f_1 = \begin{pmatrix} a & b & c & d & e & f & g & h & i \\ b & c & a & d & h & f & i & g & e \end{pmatrix}$ be a permutations of degree nine on the set $\{a, b, c, d, \ldots\ldots\ldots, i\}$.

We have $f_1 = (d)\,(f)\,(a\ b\ c)(e\ h\ g\ i)$.

4.10 Even and Odd Permutation

A permutation is said to be even or odd according as it can be expressed as a product of even or odd number of transpositions.

Theorem. Of the $n!$ permutations on n symbols, $\frac{1}{2}n!$ are even permutations and $\frac{1}{2}n!$ are odd permutations.

Proof. Out of the $n!$ permutations on n symbols let the even permutations be $e_1, e_2, \ldots, e_m$ and the odd permutations be $o_1, o_2, \ldots, o_k$.

Since a permutation is either an even permutations or an odd permutations but not both, therefore, $m + k = n!$

If A_n be the set of all permutation of degree n, then $A_n = \{e_1, e_2, \ldots e_m, o_1, o_2, \ldots o_k\}$

Let $t \in A_n$ and suppose t is a transposition.

Since A_n is a group with respect to permutation multiplication, therefore

$te_1, te_2, \ldots, te_m$ to $to_1, to_2, \ldots, to_k$ are all elements of A_n.

Obviously, $te_1, te_2, \ldots, te_m$ are all odd permutations and $to_1, to_2, \ldots, to_k$ are all even permutations.

Now no two of the permutations $te_1, te_2, \ldots, te_m$ are equal because

$te_i = te_j \Rightarrow e_i = e_j$ (by left cancellation law in the group A_n)

Therefore if $e_i \neq e_j$, then $te_i \neq te_j$

Thus the m odd permutations $te_1, \ldots te_m$ are distinct elements of A_n. But we have supposed that A_n contains exactly k odd permutations. Therefore m cannot be greater than k. Thus

$$m \leq k \qquad \ldots.(1)$$

Similarly, we can show that the k even permutations $to_1, to_2, \ldots, to_k$ are distinct elements of A_n. Therefore, we must have $k \leq m$ ….(2)

Form equations (1) and (2), it follows that $m = k = \frac{n!}{2}$.

Solved Examples

Example.4. Obtain the inverse of the following permutation:

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

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

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

Sol. (i) We have $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

To find f_1^{-1}, we interchanging the rows, we have

$$f_1^{-1} = \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Rearranging the columns, we have

$$f_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

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

To find f_2^{-1}, we interchanging the rows, we have

$$f_2^{-1} = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Rearranging the columns, we have

$$f_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

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

To find f_3^{-1}, we interchanging the rows, we have

$$f_3^{-1} = \begin{pmatrix} 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Rearranging the columns, we have

$$f_3^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Example.5. Let $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ be two permutations of degree three. To show that $f_1 f_2 = f_2 f_1$.

Sol. It is given that

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

Then we have

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

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

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

and

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

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

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

Hence $f_1 f_2 = f_2 f_1$.

Example.6. How many times $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ **be multiplied to itself to produce** $I_P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$**?**

Sol. We have $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$

Then we have

$$f_1^2 = f_1 . f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

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

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

Now we have

$$f_1^3 = f_1^2 . f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

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

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

$$= I_P.$$

Example.7. Prove that the set A_3 of three permutations $(a), (a\ b\ c), (a\ c\ b)$ or $\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$ on three symbols a, b, c forms a finite abelian group with respect to the permutation multiplication.

Sol. Let $f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$, $f_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$ and $f_3 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$ are three permutations.

For preparing the composition table, the composition being denoted multiplicatively.

Product of Permutations	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_3	f_1
f_3	f_3	f_1	f_2

We have $f_2 f_2 = (abc)(abc) = (acb) = f_3$,

Then we have

$$f_2 f_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} b & c & a \\ c & a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

and

$$f_2 f_3 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} b & c & a \\ a & b & c \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}.$$

$= I_P = f_1$ = identity permutation, and so on.

Here all the entries in the composition table are elements of A_3. Therefore A_3 is closed with respect to multiplication of permutations. Multiplication of permutations is an associative composition. Here f_1 is the identity element.

Each element possesses inverse. We have $f_1^{-1} = f_1,\ f_2^{-1} = f_3,\ f_3^{-1} = f_2.$

The composition is commutative since the corresponding rows and columns of the composition table are identical. The number of elements in the set A_3 is 3. In fact A_3 is the set of all even permutations of degree 3. Hence A_3 is the finite abelian group of order 3 with respect to permutation multiplication.

4.11 Summary

Let $A = \{a_1,\ a_2,\ a_3, ..., a_n\}$ be a finite set having n distinct elements. A permutation is a function which is one-one onto.

The number of elements in the finite set A is called as the degree of permutation.

Let f_1 and f_2 are two permutation of degree n. Then f_1 and f_2 are said to be equal permutations if we have $f_1(a) = f_2(a), \forall a \in A.$

If $A=\{a_1,\ a_2\}$ is a finite set having two elements, then the identity permutation is defined as

$$I_p=\begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}.$$

Consider f_1 and f_2 are two permutation of degree n. Then the product f_1 and f_2 is denoted as $f_1 f_2$, is obtained by first carrying out the operation defined by f_1 and then by f_2.

Let $f=\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & ..... & a_n \\ b_1 & b_2 & b_3 & b_4 & ..... & b_n \end{pmatrix}$ be a permutation of degree n then $f^{-1}=\begin{pmatrix} b_1 & b_2 & b_3 & b_4 & ..... & b_n \\ a_1 & a_2 & a_3 & a_4 & ..... & a_n \end{pmatrix}$ is known as the inverse permutation of degree n such that f $f^{-1}=I_P$.

The set A_n of all permutations of n symbols is a finite group of order $n!$ with respect to composite of mappings as the operation. For $n\le 2$, this group is abelian and for $n>2$ it is always non-abelian.

A permutation is known as cyclic permutation if objects are replaced cyclically in it.

The number of objects in a cyclic is called its length.

A cycle does not change by changing the place of its elements provided their cyclic order is not changed.

A cycle of length two is called a transposition.

Two cycles are said to be disjoint if they have no symbols in common.

Every permutation can be expressed as a product of disjoint cycles.

Of the $n!$ permutations on n symbols, $\frac{1}{2}n!$ are even permutations and $\frac{1}{2}n!$ are odd permutations.

4.12 Terminal Questions

Q.1. Write down all the permutations on three symbols a, b, c. Which of these permutations are even?

Q.2. Define a permutation. If $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, find AB and BA.

Q.3. If $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, then find $f_1 f_2$.

Q.4. Find the inverse of each of the following permutations:

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ (iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Q.5. Show that the set P_3 of all permutations on three symbols 1, 2, 3 is a finite non-abelian group of order 6 with respect to permutation multiplication as composition.

Q.6. Write down all the permutations on four symbols 1, 2, 3, 4. Which of these permutations are even?

Q.7. Show that the four permutations $I, (ab), (cd), (ab)(cd)$ on four symbols a, b, c, d form a finite abelian group with respect to the permutation multiplication.

Answer:

6. $4!$ i.e., 24 permutations of degree 4. If P_4 is the set of all these permutations, then

$$P_4 = \{(1), (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143), (234), (243),\}$$

$$(12)(34), (23)(14), (31)(24), (1234), (1243), (1324), (1342), (1423), (1432).$$

If A_4 is the set of all even permutations of degree 4, then A_4 will have $\frac{1}{2} \times 4!$ i.e., 12 elements.

Thus, $A_4 = \{(1),(123),(132),(124),(142),(134),(143),(234),(243),(12)(34),(23)(14),(31)(24)\}$.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

UNIT- 5: Order of an element of a group and Isomorphism on Groups

Structure

5.1 Introduction

The ideas of order of an element and group isomorphism are important parts of group theory, a branch of mathematics developed in the 1800s by mathematicians like Évariste Galois and Niels Henrik Abel. The *order* of an element in a group is the smallest number of times you need to combine it with itself to get back to the group's identity element (which acts like zero in addition or one in multiplication). This helps us understand how elements behave and how smaller groups can form within a larger group.

A group isomorphism is a special kind of mapping between two groups that shows they are basically the same in structure, even if they look different. Isomorphisms help mathematicians study groups in a more general way, focusing on structure rather than appearance. These ideas are used in many areas, such as cryptography (for secure communication), physics (to study symmetries in nature), chemistry (to

understand molecular shapes), and computer science (in coding and data structures). Knowing about element order and isomorphisms helps us understand how systems work and solve real-world problems.

5.2 Objectives

After studying this unit the learner will be able to understand the :

- Order of an element of a group
- Some important theorems on order of an element of a group
- Homomorphic mapping and isomorphic mapping
- Isomorphic Groups

5.3 Order of an element of a group

Let G be a group and e be the identity of a group G. An element $a \in G$ is said to be of order n if n is the least positive integer such that $a^n = e.$

or

If $a^n = e$ then $o(a) = n,$ where e is the identity element of G and a is any element of G.

Note: 1. In any group the identity element e is always of order one and it is the only element of order one. We have $e^1 = e \Rightarrow o(e) = 1.$

2. The symbol $o(a)$ is used to denote the order of $a.$

3. In additive notation we use the words $na = e$ in place of $a^n = e.$

4. If $na \neq e$ for any positive integer n then a said to be of zero order or infinite order.

Solved Examples

Example.1. Let $G=\{1,\ \omega,\ \omega^2\}$ be a finite multiplicative group. Find the order of each element of G.

Sol. It is given that $G=\{1,\ \omega,\ \omega^2\}$.

Here G is a finite multiplicative group so 1 is the identity element, i.e., $o(1)=1$.

We have

$(\omega)^1=\omega,$

$(\omega)^2=\omega^2,$

$(\omega)^3=\omega^3=1$ (*i.e.*, 1 is an identity element)

Therefore $o(\omega)=3.$

Now we have

$(\omega^2)^1=\omega^2,$

$(\omega^2)^2=\omega^4=\omega^3.\omega=\omega,$

$(\omega^2)^3=\omega^6=\omega^3.\omega^3=1.1=1$ (*i.e.*, 1 is an identity element)

Therefore $o(\omega^2)=3.$

Hence the order of the elements 1, ω, ω^2 are 1, 3 and 3.

Example.2. Find the order of the permutation $A=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$**.**

Sol. It is given that $A=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}$.

We have

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

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

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

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

$$A^3=A^2A$$

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

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

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

Hence $o(A)=3.$

Example.3. Let $G=\{1,\ -1,\ i,\ -i\}$ be a finite multiplicative group. Find the order of each element of G.

Sol. It is given that $G=\{1,\ -1,\ i,\ -i\}$.

Here G is a finite multiplicative group so 1 is the identity element, i.e., $o(1)=1.$

We have

$$(-1)^1=-1,$$

$$(-1)^2=1.$$ (*i.e.*, 1 is an identity element)

Therefore $o(-1)=2.$

Now we have

$$(i)^1=i,$$

$$(i)^2=-1,$$

$$(i)^3=i^2.i=(-1).i=-i,$$

$$(i)^4=i^2.i^2=(-1).(-1)=1.$$ (*i.e.*, 1 is an identity element)

Therefore $o(i)=4.$

Again we have

$$(-i)^1=-i,$$

$$(-i)^2=i^2=-1,$$

$$(-i)^3=i^2.(-i)=(-1).(-i)=i,$$

$$(-i)^4=i^2.i^2=(-1).(-1)=1.$$ (*i.e.*, 1 is an identity element)

Therefore $o(-i)=4.$

Hence the order of the elements $1,\ -1,\ i, -i$ are 1, 2, 4 and 4.

Example.4. Let $G=\{a,\ a^2,\ a^3, a^4,\ a^5,\ a^6=e\}$ be a finite multiplicative group. Find the order of each element of G.

Sol. It is given that $G=\{a,\ a^2,\ a^3, a^4,\ a^5,\ a^6=e\}$.

Here G is a finite multiplicative group and it is given that $a^6=e$ is the identity element of G, i.e., $o(a^6)=1$.

We have

$$a^6=e \ \Rightarrow o(a)=6.$$

$$(a^2)^3=a^6=e \ \Rightarrow o(a^2)=3.$$

$$(a^3)^2=a^6=e \ \Rightarrow o(a^3)=2.$$

$$(a^4)^3=a^{12}=(a^6)^2=e^2=e \ \Rightarrow o(a^4)=3.$$

$$(a^5)^6=a^{30}=(a^6)^5=e^5=e \ \Rightarrow o(a^5)=6.$$

$$(a^6)^1=a^6=e \ \Rightarrow o(a^6)=1.$$

Hence the order of elements $a,\ a^2,\ a^3, a^4,\ a^5,\ a^6$ are 6, 3, 2, 3, 6, 1.

Example.5. Let $G=\{0,\ 1,\ 2, 3,\ 4,\ 5\}$ be a finite group with addition modulo 6. Find the order of each element of G.

Sol. It is given that $G=\{0,\ 1,\ 2, 3,\ 4,\ 5\}$.

Here G is a finite group with addition modulo 6 and 0 is the identity element of G, i.e., $o(0)=1$.

We have

$$(1)^1 = 1,$$

$$1^2 = 1 +_6 1 = 2,$$

$$1^3 = 1 +_6 1 +_6 1 = 1 +_6 2 = 3,$$

$$1^4 = 1 +_6 1 +_6 1 +_6 1 = 1 +_6 3 = 4,$$

$$1^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 1 +_6 4 = 5,$$

$$1^6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 1 +_6 5 = 0$$ (*i.e.*, 0 is an identity element)

Therefore $o(1) = 6.$

Now we have

$$2^1 = 2,$$

$$2^2 = 2 +_6 2 = 4,$$

$$2^3 = 2 +_6 2^2 = 2 +_6 4 = 0$$ (*i.e.*, 0 is an identity element)

Therefore $o(2) = 3.$

Now we have

$$3^1 = 3,$$

$$3^2 = 3 +_6 3 = 0,$$ (*i.e.*, 0 is an identity element)

Therefore $o(3) = 2.$

Now we have

$$4^1 = 4,$$

$4^2 = 4 +_6 4 = 2,$

$4^3 = 4 +_6 4^2 = 4 +_6 2 = 0,$ (*i.e.*, 0 is an identity element)

Therefore $o(4) = 3.$

Now we have

$5^1 = 5,$

$5^2 = 5 +_6 5 = 4,$

$5^3 = 5 +_6 5^2 = 5 +_6 4 = 3,$

$5^4 = 5 +_6 5^3 = 5 +_6 3 = 2,$

$5^5 = 5 +_6 5^4 = 5 +_6 2 = 1,$

$5^6 = 5 +_6 5^5 = 5 +_6 1 = 0,$ (*i.e.*, 0 is an identity element)

Hence the order of elements $0,\ 1,\ 2,\ 3,\ 4,\ 5$ are 6, 3, 2, 3, 6.

Example.6. To show that in the infinite multiplicative group of non-zero rational numbers, the order of every element except the elements 1 and -1 is infinite.

Sol. It is given that in the infinite multiplicative group of non-zero rational numbers, the order of every element except the elements 1 and -1 is infinite.

We have

$(1)^1 = 1,$ (*i.e.*, 1 is an identity element)

Therefore $o(1) = 1.$

Now we have

$(-1)^1 = -1,$

$(-1)^2 = 1.$ (*i.e.*, 1 is an identity element)

Therefore $o(-1) = 2.$

Now $2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16,\ 2^5 = 32, \ldots\ldots$ and so on.

Thus there exists no positive integer n such that $2^n = 1$ (*i.e.*, identity element). Therefore $o(2)$ is infinite.

Check your Progress

Q.1. What do you mean by order of an element of a group?

Q.2. To show that in the additive group of integers the order of every element except 0 is infinite, where 0 is the identity element.

Q.3. Let $G = \{1,\ 2, 3,\ 4,\ 5,\ 6\}$ be a finite group with addition modulo 7. Find the order of each element of G.

Q.4. Let $G = \{1,\ 5, 7,\ 11\}$ be a finite group with multiplication modulo 12. Find the order of each element of G.

Q.5. Find the order of each element of the group $G = \{0,\ 1,\ 2,\ 3\}, +_4$.

5.4 Some important theorems on order of an element of a group

Theorem.1. The order of every element of a finite group is finite and is less than or equal to the order of the group.

Proof. Consider G is a finite multiplicative group and $a \in G$. Let us consider all the positive integral powers of a *i.e.,* $a, a^2, a^3, a^4, \ldots.$ all these are elements of G, by closure property. Since G has a finite number of elements, therefore all the integral powers of a cannot be distinct elements of G. Let us consider that $a^r = a^s \, (r > s)$.

Now we have

$$a^r = a^s$$

$$\Rightarrow \quad a^{r-s} = a^s a^{-s} \qquad \left[\because a^{-s} \in G\right]$$

$$\Rightarrow \quad a^{r-s} = a^0$$

$$\Rightarrow \quad a^{r-s} = e$$

$$\Rightarrow \quad a^m = e \text{ where } m = r - s.$$

Since $r > s,$ therefore m is a positive integers. Thus the set of all those positive integers m such that $a^m = e$ has a least members, say n. Thus there exists a least positive integer n such that $a^n = e$. Therefore $o(a)$ is finite.

Now to prove that $o(a) \le o(G)$.

Let $o(a) = n$ where $n > o(G)$. Since $a \in G,$ therefore using the closure property $a, a^2, a^3, a^4, \ldots\ldots, a^n$ are elements of G. No two of these are equal.

If possible, suppose $a^r = a^s, 1 \le s < r \le n.$ Then we have $a^{r-s} = e.$ Since $0 < r - s < n,$ therefore $a^{r-s} = e$ implies that the order of a is less than n. This is a contradiction.

Thus $a, a^2, a^3, a^4, \ldots\ldots, a^n$ are n distinct elements of G. Since $n > o(G)$, therefore this is not possible.

Hence we must have $o(a) \le o(G)$.

Theorem 2. The order of an element a of a group is the same as that of its inverse a^{-1}.

Proof. Consider n and m are the orders of a and a^{-1} respectively of a group.

We have $o(a) = n \Rightarrow a^n = e$ (identity element)

$\Rightarrow \quad (a^n)^{-1} = e^{-1}$

$\Rightarrow \quad (a^{-1})^n = e$

$\Rightarrow \quad o(a^{-1}) \leq n$

$\Rightarrow \quad m \leq n$.

Also we have

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

$\Rightarrow \quad (a^{-1})^m = e$

$\Rightarrow \quad (a^m)^{-1} = e$

$\Rightarrow \quad a^m = e \qquad [\because b^{-1} = e \Rightarrow b = e]$

$\Rightarrow \quad o(a) \leq m$

$\Rightarrow \quad n \leq m$.

Now we have $m \leq n$ and $n \leq m$

$\Rightarrow \quad m = n$

If the order of a is infinite, then the order of a^{-1} cannot be finite. Because we have

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

$\Rightarrow \quad o(a) \leq m$

$\Rightarrow$ $o(a)$ is finite.

Therefore if the order of a is infinite, then the order of a^{-1} must also be infinite.

Hence, in all cases, $o(a) = o(a^{-1})$.

Theorem.3. If the element a of a group G is of order n, then $a^m = e$ if and only if n is a divisor of m.

Proof. Suppose n is a divisor of m. Then there exists an integers q such that $nq = m$.

Now we have

$$a^m = a^{nq}$$

$$= (a^n)^q$$

$$= e^q \qquad [\because o(a) = n \Rightarrow a^n = e]$$

$$= e.$$

Conversely, suppose $a^m = e$.

Since m is an integer and n is a positive integer, then by using division algorithm, there exist integers q and r such that $m = nq + r$, where $0 \le r < n$.

Now we have

$$a^m = a^{nq+r}$$

$$= a^{nq} a^r$$

$$= (a^n)^q a^r$$

$$= e^q a^r \qquad [\because a^n = e]$$

$$= ea^r$$
$$= a^r .$$

$\therefore \quad a^m = e$

$\Rightarrow \quad a^r = e$.

Since $0 \le r < n$, therefore $a^r = e$ this implies r must be equal to zero because otherwise $o(a)$ will not be equal to n.

If $o(a) = n$, then there will exist no positive integer $r < n$ such that $a^r = e$.

Now we see that

$r = 0$

$\Rightarrow \quad m = nq$

$\Rightarrow \quad n$ is a divisor of m.

Theorem.4. The order of the elements a and $x^{-1}ax$ are the same where a, x are any two elements of a group.

Proof. Let n and m be the orders of a and $x^{-1}ax$ respectively of a group G.

Now we have

$$\left(x^{-1}ax\right)^2 = \left(x^{-1}ax\right)\left(x^{-1}ax\right)$$
$$= x^{-1}a\left(xx^{-1}\right)ax$$
$$= x^{-1}aax$$
$$= x^{-1}a^2x$$

In general, we get

$$\left(x^{-1}ax\right)^n = x^{-1}a^n x$$

$$= x^{-1}ex \qquad \left[\because o(a) = n \Rightarrow a^n = e\right]$$

$$= x^{-1}x$$

$$= e.$$

Therefore we have

$$o\left(x^{-1}ax\right) \le n \Rightarrow m \le n.$$

Again we have

$$o\left(x^{-1}ax\right) = m$$

$\Rightarrow \quad \left(x^{-1}ax\right)^m = e$

$\Rightarrow \quad x^{-1}a^m x = e$

$\Rightarrow \quad x^{-1}a^m x = x^{-1}x$

$\Rightarrow \quad a^m x = x$ (using left cancellation law)

$\Rightarrow \quad a^m x = ex$

$\Rightarrow \quad a^m = e$ (using right cancellation law)

Finally, we get

$$m \le n,\ n \le m \quad \Rightarrow \quad m = n.$$

Hence the order of the elements a and $x^{-1}ax$ are the same where a, x are any two elements of a group.

Theorem.5. The order of any integral power of an element a cannot exceed the order of *a*.

Proof. Consider a^k is any integral power of a.

Suppose $o(a) = n$.

Now we have

$$o(a) = n$$

$\Rightarrow$ $a^n = e$ (i.e., identity element)

$\Rightarrow$ $\left(a^n\right)^k = e^k$

$\Rightarrow$ $a^{nk} = e$

$\Rightarrow$ $\left(a^k\right)^n = e$

$\Rightarrow$ $o\left(a^k\right) \leq n$.

Hence the order of any integral power of an element a cannot exceed the order of *a*.

Theorem 6. If a **is an element of order** n **and** p **is prime to** n, **then** a^p **is also of order** n.

Proof. Consider that m is the order of a^p.

Now we have

$$o(a) = n$$

$\Rightarrow$ $a^n = e$

$\Rightarrow$ $\left(a^n\right)^p = e^p = e$

$\Rightarrow$ $\left(a^p\right)^n = e$

$\Rightarrow$ $o\left(a^p\right) \leq n$

$\Rightarrow \qquad m \le n$.

Since p, n are relative primes, there exist integers x and y such that $px + ny = 1$.

Now we have

$$a = a^1$$

$$= a^{px+ny}$$

$$= a^{px} a^{ny}$$

$$= a^{px} \left(a^n\right)^y$$

$$= a^{px} e^y$$

$$= a^{px} e$$

$$= a^{px}$$

$$= \left(a^p\right)^x .$$

Again we have

$$a^m = \left[\left(a^p\right)^x\right]^m$$

$$= \left(a^p\right)^{mx}$$

$$= \left[\left(a^p\right)^m\right]^x$$

$$= e^x \qquad \left[\because o\left(a^p\right) = m \Rightarrow \left(a^p\right)^m = e\right]$$

$$= e .$$

$\therefore \qquad o(a) \le m \Rightarrow n \le m.$

Finally we have shown that $m \le n$ and $n \le m \Rightarrow m = n$.

Solved Examples

Example.7. Consider that $axa = b$ in a group G, find the value of x.

Sol. It is given that G is a group and $axa = b$.

Now we have $axa = b$

$\Rightarrow \quad a^{-1}(axa) = a^{-1}b$

$\Rightarrow \quad (a^{-1}a)(xa) = a^{-1}b$

$\Rightarrow \quad e(xa) = a^{-1}b$

$\Rightarrow \quad xa = a^{-1}b$

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

$\Rightarrow \quad x(aa^{-1}) = a^{-1}ba^{-1}$

$\Rightarrow \quad xe = a^{-1}ba^{-1}$

$\Rightarrow \quad x = a^{-1}ba^{-1}.$

Example.8. Prove that if for every element a in a group G, $a^2 = e$, then G is an abelian group.

Sol. Consider a and b are any two elements of the group G. Then ab is also an element of G.

So we have

$$(ab)^2 = e.$$

Now we have

$$(ab)^2 = e$$

$$\Rightarrow \quad (ab)(ab) = e$$

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

$$\Rightarrow \quad b^{-1}a^{-1} = ab \qquad .....(1)$$

But we have

$$a^2 = e$$

$$\Rightarrow \quad aa = e$$

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

Similarly, we have

$$b^2 = e$$

$$\Rightarrow \quad b^{-1} = b$$

Therefore form equation (1), we get

$$ba = ab.$$

Thus we have $ab = ba \quad \forall\, a, b \in G.$

Hence G is an abelian group.

Example.9. Show that if every element of a group G is its own inverse, then G is abelian.

Sol. Consider a and b are any two elements of a group G. Then ab is also an element of G. So, we have

$(ab)^{-1} = ab$ as it is given that every element is its own inverse.

Now we have

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

$$\Rightarrow \quad b^{-1}a^{-1} = ab$$

$$\Rightarrow \quad ba = ab \qquad \left[\because \quad a^{-1} = a,\ b^{-1} = b\right]$$

Thus we have $ab = ba \ \forall\, a, b \in G.$ Hence G is an abelian group.

Example.10. Show that if a, b are any two elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

Sol. Suppose G is an abelian group.

Then we have

$$(ab)^2 = (ab)(ab)$$

$$= a(ba)b$$

$$= a(ab)b \qquad [\because G \text{ is abelian } \Rightarrow ab = ba]$$

$$= (aa)(bb)$$

$$= a^2b^2.$$

Conversely, consider a, b are any two elements of a group G.

Then we have

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

$$\Rightarrow \quad (ab)(ab) = (aa)(bb)$$

$\Rightarrow \quad a(ba)b = a(ab)b$

$\Rightarrow \quad (ba)b = (ab)b$ [using left cancellation law]

$\Rightarrow \quad ba = ab$ [using right cancellation law]

Hence G is an abelian group.

Example.11. Prove that a group G is abelian if $b^{-1}a^{-1}ba = e \ \forall a, b \in G.$

Sol. We have $b^{-1}a^{-1}ba = e$

$\Rightarrow \quad (b^{-1}a^{-1})(ba) = e$

$\Rightarrow \quad (b^{-1}a^{-1})^{-1} = ba \qquad [\because ba = e \ \Rightarrow \ a^{-1} = b]$

$\Rightarrow \quad (a^{-1})^{-1}(b^{-1})^{-1} = ba \qquad [\because (ab)^{-1} = b^{-1}a^{-1}]$

$\Rightarrow \quad ab = ba \qquad [\because (a^{-1})^{-1} = a]$

Hence G is an abelian group.

5.5 Homomorphism mapping

Suppose G and G' are any two multiplicative groups. A mapping f of G into G' is said to be a homomorphism mapping (or a homomorphism) of G into G' if and only if $f(ab) = f(a)\,f(b) \ \forall a, b \in G.$

If f is a homomorphism mapping of a group G onto the group G' so that $f(G) = G'$, then the group G' is called a homomorphic image of the group G.

5.6 Isomorphic mapping

Suppose G and G' are any two multiplicative groups. A mapping f of G into G' is said to be an isomorphic mapping (or an isomorphism) of G into G' if

(i) f is one –to-one.

(ii) $f(ab) = f(a) f(b) \forall a, b \in G$.

5.7 Isomorphic Groups

Suppose G and G' are any two multiplicative groups. Then we say that the group G is isomorphic to the group G' if the mapping f preserves the compositions in G and G'.

If the group G is isomorphic to the group G', i.e., we write in notation form $G \cong G'$.

Check your Progress

Q.1. Define the homorphism mapping.

Q.2. What is isomorphic mapping.

Q.3. Explain the concept of isomorphic groups.

Solved Examples

Example.12. Show that the multiplicative group $G = \{1, -1, i, -i\}$ is isomorphic to group $G' = \{0, 1, 2, 3\}$ under addition modulo 4.

Sol. It is given that $G = \{1, -1, i, -i\}$ is a multiplicative group and $G' = \{0, 1, 2, 3\}$ is a group under addition modulo 4.

Here the identity element of G is 1 and G' is 0. Let $f:G\to G'$ then we take $f(1)=0.$

To find the f- images of other elements in isomorphism first we determine the order of elements in G and G'.

The order of elements of G are $o(-1)=2,\quad o(i)=4,\ o(-i)=4.$

The order of elements of G' are $o(1)=4,\quad o(2)=2,\ o(3)=4.$

Here we see that the $o(-1)=2$ and $o(2)=2$ so we have $f(-1)=2.$

Similarly we take $f(i)=1$ and $f(-i)=3.$

Hence it is clear that f is one-one and onto.

Composition table for G

o	1	-1	*i*	-*i*
1	1	-1	*i*	-*i*
-1	-1	1	-*i*	*i*
i	*i*	-*i*	-1	1
-*i*	-*i*	*i*	1	-1

Composition table for G'

$+_4$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

Thus from the above composition table if we replace each element of G by its image we get table for G'. Hence $f(a*b)=f(a)*f(b)$. Thus $G\cong G'.$

Example.13. If R is the additive group of real numbers and R_+ the multiplicative group of positive

real numbers, prove that the mapping $f : R \to R_+$ defined by $f(x) = e^x \;\forall\; x \in R$ is an isomorphism of R onto R_+.

Sol. It is given that R is an additive group of real numbers and R_+ the multiplicative group of positive real numbers. Also given that the mapping $f : R \to R_+$ defined by $f(x) = e^x \;\forall\; x \in R.$ If x is any real number, positive, zero or negative, then e^x is always real number. Also e^x is unique. Therefore if $f(x) = e^x$, then $f : R \to R_+$.

(i) f is one-one: Consider $x_1, x_2 \in R.$

Then we have

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

$$\Rightarrow \quad e^{x_1} = e^{x_2} \qquad \left[\text{By the definition of } f,\ f(x) = e^x\right]$$

$$\Rightarrow \quad \log e^{x_1} = \log e^{x_2}$$

$$\Rightarrow \quad x_1 \log e = x_2 \log e$$

$$\Rightarrow \quad x_1 = x_2.$$

Therefore here we see that the two elements in R have the same f-image in R_+ only if they are equal. Consequently distinct elements in R have distinct f-images in R_+.

Hence f is one-one.

(ii) f is onto: Suppose that y is any element of R_+ *i.e.,* y is any positive real number. Then $\log y$ is a real number *i.e.,* $\log y \in R.$

Now we have $f(\log y) = e^{\log y} = y.$ Thus $y \in R_+$ this implies that there exist $\log y \in R$ such that $f(\log y) = y$. Therefore each element of R_+ is the f-image of some element of $R.$

Hence f is onto.

(iii) f preserves group compositions: Consider x_1 and x_2 are any two elements of R. Then we have

$$f(x_1 + x_2) = e^{x_1 + x_2} \qquad \text{[by definition of } f \text{]}$$

$$= e^{x_1} e^{x_2}$$

$$= f(x_1) f(x_2). \qquad \left[\because f(x_1) = e^{x_1} \text{ and } f(x_2) = e^{x_2}\right]$$

Thus f preserves compositions in R and R_+. Here the composition in R is addition and the composition in R_+ is multiplication. Therefore f is an isomorphism of R onto R_+ i.e., $R \cong R_+$.

Example.14. Let R_+ be the multiplicative group of all positive real numbers and R be the additive group of all real numbers. Show that the mapping $g : R_+ \to R$ defined by $g(x) = \log x \;\forall\; x \in R_+$ is an isomorphism.

Sol. It is given that R_+ be the multiplicative group of all positive real numbers and R be the additive group of all real numbers. Also given that the mapping $g : R_+ \to R$ defined by $g(x) = \log x \;\forall\; x \in R_+$**.**

If x is any positive real number, then $\log x$ is definitely a real number. Also $\log x$ is unique. Therefore if $g(x) = \log x$, then $g : R_+ \to R$.

(i) g is one-one**:** Consider $x_1, x_2 \in R_+$.

Then we have $g(x_1) = g(x_2)$

$\Rightarrow \qquad \log x_1 = \log x_2$

$\Rightarrow \qquad e^{\log x_1} = e^{\log x_2}$

$\Rightarrow \qquad x_1 = x_2$.

Therefore g is one-to-one.

(ii) g is onto. Suppose that y is any element of R *i.e.,* y is any real number. Then e^y is definitely a positive

real number $i.e., e^y \in R_+$.

Now we have $g\left(e^y\right) = \log e^y = y$. Thus $y \in R$ this implies that there exist $e^y \in R_+$ such that $g\left(e^y\right) = y$.

Therefore each element of R is the g- image of some element of R_+. Thus g is onto.

(iii) g preserves group compositions. Consider x_1 and x_2 are any two elements of R_+. Then we have

$$g(x_1 x_2) = \log(x_1 x_2) \qquad \text{[by definition of g]}$$

$$= \log x_1 + \log x_2$$

$$= g(x_1) + g(x_2) \qquad \text{[by definition of g]}$$

Thus g preserves compositions in R_+ and R. Here the composition in R_+ is multiplication and the composition in R is addition. Therefore g is an isomorphism of R_+ onto R i.e., $R_+ \cong R$.

Example.15. Show that the additive group of integers $G = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$ is isomorphic to the additive group $G' = \{\ldots\ldots, -3m, -2m, -1m, 0, 1m, 2m, 3m, \ldots\ldots\}$, where m is any fixed integer and not equal to zero.

Sol. It is given that additive group of integers $G = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$ and additive group $G' = \{\ldots\ldots, -3m, -2m, -1m, 0, 1m, 2m, 3m, \ldots\ldots\}$.

If $x \in G$, then obviously $mx \in G'$. Let $f : G \to G'$ be defined by $f(x) = mx \; \forall \; x \in G$.

(i) f is one-one: Consider $x_1, x_2 \in G$.

Then we have $f(x_1) = f(x_2)$

$\Rightarrow \quad mx_1 = mx_2 \qquad$ [by definition of f]

$\Rightarrow \quad x_1 = x_2. \qquad [\because m \neq 0]$

Therefore f is one-to-one.

(ii) f is onto: Suppose that y is any element of G'. Then obviously $y/m \in G$. Also $f(y/m) = m(y/m) = y$. Thus $y \in G'$ this implies that there exists $y/m \in G$ such that $f(y/m) = y$. Therefore each element of G' is the $f-$image of some element of G.

Hence f is onto.

(iii) f preserves group compositions: Consider x_1 and x_2 are any two elements of G. Then we have

$$f(x_1 + x_2) = m(x_1 + x_2) \qquad \text{[by definition of } f \text{]}$$

$$= mx_1 + mx_2 \qquad \text{[by distributive law for integers]}$$

$$= f(x_1) + f(x_2). \qquad \text{[by definition of } f \text{]}$$

Thus f preserves compositions in G and G'. Therefore f is an isomorphic mapping of G onto G' i.e., $G \cong G'$.

5.8 Summary

Let G be a group and e be the identity of a group G. An element $a \in G$ is said to be of order n if n is the least positive integer such that $a^n = e$.

The symbol $o(a)$ denotes the order of a. In additive notation we use the words $na = e$ in place of $a^n = e$.

If $na \neq e$ for any positive integer n then a said to be of zero order or infinite order.

The order of every element of a finite group is finite and is less than or equal to the order of the group. The order of an element a of a group is the same as that of its inverse a^{-1}. If the element a of a group G is of order n, then $a^m = e$ if and only if n is a divisor of m.

Suppose G and G' are any two multiplicative groups. A mapping f of G into G' is said to be a homomorphism mapping (or a homomorphism) of G into G' if and only if

$f(ab) = f(a)\,f(b) \quad \forall\, a, b \in G.$ If f is a homomorphic mapping of a group G onto the group G' so that $f(G) = G'$, then the group G' is called a homomorphic image of the group G.

Suppose G and G' are any two multiplicative groups. A mapping f of G into G' is said to be an isomorphic mapping (or an isomorphism) of G into G' if

(i) f one –to-one. (ii) $f(ab) = f(a)\,f(b) \forall\, a, b \in G$.

Suppose G and G' are any two multiplicative groups. Then we say that the group G is isomorphic to the group G' if there mapping f preserves the compositions in G and G'. If the group G is isomorphic to the group G', i.e., we write in notation form $G \cong G'$.

5.9 Terminal Questions

Q.1. Define the order of an element of a group.

Q.2. To show that the order of any power of an element a of a group G is a multiple of the order of a.

Q.3. Define the order of an element in (i) an additive group, (ii) a multiplicative group.

Q.4. Discuss between the order of a group and the order of an element in a group. Prove that if

$a, x \in G$, then a and xax^{-1} have the same order in G.

Q.5. Prove that if $a^2 = a, a \in G$, then $a = e$.

Q.6. Prove that a group G is abelian if every element of G except the identity element is of order two.

Q.7. Find the order of each element of the group $(\{0, 1, 2, 3, 4\}, +_5)$.

Q.8. Find the order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$.

Q.9. If the elements a, b and ab of a group are each of order 2, prove that $ab = ba$.

Q.10. If a is an element of a group, prove that the integral powers of a form a multiplicative group.

Q.11. Prove that a group G is abelian iff $(ab)^{-1} = a^{-1}b^{-1} \forall a, b \in G$.

Q.12. If in the group G, $a^5 = e, ab\,a^{-1} = b^{-2}$ for $a, b \in G$ then find $o(b)$.

Q.13. What do you mean by homomorphic and isomorphic mapping?

Q.14. Define the isomorphic groups.

Q.15. Show that the group $[\{0, 1, 2, 3\}, +_4]$ is isomorphic to the group $[\{1, 2, 3, 4\}, \times_5]$.

Q.16. Show that the multiplicative group $\{1, -1, i, -i\}$ is isomorphic to the group of residue classes modulo 4 under addition of residue classes.

Q.17. Show that the set C of all complex numbers under addition is a group which is isomorphic to itself under the identity mapping as well as under the mapping which takes every complex number into its conjugate complex.

Q.18. Show that the multiplicative group $\{1, \omega, \omega^2\}$ is isomorphic to the group of residue classes modulo 3 under addition of residue classes.

Answer

7. $o(0) = 1$ and each other element is of order 5.

8. 3.

12. If $b = e$, then $o(b) = 1$ and if $b \neq e$, then $o(b) = 31$.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

UNIT- 6: Subgroup and Cosets

Structure

6.1 Introduction

Subgroups and cosets are fundamental concepts in group theory, a key area of abstract algebra. A subgroup is a subset of a group that itself satisfies the group properties under the same operation. Galois notably used group structures to explore the solvability of polynomial equations, laying the foundation for modern

algebra. cosets, which divide a group into distinct, equal-sized parts relative to a subgroup, were introduced to deepen the understanding of group structure. They are instrumental in proving crucial theorems, such as Lagrange's Theorem, which states that the order of a subgroup divides the order of the entire group.

Moreover, cosets play a key role in forming quotient groups, allowing for a more detailed classification of groups. Subgroups and cosets are widely used in both pure and applied mathematics, including fields like number theory, geometry, and topology. Beyond mathematics, they have significant roles in physics, cryptography, coding theory, and chemistry, particularly in understanding molecular structures. In computer science, subgroup structures are vital in algorithm design for computational group theory and in developing secure communication systems. Their power to simplify and interpret complex group behaviors makes them invaluable across various scientific and mathematical disciplines.

6.2 Objectives

After studying this unit the learner will be able to understand the :

- Complexes and Subgroups of a group
- Algebra of complexes of a group, and Intersection of subroups and Cosets
- Lagrange's theorem, Cayley's theorem, Fermat's theorem, and Euler's theorem

6.3 Subgroup and Complexes

Subgroup

Let G be a group and H is a non-empty subset of G. Then H is said to be a subgroup of G if H itself a group under the same operations as in G.

Complexes

Let G be a group. Then any non-empty subset H of G is known as complex of G.

Note: 1. Every subgroup of G is a complex of G but every complex is not always a subgroup.

2. We know that every set is a subset of itself.

3. If G is a group, then G itself is a subgroup of G. Also if e is the identity of G, then the subset of G containing only one element *i.e.,* e is also a subgroup of G. These two subgroups (itself G and e) of G are known as trivial or improper subgroups and if others subgroups of G are available then they are known as proper subgroups of G.

4. The identity of a subgroup is the same as that of the group.

5. The inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

6. The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$.

7. The group of integers with respect to addition is a subgroup of the group of all rational numbers with respect to addition.

8. The group of even integers with respect to addition is a subgroup of the group of all integers with respect to addition.

9. The multiplicative group of positive rational number is a subgroup of the multiplicative group of all non-zero rational numbers.

10. The order of any element of a subgroup is the same as the order of that element regarded as a member of the group.

6.4 Algebra of Complexes of a group

Let G be a group and H and K are any two complexes of group G, then

$$HK = \{x \in G \mid x = hk, h \in H, k \in K\}.$$

Clearly, $HK \subseteq G$. Therefore HK is a complex of G consisting of the elements of G achieved on multiplying each member of H with each member of K.

Note: 1. Let G be a group and H, K, L are any three complexes of G, then $(HK)L = H(KL)$.

2. Let H be any complex of G. Then we define $H^{-1} = \{h^{-1} : h \in H\}$ *i.e.,* H^{-1} is the complex of G consisting of the inverse of the elements of H.

Theorem 1. If H and K are any two complexes of group G, then $(HK)^{-1} = K^{-1}H^{-1}$.

Proof. Let x be any arbitrary element of $(HK)^{-1}$. Then we have

$$x = (hk)^{-1}, \quad h \in H, k \in K$$

$$= k^{-1}h^{-1} \in K^{-1}H^{-1} \qquad [\because k^{-1} \in K^{-1}, h^{-1} \in H^{-1}]$$

$\therefore \qquad (HK)^{-1} \subseteq K^{-1}H^{-1}.$

Again let y be any arbitrary element of $K^{-1}H^{-1}$.

Then we have

$$y = k^{-1}h^{-1}, \quad k \in K, h \in H$$

$$= (hk)^{-1} \in (HK)^{-1} \qquad [\because hk \in HK]$$

Therefore we have $K^{-1}H^{-1} \subseteq (HK)^{-1}$

Hence $(HK)^{-1} = K^{-1}H^{-1}$

Theorem 2. If H is any subgroup of G, then $H^{-1} = H$. Also show that the converse is not true.

Proof. Let h^{-1} be any arbitrary element of H^{-1}. Then $h \in H$. Now H is a subgroup of G. Therefore $h \in H \Rightarrow h^{-1} \in H$. Thus $h^{-1} \in H^{-1} \Rightarrow h^{-1} \in H$. Therefore we have $H^{-1} \subseteq H$.

Again we have

$h \in H \quad \Rightarrow \quad h^{-1} \in H \qquad [\because H \text{ is itself a group}]$

$\Rightarrow \quad \left(h^{-1}\right)^{-1} \in H^{-1} \qquad [\text{ by definition of } H^{-1}]$

$\Rightarrow \quad h \in H^{-1}.$

Therefore we have $H \subseteq H^{-1}$.

Hence $H^{-1} = H$.

If H is a complex of a group G and $H^{-1} = H$, then it is not necessary that H is a subgroup of G. For example, $H = \{-1\}$ is a subgroup of the multiplicative group $G = \{-1, 1\}$. Also $H^{-1} = \{-1\}$ since -1 is the inverse of -1 in G. But $H = \{-1\}$ is not a subgroup of G. We have $(-1)(-1) = 1 \notin H$. Thus H is not closed with respect to multiplication.

Theorem 3. If H is any subgroup of a group G, then $HH = H$.

Proof. Let $h_1 h_2$ be any element of HH where $h_1 \in H, h_2 \in H$.

Since H is a subgroup of G, therefore, $h_1 h_2 \in H \Rightarrow h_1 h_2 \in H$.

Therefore we have $HH \subseteq H$.

Now let h be any element of H. Then we can write $h = he$ where e is the identity of G.

Now we have $he \in HH$, since $h \in H, e \in H$. Thus $H \subseteq HH$.

Hence $H = HH$.

Theorem.4. A non-empty subset H of a group G is a subgroup of G if and only if

(i) $a \in H, b \in H \Rightarrow ab \in H$; **(ii)** $a \in H \Rightarrow a^{-1} \in H$ **where** a^{-1} **is the inverse of** a **in** G**.**

Proof. Necessary Conditions: Let H be a subgroup of G. Then H itself a group under the same operation as in *G*. Thus *H* must be closed with respect to multiplication *i.e.*, the composition in *G*.

Therefore we have $a \in H, b \in H \Rightarrow ab \in H$.

Let $a \in H \Rightarrow a^{-1} \in H$ (since H itself is a group).

Therefore we have $a \in H \Rightarrow a^{-1} \in H$, where a^{-1} is the inverse of a in G .

Sufficient Conditions:

Closure Property: It is given that $a \in H, b \in H \Rightarrow ab \in H$, therefore H is closed with respect to multiplication.

Associativity. The elements of H are also the elements of G. Since G is Associative. Therefore H is also associative under the same operation as in *G*.

Identity Property: We know that the identity of the subgroup is the same as the identity of the group.

Now we have

$a \in H \Rightarrow a^{-1} \in H$. [From the given condition (ii)]

Further $a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H$ [From the given condition (i)]

Therefore we have $e \in H$.

Hence the identity e is an element of H .

Inverse Property: Since $a \in H \Rightarrow a^{-1} \in H$, therefore each element of H possesses inverse. Hence H itself is a group under the same operation as in G. Therefore H is a subgroup of G .

Theorem.5. A necessary and sufficient condition for a non-empty subset H **of a group** G **to be** a **subgroup is that** $a \in H, b \in H \Rightarrow ab^{-1} \in H$**, where** b^{-1} **is the inverse of** b **in** G**.**

Proof. Necessary Condition: Let H be a subgroup of G. Then H itself a group under the same operation as in *G*.

Let $a \in H, b \in H$. Now each element of H must possess inverse because H itself is a group.

Therefore we have $b \in H \Rightarrow b^{-1} \in H$.

Additionally, H must be closed with respect to multiplication *i.e.,* the composition as in G. Therefore we have $a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Sufficient Condition:

It is given that $a \in H, b \in H \Rightarrow ab^{-1} \in H$.

We are to prove that H is a sub-group of G.

Identity Property: We have

$$a \in H, a \in H \Rightarrow aa^{-1} \in H \qquad \text{[using the given condition]}$$

$$\Rightarrow \quad e \in H.$$

Hence the identity e is an element of H.

Inverse Property: Let a be any element of H. Using the given condition, we have

$$e \in H, a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H.$$

Hence the each element of H possesses inverse.

Closure Property. Let $a, b \in H$. Then as shown above $b \in H \Rightarrow b^{-1} \in H$. Therefore using the given condition, we have

$$a \in H, b^{-1} \in H \Rightarrow a\left(b^{-1}\right)^{-1} \in H \Rightarrow ab \in H.$$

Hence *H* is closed with respect to the composition as in G.

Associativity. The elements of H are also the elements of G. Since G is Associative. Therefore H is also associative under the same operation as in *G*.

Hence H itself is a group for the composition in G. Therefore H is a subgroup of G.

Theorem.6. If H, K are two subgroups of a group G, then HK is a subgroup of G, iff $HK = KH$.

Proof. Let H and K be any two subgroups of a group G. Let $HK = KH$. In order to prove that HK is a subgroup of G it is sufficient to prove that $(HK)(HK)^{-1} = HK$.

We have

$$(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1})$$

$$= H(KK^{-1})H^{-1} \qquad \text{(Due to associativity)}$$

$$= (HK)H^{-1} \qquad [\because K \text{ is a subgroup} \Rightarrow KK^{-1} = K]$$

$$= (KH)H^{-1} \qquad [\because HK = KH]$$

$$= K(HH^{-1}) \qquad \text{(Due to associativity)}$$

$$= KH \qquad [\because H \text{ is a subgroup} \Rightarrow HH^{-1} = H]$$

$$= HK. \qquad [\because HK = KH]$$

Therefore $HK = KH$ this implies HK is a subgroup of G.

Conversely, consider that HK is a subgroup.

Then we have

$$(HK)^{-1} = HK$$

$\Rightarrow \qquad K^{-1}H^{-1} = HK$

$\Rightarrow \qquad KH = HK \qquad \left[\because K \text{ is a subgroup} \Rightarrow K^{-1} = K \text{ and similarly } H^{-1} = H\right]$

Hence $HK = KH$.

Note: 1. If H, K are subgroups of an abelian group $G,$ then HK is a subgroup of G .

6.5 Intersection of Subgroups

Theorem.7. If H_1 and H_2 are two subgroups of a group $G,$ then $H_1 \cap H_2$ is also a subgroup of G

Proof. Suppose H_1 and H_2 are any two subgroups of $G.$ Then $H_1 \cap H_2 \neq \varnothing,$ since at least the identity element e is common to both H_1 and H_2 .

To prove that $H_1 \cap H_2$ is a subgroup, first we have to prove that

$$a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2 .$$

Now we have

$$a \in H_1 \cap H_2 \Rightarrow a \in H_1$$

and $\quad a \in H_2, b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$.

But H_1, H_2 are subgroups of G. Therefore we have

$$a \in H_1, b \in H_1 \Rightarrow ab^{-1} \in H_1,$$

$$a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2 .$$

Finally, we have $\quad ab^{-1} \in H_1, ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2 .$

Therefore we have shown that $\quad a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2 .$

Hence $H_1 \cap H_2$ is a subgroup of G.

Note: 1. Arbitrary intersection of subgroups *i.e.*, the intersection of any family of subgroups of a group is a subgroup.

2. The union of two subgroups is not necessarily a subgroup.

For example, let G be an additive group of integers.

Then we have

$$H_1 = \{\ldots\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}$$

and $H_2 = \{\ldots\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\ldots\}$ are both subgroups of G.

Now we have $H_1 \cup H_2 = \{\ldots\ldots, -4, -3, -2, 0, 2, 3, 4, 6, \ldots\ldots\}$.

Clearly, $H_1 \cup H_2$ is not closed with respect to addition as $2 \in H_1 \cup H_2, 3 \in H_1 \cup H_2$ but $2+3$ *i.e.*, $5 \notin H_1 \cup H_2$. Therefore $H_1 \cup H_2$ is not a subgroup of G.

However, $H_1 \cap H_2 = \{\ldots\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\ldots\}$ is a subgroup of G.

Solved Examples

Example.1. Let G be the additive group of integers. Then prove that the set of all multiples of integers by a fixed integer m is a subgroup of G.

Sol. It is given that G be the additive group of integers. So we have $G = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$ is the additive group of integers.

Let m be any fixed integer. Let $H = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots.\}$. Then we have $H \subseteq G$.

To prove that H is a subgroup of G. Let $a = rm$ and $b = sm$ be any two elements of H, where r and s are some integers. The inverse of sm in G is $(-s)$m *i.e.*, $-b = (-s)m$.

Now we have $a-b=rm+(-s)m=(r-s)m\in H$ since $r-s$ is also some integer.

Therefore we have $a\in H, b\in H \Rightarrow a-b\in H$.

Hence H is a subgroup of G.

6.6 Cosets

Here we introduce the important concept of right cosets and left cosets of a subgroup. Cosets are specific kind of subsets associated with a subgroup.

Let G be a group and H is any subgroup of G. Let a be any element of G. Then the set $Ha=\{ha:\in H\}$ is known as a right coset of H in G generated by a. Similarly the set $aH=\{ah:h\in H\}$ is known as the left coset of H in G generated by a.

Clearly, Ha and aH are both subsets of G.

If e is the identity element of G, then we have $He=H=eH$. Therefore H itself is a right as well as a left coset.

Note : 1. In the composition in the group G has been denoted additively, then the right coset of H in G generated by a is defined as $H+a=\{h+a:h\in H\}$. Similarly the left coset $a+H=\{a+h:h\in H\}$.

Example.2. Let G be the additive group of integers *i.e.,* $G=\{.....,-3,-2,-1,0,1,2,3,.....\}$. Let H be the subgroup of G obtained on multiplying each element of G by 3. Then we have $H=\{.....,-9,-6,-3,0,3,6,9,.....\}$.

Since the group G is abelian, any right coset will be equal to the corresponding left coset. Let us form the right cosets of H in G.

We have $0\in G$ and $H=H+0=\{...,9,-6,-3,0,3,6,9,....\}$.

Again we have $1\in G$ and $H+1=\{...,-8,-5,-2,1,4,7,10,...\}$.

Then we have $2 \in G$ and $H+2=\{....,-7-4,-1,2,5,8,11,...\}$.

Here we see that the right cosets $H, H+1$ and $H+2$ are all distinct and moreover these are disjoint *i.e.*, have no element common.

Now we have $3 \in G$ and $H+3=\{...,-6,-3,0,3,6,9,12,....\}$.

Here we see that $H+3=H$. Also we observe that $3 \in H$.

Again we have $4 \in G$ and $H+4=\{....,-5,-2,1,4,7,10,13,....\}$.

Here we see that $H+4=H+1$. Also we observe that $4 \in H+1$.

Similarly the right coset $H+5$ coincides with $H+2, H+6$ with $H, H+(-1)$ with $H+2, H+(-2)$ with $H+1$ and so on.

Hence we get only three distinct right cosets i.e., $H,\ H+1,\ H+2$.

Clearly, $G=H \cup (H+1) \cup (H+2)$.

Theorem.8. If H is any subgroup of G and $h \in H$, then $Hh=H=hH$.

Proof. Consider $h \in H$. Then to prove that $Hh=H$. Suppose h' is any arbitrary element of H. Then $h'h$ is an arbitrary element of Hh.

Since H is a subgroup, we have $h' \in H, h \in H \Rightarrow h'h \in H$.

Therefore every element of Hh is also an element of H. Hence $Hh \subseteq H$.

Again we have

$$h'=h'(h^{-1}h) \qquad [\because h^{-1}h=e]$$

$$=(h'h^{-1})h$$

$\in Hh \qquad \left[\because h \in H \Rightarrow h^{-1} \in H \text{ and } h' \in H, h^{-1} \in H \Rightarrow h'h^{-1} \in H\right].$

Therefore every element h' of H is also an element of Hh. Hence $H \subseteq Hh$.

Finally, we get $Hh \subseteq H$ and $H \subseteq Hh \Rightarrow Hh = H$.

Similarly we can prove that $hH = H$.

Theorem.9. If a, b **are any two elements of group G and H any subgroup of G, then**

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \text{ and } aH = bH \Leftrightarrow a^{-1}b \in H.$$

Proof. Since a is an element of Ha, therefore

$$Ha = Hb$$

Now we have

$$a \in Hb$$

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

$$\Rightarrow \quad ab^{-1} \in H\left(bb^{-1}\right)$$

$$\Rightarrow \quad ab^{-1} \in He$$

$$\Rightarrow \quad ab^{-1} \in H$$

Conversely, we have

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

$$\Rightarrow \quad Hab^{-1} = H \qquad \left[\because h \in H \Rightarrow Hh = H\right]$$

$$\Rightarrow \quad H\,ab^{-1}b = Hb$$

$$\Rightarrow \quad Hae = Hb$$

$\Rightarrow \qquad Ha = Hb.$

Similarly we can prove that $aH = bH \Leftrightarrow a^{-1}b \in H$.

Theorem.10. If a, b **are any two elements of a group** G **and** H **any subgroup of** G, **then** $a \in Hb \Leftrightarrow Ha = Hb$ **and** $a \in bH \Leftrightarrow aH = bH$ **.**

Proof. We have

$a \in Hb$

$\Rightarrow \qquad ab^{-1} \in Hbb^{-1}$

$\Rightarrow \qquad ab^{-1} \in He$

$\Rightarrow \qquad ab^{-1} \in H$

$\Rightarrow \qquad Hab^{-1} = H$

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

$\Rightarrow \qquad Hae = Hb$

$\Rightarrow \qquad Ha = Hb.$

Conversely, Consider $Ha = Hb$.

Since $a \in Ha,$ therefore we have $a \in Hb$.

Theorem.11. Any two right (left) cosets of a subgroup are either disjoint or identical.

Proof. Suppose H is a subgroup of a group G and let Ha and Hb be two right cosets of H in G.

Suppose Ha and Hb are not disjoint. Then there exists at least one element, say $c,$ such that $c \in Ha$ and $c \in Hb$. Let $c = h_1 a$ and $c = h_2 b$, where $h_1, h_2 \in H$.

Then we have

$$h_1 a = h_2 b$$

or $$h_1^{-1} h_1 a = h_1^{-1} h_2 b$$

or $$ea = \left(h_1^{-1} h_2\right) b$$

or $$a = \left(h_1^{-1} h_2\right) b \, .$$

Since H is a subgroup, therefore we have

$$h_1^{-1} h_2 \in H \, .$$

Consider $h_1^{-1} h_2 = h_3$.

Then we have $a = h_3 b$.

Now we have

$$Ha = Hh_3 b$$

$$= \left(Hh_3\right) b$$

$$= Hb \qquad \left[\because h_3 \in H \Rightarrow Hh_3 = H\right]$$

Therefore the two right cosets are identical if they are not disjoint.

Thus either $Ha \cap Hb = \varnothing$ or $Ha = Hb$.

Similarly, we can prove that either $aH \cap bH = \varnothing$ or $aH = bH$.

6.7 Lagrange's Theorem

Theorem.12. The order of each subgroup of a finite group is a divisor of the order of the group.

Proof. Let G be a group of a finite order n. Let H be a subgroup of G and let $o(H)=m$. Suppose $h_1, h_2, ..., h_m$ are the m members of H.

Let $a \in G$. Then Ha is a right coset of H in G and we have $Ha = \{h_1 a, h_2 a, ..., h_m a\}$. Ha has m distinct members, since $h_i a = h_j a \Rightarrow h_i = h_j$.

Therefore each right coset of H in G has m distinct members. Any two distinct right cosets of H in G are disjoint i.e., they have no element in common. Since G is a finite group, the number of distinct right cosets of H in G will be finite, say, equal to k. The union of these k distinct right cosets of H in G is equal to G. Thus if $Ha_1, Ha_2, ..., Ha_k$ are the k distinct right cosets of H in G, then

$$G = Ha_1 \cup Ha_2 \cup ..... \cup Ha_k$$

This implies the number of element in G = the number of elements in Ha_1

+ the number of elements in Ha_1 + ... + the number of elements in Ha_k

[$\because$ Two distinct right cosets are mutually disjoint]

Therefore we have

$$o(G) = km$$

$$\Rightarrow \quad n = km$$

$$\Rightarrow \quad k = \frac{n}{m}$$

$\Rightarrow$ m is a divisor of n

$\Rightarrow$ $o(H)$ is a divisor of $o(G)$.

Hence the order of each subgroup of a finite group is a divisor of the order of the group.

Theorem.13. The order of every element of a finite group is a divisor of the order of the group.

Proof. Suppose G is a finite group of order n. let $a \in G$ and let $o(a) = m$. To prove that m is a divisor of n.

Let $H = \{...., a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, ...\}$ be the subset of G consisting of all integral powers of a. Then we know that H is a subgroup of G. We shall show that H contains only m distinct elements and that they are $a, a^2, a^3, ..., a^m = e = a^0$.

Let $1 \le r \le m, 1 \le s \le m$ and $r > s$.

Then we have $a^r = a^s$

$\Rightarrow \quad a^r a^{-s} = a^s a^{-s}$

$\Rightarrow \quad a^{r-s} = a^0$

$\Rightarrow \quad a^{r-s} = e$.

Thus there exists a positive integer $r - s$ less than m such that $a^{r-s} = e$. But m is the least positive integer such that $a^m = e$. Therefore $a^r \neq a^s$. Therefore $a, a^2, a^3, ..., a^m = a^0 = e$ are all distinct elements of H.

Now suppose m is any element of H, where t is any integer. Using the division algorithm, we have

$t = mp + q$ where p and q are some integers and $0 \le q < m$.

Now we have

$$a^t = a^{mp+q}$$

$$= a^{mp} a^q$$

$$= \left(a^m\right)^p a^q$$

$$= e^p a^q$$

$= ea^q$

$= a^q$.

Since $0 \le q < m,$ therefore a^q is one of the m elements $a, a^2, ..., a^m = a^0$.

Hence H has only m distinct elements.

The order of H is m . By Lagrange's theorem m is a divisor of n .

Theorem.14. If G is a finite group of order n and $a \in G,$ then $a^n = e$.

Proof. In a finite group, the order of each element is finite. Suppose $o(a) = m$. The subset H of G consisting of all integral powers of a is a subgroup of G and the order of H is m . By Lagrange's theorem m is a divisor of n .

Consider $k = \frac{n}{m}$.

Then we have $n = mk$.

Now $a^n = a^{mk} = (a^m)^k = e^k$ $\quad [\because o(a) = m \Rightarrow a^m = e]$

$= e$.

Theorem.15. Let H and K be finite subgroups of a group G . Then $o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$.

Proof. Let HK is a subset of G . It is not necessary that it will be a subgroup of G . Using $o(HK)$ we mean the number of distinct elements in HK .

Consider $D = H \cap K$. Then D is a subgroup of G and $D \subseteq K$. Therefore D is a subgroup of K . Since K is finite, therefore the number of distinct right cosets in right coset decomposition of K with respect to D is finite. Let it be m . Using Lagrange's theorem, we have $m = \frac{o(K)}{o(D)}$.

If $Dk_1, Dk_2, ..., Dk_m$ are the distinct right cosets of D in K, then we have

$$K = Dk_1 \cup Dk_2 \cup ..... \cup Dk_m = \bigcup_{i=1}^{m} Dk_i .$$

Observe that $k_1, k_2, ..., k_m$ are some distinct elements in K.

Now we have $HK = H\left(\bigcup_{i=1}^{m} Dk_i\right)$

$$= \bigcup_{i=1}^{m} HDk_i$$

$$= \bigcup_{i=1}^{m} Hk_i \qquad \left[\because D \subseteq H \Rightarrow HD = H\right]$$

$$= Hk_1 \cup Hk_2 \cup ..... \cup Hk_m . \qquad .....(1)$$

We shall show that the cosets $Hk_1, Hk_2, .., Hk_m$ are pairwise distinct. Suppose we have

$$Hk_i = Hk_j$$

$$\Rightarrow \quad k_i k_j^{-1} \in H \cap K \qquad \left[\because k_i, k_j \in K \Rightarrow k_i k_j^{-1} \in K\right]$$

$$\Rightarrow \quad k_i k_j^{-1} \in D$$

$$\Rightarrow \quad Dk_i = Dk_j$$

$$\Rightarrow \quad k_i = k_j . \qquad \left[\because Dk_1, ..., Dk_m \text{ are distinct cosets}\right]$$

Thus $Hk_1, Hk_2, ..., Hk_m$ are distinct right cosets and so they are pairwise disjoint also. The number of elements in each of them is equal to $o(H)$ i.e., the number of elements in H. Therefore from (1) we conclude that the number of elements in HK is equal to $m \times o(H)$.

Therefore we have

$$o(HK) = m \times o(H)$$

$$= \frac{o(K)}{o(D)}.o(H)$$

$$= \frac{o(H)o(K)}{o(H \cap K)}.$$

Solved Examples

Example.3. Show that two right cosets Ha, Hb are distinct if and only if the two left cosets $a^{-1}H, b^{-1}H$ are distinct.

Sol. In order to prove the given statement we shall prove that two right cosets Ha, Hb are equal if and only if the two left cosets $a^{-1}H, b^{-1}H$ are equal.

Now we have

$$Ha = Hb$$

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

$\Leftrightarrow$ $ab^{-1}H = H$ $\quad [\because h \in H \Leftrightarrow hH = H]$

$\Leftrightarrow$ $a^{-1}ab^{-1}H = a^{-1}H$

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

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

6.8 Cayley's Theorem

Theorem.16. Every finite group G is isomorphic to a permutation group.

Proof. Let G be a finite group. If $a \in G$, then for every x in G the product ax is also an element

of G. Now consider the function f_a from G into G defined by

$$f_a(x) = ax \;\forall\; x \in G.$$

The function f_a is one-one because if $x, y \in G,$ then we have

$$f_a(x) = f_a(y)$$

$$\Rightarrow \quad ax = ay$$

$$\Rightarrow \quad x = y \qquad \text{[by left cancellation law in } G\text{]}$$

The function f_a is also onto because if x is any element of $G,$ then $\exists$ an element $a^{-1}x$ in G such that

$$f_a\left(a^{-1}x\right) = a\left(a^{-1}x\right)$$

$$= \left(aa^{-1}\right)x$$
$$= ex$$
$$= x$$

Thus f_a is a one-one function from G onto G. Therefore f_a is a permutation on G. Let G' denote the set of all such one-one onto functions defined on G corresponding to every element of G *i.e.,*

$$G' = \{ f_a : a \in G \}.$$

First we shall that G' is a group with respect to the operation known as composite or product of two functions.

Closure Property. Let $f_a, f_b \in G'$ where $a, b \in G$. From our definition of product of two functions, we have

$$(f_a f_b)(x) = f_a\left[f_b(x)\right] = f_a(bx) = a(bx) = (ab)x = f_{ab}(x) \text{ for all } x \in G.$$

Therefore by the definition of equality of two functions, we have

$$f_a f_b = f_{ab}. \qquad \text{…….(1)}$$

Since $ab \in G,$ therefore $f_{ab} \in G'$ and thus G' is closed with respect to the product of functions.

Associativity. Let $f_a, f_b, f_c \in G'$ where $a, b, c \in G$. Then we have

$$f_a(f_b f_c) = f_a f_{bc} \qquad \left[\because \text{from}(1), \quad f_b f_c = f_{bc}\right]$$

$$= f_{a(bc)} \qquad \left[\text{from } (1)\right]$$

$$= f_{(ab)c} \qquad \left[\text{by associativity in } G\right]$$

$$= f_{ab} f_c \qquad \left[\text{from}(1)\right]$$

$$= (f_a f_b) f_{c.} \qquad \left[\text{from } (1)\right]$$

Therefore given operation is associative.

Inverse Property. If a^{-1} is the inverse of a in $G,$ then $f_{a^{-1}}$ is the inverse of f_a in G' because

$$f_{a^{-1}} f_a = f_{a^{-1}a} = f_e$$

and $\quad f_a f_{a^{-1}} = f_{aa^{-1}} = f_{aa^{-1}} = f_e.$

Therefore G' is a group.

Now we shall show that $G \cong G'$.

Consider the function ϕ from G into G' defined by $\phi(a) = f_a \ \forall\, a \in G$.

ϕ is one-one. If $a, b \in G,$ then we have

$$\phi(a) = \phi(b)$$

$$\Rightarrow \qquad f_a = f_b$$

$$\Rightarrow \qquad f_a(x) = f_b(x) \ \forall\, x \in G$$

$\Rightarrow \qquad ax = bx \;\forall\, x \in G$

$\Rightarrow \qquad a = b$.

Hence ϕ is one-one.

ϕ is onto. Let f_a be any element of G'. Then $a \in G$ and we have $\phi(a) = f_a$. Therefore ϕ is onto.

ϕ preserves group compositions: If $a, b \in G,$ then we have

$$\phi(ab) = f_{ab} \qquad [\text{by def. of } \phi]$$

$$= f_a f_b. \qquad [\text{from}(1)]$$

$$= \phi(a)\phi(b) \qquad [\text{by def. of } \phi]$$

Therefore ϕ preserves group compositions in G and G'.

Hence $G \cong G'$.

6.9 Fermat's Theorem

Theorem.17. If p is a prime number and a is any integer then $a^p \equiv a \pmod{p}$.

Proof. Consider G is the set of non-zero residue classes of integers modulo p. If p is prime then G is a group of order $p-1$ with respect to multiplication of residue classes. Suppose a is any integer.

Case-I: If p is a divisor of a then $[a] = [o]$ and therefore $[a] \notin G$ but

$$p \mid a \;\Rightarrow\; p \mid a^p$$

$$\Rightarrow\; p \mid a^p - a$$

$$\Rightarrow\; a^p \equiv a \pmod{p}.$$

Case-II: If p is not a divisor of a then $[a] \neq [o]$ and therefore $[a] \in G$.

Hence we have

$$[a]^{o(G)} = [1]$$

$$\Rightarrow \quad [a]^{p-1} = 1$$

$$\Rightarrow \quad a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \quad a^{p-1} - 1 \text{ is divisible by } p$$

$$\Rightarrow \quad a\left(a^{p-1} - 1\right) \text{ is divisible by } p$$

$$\Rightarrow \quad a^{p} - a \text{ is divisible by } p$$

$$\Rightarrow \quad a^{p} \equiv a \pmod{p}.$$

Hence if p is a prime number and a is any integer then $a^{p} \equiv a \pmod{p}$.

6.10 Euler's Theorem

Theorem.18. If n is a positive integer and a is any integer prime to n then $a^{\phi(n)} \equiv 1 \pmod{n}$, where ϕ is Euler function.

Proof. Consider $[x]$ be residue class of the set of integers mod *n*. Consider $G = \{[x] : a$ is an integer relatively prime to *n* $\}$. Then G is a group of order $\phi(n)$ with respect to multiplication of residue classes of G.

Now we have

$$[a] \in G \qquad \Rightarrow \qquad [a]^{o(G)} = 1$$

$$\Rightarrow \qquad [a]^{\phi(n)} = [1]$$

$$\Rightarrow \qquad [a][a] \ldots\ldots\ldots\ldots \phi(n) \text{ times} = [1]$$

$$\Rightarrow \qquad [a.a \ldots\ldots\ldots\ldots \phi(n) \text{ times}] = [1]$$

$$\Rightarrow \qquad \left[a^{\phi(n)}\right] = [1]$$

$$\Rightarrow \qquad a^{\phi(n)} \equiv 1 \pmod{n}.$$

Hence if n is a positive integer and a is any integer prime to n then $a^{\phi(n)} \equiv 1 \pmod{n}$, where ϕ is Euler function.

6.11 Summary

Let G be a group and H is a non-empty subset of G. Then H is said to be a subgroup of G if H itself a group under the same operations as in G.

Let G be a group. Then any non-empty subset H of G is known as complex of G.

Every subgroup of G is a complex of G but every complex is not always a subgroup. The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$.

Let G be a group and H and K are any two complexes of group G, then $HK = \{x \in G \mid x = hk, h \in H, k \in K\}$.

A non-empty subset H of a group G is a subgroup of G if and only if

(i) $a \in H, b \in H \Rightarrow ab \in H$; (ii) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G.

A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$, where b^{-1} is the inverse of b in G.

The union of two subgroups is not necessarily a subgroup.

Let G be a group and H is any subgroup of G. Let a be any element of G. Then the set $Ha = \{ha :\in H\}$ is known as a right coset of H in G generated by a. Similarly the set $aH = \{ah : h \in H\}$ is known as the left coset of H in G generated by a.

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

Every finite group G is isomorphic to a permutation group.

If p is a prime number and a is any integer then $a^p \equiv a \pmod{p}$.

If n is a positive integer and a is any integer prime to n then $a^{\phi(n)} \equiv 1 \pmod{n}$, where ϕ is Euler function.

6.12 Terminal Questions

Q.1. Define the subgroup and complexes.

Q.2. What do you mean by left and right Cosets ?

Q.3. Prove that the only right (or left) coset of a subgroup H in a subgroup H in a group G which is also a subgroup of G is H itself.

Q.4. Let a be an element of a group G. The set $H = \{a^n : n \in I\}$ of all integral powers of a is a subgroup of G.

Q.5. State and prove Lagrange's theorem.

Q.6. Let H be a subgroup of a group G and define $T = \{x \in G : xH = Hx\}$. Prove that T is a subgroup of G.

Q.7. State and prove Cayley's theorem.

Q.8. State and prove Fermat's theorem.

Q.9. State and prove Euler's theorem.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

U. P. Rajarshi Tandon
Open University

Master of Science

PGMM -106/MAMM-106
Advanced Algebra

Block

3 Advanced Group Theory

Unit- 7

Cyclic Group

Unit- 8

Normal Subgroup

Unit- 9

Homomorphism

Block-3

Advanced Group Theory

Cyclic and normal subgroups are key concepts in group theory, developed in the 19th century by mathematicians like Évariste Galois. A cyclic group is generated by a single element and is used in number theory, cryptography, geometry, coding theory, computer science, and topology due to its regular structure. A normal subgroup, introduced by Galois, remains unchanged under certain operations and helps form quotient groups. It is essential in understanding group structure and has applications in algebra, geometry, physics, and many scientific fields. Both are simple yet powerful tools widely used in mathematics and technology. A homomorphism is a map between groups that preserves their structure. It helps in understanding group relationships, identifying normal subgroups, and forming quotient groups. Homomorphisms are key to simplifying and comparing groups and have important applications in fields like cryptography, coding theory, and physics.

In the seventh unit, we shall discuss about the cyclic group and some important theorems on cyclic groups. Normal subgroup, simple group, conjugate element, centre of a group, conjugate subgroup and quotient groups are also discussed in details in unit eight. Ninth unit introduced the concept of Homomorphism on groups, Kernel of a homomorphism, fundamental theorem on homomorphism of groups, automorphisms and inner automorphisms, Maximal subgroup, Composition series of a group, Jordon Holder's theorem, Solvable groups, Direct products, Sylow's theorem.

UNIT- 7: Cyclic Group

Structure

7.1 Introduction

The idea of a cyclic group is an important part of group theory, which was developed during the 19th century. Mathematicians like Évariste Galois, Cauchy, and Cayley played key roles in the development of cyclic group theory. A cyclic group is a group where all elements can be created by repeatedly applying a group operation to a single element, known as the generator. Because of their simple and regular structure, cyclic groups were among the first types of groups studied in mathematics. They are very useful in number theory, especially in understanding patterns in modular arithmetic, and are used in cryptography to help protect information, like in RSA and Diffie-Hellman encryption.

Cyclic groups also appear in geometry, where they describe rotations and patterns, and in coding theory, where they help create codes that detect and fix errors. In computer science, they are useful for studying systems with repeating behavior, like state machines. Even in topology, they help describe loops and

paths, such as the circular path around a circle. Overall, cyclic groups are simple but powerful tools used in many areas of mathematics and technology.

7.2 Objectives

After studying this unit the learner will be able to understand the :

- Cyclic group
- Some important theorem on cyclic group

7.3 Cyclic Group

Let G be a group and a is any element of G. Then G is said to be a cyclic group if there exist atleast one element in G whose order is equal to the order of G.

or

Let G be a group and a is any element of G. If every element $x \in G$ is of the form a^n, where n is some integer, then G is known as cyclic group. The element a is then a generator of G.

Solved Examples

Example.1. Let $G = \{1, \omega, \omega^2\}$ be a finite multiplicative group. To show that G is cyclic group and find the generators of G.

Sol. It is given that $G = \{1, \omega, \omega^2\}$. We know that the order of G is equal to number of distinct element in G, i.e., $o(G) = 3$.

Here G is a finite multiplicative group so 1 is the identity element, i.e., $o(1) = 1$.

We have

$$(\omega)^1 = \omega,$$

$(\omega)^2 = \omega^2,$

$(\omega)^3 = \omega^3 = 1$ (*i.e.*, 1 is an identity element)

Therefore $o(\omega) = 3.$

Here we see that the order of ω is equal to order of group G, i.e., $o(\omega) = o(G) = 3.$

Thus ω is a generator of G. Also the group G elements can be written as in form of $(\omega,\ \omega^2,\ \omega^3 = 1)$.

Now we have

$(\omega^2)^1 = \omega^2,$

$(\omega^2)^2 = \omega^4 = \omega^3.\omega = \omega,$

$(\omega^2)^3 = \omega^6 = \omega^3.\omega^3 = 1.1 = 1$ (*i.e.*, 1 is an identity element)

Therefore $o(\omega^2) = 3.$

Here we see that the order of ω^2 is equal to order of group G, i.e., $o(\omega^2) = o(G) = 3.$

Thus ω^2 is a generator of G. Also the group G elements can be written as in form of

$(\omega^2,\ (\omega^2)^2 = \omega, (\omega^2)^3 = 1).$

Therefore, both two elements of G $(\omega$ and $\omega^2)$ are generators of G.

Hence the given finite multiplicative group G is cyclic.

Example.2. Let $G = \{1,\ -1,\ i, -i\}$ be a finite multiplicative group. To show that G is cyclic group and find the generators of G.

Sol. It is given that $G=\{1,\ -1,\ i,\ -i\}$. We know that the order of G is equal to number of distinct elements in G, i.e., $o(G)=4.$

Here G is a finite multiplicative group so 1 is the identity element, i.e., $o(1)=1.$

We have

$$(-1)^1=-1,$$

$$(-1)^2=1.$$ (*i.e.*, 1 is an identity element)

Therefore $o(-1)=2.$

Now we have

$$(i)^1=i,$$

$$(i)^2=-1,$$

$$(i)^3=i^2.i=(-1).i=-i,$$

$$(i)^4=i^2.i^2=(-1).(-1)=1.$$ (*i.e.*, 1 is an identity element)

Therefore $o(i)=4.$

Here we see that the order of i is equal to order of group G, i.e., $o(i)=o(G)=4.$

Thus i is a generator of G. Also the group G elements can be written as in form of $(i,\ i^2=-1,\ i^3=-i,\ i^4=1).$

Again we have

$$(-i)^1=-i,$$

$(-i)^2 = i^2 = -1,$

$(-i)^3 = i^2.(-i) = (-1).(-i) = i,$

$(-i)^4 = i^2.i^2 = (-1).(-1) = 1.$ (*i.e.*, 1 is an identity element)

Therefore $o(-i) = 4.$

Here we see that the order of $-i$ is equal to order of group G, i.e., $o(-i) = o(G) = 4.$

Thus $-i$ is a generator of G. Also the group G elements can be written as in form of $\left((-i)^1 = -i,\ (-i)^2 = -1,\ (-i)^3 = i,\ (-i)^4 = 1\right).$

Therefore, both two elements of G $(i$ and $-i)$ are generators of G.

Hence the given finite multiplicative group G is cyclic.

Example.3. Let $G = \{a,\ a^2,\ a^3, a^4,\ a^5,\ a^6 = e\}$ be a finite multiplicative group. To show that G is cyclic group and find the generators of G.

Sol. It is given that $G = \{a,\ a^2,\ a^3, a^4,\ a^5,\ a^6 = e\}$. We know that the order of G is equal to number of distinct elements in G, i.e., $o(G) = 6.$

Here G is a finite multiplicative group and it is given that $a^6 = e$ is the identity element of G, i.e., $o(a^6) = 1.$

We have

$a^6 = e \ \Rightarrow o(a) = 6.$

$(a^2)^3 = a^6 = e \ \Rightarrow o(a^2) = 3.$

$\left(a^3\right)^2 = a^6 = e \Rightarrow o\left(a^3\right) = 2.$

$\left(a^4\right)^3 = a^{12} = \left(a^6\right)^2 = e^2 = e \Rightarrow o\left(a^4\right) = 3.$

$\left(a^5\right)^6 = a^{30} = \left(a^6\right)^5 = e^5 = e \Rightarrow o\left(a^5\right) = 6.$

$\left(a^6\right)^1 = a^6 = e \Rightarrow o\left(a^6\right) = 1.$

Here we see that the order of a and a^5 is equal to order of group G, *i.e.,* $o(a) = o\left(a^5\right) = o(G) = 6.$ Therefore, both two elements of G (a and a^5) are generators of G.

Hence the given finite multiplicative group G is cyclic.

Example.4. Let $G = \{0,\ 1,\ 2, 3,\ 4,\ 5\}$ be a finite group with addition modulo 6. To show that G is cyclic group and find the generators of G.

Sol. It is given that $G = \{0,\ 1,\ 2, 3,\ 4,\ 5\}$. We know that the order of G is equal to number of distinct elements in G, i.e., $o(G) = 6.$

Here G is a finite group with addition modulo 6 and 0 is the identity element of G, i.e., $o(0) = 1.$

We have

$(1)^1 = 1,$

$1^2 = 1 +_6 1 = 2,$

$1^3 = 1 +_6 1 +_6 1 = 1 +_6 2 = 3,$

$1^4 = 1 +_6 1 +_6 1 +_6 1 = 1 +_6 3 = 4,$

$1^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 1 +_6 4 = 5,$

$1^6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 1 +_6 5 = 0$ (*i.e.*, 0 is an identity element)

Therefore $o(1) = 6.$

Here we see that the order of 1 is equal to order of group G, i.e., $o(1) = o(G) = 6.$

Thus 1 is a generator of G. Also the group G elements can be written as in form of $\left(1^1 = 1,\ 1^2 = 2,\ 1^3 = 3,\ 1^4 = 4\ , 1^5 = 5,\ 1^6 = 0\right).$

Now we have

$2^1 = 2,$

$2^2 = 2 +_6 2 = 4,$

$2^3 = 2 +_6 2^2 = 2 +_6 4 = 0$ (*i.e.*, 0 is an identity element)

Therefore $o(2) = 3.$

Now we have

$3^1 = 3,$

$3^2 = 3 +_6 3 = 0,$ (*i.e.*, 0 is an identity element)

Therefore $o(3) = 2.$

Now we have

$4^1 = 4,$

$4^2 = 4 +_6 4 = 2,$

$4^3 = 4 +_6 4^2 = 4 +_6 2 = 0,$ (*i.e.*, 0 is an identity element)

Therefore $o(4) = 3.$

Now we have

$5^1 = 5,$

$5^2 = 5 +_6 5 = 4,$

$5^3 = 5 +_6 5^2 = 5 +_6 4 = 3,$

$5^4 = 5 +_6 5^3 = 5 +_6 3 = 2,$

$5^5 = 5 +_6 5^4 = 5 +_6 2 = 1,$

$5^6 = 5 +_6 5^5 = 5 +_6 1 = 0,$ (*i.e.*, 0 is an identity element)

Therefore $o(5) = 6.$

Here we see that the order of 5 is equal to order of group G, *i.e.*, $o(5) = o(G) = 6.$

Thus 5 is a generator of G. Also the group G elements can be written as in form of $\left(5^1 = 5,\ 5^2 = 4,\ 5^3 = 3,\ 5^4 = 2\ , 5^5 = 1,\ 5^6 = 0\right).$

Here we see that the order of 1 and 5 is equal to order of group G, *i.e.*, $o(1) = o(5) = o(G) = 6.$ Therefore, both two elements of G namely 1 and 5 are generators of G.

Hence the given finite group G with addition modulo 6 is cyclic.

Check your Progress

Q.1. What do you mean by cyclic group?

Q.2. Explain the concept of generator.

Q.3. Let $G = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$ be a finite group with addition modulo 7. To show that G is cyclic group and find the generators of G.

Q.4. Let $\left(G=\{0,\ 1,\ 2,\ 3,\ 4,\ 5\},+_6\right)$ be a finite group. To show that G is cyclic group and find the generators of G.

Q.5. Let $G=\{0,\ 1,\ 2,\ 3\},+_4$ be a finite group. To show that G is cyclic group and find the generators of G.

7.4 Some important Theorems on Cyclic Groups

Theorem 1. Every cyclic group is an abelian group.

Proof. Let G be a cyclic group whose generator is a. Suppose x, y are any two elements of G. Then there exist integers r and s such that

$$x = a^r, y = a^s.$$

Now we have

$$xy = a^r a^s$$

$$= a^{r+s}$$
$$= a^{s+r}$$

$$= a^s a^r$$
$$= yx$$

Therefore we have

$$xy = yx \quad \forall\, x, y \in G.$$

Hence G is abelian.

Theorem 2. If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof. Let G be a cyclic group whose generator is a. Consider a^r be any element of G, where r is some integer.

Now we can write $a^r = \left(a^{-1}\right)^{-r}$. Some $-r$ is also some integer, therefore each element of G is generated by a^{-1}. Therefore a^{-1} is also a generator of G.

Theorem.3. Every group of prime order is cyclic.

Proof. Suppose G is a finite group whose order is a prime number p; then to show that G is a cyclic group.

Note that an integer p is said to be a prime number if $p \neq 0,\ p \neq \pm 1,$ and if the only divisors of p are $\pm 1, \pm p$.

Since G is a group of prime order, therefore G must contain at least 2 elements. Note that 2 is the least positive prime integer.

Therefore there must exist an elements $a \in G$ such that $a \neq$ the identity element e.

Since a is not the identity element, therefore $o(a)$ is definitely ≥ 2. Let $o(a) = m$. Then $H = \{a\}$ is a cyclic subgroup of G and $o(H) = o(a) = m$.

Using Lagrange's theorem m must be a divisor of p. But p is prime and $m \geq 2$. Hence $m = p$.

Therefore $H = G$. Since H is cyclic, therefore G is cyclic and a is a generator of G.

Theorem 4. Every subgroup of a cyclic group is cyclic.

Proof. Suppose $G = \{a\}$ is a cyclic group generated by a. If $H = G$ or $\{e\}$, then obviously H is cyclic.

Therefore H is a proper subgroup of G. The elements of H are integral powers of a. If $a^s \in H$, then the inverse of a^s *i.e.,* $a^{-s} \in H$.

Thus H contains elements which are positive as well as prove that $H = \{a^m\}$ *i.e.,* H is cyclic and is generated by a^m.

Let a^t be any arbitrary element of H. Using division algorithm, there exist integers q and r such that

$t = mq + r, 0 \le r < m$.

Now we have $a^m \in H \Rightarrow \left(a^m\right)^q \in H$ [by closure property]

$\Rightarrow \quad a^{mq} \in H$

$\Rightarrow \quad \left(a^{mq}\right)^{-1} \in H$

$\Rightarrow \quad a^{-mq} \in H$.

Also we have

$a^t \in H, a^{-mq} \in H$

$\Rightarrow \quad a^t a^{-mq} \in H$

$\Rightarrow \quad a^{t-mq} \in H$

$\Rightarrow \quad a^r \in H \qquad \left[\because r = t - mq\right]$

Now m is the least positive integer such that $a^m \in H$ and $0 \le r < m$. Therefore must be equal to 0. Hence $t = mq$.

Therefore $a^t = a^{mq} = \left(a^m\right)^q$.

Thus every element $a^t \in H$ is of the form $\left(a^m\right)^q$. Therefore H is cyclic and a^m is a generator of H.

Solved Examples

Example.5. Show that the group $\left(\{1, 2, 3, 4, 5, 6\}, \times_7\right)$ is cyclic. How many generators are there?

Sol. Let $G = \left(\{1, 2, 3, 4, 5, 6\}, \times_7\right)$ be a group. If there exists an element $a \in G$ such that $o(a) = 6$ *i.e.*, equal to the order of the group G then the group G will be a cyclic group and a will be a generator of G.

We see that $o(3) = 6$ because

$3^1 = 3, 3^2 = 3 \times_7 3 = 2, 3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6,$

$3^4 = 6 \times_7 3 = 4 \times_7 3 = 5, 3^6 = 5 \times_7 3 = 1$ *i.e.*, the identity element.

Therefore G is cyclic and 3 is a generator of G.

Here we can write $G = \left\{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\right\}$.

Now 5 is prime to 6. Therefore 3^5 *i.e.*,5 is also a generator of G.

Example.6. How many generators are there of the cyclic group G of order 8?

Sol. Suppose a is a generator of G. Also it is given that $o(a) = 8.$ Here we can write

$$G = \left\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\right\}.$$

We know that if G is a cyclic group generated by a and $o(a) = n,$ then a^m is a generator of G if and only if m and n are relatively prime. So we make the following observations:

7 is prime to 8, therefore a^7 is also a generator of G.

5 is prime to 8, therefore a^5 is also a generator of G.

3 is prime to 8, therefore a^3 is also a generator of G.

Since 2 and 8, 4 and 8, 6 and 8, 8 and 8 are not relatively prime, therefore none of the elements a^2, a^4, a^6 and a^8 can be a generator of G.

Thus there are only four generators of G *i.e.,* a, a^3, a^5, a^7.

Example.7. Give an example of a finite abelian group which is not cyclic.

Sol. Let G be the set of the four matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

It can be easily seen that G is an abelian group with respect to multiplication of matrices. The identity element of this group is the identity matrix I.

Now we find the order of each element of G.

We have $o(I)=1.$

Also we have

$$A^2=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=I; \qquad \therefore o(A)=2;$$

$$B^2=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=I; \qquad \therefore o(B)=2;$$

$$C^2=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=I; \qquad \therefore o(C)=2;$$

Now G is a group of order 4 and G contains no elements of order 4. Therefore G is not a cyclic group. Hence G is a finite abelian group which is not cyclic.

6.11 Summary

Let G be a group and a is any element of G. Then G is said to be a cyclic group if there exist atleast one element in G whose order is equal to the order of G.

Let G be a group and a is any element of G. If every element $x\in G$ is of the form a^n, where n is some integer, then G is known as cyclic group. The element a is then a generator of G.

Every cyclic group is an abelian group. If a is a generator of a cyclic group $G,$ then a^{-1} is also a generator of G.

Every group of prime order is cyclic and every subgroup of a cyclic group is cyclic.

6.12 Terminal Questions

Q.1. Define the cyclic group.

Q.2. What do you mean by generators of a group ?

Q.3. If ω be the cube root of unity, show that the set $\{1, \omega, \omega^2\}$ is a cyclic group of order 3 with respect to multiplication.

Q.4. Find the order of each element in the multiplicative group of residues $1, 2, 3, 4, 5, 6$ prime to 7.

Q.5. Show that every finite group of order less than six must be abelian.

Q.6. Show that every isomorphic image of a cyclic group is again cyclic.

Q.7. To show that every proper subgroup of an infinite cyclic group is infinite.

Q.8. If G is an infinite cyclic group, then G has exactly two generators and G is isomorphic to the additive group of integers.

Q.9. A cyclic group G with generator of finite order n, is isomorphic to the multiplicative group of n th roots of unity.

Q.10. A cyclic group G with a generator of finite order n is isomorphic to the additive group of residue classes modulo n.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

UNIT-8: Normal Subgroup

Structure

8.1 Introduction

The idea of a normal subgroup came from the work of Évariste Galois in the 1800s. He used it while studying when polynomial equations could be solved using simple algebraic methods. Galois realized that some subgroups of a group remain unchanged under certain operations, and these special subgroups became known as normal subgroups. His work helped create the branch of mathematics we now call group theory, and the idea of normal subgroups became important for understanding the internal structure of groups.

Normal subgroups are very useful in many areas of mathematics and science. They help form quotient groups, which break larger groups into simpler parts. They also play an important role in homomorphisms, showing how two groups are related. In Galois theory, they help determine whether equations can be solved easily. In geometry and physics, normal subgroups are used to study symmetry and structure, such as in crystals or particle behavior. Because of their wide applications, normal subgroups are a fundamental concept in both pure and applied mathematics.

8.2 Objectives

After reading this unit the learner should be able to understand about the:

- Normal subgroup and simple group
- Conjugate elements and normalizer of an element of a group, and self conjugate elements
- The centre of a group
- Conjugate subgroup and normalizer of a subgroup of a group
- Self conjugate subgroups and quotient groups

8.3 Normal Subgroup

A subgroup H of a group G is said to be normal subgroup of G if for every $x \in G$ and for every $h \in H, xhx^{-1} \in H$.

From this definition we can immediately conclude that H is a normal subgroup of G if and only if $xHx^{-1} \subseteq H \; \forall \; x \in G$.

Note: 1. Consider G is an abelian group with operation multiplication. Let H be any subgroup of G. If x is any element of G, then Hx is a right coset of H in G and xH is a left coset of H in G. Also G is abelian, therefore we must have $Hx = xH \; \forall x \in G$.

2. However, if it is possible that G is not abelian, yet it keeps a subgroup H such that $Hx = xH \; \forall x \in G$. Such subgroups of a group G come under the category of normal subgroups and these are very important.

3. Consider G is a group and we have $x \in G \Rightarrow x^{-1} \in G$. Therefore H is normal subgroup of G if and only if $x^{-1}h\left(x^{-1}\right)^{-1}$ *i.e.,* $x^{-1}hx \in H \; \forall \; x \in G$ and $\forall h \in H$.

4. Every group G prossesses at least two normal subgroups namely G itself and the subgroup consisting of the identity element e alone. These are known as improper normal subgroups. There exist groups of which these are the only normal subgroups. Such groups are known as simple groups.

5. Since every cyclic group is abelian, therefore every subgroup of a cyclic group is normal.

8.4 Simple Group

A group having no proper normal subgroups is known as a simple group. Every group of prime order is simple. Using Lagrange's theorem such a group has no proper subgroups.

Theorem.1: A subgroup H of a group G is normal if and only if $xHx^{-1} = H \; \forall \; x \in G$.

Proof . Consider $xHx^{-1} = H \; \forall \; x \in G$. Therefore H is normal subgroup of G.

Converse. Let H be a normal subgroup of G.

Then $xHx^{-1} \subseteq H \; \forall \; x \in G$ …….(1)

$x \in G \Rightarrow x^{-1} \in G.$

Therefore we have

$$x^{-1}H\left(x^{-1}\right)^{-1} \subseteq xHx^{-1} \; \forall \; x \in G$$

$(x^{-1}H(x^{-1})^{-1}$ is a subset of H i.e. $x^{-1}Hx$ is a subset of H

for all $\Rightarrow$ $H \subseteq xHx^{-1} \; x \in G.$ ……(2)

From equations (1) and (2), we conclude that $xHx^{-1} = H$ for all $x \in G$

Hence a subgroup H of a group G is normal if and only if $xHx^{-1} = H \; \forall \; x \in G.$

Theorem.2. A subgroup H of a group G is a normal subgroup of G if and only if each left coset of H in G is a right coset of H in G.

Proof: Let G be a group and H is a normal subgroup of G.

Then we have

$$xHx^{-1} = H \quad \forall \; x \in G$$

$\Rightarrow$ $\left(xHx^{-1}\right)x = Hx$ for all $x \in G$

$\Rightarrow$ $xH = Hx$ for all $x \in G.$

This implies each left coset xH is the right coset Hx.

Conversely, suppose that each left coset of H in G is a right coset of H in G. Let x be any element of G. Then we have $xH = Hy$, for some $y \in G.$

Since $e \in H,$ therefore $xe = x \in xH.$

Therefore we have

$x \in Hy \qquad [\because \quad Hy = xH]$

But $x \in Hy \quad \Rightarrow \quad Hx = Hy$.

Thus $Hx = xH$. $\qquad [\because \quad Hy = xH]$

Thus we have

$$xH = Hx \quad \forall\, x \in G$$

$$\Rightarrow \qquad xHx^{-1} = Hxx^{-1} \quad \forall\, x \in G$$

$$\Rightarrow \qquad xHx^{-1} = H \;\forall\, x \in G.$$

This implies H is a normal subgroup of G.

Thus H is a normal subgroup of $G \Leftrightarrow xH = Hx \;\forall\, x \in G$.

Hence a subgroup H of a group G is a normal subgroup of G if and only if each left coset of H in G is a right coset of H in G.

Theorem.3. A subgroup H of a group G is a normal subgroup of G if and only if the product of two right cosets of H in G is again a right coset of H in G.

Proof . Let H be a normal subgroup of a group G. Let a, b be any two elements of G. Then Ha and Hb are two right cosets of H in G. We have

$$(Ha)(Hb) = H(aH)b$$

$$= H(Ha)b \qquad [\because H \text{ is normal } \Rightarrow Ha = aH]$$

$$= HHab$$

$$= Hab \qquad [\because HH = H]$$

Since $a \in G, b \in G \Rightarrow ab \in G,$ therefore Hab is also a right coset of H in G. Thus the product of the

right cosets Ha and Hb is the right coset Hab.

Converse. Let H be a subgroup of G such that the product of two right cosets of H in G is again a right coset of H in G. Let x be any element of G. Then $x^{-1} \in G$. Therefore Hx and Hx^{-1} are two right cosets of H in G.

Consequently, by hypothesis $HxHx^{-1}$ is also a right coset of H in G. Since $e \in H$, therefore we have $ex\,ex^{-1} = e$ is an element of the right coset $Hx\,Hx^{-1}$. But H itself is a right coset of H in G and $e \in H$

Also if two right cosets have one element common they must be identical.

Therefore we must have

$$Hx\,Hx^{-1} = H \ \forall\, x \in G$$

$$\Rightarrow \qquad h_1 x h x^{-1} \in H \ \forall\, x \in G \text{ and } \forall\, h_1, h \in H$$

$$\Rightarrow \qquad h_1^{-1}\left(h_1 x h x^{-1}\right) \in h_1^{-1} H \ \forall\, x \in G \text{ and } \forall\, h_1, h \in H$$

$$\Rightarrow \qquad x h x^{-1} \in H \ \forall\, x \in G \text{ and } \forall\, h \in H \qquad \left[\because h_1^{-1} H = H \text{ as } h_1^{-1} \in H \text{ since } n_1 \in H\right]$$

This implies H is a normal subgroup of G.

Hence a subgroup H of a group G is a normal subgroup of G if and only if the product of two right cosets of H in G is again a right coset of H in G.

Theorem.4. The intersection of any two normal subgroups of a group is a normal subgroup.

Proof. Let H and K be two normal subgroup of a group G. Since H and K are subgroup of G, therefore $H \cap K$ is also a subgroup of G. Now to prove that $H \cap K$ is a normal subgroup of G. Let x be any element of G and n be any element of $H \cap K$. Now we have

$$n \in H \cap K \ \Rightarrow \ n \in H, n \in K.$$

Since H is a normal subgroup of G, therefore we have

$x \in G, n \in H \Rightarrow xnx^{-1} \in H.$

Similarly, we have $xnx^{-1} \in K.$

Now we have

$$xnx^{-1} \in H,\ xnx^{-1} \in K \Rightarrow xnx^{-1} \in H \cap K$$

Thus we have

$$x \in G, n \in H \cap K \Rightarrow xnx^{-1} \in H \cap K.$$

Hence $H \cap K$ is a normal subgroup of G.

Solved Examples

Example.1. Show that every subgroup of an abelian group is normal.

Sol. Let G be an abelian group and H a subgroup of G. Let x be any element of G and h any element of H. We have

$$xhx^{-1} = xx^{-1}h \qquad \left[\because G \text{ is abelian} \Rightarrow x^{-1}h = hx^{-1}\right]$$

$$= eh = h \in H.$$

Thus $x \in G, h \in H \Rightarrow xhx^{-1} \in H.$

Hence H is normal in G.

Example.2. Let P_n be the symmetric group on n symbols. Prove that A_n is a normal subgroup of P_n.

Sol. Let α be any element of P_n and β any element of A_n. Then β is even permutation and α may be odd or even. We claim that $\alpha\beta\alpha^{-1}$ is an even permutation.

If α is odd, then α^{-1} is also odd. Now $\alpha\beta$ is odd and consequently $\alpha\beta\alpha^{-1}$ is even.

If α is even, then α^{-1} is also even. Now $\alpha\beta$ is even and consequently $\alpha\beta\alpha^{-1}$ is even.

Thus $\alpha \in P_n, \beta \in A_n \Rightarrow \alpha\beta\alpha^{-1} \in A_n$.

Hence A_n is a normal subgroup of P_n.

Example.3. If G is a group and H is a subgroup of index 2 in G prove that H is a normal of G.

Sol. Let H be a subgroup of index 2 in a group G.Then the number of distinct right (left) cosets of H in G is 2.

Let x be any element of G. If $x \in H$, then we have $xH = H = Hx$.

If $x \notin H$, then the right coset Hx is distinct from H and the left coset xH is distinct from H. But H is of index 2; therefore the number of distinct right (left) cosets in right (left) coset decomposition of G will be 2.

Therefore the cosets H, Hx, xH are such that

$$G = H \cup Hx = H \cup xH.$$

But there is no element common to H and Hx and also there is no element common to H and xH.

Therefore we must have $Hx = xH$.

Thus we have $Hx = xH \quad \forall\, x \in G$.

Hence H is a normal subgroup of G.

Check your progress

Q.1. What do you mean by normal subgroup?

Q.2. Define simple group.

Q.3. Give an example of each of the following:

(i) A sub-group H of some group G, which is not normal in G.

(ii) A non-trivial sub-group H of a non-abelian group G, which is normal in G.

Q.4. If H is a subgroup of G and N is a normal subgroup of G, show that $H \cap N$ is a normal subgroup of H.

8.5 Conjugate Elements

If a, b be two elements of a group G, then b is said to be conjugate to a if there exists an element $x \in G$ such that $b = x^{-1}ax$.

If $b = x^{-1}ax$, then b is also known as the transform of a by x.

If b is conjugate to a then symbolically we shall write $b - a$ and this relation in G will be called the relation of conjugacy. Thus $b - a$ if and only if $b - x^{-1}ax$ for some $x \in G$.

Theorem.5. The relation of conjugacy is an equivalence relation on G.

Proof. Reflexivity. If a is any element of G, then we have $a = e^{-1}ae \Rightarrow a \sim a.$

Thus we have

$$a \sim a \quad \forall a \in G.$$

Therefore the relation is reflexive.

Symmetry. We have $a \sim b \Rightarrow a = x^{-1}bx$ for some $x \in G$.

$\Rightarrow \qquad xax^{-1} = x\left(x^{-1}bx\right)x^{-1}$

$\Rightarrow \qquad xax^{-1} = b$

$\Rightarrow \qquad b = \left(x^{-1}\right)ax^{-1}$, where $x^{-1} \in G$

$\Rightarrow \qquad b \sim a$.

Therefore the relation is symmetric.

Transitivity. Let $a \sim b,\ b \sim c$. Then we have

$$a = x^{-1}bx, b = y^{-1}cy \text{ for some } x, y \in G.$$

From this we get

$$a = x^{-1}\left(y^{-1}cy\right)x \qquad \left[\because b = y^{-1}cy\right]$$

$$= (yx)^{-1} c(yx), \text{ where } yx \in G.$$

Thus $a \sim c$ and thus the relation is transitive.

Hence the relation of conjugacy in a group G is an equivalence relation. Therefore it will partition G into disjoint equivalence classes called classes of conjugate elements. These classes will be such that

(i) Any two elements of the same class are conjugate.

(ii) No two elements of different classes are conjugate.

The collection of all elements conjugate to an element $a \in G$ will be symbolically denoted by $C(a)$ or by $\bar{a}$. Thus $C(a) = \{x \in G : x \sim a\}$. $C(a)$ will be called the conjugate class of a in G. We have $\left(y^{-1}ay\right) \sim a$ for all $y \in G$. Also if $b \sim a$ then b must be equal to $y^{-1}ay$ for some $y \in G$. Therefore $C(a) = \{y^{-1}ay : y \in G\}$.

If G is a finite group, then the number of distinct elements in $C(a)$ will be denoted by c_a.

8.6 Normalizer of an element of a group

If $a \in G$, then $N(a)$, the normalizer of a in G is the set of all those elements of G which commute with a. Symbolically $N(a) = \{x \in G : ax = xa\}$.

Theorem.6. The normalize $N(a)$ of $a \in G$ is a subgroup of G.

Proof. Using the definition of Normalizer of an element of a group, we have $N(a) = \{x \in G : ax = xa\}$

Suppose $x_1, x_2 \in N(a)$. Then we have $ax_1 = x_1a,\ ax_2 = x_2a$.

First we show that $x_2^{-1} \in N(a)$.

Now we have

$$ax_2 = x_2a$$

$$\Rightarrow \quad x_2^{-1}(ax_2)x_2^{-1} = x_2^{-1}(x_2a)x_2^{-1}$$

$$\Rightarrow \quad x_2^{-1}a = ax_2^{-1}$$

$$\Rightarrow \quad x_2^{-1} \in N(a)$$

Now we shall show that $x_1x_2^{-1} \in N(a)$.

We have

$$\begin{aligned} a(x_1x_2^{-1}) &= (ax_1)x_2^{-1} \\ &= (x_1a)x_2^{-1} \\ &= x_1(ax_2^{-1}) \\ &= x_1(x_2^{-1}a) \\ &= (x_1x_2^{-1})a. \end{aligned}$$

Therefore $x_1x_2^{-1} \in N(a)$.

Thus $x_1, x_2 \in N(a) \Rightarrow x_1 x_2^{-1} \in N(a)$.

Hence $N(a)$ is a subgroup of G.

Note 1. It should be noted that $N(a)$ is not necessarily a normal subgroup of G.

2. Since $ex = xe \ \forall\, x \in G$, therefore we have $N(e) = G$.

3. If G is an abelian group and G. Then two elements $a \in G$, then $ax \ \forall\, x \in G$. Therefore we have $N(a) = G$.

Theorem.7. Let a be any element of a group G. Then two elements $x, y \in G$ give rise to the same conjugate of a if and only if they belong to the same right cost of the normalizer of a in G. Hence show that is G is a finite group, then $C_a = \dfrac{o(G)}{o[N(a)]}$, *i.e.*, the number of elements conjugate to a in G is the index of the normalize of a in G.

Proof. We have $x, y \in G$ are in the same right coset of N(a) in G.

$\Leftrightarrow$ $N(a)x = N(a)y$

$[\because x \in N(a)x,\ y \in N(a)y.$ Note that if H is a subgroup, then $x \in Hx]$

$\Leftrightarrow$ $xy^{-1} \in N(a)$ $[\because$ If H is a subgroup, then Ha = Hb $\Leftrightarrow ab^{-1} \in H]$

$\Leftrightarrow$ $axy^{-1} = xy^{-1}a$ [by definition of N(a)]

$\Leftrightarrow$ $x^{-1}(axy^{-1})y = x^{-1}(xy^{-1}a)y$

$\Leftrightarrow$ $x^{-1}ax = y^{-1}ay$

$\Leftrightarrow$ x, y give rise to the same conjugate of a.

Hence the first result follows.

Now consider the right coset decomposition of G with respect to the subgroup N(a). We have just proved that if $x, y \in G$ are in the same right coset of N(a) in G, then they give the same conjugate of a.

Further if x, y are in different right cosets of N(a) in G, then they give rise to different conjugates of a. The reason is that if x,y give the same conjugate of a, then they must belong to the same right coset of N(a) in G. Thus there is a one to one correspondence between the right cosets of N(a) in G and the conjugates of a.

Therefore, if G is a finite group, then we have

C_a = the number of distinct element in C(a)

= the number of distinct right cosets of $N(a)$ in G

= the index of $N(a)$ in G.

$$= \frac{o(G)}{o[N(a)]}.$$

8.7 Self-Conjugate elements

An element $a \in G$ said to be self-conjugate if a is the only member of the class C (a) of elements conjugate to a *i.e.*, if $C(a) = \{a\}$.

Thus, a, is self-conjugate if and only if $a = x^{-1}ax \;\forall\; x \in G$ or $xa = ax \;\forall\; x \in G$. Therefore a is self-conjugate element is one which commutes with each element of the group.

If a is a self-conjugate element, then we have $a = x^{-1}ax \;\forall\; x \in G$.

Thus the transform of a by every element of G remains equal to a. Therefore sometimes a self-conjugate element is also known as an invariant element.

8.8 The centre of a group

The set Z of all self-conjugate elements of a group G is known as the centre of G. It denoted as

$$Z = \{z \in G : zx = xz \ \forall\ x \in G\}.$$

Theorem.8. The centre Z of a group G is a normal subgroup of G.

Proof. Using the definition of the centre of a group, we have We have $Z = \{z \in G : zx = xz \ \forall\ x \in G\}$.

First we shall prove that Z is a subgroup of G.

Let $z_1, z_2 \in Z$. Then $z_1 x = xz_1$ and $z_2 x = xz_2$ for all $x \in G$.

Now we have

$$z_2 x = xz_2 \ \forall\ x \in G$$

$$\Rightarrow \quad z_2^{-1}(z_2 x) z_2^{-1} = z_2^{-1}(xz_2) z_2^{-1}$$

$$\Rightarrow \quad xz_2^{-1} = z_2^{-1} x \quad \forall\ x \in G$$

$$\Rightarrow \quad z_2^{-1} \in Z$$

Now we have

$$(z_1 z_2^{-1}) x = z_1 (z_2^{-1} x)$$

$$= z_1 (x z_2^{-1})$$

$$= (z_1 x) z_2^{-1}$$

$$= (xz_1) z_2^{-1}$$

$$= x(z_1 z_2^{-1}) \quad \forall\ x \in G$$

Therefore $z_1 z_2^{-1} \in Z$.

Thus $z_1, z_2 \in Z \ \Rightarrow \ z_1 z_2^{-1} \in Z$.

Hence Z is a normal subgroup of G.

Theorem.9. Let $a \in Z$ if and only if $N(a) = G$. If G is finite, $a, \in Z$ if and only if $o[N(a)] = o(G)$.

Proof. Let $a \in Z$. Then by definition of Z, we have

$$ax = xa \quad \forall\, x \in G .$$

Also $N(a) = \{x \in G : ax = xa\}$.

Now we have

$a \in Z \Leftrightarrow ax = xa \quad \forall\, x \in G$ [by definition of Z]

$\Leftrightarrow x \in N(a) \quad \forall\, x \in G$ [by definition of N(a)]

$\Leftrightarrow N(a) = G .$ [$\because N(a) \subseteq G$ and eah element of G is in N(a)]

If the group G is finite, then we have

$$N(a) = G$$

$\Leftrightarrow \quad o(G) = o[N(a)]$.

Therefore if the group G is finite, then $a \in Z$ if and only if $o[N(a)] = o(G)$.

8.9 Conjugate Subgroup

If A, B be two subgroup of a group G, then B is said to be conjugate to A if there exists an element $x \in G$ such that $B = x^{-1}Ax$.

Note: 1. If $B = x^{-1}Ax$, then B is also called the transform of A by x.

2. If B is conjugate to A, then symbolically we shall write $B \sim A$.

8.10 Normalizer of a Subgroup of a Group

If A is a subgroup of a group G, then $N(A)$, the normalizer of A in G is the set of all those elements of G which commute with A. It is denoted as

$$N(A) = \{x \in G : xA = Ax\}.$$

8.11 Self-Conjugate Subgroups

A subgroup A of a group G is said to be self-conjugate if A is the only member of the class $C(A)$ of subgroups conjugate to A.

Thus, A, is self conjugate if and only if

$$A = x^{-1}Ax \;\forall\; x \in G \quad \text{or } xA = Ax \;\forall\; x \in G$$

or A is a normal subgroup of G.

If A is a self- conjugate subgroup of a group G, then we have $A = x^{-1}Ax \;\forall\; x \in G$. Thus the transform of A by every element of G remains equal to A. Therefore sometimes a self-conjugate subgroup is a also called an invariant subgroup. It is quite obvious that a subgroup of a group G is invariant if and only if it is normal. Therefore sometimes a normal subgroup is also called an invariant subgroup.

8.12 Quotient Groups

If G is a group and H is a normal subgroup of G, then the set G/H of all cosets of H in G is a group. The identity element of the quotient group G/H is H.

Theorem.10. The set of all cosets of a normal subgroup is a group with respect to multiplication of complexes as the compostion.

Proof. Let H be a normal subgroup of a group G. Since H is normal in G, therefore each right coset will be equal to the corresponding left coset. Thus there is no distinction between right and left cosets and we shall call them simply as cosets. Consider G/H is the collection of all cosets of H in G i.e., suppose

$$G/H = \{Ha : a \in G\}.$$

Closure Property:

Consider $a, b \in G$. Then we have $(Ha)(Hb) = H(aH)b = H(Ha)b = HHab = Hab.$

Since $ab \in G$, therefore Hab is also a coset of H in G. So $Hab \in G/H$.

Thus G/H is closed with respect to coset multiplication.

Associativity:

Suppose $a, b, c \in G$. Then we have $Ha, Hb, Hc \in G/H$.

Now we have

$$Ha[(Hb)(Hc)] = Ha(Hbc)$$

$$= Ha(bc)$$

$$= H(ab)c$$

$$= (Hab)Hc$$

$$= [(Ha)(Hb)]Hc.$$

Thus the product in G/H satisfies the associative law.

Identity Property: We have $H = He \in G/H$. Also if Ha is any element of G/H, then we have

$$H(Ha) = (He)(Ha)$$

$$= Hea$$

$$= Ha$$

and similarly $(Ha^{-1})(Ha) = Ha^{-1}a = He = H$.

Therefore the coset H is the identity element.

Inverse Property: Let $Ha \in G/H$. Then $Ha^{-1} \in G/H$.

Now we have

$$(Ha)(Ha^{-1}) = Haa^{-1} = He = H.$$

Then $Ha^{-1}a = He = H$.

Thus coset Ha^{-1} is the inverse of Ha i.e., $(Ha)^{-1} = Ha$. Thus each element of G/H possesses inverse.

Hence G/H is a group with respect to product of cosets.

Solved Examples

Example.4. Let I be the additive group of integers. Let H be a subgroup of I such that $H = \{mx : x \in \mathrm{I}\}$ where m is a fixed positive integer. Write the elements of the quotient group I/H. Also prepare a composition table for I/H when $m = 5$.

Sol. Since I is an abelian group, therefore H is normal in I. The elements of I/H are the cosets of H in I namely

$$H + 0 = H = \{\ldots -2m, -m, 0, 2m, \ldots.\}$$

$$H + 1 = \{\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots.\}$$

$$H + 2 = \{\ldots, -2m+2, -m+2, 2, m+2, 2m+2, \ldots.\}$$

....
....

$$H + (m-2) = \{\ldots., -m-2, -2, m-2, 2m-2, 3m-2, \ldots\}$$

$$H + (m-1) = \{\ldots., -m-1, -1, m-1, 2m-1, 3m-1, \ldots\}.$$

These are the only distinct cosets of H in I. Because if s is any integer, then by division algorithm there exist integers q and r such that $s = mq + r$ where $0 \le r \le m-1$.

We have $H + s = H + mq + r = H + r$ $\quad [\because mq \in H$ and this gives $H + mq = H]$.

Thus $H + s$ is one of the above m cosets of H in I. Thus there are m distinct elements in

the set I/H.

When $m = 5$, the distinct elements in I/ H are $H, H+1, H+2, H+3, H+4$.

If $a, b \in I$, then $(H + a) + (H + b) = H + (a + b)$.

Also $H + a = H + b \Leftrightarrow a - b \in H$. Thus $H + 2 = H + 7, H + 3 = H + 8$ and so on.

Hence the composition table for I /H is as given below:

	H	$H+1$	$H+2$	$H+3$	$H+4$
H	H	$H+1$	$H+2$	$H+3$	$H+4$
$H+1$	$H+1$	$H+2$	$H+3$	$H+4$	H
$H+2$	$H+2$	$H+3$	$H+4$	H	$H+1$
$H+3$	$H+3$	$H+4$	H	$H+1$	$H+2$
$H+4$	$H+4$	H	$H+1$	$H+2$	$H+3$

Example.5. If G is a finite group and H is a normal subgroup of G, then $o(G/H) = \dfrac{o(G)}{o(H)}$**.**

Sol. We have

$o(G/H) =$ number of distinct right cosets of H in G

$$= \frac{\text{Number of elements in G}}{\text{Number opf elements in H}} \qquad \text{[by Lagrange's theorem]}$$

$$= \frac{o(G)}{o(H)}.$$

Example.6. Show that every quotient group of an abelian group is abelian and the converse is not

true.

Sol. Suppose G is an abelian group and H be a subgroup of G. Then H is a normal subgroup of G. If $a, b \in G,$ then Ha, Hb are any two elements of G/ H. We have

$$(Ha)(Hb) = Hab = Hba \qquad [\because G \text{ is ablian} \Rightarrow ab = ba]$$

Therefore G/H is abelian.

The converse is not true. For example if P_3 be the symmetric group of degree 3 and A_3 be the alternating group of degree 3, then P_3/A_3 is an abelian group while P_3 is not an abelian group. The group P_3/A_3 is of order 2, and every group of order 2 is abelian.

Example.7. Show that every quotient group of a cyclic group is cyclic and the converse is not true.

Sol. Let G be a cyclic group and a be a generator of G. Let H be a subgroup of G. Since every cyclic group is abelian, therefore H is a normal subgroup of G. Let a^n be any element of G where integer n. Therefore G/ H is a cyclic group and Ha is a generator of it.

The converse is not true. For example P_3/A_3 is cyclic while P_3 is not cyclic.

8.13 Summary

A subgroup H of a group G is said to be normal subgroup of G if for every $x \in G$ and for every $h \in H, xhx^{-1} \in H$. Since every cyclic group is abelian, therefore every subgroup of a cyclic group is normal.

A group having no proper normal subgroups is known as a simple group. Every group of prime order is simple. Using Lagrange's theorem such a group has no proper subgroups.

A subgroup H of a group G is normal if and only if $xHx^{-1} = H \ \forall\, x \in G.$

A subgroup H of a group G is a normal subgroup of G if and only if each left coset of H in G is a right coset of H in G .

The intersection of any two normal subgroups of a group is a normal subgroup.

If a, b be two elements of a group G, then b is said to be conjugate to a if there exists an element $x \in G$ such that $b = x^{-1}ax$. If $b = x^{-1}ax$, then b is also known as the transform of a by x.

If $a \in G$, then $N(a)$, the normalizer of a in G is the set of all those elements of G which commute with a. Symbolically $N(a) = \{x \in G : ax = xa\}$.

An element $a \in G$ said to be self-conjugate if a is the only member of the class C (a) of elements conjugate to a i.e., if $C(a) = \{a\}$.

The set Z of all self-conjugate elements of a group G is known as the centre of G. It denoted as

$$Z = \{z \in G : zx = xz \nvdash x \in G\}.$$

If A, B be two subgroup of a group G, then B is said to be conjugate to A if there exists an element $x \in G$ such that $B = x^{-1}Ax$.

If A is a subgroup of a group G, then $N(A)$, the normalizer of A in G is the set of all those elements of G which commute with A. Symbolically $N(A) = \{x \in G : xA = Ax\}$.

A subgroup A of a group G is said to be self-conjugate if A is the only member of the class $C(A)$ of subgroups conjugate to A.

If G is a group and H is a normal subgroup of G, then the set G/H of all cosets of H in G is a group. The identity element of the quotient group G/H is H.

8.14 Terminal Questions

Q.1. Explain the concept of Normal subgroup with example.

Q.2. What do you mean by simple group?

Q.3. The normalize $N(A)$ of a subgroup A of a group G is a subgroup of G.

Q.4. Define normalizer of a subgroup of a group.

Q.5. What do you mean by centre of a group?

Q.6. Define Quotient Group.

Q.7. Is a group of order 121 abelian?

Q.8. Let P_3 be the symmetric group on three symbols a, b, c and A_3 be the alternating group on three symbols a, b, c. From the composition table for the quotient group P_3 / A_3.

Q.9. If N is normal in G and $a \in G$ is of order n, prove than the order, m, of N*a* in G/N is a divisor of *n*.

Q.10. Let Z be the centre of a group G. If $a \in Z$, then prove that the cyclic subgroup $\{a\}$ of G generated by a is a normal subgroup of G.

ANSWERS

7. Yes.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

UNIT-9: Homomorphism

Structure

9.1 Introduction

The study of group homomorphisms, kernels, maximal subgroups, solvable groups, the Jordan–Hölder theorem, *p*-Sylow subgroups and Sylow's theorems plays a central role in modern algebra due to their importance and wide-ranging applications. A homomorphism helps us compare two groups while keeping their structure, and its kernel explains how quotient groups are formed. Maximal subgroups show the "largest" proper subgroups inside a group, while solvable groups are useful in finding out whether polynomial equations can be solved by radicals in Galois theory. The Jordan–Hölder theorem tells us that when we break down a finite group step by step, the simple building blocks are always the same. *p*-Sylow subgroups and Sylow's theorems help us study the existence and properties of subgroups whose order is a power of a prime number. All these ideas are not only central in pure mathematics but are also applied in number theory, physics, and cryptography.

9.2 Objectives

After reading this unit the learner should be able to understand about the:

- Homomorphisms of Groups
- Kernel of a Homomorphism
- Fundamental theorem on Homomorphism of Groups
- Automorphisms of a group , Inner Automorphism
- Maximal Subgroups, Composition series of a group and Jordan-holder Theorem
- Solvable Groups and Direct Products
- p-Sylow Subgroup and Sylow's Theorem

9.3 Homomorphism of Groups

Homomorphism into

A mapping f from a group G into a group G′ is said to be homorphism of G into G′ if

$$f(a\,\mathrm{b}) = f(a)\,f(\mathrm{b}) \quad \forall\ a,\ b \in G\,.$$

Homomorphism onto

A mapping *f* from a group G onto a group G′ is said to be a homorphism of G onto G′ if

$$f(ab) = f(a)\,f(b)\ \forall\, a,\ b \in G\,.$$

Also then G′ is said to be a homomorphic image of G.

Endomorphism

A homomorphism of a group into itself is called an endomorphism.

Theorem.1: If *f* is a homomorphism of a group G into a group G', then

(i) $f(e) = e'$**, where e is the identity of G and** e' **is the identity of** G'.

(ii) $f\left(a^{-1}\right) = \left[f(a)\right]^{-1}\ \forall\, a \in G.$

(iii) If the order of $a \in G$ **is finite, then the order of** $f(a)$ **is a divisor of the order of *a*.**

Proof: (i) Let $a \in G.$ Then we have $f(a) \in G'$.

Now we have

$$f(a)e' = f(a) \qquad [\because\ e' \text{is the identity of G}']$$

$$= f(ae) \qquad [\because e \text{ is the identity of G}]$$

$= f(a) f(e)$ $\quad [\because f$ is a homomorphism$]$

Now G′ is a group.

Hence $f(a)e' = f(a) f(e) \Rightarrow e' = f(e)$.

(ii) Let *a* be any element of G. Then we have $a^{-1} \in G.$

Now we have

$$e' = f(e) = f(aa^{-1}) = f(a) f(a^{-1}).$$

Therefore $f(a^{-1})$ is the inverse of $f(a)$ in the group G′.

Thus we have

$$f(a^{-1}) = \{f(a)\}^{-1}.$$

(iii) Let $a \in G$ and $o(a) = m.$

Now we have $o(a) = m \Rightarrow a^m = e.$

$\therefore \quad f(a^m) = f(e) \Rightarrow \quad f(aaa,,,,,,m\ times) = e'$

$\Rightarrow \ f(a) f(a).....m$ times $= e' \Rightarrow [f(a)]^m = e'.$

Hence, if n is the order of f (a) in G', then *n* must be a divisor of *m*.

Solved Examples

Example.1. Show that the mapping *f* of the symmetric group P_n onto the multiplicative group $G' = \{1, -1\}$, defined by $f(\alpha) = 1$ or -1 according as α is an even or odd permutation in P_n, is a homomorphism of P_n onto G'.

Sol. We know that the product of two permutations is even if both are even or both are odd, whereas the product of one even and one odd permutation is odd. Now we shall show that

$$f(\alpha\beta) = f(\alpha).f(\beta) \ \forall \alpha, \beta \in P_n$$

(i) If α, β are both even, then we have

$$f(\alpha\beta) = 1 = 1.1 = f(\alpha) f(\beta)$$

(ii) If α, β are both odd, then we have

$$f(\alpha\beta) = 1 = (-1)(-1) = f(\alpha) f(\beta)$$

(iii) If α is odd and β is even, then we have

$$f(\alpha\beta) = -1 = (-1)(1) = f(\alpha) f(\beta)$$

(iv) If α is even and β is odd, then we have

$$f(\alpha\beta) = -1 = (1)(-1) = f(\alpha) f(\beta)$$

Thus we have $f(\alpha\beta) = f(\alpha) f(\beta) \forall \alpha, \beta \in P_n$

Also obviously f is onto G′. Hence f is a homomorphism of P_n onto G'.

Example.2: Let G be the group of all ordered pairs (a,b) of real number with the binary operation denoted additively and defined by $(a,b)+(c,\mathrm{d}) = (a+c, b+d)$. Further let G' be the additive group of all real numbers. Then the mapping $f: G \to G'$ defined by $f(a,b) = a \quad \forall (a,b) \in G$ is a homomorphism of G onto G′.

Solution: It can be easily proved that G is a group with respect to the given binary operation. The ordered pair (0, 0) is the identity element and the ordered pair $(-a,-b)$ is the inverse of (a,b).

Consider (a,b) and (c,d) be any two elements of G. Then using definition of *f*, we have

$$f(a,b)=a, \quad f(c,d)=c.$$

Now we have $f\{(a,b)+(c,d)\}=f(a+c,b+d)=a+c=f(a,b)+f(c,\mathrm{d})$

Also obviously *f* is onto G′ . Hence *f* is a homomorphism of G onto G′.

Example.3: Let G be a group and let e be the identity element of G. Then the mapping $f:G\to G$ defined by $f(a)=e\,\forall\, a\in G$ is an endomorphism of G.

Solution: Suppose *a, b* are any two elements of G.

Then we have $f(a)=e, \quad f(b)=e.$

Now we have

$$f(ab)=e=ee=f(a)\,f(b)$$

Therefore f is a homomorphism of G into G. Hence *f* is an endomorphism of G.

9.4 Kernel of a Homomorphism

If *f* is a homomorphism of a group G into a group G′, Then the set K of all those elements of G which are mapped by *f* onto the identity e′ of G′ is called the kernel of the homomorphism *f*.

Thus if *f* is a homomorphism of G into G′, then K is the kernel of *f* if

$$K=\{x\in G: f(x)=e',\ \text{where e' is the identity of G'}\}.$$

Theorem.2: If f is a homomorphism of a group G into a group G′with kernel K,then K is a normal subgroup of G.

Proof: Let *f* be a homomorphism of a group G into a group G′ and e, e′ are the identities of G and G′ respectively. Let K be the kernel of *f*. Then $K=\{x\in G: f(x)=e'\}$.

Since $f(e)=e'$, therefore at least $e \in K$. Therefore K is non empty.

Now let $a,b \in K$, then we have $f(a)=e', f(b)=e'$.

Now we have

$$f(ab^{-1}) = f(a)\, f(b^{-1}) = f(a)\{f(b)\}^{-1} = e'e'^{-1} = e'.$$

$\therefore \quad ab^{-1} \in K.$

Thus we have $a,b \in K \Rightarrow ab^{-1} \in K.$

Therefore K is a subgroup of G. Now to prove that K is normal in G. Let g be any element of G and k be any element of K. Then we have $f(k)=e'$.

Now we have

$$f(gkg^{-1}) = f(g)\, f(k)\, f(g^{-1}) = f(g)e'\left[f(g)\right]^{-1} = f(g)\left[f(g)\right]^{-1} = e'$$

$$\therefore \quad gkg^{-1} \in K.$$

Therefore $g \in G, K \in K \Rightarrow gkg^{-1} \in K$.

Hence K is a normal subgroup of G.

9.5 Fundamental theorem on Homomorphism of Groups

The Fundamental Theorem of Homomorphism is significant as it creates a strong link between homomorphism, normal subgroups, quotient groups, and isomorphisms. It demonstrates that every homomorphic image of a group can be viewed as a quotient of the original group by its kernel, thereby making the study of group structures more manageable. The theorem has extensive applications: in number theory, it forms the basis of modular arithmetic and congruences; in linear algebra, it leads to the rank–nullity theorem; in Galois theory, it provides insight into field extensions; and in geometry and physics, it aids in the study of symmetry and structural properties. Moreover, it plays an important role in computer science and cryptography, where modular groups are essential. Owing to its unifying role and

wide-ranging applications, the theorem is regarded as a fundamental result in both pure and applied Mathematics.

Theorem.3: Every homomorphic image of a group G is isomorphic to some quotient group of G.

Proof: Let G′ be the homomorphic image of a group G and f be the corresponding homomorphism. Then *f* is a homomorphism of G onto G′. Let K be the kernel of this homomorphism. Then K is a normal subgroup of G. Now we shall prove that

$$G/K \cong G'$$

If $a \in G$, then $Ka \in G/K$ and $f(a) \in G'$. Consider the mapping $\phi : G/K \to G'$ such that $\phi(Ka) = f(a) \forall a \in G$.

First we shall show that the mapping ϕ is well-defined i.e., if $a, b \in G$ and $Ka = Kb$, then $\phi(Ka) = \phi(Kb)$.

We have $Ka = Kb \Rightarrow ab^{-1} \in K \Rightarrow f(ab^{-1}) = e'$ (identity of G')

$$\Rightarrow f(a) f(b^{-1}) = e'$$

$$\Rightarrow f(a)[f(b)]^{-1} = e'$$

$$\Rightarrow f(a)[f(b)]^{-1} f(b) = e' \text{f}(b)$$

$$\Rightarrow f(a)e' = f(b) \Rightarrow f(a) = f(b)$$

$$\Rightarrow \phi(Ka) = \phi(Kb)$$

$\therefore \phi$ is well defined

ϕ is one-one,

we have $\phi(Ka)=\phi(Kb)\Rightarrow f(a)=f(b)$

$$\Rightarrow f(a)\left[f(b)\right]^{-1}=f(b)\left[f(b)\right]^{-1}\Rightarrow f(a)\,f\left(b^{-1}\right)=e'\Rightarrow f\left(ab^{-1}\right)=e'$$

$\Rightarrow ab^{-1}\in K$ [$\because K$ is kernel]

$\Rightarrow Ka=Kb.$

$\therefore \phi$ is one-one,

ϕ is onto G'

Let y be any element of G'. Then $y=f(a)$ for some $a\in G$ because f is onto G′

Now $Ka\in G/K$ and we have $\phi(Ka)=f(a)=y.$

$\therefore \phi$ is onto G'

Finally we have $\phi\left[(Ka)(Kb)\right]=\phi(Kab)=f(ab)$

$$=f(a)\,f(b)=\phi(Ka)\phi(Kb)$$

$\therefore \phi$ is an isomorphism of G/K onto G′. Hence $G/K\cong G'$.

Solved Examples

Example.4: Let *f* be a homomorphism mapping of a group G into a group G′. Let $f(G)$ be the homomorphic image of G in G′. Then $f(G)$ is a subgroup of G′.

Solution: We have $f(G)=\{f(x):x\in G\}$. Obviously $f(b)=b'$ for some $a,b\in G.$

Now we have

$$a'(b')^{-1}=f(a)\left[f(b)\right]^{-1}=f(a)\,f\left(b^{-1}\right)=f\left(ab^{-1}\right)\in f(G)$$

Since $ab^{-1} \in G$

Therefore, we have $a', b' \in f(G) \quad \Rightarrow \quad a'(b')^{-1} \in f(G)$.

Hence $f(G)$ is a subgroup of G'.

Example.5: Show that every homomorphic image of an abelian group is abelian and converse is not true.

Solution: Let G be an abelian group. Let f be a homomorphic mapping of G onto a group G′. Then G′ is a homomorphic image of G.

Let a', b' be any two elements of G'. Then we have $f(a) = a'$, $f(b) = b'$ for some $a, b \in G$. Now we have

$$a'b' = f(a) f(b) = f(ab) = f(ba) = f(b) f(a) = b'a'.$$

Thus G' is abelian.

The converse is not true. P_3 is a non abelain group. A_3 is a normal subgroup of P_3. The quotient group P_3 / A_3 is a homomorphic image of P_3. Now P_3 / A_3 is order 2 and is abelian.

Check your progress

Q.1. Explain the concept of homomorphism.

Q.2. Define kernel of homomorphism.

Q.3. What do you mean by Fundamental theorem on Homomorphism of Groups?

Q.4. Define endomorphism.

9.6 Automorphisms of a group

An isomorphic mapping of a group G onto itself is called an automorphism of G. Thus $f : G \xrightarrow{\text{onto}} G$ is an automorphism of G if

$$f(ab) = f(a)\, f(b) \quad \forall\, a, b \in G.$$

Solved Examples

Example.6. Show that the mapping $f : I \to I$ such that $f(x) = -x \quad \forall\, x \in I$ is an automorphism of the additive group of integers I.

Solution: Obviously the mapping *f* is one-one onto.

Let x_1, x_2 be any two elements of I. Then we have

$$f(x_1 + x_2) = -(x_1 + x_2)$$

$$= (-x_1) + (-x_2)$$

$$= f(x_1) + f(x_2)$$

Hence *f* is an automorphism of I.

Example.7: Show that $f : G \to G$ be such that $f(x) = x^{-1} \forall\, x \in G$, is an automorphism of a group G iff G is abelian.

Solution: Let $f : G \to G$ be such that $f(x) = x^{-1} \forall\, x \in G$. The function f is one-one because

$$f(x) = f(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y$$

Also if $x \in G$, then $x^{-1} \in G$ and we have $f(x^{-1}) = (x^{-1})^{-1} = x.$

Hence f is onto.

Now suppose G is abelian. Let *a*, *b* be any two elements of G.

Then we have

$$f(ab) = (ab)^{-1}$$

$$= b^{-1}a^{-1} = a^{-1}b^{-1} \qquad [\because G \text{ is abelian}]$$

$$= f(a)\, f(b)$$

Hence f is an automorphisms of G.

Conversely, suppose that f is an automorphism of G. Let $a, b \in G$.

Now we have

$$f(ab) = (ab)^{-1}$$

$$= b^{-1}a^{-1}$$

$$= f(b)\, f(a)$$

$$= f(ba).$$

Since f is one-one, therefore

$$f(ab) = f(ba)$$

$$\Rightarrow \quad ab = ba$$

Hence G is abelian.

Theorem.4: The set of all automorphisms of a group forms a group with respect to composite of functions as composition.

Solution: Let A(G) be the set of all automorphim. Then to prove A(G) is a group, we prove the following group axioms:

Closure property: Let $f, g \in A(G)$. Then f, g are one-one mapping of G onto itself. Therefore g *f* is also a one-one mapping of G onto itself.

If *a*, b be any two elements of G, we have

$$(gf)(ab) = g[f(ab)]$$

$$= g[f(a) f(b)]$$

$$= g[f(a)]g[f(b)]$$

$$= [(gf)(a)][(gf)(b)]$$

$\therefore$ gf is also an automorphism of G.

Thus $A(G)$ is closed with respect to composite composition.

Associative property: We know that composite of arbitrary mappings is associative. Therefore composite of automorphisms is also associative.

Identity Property: The identity function I on G is also an automorphism of G. Obviously, I is one-one and if $a,b \in G$ then $I(ab) = ab = I(a)I(b)$.

Thus $I \in A(G)$ and if $f \in A(G)$, we have $If = f = fI$.

Inverse Property: Let $f \in A(G)$. Since f is a one-one mapping of G onto itselt, therefore f^{-1} exists and is also a one-one mapping of G onto itself. We shall show that f^{-1} is also an automorphism of G. Let $a, b \in G$. Then there exist $a', b' \in G$ such that

$$f^{-1}(a) = a' \Leftrightarrow f(a') = a$$

$$f^{-1}(b) = b' \Leftrightarrow f(b') = b$$

Now we have

$$f^{-1}(ab) = f^{-1}\left[f(a') f(b') \right]$$

$$= f^{-1}\left[f(a'b') \right]$$

$$= a'b'$$

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

$\therefore$ f^{-1} is an automorphism of G and thus

$$f \in A(G) \Rightarrow f^{-1} \in A(G).$$

Therefore each element of $A(G)$ possesses inverse.

Hence $A(G)$ is a group with respect to composite composition.

9.7 Inner Automorphism

If G is a group, the mapping $f_a : G \to G$ defined by

$$f_a(x) = a^{-1}xa \quad \forall\, x \in G$$

is an automorphism of G known as inner automorphism. Also an automorphism which is not inner is called an outer automorphism.

Theorem.5: Let *a* be a fixed element of a group G. Then the mapping $f_a : G \to G$ defined by $f_a(x) = a^{-1}xa \ \forall\, x \in G$ is an automorphism of G.

Proof: The mapping f_a is one-one. Let x, y be any two elements of G. Then

$$f_a(x) = f_a(y)$$

$\Rightarrow \quad a^{-1}xa = a^{-1}ya$

$\Rightarrow \quad x = y,$ by cancellation laws

The mapping f_a is also onto G. If y is any element of G, then $aya^{-1} \in G$ and we have

$$f_a\left(aya^{-1}\right) = a^{-1}\left(aya^{-1}\right)a = y$$

$\therefore f_a$ is onto G.

Finally if $x, y \in G$ then $f_a(xy) = a^{-1}(xy)a = \left(a^{-1}xa\right)\left(a^{-1}ya\right) = f_a(x)\, f_a(y)$. Hence f_a is an automorphism of G.

9.8 Maximal Subgroups

A normal subgroup H of a group G is said to be maximal if there exists no proper subgroup K of G which properly contains H.

Thus a normal subgroup H of a group G is maximal if and only if there exists no normal subgroup K of G such that $H \subset K \subset G$, where the symbol $\subset$ stands for proper inclusion.

Theorem.6: A normal subgroup H of G is maximal if and only if the quotient group G/H is simple.

Proof: Suppose H is maximal and G/H is not simple (a group is said to be simple if it possesses no proper normal sub-groups). Let K/H be a proper normal subgroup of G/H. Then K will be a normal subgroup of G containing H. Since K/H is a proper subgroup of G/H, Therefore $H \subset K \subset G$. Thus K is a normal subgroup of G and $H \subset K \subset G$. Therefore H is not maximal. This contradicts the hypothesis that H is maximal in G. Hence G/H must be simple.

Conversely, let G / H be simple and let H be not maximal, Since H is not maximal, therefore there exists a normal subgroup K of G such that $H \subset K \subset G$. Then K / H is a normal subgroup of G / H. Since $H \subset K \subset G,$ therefore K/H is a proper normal subgroup of G/H i.e., neither K/H is equal to the entire

group G/H nor K/H is equal to the identity subgroup H/H. Consequently G/H is not simple. This contradicts the hypothesis that G/H is simple.

Hence H must be maximal in G.

9.9 Composition series of a group and Jordan-Holder Theorem

Let G be a group. Then a finite sequence of its subgroups

$$G = H_1, H_2, H_3, ..., H_n = \{e\} \qquad \ldots\ldots (1)$$

is called a composition series for G if each H_i except H_1 is a maximal normal subgroup of H_{i-1}.

The quotient groups G/H_1, H_2/H_3,…… H_{n-1}/H_n which are necessarily simple are then called composition factor groups or composition quotient groups of the composition series (1).

Example.1: Let $G = P_3 = \{I, (12), (23), (31), (123), (132)\}$ and let $H_2 = \{I, (123), (132)\}$. Then G, H_2, $\{I\}$ is a composition series for G. Obviously H_2 is a maximal normal subgroup of G and $\{I\}$ is a maximal normal subgroup of H_2.

Example.2: Let G be a cyclic group of order 6 generated by *a i.e.*, let $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$. Then we have $G, H_2 = \{e, a^3\}, \{e\}$ and $G, N_2 = \{e, a^2, a^4\}, \{e\}$ are two different composition series for G.

Example.3: Let G be a cyclic group $\{a\}$ of order 12 generated by a. Then $\{a\}, \{a^2\}, \{a^4\}, \{e\}$ and $\{a\}, \{a^3\}, \{a^6\}, \{e\}$ are two different composition series for G.

Theorem.7: There exists at least one composition series for every finite group G.

Proof: We have to prove the theorem by mathematical induction on order of finite group G and let us assume that the theorem is true for each group of order < order of G.

Case I. If G is simple, then G, $\{e\}$ is a composition series for G.

Case II. Suppose G is not simple. Then there exists a proper normal subgroup H of G. If H is maximal in G and $\{e\}$ is maximal in H, then G, $H, \{e\}$ is a composition series.

Supoose H is not maximal in G but $\{e\}$ is maximal in H. Then Three exists a normal subgroup K of G such that $G \supset K \supset H$. If K is maximal in G and H is maximal in K then G, K, H, $\{e\}$ is composition series.

Now suppose that H is maximal in G but $\{e\}$ is not maximal in H, Then there exists a normal subgroup J of H such that

$$H \supset J \supset \{e\} .$$

If $\{e\}$ is maximal in J and J is maximal in H, Then G, H, J, $\{e\}$ is a composition series.

Next suppose that H is not maximal in G and e is not maximal in H than there exists a normal subgroup L of G such that $G \supset L \supset H$. Also there exists a normal subgroup N of H such that; $H \supset N \supset \{e\}$. Thus $G \supset L \supset H \supset N \supset \{e\}$. If L is maximal in G, H is maximal in L, N is maximal in H and $\{e\}$ is maximal in N then G, L, H, N, $\{e\}$ is a composition series.

Since G is finite, there are only a finite number of subgroups and ultimately we must reach a composition series.

Theorem.8: (Jordan-Holder Theorem) Let G be a finite group with two composition series

$$G, H_1, H_2, ..., H_n = \{e\} \qquad \text{……. (1)}$$

and $$G, K_1, K_2, ..., K_m = \{e\} \qquad \text{…… (2)}$$

Then $n = m$ and the two corresponding series of composition quotient groups, viz.,

$$G / H_1, H_1 / H_2, ..., H_{n-1} / H_n$$

And $G / K_1, K_1 / K_2, ..., K_{m-1} / K_m$

are abstractly identity *i.e,.* they can be put into one-one correspondence such that the corresponding quotient groups are isomorphic.

Proof: We Shall prove that theorem by the method of induction on the order of the group G. Assuming that the theorem is true for all groups of order less than that of G, we shall prove it is also true for G. We need not worry about starting the induction because the theorem is obviously true for any group of order one.

Now two cases aries:

Case 1: When $H_1 = K_1$, in this case after removing G from (1) and (2), we get the remaining series as two composition series for H_1.But the order of H_1 is less than that of G because H_1 is a proper normal subgroup of G. Therefore by our induction hypothesis, the theorem is true for H_1. Since $G / H_1 = G / K_1$, therefore the theorem will remain true if we replace G in each of the series (1) and (2).

Case 2: When $H_1 \neq K_1$, by the third law of isomorphism, we have $H_1K_1 / H_1 \cong K_1 / H_1 \bigcap K_1$,

and $H_1K_1 / K_1 \cong H_1 / H_1 \bigcap K_1$,

Also H_1K_1 is a normal subgroup of G containing H_1. Since H_1 is maximal in G, therefore we must have $H_1K_1 = G$

$\therefore \quad G / H_1 \cong K_1 / D$ where $D = H_1 \bigcap K_1$

And $G / K_1 \cong H_1 / D$

Now H_1 is maximal in G implies that G / H_1 is simple. Therefore K_1 / D is simple and this implies that D is a maximal normal subgroup of K_1. Similarly D is a maximal normal subgroup of H_1.

Let $D, D_1, D_2, ..., D_t = \{e\}$

be a composition series for D. Then

$$G, H_1, D, D_1, D_2, ..., D_t = \{e\} \quad \text{…… (3)}$$

and $$G, K_1, D, D_1, D_2, ..., D_t = \{e\} \quad \text{…… (4)}$$

are two composition series for G. Let us write the composition quotient groups of (3) and (4) in the order

$$G / H_1, H_1 / D,\ D / D_1, D_1 / D_2, ..., D_{t-1} / D_t \quad \text{….. (5)}$$

And $$K_1 / D, G / K_1 D / D_1, D / D_2, ..., D_{t-1} / D_t \quad \text{…… (6)}$$

The quotient groups in (5) and (6) are equal in number and the corresponding quotient groups are isomorphic i.e., G/H_1 and K_1/D, H_1/D and G/K_1, D/D_1 and D/D_1,….., are isomorphic.

Now (1) and (3) are two composition series for G each having H_1 in the second place. Therefore by case 1, the quotient groups defined by (1) and (3) may be put into one-one correspondence so that the corresponding quotient groups are isomorphic. Similarly the quotient groups defined by (2) and (4) may be put into one-one correspondence so that the corresponding quotient groups are isomorphic.

Hence the quotient groups defined by (1) and (2) are equal in number and are isomorphic in some order because the relation of isomorphism in the set of all groups is an equivalence relation. This complete the proof of the theorem.

Check your progress

Q.1. Explain the concept of automorphism of a group.

Q.2. Define maximal subgroups.

Q.3. What do you mean by inner automorphism?

Q.4. What is the composition series of a group?

Q.R. Sate the Jordan-Holder theorem.

9.10 Solvable Groups

A group G is said to be solvable if we can find a finite chain of subgroups

$$G = N_0 \supseteq N_1 \supseteq N_2 \supseteq ..... \supseteq N_k = (e)$$

Such that each N_i is a normal subgroup of N_{i-1} and each quotient group N_{i-1} / N_i is abelain. The above series, then is referred to as a solvable series for G.

Subnormal series of a group

A finite sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq .... \supseteq G_k = (e)$$

of a group G is called a subnormal series of G if G_{i+1} is a normal subgroup of $G_i \forall i = 0, 1, ..., k-1$. The quotient groups G_l / G_{i+1} are called the factor groups of the subnormal series. Further if each G_i is a normal subgroup of G itself, then the series is said to be a normal series of G.

Solved Examples

Example.8: Show that every abelian group is solvable.

Solution: Let G be an abelian group. Take $N_0 = G$ and $N_1 = (e)$ is a normal subgroup of N_0 = G because if *a* is any element of G, then $a^{-1}ea = a^{-1}a = e \in (e)$.

Further since G is abelian, the quotient group $N_0 / N_1 = G / (e)$ is also abelian. Hence G is a solvable group.

Note that every quotient group of an abelian group is abelian.

Example.9: Show that the symmetric group P_3 of degree 3 is solvable.

Solution: The symmetric group P_3 consists of the six permutations I (identity permutation), (1, 2), (2 3), (3 1), (1 2 3) and (1 3 2) on three symbols 1, 2, 3. Let $A_3=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$ on three symbols 1, 2, 3. Then A_3 is the alternating group of permutations of degree 3. If we take

$$N_0 = P_3, N_1 = A_3, \text{ and } N_2 = (I)$$

then $$P_3 = N_0 \supseteq N_3 \supseteq N_2 = (I)$$

is a solvable series for P_3 as shown below:

we know that a A_n is a normal subgroup of P_n. Therefore $A_3 = N_1$ is a normal subgroup of $P_3=N_0$. Also (I) is a normal subgroup of N_1. The quotient groups P_3/N_1 and $N_1/(I)$ are of orders 2 and 3 respectively. We know that all groups of order 2 and 3 are abelian. Therefore the quotient groups P_3/N_1 and $N_1/(I)$ are abelian. Hence $P_3=N_0 \supseteq N_1 \supseteq N_2 = (I)$ is a solvable series for P_3 and thus P_3 is solvable.

9.11 Direct Products

Let G_1 and G_2 be any two groups and the composition in each group is being denoted by multiplicatively. Then

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

Let us define a binary operation on $G_1 \times G_2$ denoted multiplicatively as follows:

$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$ where $g_i, h_1 \in G_1$ and $g_2, h_2 \in G_2$. For this binary operation $G_1 \times G_2$ is a group and this group is called the external direct product of G_1 by G_2.

To prove $G_1 \times G_2$ is a group for the binary operation we have defined on it, we prove Group Axioms as follows:

1. Closure property: We have $g_1h_1 \in G_1$ because G_1 is a group. Similarly $g_2h_2 \in G_2$. Thus $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2) \in G_1 \times G_2$

2. Associativity: If $(g_1, g_2)(h_1, h_2), (k_1, k_2) \in G_1 \times G_2$, then

$$\left[(g_1,g_2)(h_1,h_2)\right](k_1,k_2)=(g_1h_1,g_2h_2)(k_1,k_2)=\left([g_1h_1]k_1,[g_2h_2]k_2\right)$$

$$=\left(g_1[h_1k_1],g_2[h_2k_2]\right)=(g_1,g_2)(h_1k_1,h_2k_2)=(g_1,g_2)\left[(h_1,h_2)(k_1,k_2)\right]$$

3. Existence of left identity: Let e_1,e_2 be a identity elements of G_1, G_2 respectively. If $(g_1,g_2)\in G_1\times G_2$, then $(e_1,e_2)(g_1,g_2)=(e_1g_1,e_2g_2)=(g_1,g_2)$. Therefore (e_1,e_2) is the left identity of $G_1\times G_2$

4. Existence of left inverse: Let $(g_1,g_2)\in G_1\times G_2$. Then we have $(g_1^{-1},g_2^{-1})\in G_1\times G_2$

Also we have $(g_1^{-1},g_2^{-1})(g_1,g_2)=(g_1^{-1}g_1,g_2^{-1}g_2)=(e_1,e_2)$.

Therefore (g_1^{-1},g_2^{-1}) is the left inverse of (g_1,g_2) in $G_1\times G_2$.

Hence $G_1\times G_2$ is a group under the binary operation as defined above.

Theorem.9: If G_1 and G_2 are groups, then the subsets $G_1\times\{e_2\}$ and $\{e_1\}\times G_2$ of $G_1\times G_2$ are normal subgroups of $G_1\times G_2$ isomorphic to G_1 and G_2 respectively.

Proof: Let (g_1,e_2) and (h_1,e_2) be any two elements of $G_1\times\{e_2\}$ where $g_1, h_1\in G_1$

Then $(g_1,e_2)(h_1,e_2)^{-1}=(g_1,e_2)(h_1^{-1},e_2^{-1})=(g_1,e_2)(h_1^{-1},e_2)=(g_1h_1^{-1},e_2e_2)=(g_1h_1^{-1},e_2)$

Now $g_1h_1^{-1}\in G_1$ because G_1 is a group.

$\therefore (g_1h_1^{-1},e_2)\in G_1\times\{e_2\}$.

Hence $G_1\times\{e_2\}$ is normal in $G_1\times G_2$. Now to show that $G_1\times\{e_2\}$ is normal subgroup of $G_1\times G_2$. Let (x_1,x_2) be any element of $G_1\times G_2$ and (g_1,e_2) be any element of $G_1\times\{e_2\}$

Then $(x_1,x_2)(g_1,e_2)(x_1,x_2)^{-1}=(x_1,x_2)(g_1,e_2)(x_1^{-1},x_2^{-1})=(x_1g_1x_1^{-1},x_2e_2x_2^{-1})$

$=(x_1g_1x_1^{-1},e_2)\in G_1\times\{e_2\}$ because $x_1g_1x_1^{-1}\in G_1$,

$\therefore G_1 \times \{e_2\}$ is normal in $G_1 \times G_2$.

Now to show that $G_1 \cong G_1 \times \{e_2\}$ Let $\phi : G_1 \to G_1 \times \{e_2\}$ defined by

$$\phi(g_1) = (g_1, e_2) \forall\, g_1 \in G_1$$

Obviously ϕ is one-one. Also if $g_1, h_1 \in G_1$, then

$$\phi(g_1 h_1) = (g_1 h_1, e_2) = (g_1, e_2)(h_1, e_2) = \phi(g_1)\phi(h_1)$$

$$\therefore\ G_1 \cong G_1 \times \{e_2\}$$

Similarly we can show that $\{e_1\} \times G_2$ is a normal subgroup of $G_1 \times G_2$ and is isomorphic to G_2.

9.12 *p*-Sylow Subgroup and Sylow's Theorem

_p_-Sylow Subgroup

Suppose G is a finite group and o(G) = $p^m n$ where p is a prime number and *p* is not a divisor of *n*. Then a subgroup H of G is said to be a *p*-sylow subgroup of G iff o(H) =p^m.

Theorem.10: (Sylow's theorem) Suppose G is a group of finite order and p is a prime number. If $p^m \mid o(G)$ and p^{m+1} is not a divisor of o (G) then G has a subgroup of order p^m.

Proof: We shall prove the theorem by induction on o(G).

Assuming that the theorem is true for groups of order less than that of G, we shall show that it is also true for G. To start the induction we see that the theorem is obviously true if $o(G) = 1$.

Let $o(G) = p^m n$ where p is not a divisor of n.

If $m = 0$, the theorem is obviously true. If m =1, the theorem is true by cauchy's theorem.

So let $m > 1$. Then G is a group of composite order and so G must posses a subgroup H such that $H \neq G$.

If p is not a divisor of $\frac{o(G)}{o(H)}$, then $p^m \mid o(H)$ because $o(G) = p^m n = o(H) \times \frac{o(G)}{o(H)}$

Also p^{m+1} cannot be a divisor of $o(H)$ because then p^{m+1} will be a divisor of $o(G)$ of which $o(H)$ is a divisor. Further $o(H) < o(G)$. Therefore by our induction hypothesis, the theorem is true for H. Therefore H has a subgroup of order p^m and this will also be a subgroup of G. So let us assume that for every subgroup H of G where $H \neq G$, p is a divisor of $\frac{o(G)}{o(H)}$.

Consider the class equation

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o\left[N(a)\right]} \qquad \ldots\ldots (1)$$

Since $a \notin Z \Rightarrow N(a) \neq G$, therefore according to our assumption p is a divisor of $\sum_{a \notin Z} \frac{o(G)}{o\left[N(a)\right]}$ Also $p \mid o(G)$.

Therefore from (1), we conclude that p is a divisor of o(Z). Then by Cauchy's theorem, Z has an element *b* of order *p* and Z is the centre of G. Also N = {b} is a cyclic subgroup of Z of order p. Therefore N is a cyclic subgroup of G is order *p*. Since $b \in Z$, therefore N is normal subgroup of G of order p.

Now consider the quotient group G′=G/N. We have $o(G') = o(G)/o(N) = p^m n / p = p^{m-1} n$. Thus $o(G') < o(G)$. Also $p^{m-1} \mid o(G')$ but p^m is not a divisor of $o(G')$. Therefore by our induction hypothesis G' has a subgroup, say S′ of order p^{m-1}. We know that the natural mapping $\phi : G \to G/N$ defined by $\phi(x) = Nx \; \forall \; x \in G$ is a homomorphism of G onto G/N with kernel N, Let $S = \{x \in G : \phi(x) \in S'\}$. Then S is a subgroup of G and $S' \cong S/N$.

$$\therefore \; o(S') = o(S/N) = \frac{o(S)}{o(N)}$$

Therefore $o(S) = o(S').o(N) = p^{m-1} p = p^m$

Hence S is a subgroup of G of order p^m.

Solved Examples

Example.10: If H is a *p*-sylow subgroup of G and $x \in G$, then $x^{-1}Hx$ is also a *p*-sylow subgroup of G.

Solution: Suppose G is a finite group and o(G) $= p^m n$ where *p* is a prime number and *p* is not a divisor of *n*. If H is a p-sylow subgroup of G, then $o(H) = p^m$.

Let $x \in G$ be arbitrary. Then $x^{-1}Hx$ will be a $p-sylow$ sub-group of G if $x^{-1}Hx$ is subgroup of G and if $o\left(x^{-1}Hx\right) = p^m$. First we shall prove that $x^{-1}Hx$ is a subgroup of G·

Then for $h_1, h_2 \in H$ we have

$\left(x^{-1}h_1x\right)\left(x^{-1}h_2x\right)^{-1} = x^{-1}h_1xx^{-1}h_2^{-1}\left(x^{-1}\right)^{-1} = x^{-1}h_1eh_2^{-1}x = x^{-1}h_1h_2^{-1}x \in x^{-1}Hx$ since $h_1h_2^{-1} \in H$,

H being a subgroup of G. $\therefore x^{-1}Hx$ is a subgroup of G.

Now let ψ be a mapping from H into $x^{-1}Hx$ defined as $\psi(h) = x^{-1}hx \forall h \in H$. ψ is onto. Let $x^{-1}hx$ be any element of $x^{-1}Hx$. Then $h \in H$ and we have $\psi(h) = x^{-1}hx$. Therefore ψ is onto.

ψ is one-one. Let $h_1, h_2 \in H$. Then $\psi(h_1) = \psi(h_2) \Rightarrow x^{-1}h_1x - x^{-1}h_2x \Rightarrow h_1 = h_2 \Rightarrow \psi$ is one-one.

Thus ψ is a one-to-one correspondence between the elements of H and the elements of $x^{-1}Hx$. Therefore $o\left(x^{-1}Hx\right) = o(H) = p^m$. Hence $x^{-1}Hx$ is a *p*-sylow subgroup of G.

Example.11: If a group G has only one p-sylow subgroup H, then H is normal in G.

Solution: Suppose a group G has only one p-sylow subgroup H. Let x be any element of G. Then by previous exercise, $x^{-1}Hx$ is also a p-sylow subgroup of G. But H is the only p-sylow sub-group of G. Therefore $x^{-1}Hx = H \ \forall x \in G \Rightarrow H$ is a normal subgroup of G.

9.13 Summary

A mapping *f* from a group G into a group G′ is said to be homorphism of G into G′ if

$$f(a\,b) = f(a)\,f(b) \quad \forall\ a, b \in G$$

A homomorphism of a group into itself is called an endomorphism.

If *f* is a homomorphism of a group G into a group G′, Then the set K of all those elements of G which are mapped by *f* onto the identity e′ of G′ is called the kernel of the homomorphism *f*.

Every homomorphic image of a G is isomorphic to some quotient group G.

An isomorphic mapping of a group G onto itself is called an automorphism of G. Thus
$f : G \xrightarrow{\text{onto}} G$ is an automorphism of G if

$$f(ab) = f(a)\,f(b) \quad \forall\, a, b \in G.$$

If G is a group, the mapping $f_a : G \to G$ defined by

$$f_a(x) = a^{-1}xa \quad \forall\, x \in G$$

is an automorphism of G known as inner automorphism. Also an automorphism which is not inner is called an outer automorphism.

A normal subgroup H of a group G is said to be maximal if there exists no proper subgroup K of G which properly contains H.

Let G be a group. Then a finite sequence of its subgroups

$$G = H_1, H_2, H_3, ..., H_n = \{e\} \qquad \ldots\ldots (1)$$

is called a composition series for G if each H_i except H_1 is a maximal normal subgroup of H_{i-1}.

The quotient groups G/H_1, H_2/H_3,…… H_{n-1}/H_n which are necessarily simple are then called composition factor groups or composition quotient groups of the composition series (1).

(Jordan-holder Theorem) Let G be a finite group with two composition series

$$G, H_1, H_2, ..., H_n = \{e\} \qquad \ldots\ldots. (1)$$

and $$G, K_1, K_2, ..., K_m = \{e\} \qquad \ldots\ldots (2)$$

Then $n = m$ and the two corresponding series of composition quotient groups, viz.,

$G / H_1, H_1 / H_2, ..., H_{n-1} / H_n$ and $G / K_1, K_1 / K_2, ..., K_{m-1} / K_m$

are abstractly identity *i.e,* they can be put into one-one correspondence such that the corresponding quotient groups are isomorphic.

A group G is said to be solvable if we can find a finite chain of subgroups

$$G = N_0 \supseteq N_1 \supseteq N_2 \supseteq ..... \supseteq N_k = (e)$$

Such that each N_i is a normal subgroup of N_{i-1} and each quotient group N_{i-1} / N_i is abelain. The above series, then is referred to as a solvable series for G.

Let G_1 and G_2 be any two groups the composition in each being denoted multiplicatively. Then

$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$

Suppose G is a finite group and o(G) = $p^m n$ where *p* is a prime number and *p* is not a divisor of *n*. Then a subgroup H of G is said to be a *p*-sylow subgroup of G iff o(H) =p^m.

(Sylow's theorem) Suppose G is a group of finite order and p is a prime number. If $p^m | o(G)$ and p^{m+1} is not a divisor of o (G) then G has a subgroup of order p^m.

9.14 Terminal Questions

Q.1. Explain the concept of homomorphism with example.

Q.2. What do you mean by kernel of a homomorphism?

Q.3. State and prove the Fundamental theorem on Homomorphism of Groups.

Q.4. Define automorphisms of a group.

Q.5. What do you mean by inner automorphism?

Q.6. Define Maximal subgroups.

Q.7. Explain the Composition series of a group.

Q.8. State and prove the Jordan-holder Theorem.

Q.9. Define the solvable groups.

Q.10. Sate and prove the Sylow's Theorem.

Q.11. Explain the concept of *p*-sylow subgroup.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

U. P. Rajarshi Tandon
Open University

Master of Science

PGMM -106/MAMM-106
Advanced Algebra

Block

4 Rings and Field Theory

Block-4

Rings and Field Theory

The idea of a ring came about in the late 1800s and early 1900s. Mathematicians wanted to extend the rules of arithmetic we know for whole numbers and polynomials. The term ring was first used by David Hilbert around 1890 when he was studying number fields. Later, Emmy Noether made important contributions by giving a clear and general definition of rings and studying their properties. Because of her work, ring theory became an important part of modern algebra.

The concept of an ideal was introduced earlier by Richard Dedekind in 1871. He created ideals to help solve problems in number theory, especially when unique factorization of numbers did not hold in some number systems. By grouping certain elements together into ideals, he was able to recover unique factorization in a new way. Over time, rings and ideals became key ideas in many areas of Mathematics, like number theory and algebraic geometry. Today ring theory is a basic topic studied in higher Mathematics and has many uses.

In the tenth unit, we shall discuss about the Rings, elementary properties of a ring, ring with or without zero divisors, integral domain, field, subrings and subfields. Eleventh unit introduced the concept of ideals, principal ideal, divisibility in an integral domain, greatest common divisor, polynomials rings, unique factorization domain and remainder theorem, Quotient rings, homomorphism on rings, kernel of a ring homomorphism, maximal ideals, prime ideals and Euclidean rings.

UNIT- 10: Rings

Structure

10.1 Introduction

The idea of a ring in math began in the late 1800s and early 1900s. At that time, Mathematicians wanted to understand and work with different kinds of numbers. Rings were first found when studying whole numbers and polynomials. Later, great mathematicians like Dedekind, Hilbert, and Noether clearly showed what a ring means. A ring is a set of elements where you can do addition and multiplication, following certain rules. Rings are very useful in many parts of math like number theory and geometry, where they help solve problems and study shapes. In computer science, rings are used in coding and cryptography to keep data safe. In physics, rings help describe patterns and systems, especially in quantum mechanics. Because they are used in so many areas, rings are an important part of both pure and applied Mathematics. So far, we have learned about the groups, which use one operation. Now, we will learn about the rings, which use two operations.

10.2 Objectives

After studying this unit the learner will be able to understand the :

- Ring and Ring with unity
- Commutative ring and elementary properties of a ring
- Ring with or without zero divisors
- Integral domains, field
- Division ring or skew field
- Subrings and subfields

10.3 Ring

Consider R is a non-empty set with operations (addition and multiplication) and denoted by '+' and '.' respectively *i.e.*, for all $a, b \in R$ we have $a + b \in R$ and $a.b \in R$.

Then this algebraic structure $(R, +, .)$ is known as a ring if the following properties are satisfied:

1. Addition is associative, *i.e.,* $(a+b)+c = a+(b+c) \ \forall\, a,b,c \in R.$

2. Addition is commutative, *i.e.,* $a+b = b+a \quad \forall\, a, b \in R.$

3. There exists an element denoted by 0 in R such that $0+a = a \quad \forall\, a \in R.$

4. To each element a in R there exists an element $-a$ in R such that $(-a)+a = 0.$

5. Multiplication is associative, *i.e.,* $a.(b.c) = (a.b).c \ \forall\, a,b,c \in R.$

6. Multiplication is distributive with respect to addition, *i.e.,* for all a, b, c in R,

$$\left.\begin{array}{ll} a.(b+c) = a.b + a.c & \text{Left distributive law} \\ \text{and} \quad (b+c).a = b.a + c.a & \text{Right distributive law} \end{array}\right\}$$

Since addition is commutative in $R,$ therefore we shall have $0 \in R$ such that

$$0+a = a = a+0 \ \forall\, a \in R.$$

Also if $a \in R,$ then we shall have $(-a)+a = 0 = a+(-a).$

Thus, R forms an abelian group under addition. The element that acts as the additive identity is called the zero element of the ring. Since the identity element in a group is always unique, every ring has exactly one zero element, which serves as the identity for addition. We will always represent this element by the symbol 0.

10.4 Ring with Unity

If in a ring R there exists an element denoted by 1 such that $1.a = a = a.1 \ \forall\, a \in R,$ then R is called a ring with unity element. The element $1 \in R$ is known as the unity element of the ring. Obviously 1 is the multiplicative identity of $R.$ Thus if a ring possesses multiplicative identity, then it is a ring with unity.

10.5 Commutative Ring

If in a ring R, the multiplication composition is also commutative *i.e.*, if we have $a.b = b.a \quad \forall\, a, b \in R$, then R is known as a commutative ring.

Note. Here we shall write ab in the place of $a.b$.

10.6 Elementary Properties of a Ring

Theorem.1. If R is a ring, then for all $a, b, c \in R$, we have

(i) $a0 = 0a = 0.$

(ii) $a(-b) = -(ab) = (-a)b.$

(iii) $(-a)(-b) = ab.$

(iv) $a(b-c) = ab - ac.$

(v) $(b-c)a = ba - ca.$

Proof. (i) We have

$$a0 = a(0+0) \qquad [\because\ 0+0=0]$$

$$= a0 + a0. \qquad \text{[by left distributive law]}$$

Thus we have $0 + a0 = a0 + a0. \qquad [\because\ a0 \in R \text{ and } 0 + a0 = a0]$

Now R is a group with respect to addition, therefore applying right cancellation law for addition in R, we get $0 = a0$.

Similarly, we have

$$0a = (0+0)a$$

$= 0a + 0a$ [by right distributive law]

Thus we have $0 + 0a = 0a + 0a.$ $\left[\because\ 0 + 0a = 0a\right]$

Applying right cancellation law for addition in R, we get

$$0 = 0a.$$

(ii) We have $a\left[(-b) + b\right] = a0$ $\left[\because -b + b = 0\right]$

$\Rightarrow$ $a(-b) + ab = 0$ [By using left distributive law and the result (i)]

$\Rightarrow$ $a(-b) = -(ab),$

Since in a ring $a + b = 0$

$\Rightarrow$ $a = -b.$

Similarly, we have

$$(-a + a)b = 0b$$

$\Rightarrow$ $(-a)b + ab = 0$

$\Rightarrow$ $(-a)b = -(ab),$

Since in a ring $a + b = 0$

$\Rightarrow$ $a = -b.$

(iii) We have $(-a)(-b) = -\left[(-a)b\right],$ since $a(-b) = -(ab)$

$= -\left[-(ab)\right],$ since $(-a)b = -(ab)$

$= ab,$

Since R is a group with respect to addition and in a group we have

$$-(-a)=a.$$

(iv) We have $a(b-c)=a\left[b+(-c)\right]$

$$=ab+a(-c) \qquad \text{[left distributive law]}$$

$$=ab+\left[-(ac)\right] \qquad \left[\because \quad a(-c)=-(ac)\right]$$

$$=ab-ac.$$

(v) We have $(b-c)a=\left[b+(-c)\right]a$

$$=ba+(-c)a \qquad \text{[right distributive law]}$$

$$=ba+\left[-(ca)\right]$$

$$=ba-ca$$

Solved Examples

Example.1. The set M of all $n\times n$ matrices with their elements as real numbers (rational numbers, complex numbers, integers) is a non-commutative ring with unity, with respect to addition and multiplication of matrices as the two ring compositions.

Sol. We know that the sum and product of two $n\times n$ matrices with their elements as real numbers are again $n\times n$ matrices with their elements as real numbers. Therefore M is closed with respect to addition and multiplication of matrices.

Further we observe that

(i) $A+(B+C)=(A+B)+C \quad \forall A,B,C\in M$, since the addition of matrices is an associative composition.

(ii) $A+B=B+A \quad \forall\, A,B\in M$, since the addition of matrices is commutative.

(iii) If O is the null matrix of the type $n\times n$, then $O\in M$ and we have

$$O+A=A \quad \forall\, A\in M.$$

(iv) To each matrix $A\in M$ there exists a matrix $-A\in M$ such that $(-A)+A=O$ (null matrix).

(v) $(AB)C=A(BC), \quad \forall\, A,B,C\in M$, since multiplication of matrices is associative.

(vi) $A(B+C)=AB+AC$, and $(B+C)A=BA+CA \quad \forall\, A,B,C\in M$, since matrix multiplication is distributive with respect to matrix addition.

Here M is a ring with respect to the given compositions. The null matrix O of the type $n\times n$ is the zero element of this ring *i.e.,* $O=0$.

Since the multiplication of matrices is not in general commutative, therefore the ring is a non-commutative ring. $[n>1]$

Finally if I be the unit matrix of the type $n\times n$, then $I\in M$ and we have

$$IA=A=AI \quad \forall\, A\in M.$$

Therefore the matrix I is the multiplicative identity.

Thus the ring is with unity and the matrix I is the unity element of the ring *i.e.,* I =1.

Example.2. To show that the set $R=\{0,1,2,3,4,5\}$ is a commutative ring with respect to $'+_6'$ and $'\times_6'$ as the two ring compositions.

Sol. As we have proved in groups, we should first prove that R is an abelian group with respect to $'+_6'$.

Now we form the composition table for R for the composition $\times_6$.

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

From the composition table we see that R is closed with respect to the composition '$\times_6$'. Also we know that '$\times_6$' is an associative composition in R *i.e.*,

$$a \times_6 (b \times_6 c) = (a \times_6 b) \times_6 c \quad \forall\, a, b, c \in R.$$

Further '$\times_6$' is distributive in R with respect to '$+_6$'. If a, b, c are any elements of R, then

$$a \times_6 (b +_6 c) = a \times_6 (b + c) \qquad [\because a \times_6 b \equiv (\text{mod } 6)]$$

= least non-negative remainder when $a(b+c)$ is divided by 6

= least non-negative remainder when $ab + ac$ is divided by 6

$$= (ab) +_6 (ac) = (a \times_6 b) +_6 (ac) \qquad [\because a \times_6 b \equiv ab (\text{mod } 6)]$$

$$= (a \times_6 b) +_6 (a \times_6 c) \qquad [\because a \times_6 c \equiv ac (\text{mod } 6)]$$

Similarly, we can prove that $(b +_6 c) \times_6 a = (b \times_6 a) +_6 (c \times_6 a)$.

Thus R is a ring with respect to the given compositions. Since '$\times_6$' is a commutative composition in R as is clear from the composition table also, therefore R is a commutative ring. Also 1 is the identity element for the composition '$\times_6$'.

Therefore R is a ring with unity. The integer 0 is the zero element of this ring.

10.7 Rings with or without zero divisors

A non-zero element a of a ring R is called a zero divisor or a divisor of zero if there exists an element $b \neq 0 \in R$ such that either $ab = 0$ or $ba = 0$.

A ring R is without zero divisors if the product of no two non-zero elements of R is zero *i.e.*, if $ab = 0 \Rightarrow a = 0$ or $b = 0$.

On the other hand if in a ring R there exist non-zero elements a and b such that

then R is said to be a ring with zero divisors.

Note: 1. Cancellation laws in a ring. If R is a ring then R is an abelian group with respect to addition. For addition composition the cancellation laws hold in all rings. Therefore the question of cancellation laws holding or not in a ring arises only for the multiplication composition.

We say that cancellation laws hold in a ring R if $a \neq 0, ab = ac \Rightarrow b = c$ and $a \neq 0$, $ba = ca \Rightarrow b = c$ where $a, b, c \in R$.

2. The ring $\left(\{0, 1, 2, 3, 4, 5\}, +_6, \times_6\right)$ is a ring with zero divisors. We have $2 \times_6 3 = 0,\ 3 \times_6 4 = 0$ *i.e.*, the product of two non-zero elements is equal to the zero element of the ring.

Theorem.2. A ring R is without zero divisors if and only if the cancellation laws hold in R i.e., R is without zero divisors $\Leftrightarrow$ cancellation laws hold in R.

Proof. First suppose that R has no zero divisors. Let a, b, c be any three elements of R such that $a \neq 0, ab = ac$.

We have $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$.

Since R is without zero divisors, therefore we have

$a(b - c) = 0$ and $a \neq 0$

$\Rightarrow \quad b-c=0$ *i.e.,* $b=c.$

Thus the left cancellation law holds in $R.$

Similarly, we can show that the right cancellation law holds in $R.$

Conversely suppose that the cancellation laws in hold in $R.$ If possible consider

$$ab=0, a\neq 0, b\neq 0.$$

Then we have $ab=a0,$ since $ab=a0,$

Now $a\neq 0, ab=a0\Rightarrow b=0$ by left cancellation law.

Thus we get a contradiction.

Hence R is without zero divisors.

Check your Progress

Q.1. What do you mean by ring theory?

Q.2. Explain the ring with unity.

Q.3. Define commutative ring.

Q.4. The set $2\mathrm{I}$ of all even integers is a commutative ring without unity, addition and multiplication of integers being the two ring compositions.

Q.5. The set Q of all rational numbers is a commutative ring with unity, the addition and multiplication of rational numbers being the two ring compositions.

Q,6. The set R of all real numbers is a commutative ring with unity, the addition and multiplication of real numbers being the two ring compositions.

Q.7. The set C of all complex numbers is a commutative ring with unity, the addition and multiplication of complex numbers being the two ring compositions.

10.8 Integral Domain

A ring is known as an integral domain if it (i) it is commutative (ii) it has unit element, and (iii) it is without zero divisor.

Note: 1. Inversible elements in a ring with unity. In a ring every element possesses additive inverse. Therefore the question of an element being Inversible or not arises only with respect to multiplication. If R is a ring with unity, then an element $a \in R$ is known as Inversible, if there exists $b \in R$ such that $ab = 1 = ba$. Also then we write $b = a^{-1}$.

2. 1 and -1 are the only two Inversible elements of the ring of all integers.

3. $n \times n$ non-singular matrices with real numbers as elements are the only Inversible elements of the ring of all $n \times n$ matrices with elements as real numbers.

10.9 Field

A ring R with at least two elements is called a field if it (i) is commutative, (ii) has unity,

(iii) is such that each non-zero element possesses multiplicative inverse.

For example, the ring of rational numbers $(Q, +, .)$ is a field since it is a commutative ring with unity and each non-zero element is Inversible.

Note.1. The rings of real numbers and complex numbers are also examples of fields.

2. As an example of a finite field we have the ring $\left(\{0, 1, 2, 3, 4\}, +_5, \times_5\right)$.

3. If $a, 0 \neq b$ are elements of a field F, then we shall often write $ab^{-1} = \frac{a}{b} = b^{-1}a$. In a field F, we have

$$\frac{a}{b} + \frac{c}{d} = \left(ab^{-1}\right) + \left(cd^{-1}\right) = \left(bd\right)^{-1}\left(bd\right)\left[\left(ab^{-1}\right) + \left(cd^{-1}\right)\right]$$

$$= (bd)^{-1}\left[(bd)(ab)^{-1} + (bd)\left(cd^{-1}\right)\right] = (ad+bc)(bd)^{-1} = \frac{ad+bc}{bd}.$$

[Note that multiplication of F is commutative].

Also we have $\frac{a}{b}\frac{c}{d} = \left(ab^{-1}\right)\left(cd^{-1}\right) = (ac)\left(b^{-1}d^{-1}\right) = (ac)(bd)^{-1} = \frac{ac}{bd}.$

10.10 Division Ring or Skew Field

A ring R with at least two elements is called a division ring or a skew field if it (i) has unity, (ii) is such that each non-zero element possesses multiplicative inverse. Thus a commutative division ring is a skew field.

Note:1. Every field is also a division ring. But a division ring is a field if it is also commutative.

2. For a field unity and zero are distinct elements i.e., $1 \neq 0$. Let a be any non-zero element of a field. Then a^{-1} exists and is also non-zero. For, $a^{-1} = 0 \Rightarrow aa^{-1} = a0 \Rightarrow 1 = 0 \Rightarrow a1 = a0 \Rightarrow a = 0$ which is a contradiction. Now a field has no zero divisors. Therefore $1 = a^{-1}a \neq 0.$

3. A field has no zero divisors. Therefore in a field the product of two non-zero elements will again be a non-zero element. Also the unit element $1 \neq 0$ and each non-zero element possesses multiplicative inverse which is a again a non-zero element. The multiplication is commutative as well as associative. Therefore the non-zero elements of a field form an abelian group with respect to multiplication.

Theorem.3. Every field is an integral domain.

Proof. Since a field F is a commutative ring with unity, therefore in order to show that every field is an integral domain we should show that a field has no zero divisors.

Let a, b be elements of F with $a \neq 0$ such that $ab = 0.$

Since $a \neq 0, a^{-1}$ exists and we have

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 \Rightarrow \left(a^{-1}a\right)b = 0 \Rightarrow 1b = 0 \qquad \left[\because a^{-1}a = 1\right]$$

$\Rightarrow b = 0.$ $\quad [\because 1b = b]$

Similarly, let $ab = 0$ and $b \neq 0.$

Since $b \neq 0, b^{-1}$ exists and we have

$$ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1} \Rightarrow a\left(bb^{-1}\right) = 0 \Rightarrow a1 = 0 \Rightarrow a = 0.$$

Thus in a field $ab = 0 \Rightarrow a = 0$ or $b = 0.$ Therefore a field has no zero divisors. Therefore every field is an integral domain.

But the converse in not true i.e., every integral domain is not a field. For example the ring of integers is an integral domain and it is not a field. The only Inversible elements of the ring of integers are 1 and -1.

Theorem.4. A sfield (skew-field) had no divisors of zero.

Proof. Let D be a skew –field. Then D is a ring with unit element 1 and each non-zero element of D possesses multiplicative inverse.

Let a, b be elements of D with $a \neq 0$ such that $ab = 0.$

Since $a \neq 0, a^{-1}$ exists and we have

$$ab = 0$$

$$\Rightarrow \quad a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow \quad \left(a^{-1}a\right)b = 0$$

$$\Rightarrow \quad 1b = 0$$

$$\Rightarrow \quad b = 0$$

Similarly, suppose $ab = 0$ with $b \neq 0.$

Since $b \neq 0, b^{-1}$ exists and we have

$$ab = 0$$

$\Rightarrow \quad (ab)b^{-1} = 0b^{-1}$

$\Rightarrow \quad a(bb^{-1}) = 0$

$\Rightarrow \quad a1 = 0$

$\Rightarrow \quad a = 0.$

Therefore a skew-field has no zero divisors.

Theorem.5. A finite commutative ring without zero divisors is a field. or Every finite integral domain is a field.

Proof. Let D be a finite commutative ring without zero divisors having n elements $a_1, a_2, ..., a_n$. In order to prove that D is a field, we must produce an element $1 \in D$ such that $1a = a \forall a \in D$. Also we show that for every element $a \neq 0 \in D$ there exists an element $b \in D$ such that $ba = 1$.

Let $a \neq 0 \in D$. Consider the n products $aa_1, aa_2, ..., aa_n$.

All these are elements of D. Also they are distinct.

For suppose that $aa_i = aa_j$ for $i \neq j$.

Then we have $a(a_i - a_j) = 0.$ ....(1)

Since D is without zero divisors and $a \neq 0$, therefore equation (1) implies

$a_i - a_j = 0 \Rightarrow a_i = a_j$, contradicting $i \neq j$.

$\therefore$ $aa_1, aa_2, ..., aa_n$ are all the n distinct elements of D placed in some order. So one of these elements will be equal to a. Thus there exists an element, say $1 \in D$ such that

$a1 = a = 1a.$ $[\because D$ is commutative$]$

We shall show that this element 1 is the multiplicative identity of D. Let y be any arbitrary element of D. Then from the above discussion for some $x \in D$, we shall have

$ax = y = xa.$

Now we have

$1y = 1(ax)$ $\quad [\because ax = y]$

$= (1a)x = ax$ $\quad [\because 1a = a]$

$= y$ $\quad [\because ax = y]$

$= y1$ $\quad [\because D$ is commutative]

Thus $1y = y = y1, \quad \forall\, y \in D.$ Therefore 1 is the unit element *i.e.,* the multiplicative identity of the ring $D.$

Now $1 \in D.$ Therefore from the above discussion one of the n products $aa_1, aa_2, \ldots, aa_n$ will be equal to 1. Thus there exists an element, say, $b \in D$ such that

$ab = 1 = ba.$

$\therefore b$ is the multiplicative inverse of the non-zero element $a \in D.$ Thus every non-zero element of D is Inversible.

Hence D is a field.

Solved Examples

Example.3. Prove that if $a, b \in R$ then $(a+b)^2 = a^2 + ab + ba + b^2$, where by x^2 we mean xx.

Sol. We have

$(a+b)^2 = (a+b)(a+b)$

$= a(a+b) + b(a+b)$ [by right distributive law]

$= (aa + ab) + (ba + bb)$ [by left distributive law]

$= a^2 + ab + ba + b^2$.

Example.4. If R **is a ring such that** $a^2 = a \quad \forall\, a \in R$ **then prove that**

(i) $a + a = 0 \,\forall\, a \in R$ **i.e., each element of R is its own additive inverse.**

(ii) $a + b = 0 \Rightarrow a = b.$

(iii) R is a commutative ring.

Sol. (i) $a \in R \quad \Rightarrow \quad a + a \in R.$

Now $(a+a)^2 = (a+a)$ [given]

$\Rightarrow \quad (a+a)(a+a) = a + a$

$\Rightarrow \quad (a+a)a + (a+a)a = a + a$ [Left Distributive Law]

$\Rightarrow \quad (a^2 + a^2) + (a^2 + a^2) = a + a$ [Right Distribtive Law]

$\Rightarrow \quad (a+a) + (a+a) = a + a \qquad [\because a^2 = a]$

$\Rightarrow \quad (a+a) + (a+a) = (a+a) + 0 \qquad [\because a + 0 = a]$

$\Rightarrow \quad (a+a) = 0$ [by left cancellation law for addition in R]

(ii) We have just proved that $a + a = 0.$

$\therefore \quad a + b = 0$

$\Rightarrow \quad a + b = a + a$

$\Rightarrow \quad b = a,$ by left cancellation law for addition in R .

(iii) We have

$$(a+b)^2 = (a+b)$$

$\Rightarrow$ $(a+b)(a+b) = (a+b)$

$\Rightarrow$ $(a+b)a + (a+b)b = a+b$ [Left Dist. Law]

$\Rightarrow$ $(a^2 + ba) + (ab + b^2) = a+b$ [Right Dist. Law]

$\Rightarrow$ $(a+ba) + (ab+b) = a+b$ $[\because a^2 = a, b^2 = b]$

[by commutativity and associativity of addition]

$\Rightarrow$ $ba + ab = 0$ [by left cancellation law for addition in R]

$\Rightarrow$ $ab = ba.$ [by part (ii) of this question]

Hence R is a commutative ring.

Example.5. Prove that the set M of 2×2 matrices over the field of real numbers is a ring with respect to matrix addition and multiplication. Is it a commutative ring with unity element? Find the zero element. Does this ring possess zero divisors?

Sol. Both addition and multiplication of matrices are associative compositions.

$\therefore$ $A+(B+C) = (A+B)+C \;\forall\; A,B,C \in M$

And $A(BC) = (AB)C \;\forall\; A,B,C \in M.$

Addition of matrices is a commutative composition. Therefore for all $A,B \in M$, we have $A+B = B+A.$

If O be the null matrix of the type 2×2, then $O \in M$ and $O+A = A \;\forall\; A \in M.$

Further multiplication of matrices is distributive with respect to addition.

$\therefore \quad A(B+C) = AB + AC$

and $(B+C)A = BA + CA \; \forall \; A, B, C \in M$.

$\therefore M$ is a ring with respect to the given compositions.

Multiplication of matrices is not in general a commutative composition. For example, if

$$A = \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \text{ then}$$

$$AB = \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 8 \\ 3 & 11 \end{bmatrix}$$

and $BA = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 8 & 14 \\ 3 & 5 \end{bmatrix}$

Thus $AB \neq BA$ and so the ring is non-commutative ring.

If I be the unit matrix of the type 2×2 *i.e.*, if $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $I \in M$. Also we have

$$AI = A = IA \quad \forall \in M.$$

$\therefore I$ is the multiplicative identity.

Thus the ring possesses the unit element and we have $I = 1$ (the unit element of the ring).

The null matrix $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the additive identity and is therefore the zero element of the ring i.e., $O = 0$ (the zero element of the ring).

The ring possesses zero divisors. For example if

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix},$$

Then we have

$$AB = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring.

Example.6. Show that the set of numbers of the form $a+b\sqrt{2}$, with a and b as rational numbers is a field.

Sol. Let $R = \left\{a+b\sqrt{2} : a,b \in Q\right\}$.

Let $a_1+b_1\sqrt{2} \in R$ and $a_2+b_2\sqrt{2} \in R$. Then $a_1, b_1, a_2, b_2 \in Q$.

We have

$$\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right) = \left(a_1+a_2\right)+\left(b_1+b_2\right)\sqrt{2} \in R \text{ since } a_1+a_2, b_1+b_2 \in Q.$$

Also we have

$$\left(a_1+b_1\sqrt{2}\right)\left(a_2+b_2\sqrt{2}\right) = \left(a_1a_2+2b_1b_2\right)+\left(a_1b_2+a_2b_1\right)\sqrt{2} \in R$$

$$\text{since } a_1a_2+2b_1b_2, a_1b_2+a_2b_1 \in Q.$$

Thus R is closed with respect to addition and multiplication.

All the elements of R are real numbers and we know that addition and multiplication are both associative as well as commutative compositions in the set of real numbers.

Further we have $0+0\sqrt{2} \in R$ since $0 \in Q$.

If $a+b\sqrt{2} \in R$, then we have $\left(0+0\sqrt{2}\right)+\left(0+a\right)+\left(0+b\right)\sqrt{2} = a+b\sqrt{2}$.

Therefore $0+0\sqrt{2}$ is the additive identity.

Again if $a+b\sqrt{2}\in R,$ then we have $(-a)+(-b)\sqrt{2}\in R$ and we have

$$\left[(-a)+(-b)\sqrt{2}\right]+\left(a+b\sqrt{2}\right)=0+0\sqrt{2}.$$

Thus each element of R possesses additive inverse.

Further in the set of real numbers multiplication is distributive with respect to addition.

Again $1+0\sqrt{2}\in R$ and we have

$$\left(1+0\sqrt{2}\right)\left(a+b\sqrt{2}\right)=\left(a+b\sqrt{2}\right)=\left(a+b\sqrt{2}\right)\left(1+0\sqrt{2}\right).$$

$\therefore$ $1+0\sqrt{2}$ is the multiplicative identity.

Thus R is a commutative ring with unity. The zero element of the ring is $0+0\sqrt{2}$ and the unit element is $1+0\sqrt{2}.$

Now R will be a field, if each non-zero element of R possesses multiplicative inverse.

Let $a+b\sqrt{2}$ be any non-zero element of this ring *i.e.,* at least one of a and b is not zero.

Then we have

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{\left(a+b\sqrt{2}\right)\left(a-b\sqrt{2}\right)}$$

$$=\frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$=\left(\frac{a}{a^2-2b^2}\right)-\left(\frac{b}{a^2-2b^2}\right)\sqrt{2}$$

Now if a and b are rational numbers, then we can have $a^2=2b^2$ only if $a=0,b=0.$ Since here at least one of the rational numbers a and b is not $0,$ therefore we cannot have $a^2=2b^2$ *i.e.,* $a^2-2b^2=0.$

Thus $\frac{a}{a^2-2b^2}$ and $-\frac{b}{a^2-2b^2}$ are both rational numbers and at least one of them is not zero.

$\therefore \left(\frac{a}{a^2-2b^2}\right)+\left(-\frac{b}{a^2-2b^2}\right)\sqrt{2}$ is a non-zero element of R and is the multiplicative inverse of $a+b\sqrt{2}$. Hence the given system is a field.

10.11 Subrings

Let R be a ring. A non-empty subset S of the set R is said to be a subring of R if S is closed with respect to the operations of addition and multiplication in R and S itself is a ring for these operations.

If S is a subring of a ring R, it is obvious that S is a subgroup of the additive group of R.

If R is any ring, then $\{0\}$ and R itself are always subrings of R. Theses are known as improper subrings of R. Other subrings, if any, of R are called proper subrings of R.

Check your Progress

Q.1. What do you mean by integral domain?

Q.2. Explain the field.

Q.3. Define Division Ring or Skew Field.

Q.4. To show that the rings of real numbers and complex numbers are also examples of fields.

Q.5. If a, b, c are elements of a ring R, then evaluate $(a+b)(c+d)$.

Theorem.6. The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are (i) $a \in S, b \in S \Rightarrow a-b \in S$ (ii) $a \in S, b \in S \Rightarrow ab \in S$.

Proof. Necessary conditions: Suppose $(S,+,.)$ is a subring of $(R,+,.)$

Since S is a group with respect to addition, therefore $b \in S \Rightarrow -b \in S$.

Now S is closed with respect to addition.

Thus we have

$$a \in S, b \in S \quad \Rightarrow \quad a \in S, -b \in S$$

$$\Rightarrow \quad a + (-b) \in S$$

$$\Rightarrow \quad a - b \in S.$$

Also S is closed with respect to multiplication.

$$\therefore \quad a \in S, b \in S \quad \Rightarrow \quad ab \in S.$$

Hence the conditions are necessary.

Sufficient conditions: Suppose S is a non-empty subset of R and the conditions (i) and (ii) are satisfied. From (i), we have

$$a \in S, a \in S \quad \Rightarrow \quad a - a \in S \quad \Rightarrow \quad 0 \text{ } i.e., \text{ the zero element } \in S.$$

Now since $0 \in S$, therefore from (i), we have

$$0 \in S, -b \in S \quad \Rightarrow \quad a - (-b) \in S \quad \Rightarrow \quad a + b \in S.$$

$\therefore S$ is closed with respect to addition.

Now S is a subset of R. Therefore associativity and commutativity of addition must hold in S since they hold in R.

$\therefore (S, +)$ is an abelian group.

From (ii) S is closed with respect to multiplication.

Associativity of multiplication and distributivity of multiplication over addition must hold in S since they hold in R.

Hence S is a subring of R.

Theorem.7. The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are **(i)** $S+(-S)=S$ **(ii)** $SS \subseteq S$.

Proof. Necessary conditions: Suppose S is a subring of R. Then S is a subgroup of the additive group of R.

Let $a+(-b)$ be any element of $S+(-S)$.

We have

$$a+(-b) \in S+(-S) \Rightarrow a \in S, -b \in -S \Rightarrow a \in S, b \in S$$

$\Rightarrow$ $a-b \in S$ [$\because S$ is a subgroup]

Thus $S+(-S) \subseteq S$.

Also let a be any element of S. We can write $a=a+0$.

Now S is a subgroup. Therefore $0 \in S$ or $\in -S$.

So $a+0 \in S+(-S)$. $\therefore S \subseteq S+(-S)$

Thus $S=S+(-S)$.

Also S must be closed with respect to multiplication.

$\therefore$ $a \in S, b \in S \Rightarrow ab \in S$.

Now ab is an arbitrary element of SS.

$\therefore$ $SS \subseteq S$.

Sufficient conditions: Suppose S is a non-empty subset of R satisfying the two given conditions.

We have $SS \subseteq S \Rightarrow ab \in S \nrightarrow a, b \in S$.

Therefore S is closed with respect to multiplication.

Also $S+(-S)=S \Rightarrow S+(-S)\subseteq S.$

$= a+(-b)\in S$ if $a,b\in S$

$\Rightarrow S$ is a subgroup of the addition group of R.

Thus S is a subring of R.

Theorem.8. The intersection of two subring is a subring.

Proof. Let S_1 and S_2 be two subrings of a ring R. Then $S_1\bigcap S_2$ is non empty since at least $0\in S_1\bigcap S_2.$

Now in order to prove that $S_1\bigcap S_2$ is a subring, it is sufficient to prove that

(i) $a\in S_1\bigcap S_2, b\in S_1\bigcap S_2 \Rightarrow a-b\in S_1\bigcap S_2$

and (ii) $a\in S_1\bigcap S_2, b\in S_1\bigcap S_2 \Rightarrow ab\in S_1\bigcap S_2.$

We have

$$a\in S_1\bigcap S_2 \Rightarrow a\in S_1, a\in S_2,$$
$$b\in S_1\bigcap S_2 \Rightarrow b\in S_1, b\in S_2.$$

Now S_1 and S_2 are both subrings.

$\therefore a\in S_1 b\in S_1 \Rightarrow a-b\in S_1$ and $ab\in S_1$

and $a\in S_2, b\in S_2 \Rightarrow a-b\in S_2$ and $ab\in S_2.$

Now we have

$a-b\in S_1, a-b\in S_2 \Rightarrow a-b\in S_1\bigcap S_2$

and $ab\in S_1, ab\in S_2 \Rightarrow ab\in S_1\bigcap S_2.$

Thus we have

$$a \in S_1 \bigcap S_2, b \in S_1 \bigcap S_2 \Rightarrow a-b \in S_1 \bigcap S_2 \text{ and } ab \in S_1 \bigcap S_2.$$

Hence $S_1 \bigcap S_2$ is a subring of R.

Theorem.9. An arbitrary intersection of subrings is a subring.

Proof. Let R be a ring and let $\{S_t : t \in T\}$ be any family of subrings of R. Here T is an index set and is such that $\forall t \in T, S_t$ is a subring of R. Let $S = \bigcap_{t \in T} S_t = \{x \in R : x \in S_t \ \forall t \in T\}$ be the intersection of this family of subrings of R. Then to prove that S is also a subring of R.

Obviously $S \neq \emptyset$, since at least the zero element 0 of R is in $S_t \ \forall t \in T$.

Now let a, b be any two elements of S. Then

$$a \in \bigcap_{t \in T} S_t \Rightarrow a \in S_t \ \forall t \in T$$

and $b \in \bigcap_{t \in T} S_t \Rightarrow b \in S_t \ \forall t \in T.$

But $\forall t \in T, S_t$ is a subring of R.

Therefore we have

$$a, b \in S_t \Rightarrow a-b, ab \in S_t \ \forall t \in T.$$

Consequently $a-b, ab \in \bigcap_{t \in T} S_t$.

Thus we have shown that $a, b \in \bigcap_{t \in T} S_t \Rightarrow a-b, ab \in \bigcap_{t \in T} S_t$.

Therefore $\bigcap_{t \in T} S_t$ is a subring of R.

Solved Examples

Example.7. Let R be the ring all 2×2 matrices over the field of real numbers. Let M be a subset of R and let the elements of M be matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ *i.e.,* matrices in which the elements of second column are all zeros. Then M is a subring of R.

Sol. Let $A=\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}, B=\begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ be any two elements of M.

Then $A-B=\begin{bmatrix} a_1-a_2 & 0 \\ b_1-b_2 & 0 \end{bmatrix}$.

Also $AB=\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}\begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}=\begin{bmatrix} a_1a_2 & 0 \\ b_1a_2 & 0 \end{bmatrix}$.

Now $A-B$ and AB are both members of M since the second column of $A-B$ and also of AB consists of zeros only.

Hence M is a subring of R.

Example.8. Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2×2 matrices with integral elements.

Sol. Let R be the ring of 2×2 matrices and let M be the subset of R and let the elements of M be matrices of the type $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$.

Let $A=\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, B=\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ be any two elements of M.

Then $A-B=\begin{bmatrix} a_1-a_2 & b_1-b_2 \\ 0 & c_1-c_2 \end{bmatrix}$ which is obviously an element of M.

Also we have

$$AB = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix} \text{ which is obviously an element of } M.$$

Hence M is a subring of R.

10.12 Subfields

Let F be a field. A non-empty subset K of the set F is said to be a subfield of F if K is closed with respect to the operations of additions and multiplication in F and K itself is a field for these operations.

Theorem.10. The necessary and sufficient conditions for a non-empty subset K of a field F to be a subfield of F are (i) $a \in K, b \in K \Rightarrow a - b \in K,$

(ii) $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K.$

Proof. Necessary Conditions: Suppose K is a subfield of the field F. Now K is a group with respect to addition. Therefore we have $b \in K \Rightarrow -b \in K$. Also K is closed with respect to addition.

$$\therefore \qquad a \in K, b \in K \Rightarrow a + (-b) \in K \Rightarrow a - b \in K.$$

Now each non-zero element of K possesses multiplicative inverse. Therefore $0 \neq b \in K \Rightarrow b^{-1} \in K.$

But K is closed with respect to multiplication.

$$\therefore a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K.$$

Hence the conditions are necessary.

Sufficient Conditions: Suppose K is a non-empty subset of F and the conditions (i) and (ii) are satisfied.

As we have prove in subring, we can prove that with the help of condition (i), $(K,+)$ is an abelian group.

Now let a be any non-zero element of K.

Then from (ii) we have $a \in K, 0 \neq a^{-1} \in K \Rightarrow aa^{-1} \in K \Rightarrow 1 \in K.$

Now $1 \in K$, therefore again from (ii), we have

$$1 \in K, 0 \neq a \in K \Rightarrow 1a^{-1} \in K \Rightarrow a^{-1} \in K.$$

Therefore each non-zero element of K possesses multiplicative inverse.

Now let $a \in K$ and $0 \neq b \in K$. Then $b^{-1} \in K$.

From (ii), we have $a \in K, 0 \neq b^{-1} \in K \Rightarrow a\left(b^{-1}\right)^{-1} \in K \Rightarrow ab \in K.$

Also if $b = 0$, then $ab = 0$. Then we have $0 \in K$.

$\therefore \quad ab \in K \nvdash a, b \in K.$

Associativity of multiplication and distributivity of multiplication over addition must hold in K since they hold in F. Hence K is a subfield of F.

10.13 Summary

If in a ring R there exists an element denoted by 1 such that $1.a = a = a.1 \nvdash a \in R$, then R is called a ring with unity element. The element $1 \in R$ is known as the unity element of the ring.

If in a ring R, the multiplication composition is also commutative *i.e.*, if we have $a.b = b.a \quad \nvdash a, b \in R$, then R is known as a commutative ring.

A non-zero element a of a ring R is called a zero divisor or a divisor of zero if there exists an element $b \neq 0 \in R$ such that either $ab = 0$ or $ba = 0.$

A ring R is without zero divisors if the product of no two non-zero elements of R is zero i.e., if $ab = 0 \Rightarrow a = 0$ or $b = 0$.

A ring is known as an integral domain if it (i) is commutative (ii) has unit element, and (iii) is without zero divisors.

A ring R with at least two elements is called a field if it,(i) is commutative, (ii) has unity, (iii) is such that each non-zero element possesses multiplicative inverse.

A ring R with at least two elements is called a division ring or a skew field if it (i) has unity, (ii) is such that each non-zero element possesses multiplicative inverse. Thus a commutative division ring a field.

Let R be a ring. A non-empty subset S of the set R is said to be a subring of R if S is closed with respect to the operations of addition and multiplication in R and S itself is a ring for these operations.

Let F be a field. A non-empty subset K of the set F is said to be a subfield of F if K is closed with respect to the operations of additions and multiplication in F and K itself is a field for these operations.

10.13 Terminal Questions

Q.1. Define the rings.

Q.2. What do you mean by ring with or without zero divisors?

Q.3. Explain the concept of subrings and subfields.

Q.4. Prove that the set of rational numbers (real numbers or complex numbers) is a field with respect to addition and multiplication.

Q.5. Define a field. Prove that every field is an integral domain, but there exist some integral domains which are not fields.

Q.6. Define a ring and furnish an example of (i) a non-commutative ring with unity, (ii) a commutative ring without unity.

Q.7. Is every field also a division ring? Does the set of all integers under usual addition and multiplication form a field? Give some example of field which is finite.

Q.8. Prove that the set $\{0,1,2\}$ (mod 3) is a field with respect to addition and multiplication.

Q.9. In a ring R, prove that $-(-a)=a$.

Q.10. If addition and multiplication modulo 10 is defined on the set of integers $R=\{0,2,4,6,8\}$, prove that the resulting system is a ring with unity. Is it an integral domain?

Q.11. Prove that the only idempotent elements of an integral domain with unity are 0 and 1.

Q.12. Show that the set of all 2-rowed matrices of the form $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, where a, b, c are integers is a subring of the ring M of all 2-rowed matrices with integral entries.

Q.13. Give an example to show that the union of two subrings is not necessarily a subring.

Q.14. Show that the set of even integers forms a subring of the ring of integers.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

UNIT-11: Ideals

Structure

11.1 Introduction

The idea of an ideal was first given by Richard Dedekind in 1871. He wanted to fix problems in number theory, where sometimes numbers could not be broken into prime factors in only one way. To solve this, he grouped some numbers together into sets called ideals. This helped him keep unique factorization. Later on, rings and ideals became very important in many areas of math, like studying numbers and shapes. Today, learning about rings is a basic part of advanced math and is used in many ways.

In this unit we shall discuss about the ideals, principal ideal, divisibility in an integral domain, greatest common divisor, polynomials rings, unique factorization domain and reminder theorem. Quotient rings, homomorphism on rings, kernel of a ring homomorphism, maximal ideals, prime ideals and Euclidean rings.

11.2 Objectives

After reading this unit the learner should be able to understand about the:

- Ideals and principal ideal
- Divisibility in an integral domain, greatest common divisor
- Polynomials rings
- Unique factorization domain and reminder theorem
- Quotient rings, homomorphism on rings
- Kernel of a ring homomorphism
- Maximal ideals, prime ideals and Euclidean rings.

11.3 Ideals

Left Ideal: A non-empty subset S of a ring R is said to be a left ideal of R if (i) S is a subgroup of R with respect to addition and (ii) $rs \in S \forall r \in R$ and $\forall s \in S$.

Right Ideal: A non-empty S of a ring R is said to be a right ideal of R if: (i) S is a subgroup of R under addition and (ii) $sr \in S \forall r \in R$ and $\forall s \in S$.

Ideal: A non-empty subset S of a ring R is said to be an ideal of R if: (i) S is a subgroup of R under addition *i.e.* S is a subgroup of the additive group of R and (ii) $rs \in S$ and $sr \in S$ for every $r \in R$ and every $s \in S$.

Note 1. Thus every ideal of a ring R is also a subring of R. But every subring is not an ideal.

2. If R is a commutative ring then every left ideal will also be a right ideal. Therefore in a commutative ring every left (right) ideal is an ideal.

3. A ring having no proper ideals is called a simple ring.

Theorem.1. The intersection of any two left ideals of a ring is again a left ideal of the ring.

Proof. Let I_1 and I_2 be two left ideals of a ring R. Then I_1, I_2 are subgroups of R under addition. Therefore $I_1 \bigcap I_2$ is also a subgroup of R under addition.

Now to show that $I_1 \bigcap I_2$ is a left ideal of R, we are only to show that

$$r \in R, s \in I_1 \bigcap I_2 \Rightarrow rs \in I_1 \bigcap I_2.$$

First to show that $s \in I_1 \bigcap I_2 \Rightarrow s \in I_1, s \in I_2$.

But I_1 and I_2 are left ideals of R. Therefore we have

$$r \in R, s \in I_1 \Rightarrow rs \in I_1$$

and $r \in R, s \in I_2 \Rightarrow rs \in I_2$.

Now we have $rs \in I_1, rs \in I_2 \Rightarrow rs \in I_1 \bigcap I_2$

$I_1 \bigcap I_2$ is also a left ideal of R.

Theorem.2. An arbitrary intersection of left ideals of a ring is a left ideal of the ring.

Proof. Let R be a ring and set $\{S_t : t \in T\}$ be any family of left ideals of R. Here T is an index set and is such that $\forall t \in T$. S_t is a left ideal of R. Let $S = \bigcap_{t \in T} S_t = \{x \in R : x \in S, \forall t \in T\}$ be the intersection of this family of left ideals of R. Then to prove that S is also a left ideal of R.

Obviously $S \neq \phi$, since at least 0 is in $S_t \; \forall t \in T$.

Now let a, b be any two elements of S. Then we have

$$a, b \in S \quad \Rightarrow \quad a, b \in S_t \quad \forall t \in T$$

$$\Rightarrow \quad a - b \in S_t \quad \forall t \in T \qquad [\because \forall t \in T, S_t \text{ is a left ideal of R}]$$

$$\Rightarrow \quad a - b \in \bigcap_{t \in T} S_t$$

$$\Rightarrow \quad a - b \in S$$

Now let a be any element of S and r be any element of R.

We have $a \in S \quad \Rightarrow \quad a \in \bigcap_{t \in T} S_t \quad \Rightarrow \quad a \in S_t \quad \forall t \in T$

$$\Rightarrow \quad ra \in S_t \quad \forall t \in T \quad [\because \forall t \in T, S_t \text{ is a left ideal of R}]$$

$$\Rightarrow \quad ra \in \bigcap_{t \in T} S_t \quad \Rightarrow \quad ra \in S.$$

Thus we have $a, b \in S \Rightarrow a - b \in S$ and $r \in R, a \in S \Rightarrow ra \in S.$

Therefore S is a left ideal of R.

Theorem.3. A field has no proper ideals i.e., if F is a field then its only ideals are (0) and F itself.

Proof. Let S be any non-zero ideal of the field F and let a be any non-zero element of S. We have $a^{-1} \in F$. Since S is an ideal, therefore

$$a \in S, a^{-1} \in F \Rightarrow aa^{-1} \in S \Rightarrow 1 \in S.$$

Now let x be any element of F. Then

$$1 \in S,\ x \in F \Rightarrow 1.x \in S \Rightarrow x \in S.$$

Thus each element of F belongs to S.

Therefore $F \subseteq S$. But $S \subseteq F$. Therefore $S = F$.

Thus the only ideals of F are (0) and F itself.

Theorem.4. If R is a commutative ring and $a \in R$, then $Ra = \{ra : r \in R\}$ is an ideal of R.

Proof. In order to prove that Ra is an ideal of R, we should prove that Ra is a subgroup of R under addition and that if $u \in Ra$ and $x \in R$ then xu and ux are also in Ra.

But R is a commutative ring therefore $xu = ux$. Thus we only need to check that xu is in Ra.

Now let $u, v \in Ra$. Then $u = r_1 a, v = r_2 a$ for some $r_1, r_2 \in R$.

We have $u - v = r_1 a - r_2 a = (r_1 - r_2)a \in Ra$ since $r_1 - r_2 \in R$.

Thus $u, v \in Ra \Rightarrow u - v \in Ra$.

Hence Ra is a subgroup of R under addition.

Now let $x \in R$. Then we have

$$xu = x(r_1 a) = (xr_1)a \in Ra \text{ since } xr_1 \in R.$$

Hence Ra is an ideal of R.

Theorem.5. A commutative ring with unity is a field if it has no proper ideals.

Proof. Let R be a commutative ring with unity having no proper ideals i.e., the only ideals of R are (0) and R itself.

In order to show that R is a field, we should show that each non- zero element of R possesses multiplicative inverse. Let a be any non-zero element of R.

The set $Ra = \{ra : r \in R\}$ is an ideal of R.

Since $1 \in R$, therefore $1a = a \in Ra$. Thus $0 \neq a \in Ra$. Therefore the ideal $Ra \neq (0)$. Since R has no proper ideals, therefore the only possibility is that $Ra = R$.

Thus every element of R is a multiple of a by some element of R. In particular, $1 \in R$ so it can be realized as a multiple of a. Thus there exists an element $b \in R$ such that $ba = 1$.

Therefore $a^{-1} = b$. Hence each non-zero element of R possesses multiplicative inverse.

Thus R is a field.

Solved Examples

Example.1. Prove that the subset S of all matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ with *a* and b integers, forms a subring of the ring R of all 2×2 matrices having elements as integers. Prove further that S is neither a right ideal nor a left ideal in R.

Solution. Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ be any two element of S.

Then $A - B = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S$.

Also we have $AB = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S$.

Thus S is a subring of R.

Further $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S, \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \in R$ and the product $\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \notin S$. Therefore S is not a left ideal.

Again we have $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}3 & 4\\ 2 & 1\end{bmatrix}=\begin{bmatrix}3 & 4\\ 2 & 1\end{bmatrix}\notin S.$

Therefore S is not a right ideal.

Example.2. If R is a ring and $a\in R$ let $T=\{x\in R: ax=0\}$. Prove that T is a right ideal of R.

Solution. First we see that T is not empty because

$0\in R$ is such that $a0=0.$

Let x_1, x_2 be any two elements of $T.$ Then $ax_1=0, ax_2=0.$ We have

$a(x_1-x_2)=ax_1-ax_2=0-0=0.$

$\therefore\ x_1-x_2\in T.$

$\therefore T$ is a subgroup of R under addition.

Now to show that T is a right ideal of R we are to show that $a(xy)=0,$ then xy will be an element of $T.$

We have $a(xy)=(ax)y=0y=0.$

$$\therefore\ xy\in T.$$

$\therefore T$ is a right ideal of $R.$

Example.3. Prove that the intersection of two ideals of R is an ideal of $R.$

Solution. Let S and T be two ideals of $R.$ Then S, T are subgroups of R under addition. Therefore $S\cap T$ is also a subgroup of R under addition.

Now to show that $S\cap T$ is an ideal of $R,$ we are only to show that

$$r\in R, s\in S\cap T\Rightarrow rs\in S\cap T, sr\in S\cap T.$$

We have $s\in S\cap T\Rightarrow s\in S, s\in T.$

But S and T are ideals of R. Therefore we have

$$r \in R, s \in S \Rightarrow rs \in S, sr \in S$$

and $$r \in R, s \in T \Rightarrow rs \in T, sr \in T.$$

Now we have $rs \in S, rs \in T \Rightarrow rs \in S \bigcap T$

and $$sr \in S, sr \in T \Rightarrow sr \in S \bigcap T.$$

Hence $S \bigcap T$ is also an ideal of R.

Example.4. Show that S is an ideal of $S+T$ where S is any ideal of ring R, and T any subring of R.

Solution. Since S is an ideal of R therefore S is a subring of R. Also T a subring of R. First we shall show that $S+T$ is a subring of R.

Let $a+\alpha, b+\beta \in S+T$, where $a, b \in S$ and $\alpha, \beta \in T$.

Since S is a subring, therefore $a-b \in S$. Similarly $\alpha - \beta \in T$.

$$\therefore (a+\alpha)-(b+\beta) = (a-b)+(\alpha-\beta) \in S+T.$$

Also $(a+\alpha)(b+\beta) = ab + a\beta + \alpha b + \alpha\beta = (ab + a\beta + \alpha b) + \alpha\beta.$

Now S is a subring. Therefore $a, b \in S \Rightarrow ab \in S.$

Also S is an ideal, therefore $a, b \in S$ and $\alpha, \beta \in R \Rightarrow a\beta, \alpha b, ab \in S.$

Therefore $ab + a\beta + \alpha b \in S.$

Further T is a subring implies $\alpha\beta \in T$ if $\alpha, \beta \in T.$

Hence $S+T$ is a subring of R.

Since $0 \in T$, therefore $a \in S$ can be written as

$$a = a + 0 \in S + T.$$

$$\therefore \ S \subseteq S + T.$$

Thus $S \subseteq S + T$ and $S + T$ is a subring of R.

Since S is an ideal of R, therefore S is also an ideal of $S + T$.

Check your progress

Q.1. What do you mean by ideals?

Q.2. Define the left ideal and right ideal.

Q.3. The set of integers I is only a subring but not an ideal of the ring of rational numbers $(\mathbf{Q}, +, .)$.

Q.4. If U is an ideal of a ring R with unity and $1 \in U$ prove that $U = R$.

Q.5. If U is a left ideal of a ring R, let $\lambda(U) = \{x \in R : xu = 0 \ \forall \ u \in U\}$. Prove that $\lambda(U)$ is a two sided ideal of R.

Q.6. If U, V are ideals of a ring R let UV be the set of all those elements of R which can be written as finite sums of elements of the form uv where $u \in U$ and $v \in V$. Prove that UV is an ideal of R.

11.4 Principal Ideal

An ideal S of a ring R is said to be a principal ideal if there exists an element $a \in S$ such that any ideal T of R containing a also contains S i.e., $S = (a)$.

Note: 1. Thus an ideal generated by a single element of itself is called a principal ideal.

2. If a ring R has a unity element 1, then the ideal generated by 1 is the whole ring i.e., $(1) = R$, Since every element $r \in R$ may be written as $r1$. For this reason ring itself is called the unit ideal. The ideal generated by the zero element of R. i.e. (0) consists of the zero element alone and is called the null ideal. Every ring R has at least one principal ideal, namely (0). Every ring with unity has at least two principal ideals (0) and (1).

11.5 Principal Ideal Ring

A commutative ring R without zero divisors and with unity element is a principal ideal ring if every ideal S in R is a principal ideal i.e., if every ideal S in R is of the form $S = (a)$ for some $a \in S$.

Theorem.6. If a is an element in a commutative ring R with unity, then the set $S = \{ra : r \in R\}$ is a principal ideal of R generated by the element a *i.e.,* $S = (a)$.

Proof. First we should prove that $a \in S$. Since R is a ring with unit element 1, therefore $1a = a \in S$.

Now we should prove that S is an ideal of R. So first we should prove that S is a subgroup of R under addition. Let u, v be any two elements of S. Then $u = r_1 a, v = r_2 a$ for some $r_1, r_2 \in R$.

Now we have $u - v = r_1 a - r_2 = a(r_1 - r_2) a \in S$ since $r_1 - r_2 \in R$.

$\therefore S$ is a subgroup of R under addition.

Now we should prove that S is an ideal of R. So first we should prove that S is a subgroup of R under addition. Let u, v be any two elements of S. Then $u = r_1 a, v = r_2 a$ for some $r_1, r_2 \in R$

We have $u - v = r_1 a - r_2 a = (r_1 - r_2) a \in S$ since $r_1 - r_2 \in R$.

$\therefore S$ is an ideal of R and $a \in S$.

Now in order to prove that S is an ideal generated by the element a, we should prove

that if T is an ideal of R and $a \in T$, then $S \subseteq T$.

Let ra be any element of S. Then $r \in R$. If T is an ideal of R containing a, then $a \in T, r \in R \Rightarrow ra \in T$. Thus $S \subseteq T$. Hence S is a principal ideal of R generated by the element a.

Theorem.7.. Let S be an ideal of a commutative ring R. Let a be an element of S such that $x \in S \Rightarrow x = ya$ for some $y \in R$. Then S is a principal ideal of R generated by a.

Proof. As given in the statement of the theorem, S is an ideal of R containing the element a.

Let T be any ideal of R containing a. Then S will be principal ideal of R generated by a if $S \subseteq T$.

Let x be any element of S. Then $x = ya$ for some $y \in R$.

Now we have $y \in R, a \in T \Rightarrow ya \in T$ $\quad [\because T \text{ is an ideal}]$

$\Rightarrow \quad x \in T.$ $\quad [\because x = ya]$

Thus we have $x \in S \quad \Rightarrow \quad x \in T$.

Therefore $S \subseteq T$. Hence S is a principal ideal of R generated by a.

Theorem.8. The ring of integers is a principal ideal ring.

Proof. Let $(\mathrm{I}, +, .)$ be the ring of integers. Obviously I is a commutative ring with unity and without zero divisors. Therefore I will be a principal ideal ring if every ideal in I is a principal ideal.

Let S be any ideal of the ring of integers. If S is the null ideal, then $S = (0)$ so that is a principal ideal. Therefore suppose suppose that $S \neq (0)$.

Now S contains at least one non-zero integer, say a. Since S is a subgroup of R under addition therefore $a \in S \Rightarrow -a \in S$. Thus shows that S contains at least one positive integer because if $0 \neq a$, then one of a and $-a$ must be positive.

Let S_+ be the set of all positive integers in S. Since S_+ is non empty therefore by the well ordering principal , S_+ must possess a least positive integer. Let s be this least element. We will now show that S is the principal ideal generated by s *i.e.,* $S=(s)$.

Suppose now that n is any integer in S. Then by division algorithm, there exist integers q and r such that $n=qs+r$ with $0\le r<s$.

Now $s\in S, q\in I \Rightarrow qs\in S$ $\quad[\because S \text{ is an ideal}]$

and $\quad n\in S, qs\in S \Rightarrow n-qs\in S$ $[\because S \text{ is a subgroup}]$

Of the additive group of I, we have

$$\Rightarrow r\in S. \qquad [\because n-qs=r]$$

But $0\le r<s$ and s is the least positive integer such that $s\in S$. Hence r must be 0.

$$\therefore \qquad n=qs.$$

Thus $n\in S\Rightarrow n=qs$ for some $q\in I$.

Hence S is a principal ideal of I generated by s.

Since S was an arbitrary ideal in the ring of integers therefore ring of integers is a principal ideal ring.

Theorem.9. **Every field is a principal ideal ring.**

Proof. A field has no proper ideals. The only ideals of a field are (i) the null ideal which is a

principal ideal generated by 0 and (ii) the field itself which is also a principal ideal generated by I. Thus a field is always a principal ideal ring.

11.6 Divisibility in an Integral Domain

Suppose $0\ne a$ is an element of a commutative ring R. Then a is said to divide $b\in R$, if there exists an element $c\in R$ such that $b=ac$.

For example, In the ring I of integers, we have $3|6$ since we have $6=3\times 2$ and $2\in I$. However in the ring of integers 3 is not a divisor of 7.

Also in the ring Q of rational numbers, we have $3|7$ since we have $7=3\times(7/3)$ and $7/3\in Q.$

Theorem.10. If R is a commutative ring, then $(i)\ a|b$ and $b|c \Rightarrow a|c$ i.e., the relation of divisibility in R is a transitive relation.

(ii) $a|b$ **and** $a|c \Rightarrow a|(b+c)$.

(iii) $a|b \Rightarrow a|bx$ **for all** $x\in R.$

Proof. (i) $a|b \Rightarrow b=ap$ for some $p\in R$

and $b|c \Rightarrow c=bq$ for some $q\in R.$

Now $c=bq$ and $b=ap \Rightarrow c=(ap)q \Rightarrow c=a(pq)$

$\Rightarrow a|c$ since $pq\in R.$

(ii) $a|b \Rightarrow b=ap$ for some $p\in R$

And $a|c \Rightarrow c=aq$ for some $q\in R.$

Now $b=ap$ and $c=aq \Rightarrow b+c=ap+aq \Rightarrow b+c=a(p+q)$

$\Rightarrow a|(b+c)$ since $(p+q)\in R.$

(iii) $a|b \Rightarrow b=ap$ for some $p\in R.$

Now $b=ap \Rightarrow bx=(ap)x \forall x\in R$

$\Rightarrow bx=a(px) \Rightarrow a|bx$ since $px\in R.$

11.7 Greatest Common Divisor

Let R be a commutative ring. If $a,b \in R$ then $0 \neq d \in R$ is said to be a greatest common divisors of a and b if

(i) $d \mid a$ and $d \mid b$.

(ii) Whenever $c \mid a$ and $c \mid b$ then $c \mid d$.

We shall use the notation $d = (a,b)$ denote that d is a greatest common divisors of a and b.

Now suppose $a,b \in D$ where D is an integral domain with unity element 1. Let a,b possess a greatest common divisor.

Example.5. **Add and multiply the following polynomials over the ring of integers:** $f(x) = 2x^0 + 5x + 3x^2 - 4x^3, g(x) = 3x^0 + 4x - x^3 + 5x^4.$

Solution. By our definition of the sum of two polynomials, we have

$$f(x) + g(x) = (2+3)x^0 + (5+4)x + (3+0)x^2 + (-4-1)x^3 + (0+5)x^4$$

$$= 5x^0 + 9x + 3x^2 - 5x^3 + 5x^4.$$

Also we have

$$f(x)g(x) = \left(2x^0 + 5x + 3x^2 - 4x^2\right)\left(3x^0 + 4x - x^3 + 5x^4\right)$$

$$= 6x^0 + (8+15)x + (20+9)x^2 + (-2+12-12)x^3$$

$$+ (10-5-16)x^4 + (25-3)x^5 + (15+4)x^6 - 20x^7$$

$$= 6x^0 + 23x + 29x^2 - 2x^3 - 11x^4 + 22x^5 + 19x^6 - 20x^7.$$

Example.6. Add and multiply the following polynomials over the ring $\left(\mathrm{I}_6 +_{6,} \times_6\right)$:

$f(x) = 2x^0 + 5x + 3x^2, g(x) = 1x^0 + 4x + 2x^3.$

Solution. We have $f(x) + g(x) = (2 +_6 1)x^0 + (5 +_6 4)x + (3 +_6 0)x^2 + (0 +_6 2)x^3$

$$= 3x^0 + 3x + 3x^2 + 2x^3.$$

Also we have

$$f(x)g(x) = \left(2x^0 + 5x + 3x^2\right)\left(1x^0 + 4x + 2x^3\right)$$

$$= (2 \times_6 \mathrm{I})x^0 + \left[(2 \times_6 4) +_6 (5 \times_6 \mathrm{I})\right]x + \left[(5 \times_6 4) +_6 (3 \times_6 \mathrm{I})\right]x^2$$

$$+\left[(2 \times_6 2) +_6 (3 \times_6 4)\right]x^3 + (5 \times_6 2)x^4 + (3 \times_6 2)x^5$$

$$= 2x^0 + (2 +_6 5)x + (2 +_6 3)x^2 + (4 +_6 0)x^3 + 4x^4 + 0x^5$$

$$= 2x^0 + 1x + 5x^2 + 4x^3 + 4x^4.$$

11.8 Ring of Polynomials

Theorem.11. The set $R[x]$ of all polynomials ever an arbitrary ring R is a ring with respect to addition and multiplication of polynomials.

Proof. Let $f(x), g(x) \in R[x]$. Then $f(x) + g(x)$ and $f(x)g(x)$ are also polynomials over R. Therefore $R[x]$ is closed with respect to addition and multiplication of polynomials.

Now let $f(x) = \sum a_i x^i = a_0x^0 + a_1x + a_2x^2 +, ..., g(x) = b_0x^0 + b_1x + b_2x^2 + ...,$

$h(x) = c_0x^0 + c_1x + c_2x^2 + ...$ be any arbitrary elements of $R[x]$.

Commutativity of addition. We have

$$f(x) + g(x) = (a_0 + b_0)x^0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + ...$$

$$= (b_0 + a_0)x^0 + (b_1 + a_1)x + (b_2 + a_2)x^2 + ...$$

$$= g(x) + f(x).$$

Associativity of addition. We have

$$\left[f(x) + g(x) \right] + h(x) = \sum (a_i + b_i)x^i + \sum c_i x^i = \sum \left[(a_i + b_i) + c_i \right] x^i$$

$$= \sum \left[a_i + (b_i + c_i) \right] x^i$$

$$= \sum a_i x^i + \sum (b_i + c_i) x^i$$

$$= f(x) + \left[g(x) + h(x) \right].$$

Existence of additive identity. Let $0\ (x)$ be the zero polynomial over R *i.e.*,

$$0(x) = 0x^0 + 0x + 0x^2 + ...$$

Then we have

$$f(x) + 0(x) = (a_0 + 0)x^0 + (a_1 + 0)x + (a_2 + 0)x^2 + ...$$

$$= a_n x^0 + a_1 x + a_2 x^2 + ...$$

$$= f(x).$$

Therefore the zero polynomial $0(x)$ is the additive identity.

Existence of additive inverse. Let $-f(x)$ be the polynomial over R define as $-f(x) = (-a_n)x^0 + (-a_i)x + (-a_2)x^2 + ...$

Then we have

$$-f(x) + f(x) = (-a_0 + a_0)x^0 + (-a_1 + a_1)x + (-a_2 + a_2)x^2 + ...$$

$= 0x^0 + 0x + 0x^2 + ... = 0(x)$

$=$ the additive identity.

Hence each member of $R[x]$ possesses additive inverse.

Associativity of Multiplication. We have

$$f(x)g(x) = \left(a_0x^0 + a_1x + a_2x^2 + ...\right)\left(b_0x^0 + b_1x + b_2x^2 + ...\right)$$

$$= d_0x^0 + d_1x + d_2x^2 + ... + d_lx^l + ..., \text{ where } d_l = \sum_{i+j=l} a_ib_j.$$

Now $\left[f(x)g(x)\right]h(x)$

$$= \left(d_0x^0 + d_1x + d_2x^2 + ...\right)\left(c_0x^0 + c_1x + c_2x^2 + ...\right)$$

$$= e_0x^0 + e_1x + e_2x^2 + ... + e_nx^n + ..., \quad \text{where } e_n = \text{the coeff. of } x^n \text{ in } \left[f(x)g(x)\right]h(x)$$

$$= \sum_{l+k=n} d_lc_k$$

$$= \sum_{l+k=n}\left[\left(\sum_{i+j=l} a_ib_j\right)c_k\right] = \sum_{i+j+k=n} a_ib_jc_k.$$

Similarly we can show that the coeff. of x^n in

$$f(x)\left[g(x)h(x)\right] = \sum_{i+j+k=n} a_ib_jc_k.$$

Thus $\left[f(x)g(x)\right]h(x) = f(x)\left[g(x)h(x)\right]$, since corresponding coefficients in these two polynomials are equal.

Distributivity of multiplication with respect to addition. We have

$$f(x)\left[g(x) + h(x)\right]$$

$$= \left(a_0x^0 + a_1x + a_2x^2 + ...\right)\left[\left(b_0 + c_0\right)x^0 + \left(b_1 + c_1\right)x + \left(b_2 + c_2\right)x^3 + ...\right].$$

If n is any non-negative integer, then the coefficient of x^n in

$$f(x)\left[g(x) + h(x)\right]$$

$$= \sum_{i+j=n} a_i\left(b_j + c_j\right)$$

$$= \sum_{i+j=n}\left(a_ib_j + a_ic_j\right) = \sum_{i+j=n} a_ib_j + \sum_{i+j=n} a_ic_j$$

$$= \text{Coeff. of } x^n \text{ in } f(x)g(x) + \text{Coeff. of } x^n \text{ in } f(x)h(x)$$

$$= \text{coeff. of } x^n \text{ in } \left[f(x)g(x) + f(x)h(x)\right].$$

Similarly we can prove the right distributive law. Hence $R[x]$ is a ring. This is called the ring of all polynomials over R. The zero element of this ring is the zero polynomial

$$0x^0 + 0x + 0x^2 + 0x^3 + ...$$

11.9 Unique Factorization Domain and Reminder Theorem

An integral domain R, with unity element 1 is a unique factorization domain if (a) any non-zero element in R, is either a unit or can be written as the product of a finite number of irreducible (Prime) elements of R; (b) The decomposition in part (a) is unique upto the order and associates of the irreducible elements. Thus if R is a unique factorization domain and if $a \neq 0$ is a non-unit in R, then a can be expressed as a product of a finite number of prime elements of R. Also if

$$a = p_1p_2p_3....p_np_1'p_2'p_3'...p_m'$$

Where the p_i and P_j are prime elements of R, then $m = n$ and each p_i, $1 \le i \le n$ is an associate of some $p_j, 1 \le j \le m$ and conversely each p_k' is an associate of some p_i.

Theorem.12. Let $f(x), g(x)$ and $h(x)$ be polynomials in $F[x]$ for a field F. If $f(x)|g(x)h(x)$ and the greatest common divisor of $f(x)$ and $g(x)$ is 1, then $f(x)|h(x)$.

Proof. If the greatest common divisor of $f(x)$ and $g(x)$ is 1, then by the previous theorem, there exist polynomials $m(x)$ and $n(x) \in F[x]$ such that $1 = m(x) f(x) + n(x) g(x)$.

Multiplying both members of this equation by $h(x)$, we get

$$h(x) = m(x) f(x) h(x) + n(x) g(x) h(x). \qquad ...(1)$$

But $f(x)|g(x)h(x)$, so there exists a polynomial $q(x) \in F[x]$ such that $g(x)h(x) = q(x) f(x)$.

Substituting this value of $g(x)h(x)$ in equation (1), we get

$$h(x) = m(x) f(x) h(x) + n(x) q(x) f(x)$$

$$= f(x)\left[m(x)h(x) + n(x)q(x)\right],$$

Which shows that $f(x)$ is a divisor of $h(x)$. Hence the theorem.

Theorem.13. If $f(x)$ is an irreducible polynomial in $F[x]$ for a field F and $f(x)|g(x)h(x)$, where $g(x), h(x) \in F[x]$ then $f(x)$ divides at least one of $g(x)$ or $h(x)$.

Proof. Suppose that $f(x)$ does not divides $g(x)$. Since $f(x)$ is prime therefore $f(x)$ does not divide $g(x)$ implies that $f(x)$ and $g(x)$ are relatively prime. Therefore the greatest common divisor of $f(x)$ and $g(x)$ is 1. Hence by previous theorem, we get that $f(x)|h(x)$.

The Unique Factorization Theorem for polynomials over a field.

Theorem.14. Let $f(x)$ be a non-zero polynomial in $F[x]$, where F is a field. Then either $f(x)$ is a unit in $F[x]$ or $f(x) = a p_1(x) p_2(x) .... p_m(x)$, where each $p_i(x), 1 \le i \le m,$ is the leading

coefficient of $f(x)$. Further the factors $p_1(x), p_2(x), \ldots, p_m(x)$ are unique except for the order in which they appear.

Proof. We shall prove the theorem in two parts. First we shall prove that $f(x)$ can be factored as required and then we shall show that the factors are unique.

Let $f(x)$ be a non-zero element of $F[x]$. Then either $f(x)$ is a unit in $F[x]$ i.e., deg $f(x)$ is 0 or deg $f(x) > 0$. If deg $f(x) > 0$, and the leading coefficient of $f(x)$ is a .We are to prove that $f(x)$ can be expressed as a product of a and a finite number of irreducible monic polynomials in $F[x]$. The proof will be by induction on the degree of $f(x)$.

Suppose $f(x)$ is of degree one. Let $f(x) = b + ax$ for $a, b \in F$ and $a \neq 0$. We can write $f(x) = a(a^{-1}b + x)$. Therefore the theorem hold in the case where $f(x)$ has degree one since $f(x)$ is irreducible and monic. Now assume, as the induction hypothesis, that every polynomial of degree less than n can be factored as stated in the theorem. Consider an arbitrary polynomial $f(x)$ of degree n having a as its leading coefficient. We can write $f(x) = af_1(x)$, where $f_1(x) = a^{-1}f(x)$ and $f_1(x)$ is monic. If $f_1(x)$ is irreducible, then $f_1(x)$ is also irreducible and the theorem holds. If $f(x)$ is reducible, then it can be factored as $f(x) = g(x)h(x)$ where neither $g(x)$ nor $h(x)$ is a unit in $F[x]$. Now the degree of $f(x)$ is equal to the sum of the degrees of $g(x)$ and $h(x)$. Also $g(x)$ and $h(x)$ are not units in $F[x]$, so each of them must be of degree one or larger. Hence both $g(x)$ and $h(x)$ have degrees less than n. Therefore by our induction hypothesis we can write.

$$g(x) = cx_1(x)\alpha_2(x)....\alpha_3(x), h(x) = d\beta_1(x)\beta_2(x).....\beta_t(x)$$

where each $\alpha_i(x)$ and each $\beta_j(x)$ is monic and ireeducible and where c and d are leading coefficients of $g(x)$ and $h(x)$ respectively. Thus we have $f(x) = cd\alpha_1(x)\alpha_2(x)\alpha_3(x)....\alpha_t(x)\beta_1(x)\beta_2(x)....\beta_1(x)$.

Since the leading coefficient of $f(x)$ is a, therefore we must have $a = cd$ because each $\alpha(x)$ and each $\beta(x)$ is monic. Therefore $f(x) = \alpha x_1(x)\alpha_2(x)....\alpha_1(x)\beta_1(x)\beta_2(x)....\beta_t(x)$.

The factorization of $f(x)$ satisfies the requirements of the theorem. Hence the theorem holds for all polynomials of degree n, and by the principle of induction, for all polynomials of arbitrary degree.

In order to prove that the factors are unique, let us suppose that $f(x) = ap_1(x)\,p_2(x)....p_m(x) = aq_1(x)q_2(x)....q_n(x)$ where each $p(x)$ and each $q(x)$ is irreducible and monic. Then we shall prove that $n = m$ and each $p(x)$ is equal to some $q(x)$ and each $q(x)$ is equal to some $p(x)$. From these two decompositions of $f(x)$, we have

$$p_1(x)\,p_2(x)....p_m(x) = q_1(x)\,q_2(x)....q_n(x).$$

Now $p_1(x)\,|\,p_1(x)\,q_2(x)....q_m(x)$. Therefore $p_1(x)\,|\,q_1(x)\,q_2(x)....q_n(x)$.

$p_1(x)$ must divide at least one of $q_1(x), q_2(x), ..., q_n(x)$. Suppose $p_1(x)\,|\,q_1(x)$. It means $q_1(x) = up_1(x)$ where u is a unit in $F[x]$ i.e., u is a non-zero element of F. Since $q_1(x)$ and $p_1(x)$ are monic therefore u must be equal to 1 and we have $p_1(x) = q_1(x)$. Thus we have

$$p_1(x)\,p_2(x)....p_m(x) = p_1(x)\,q_2(x)....q_n(x).$$

Cancelling $0 \neq p_1(x)$ from both sides, we get

$$p_2(x)\,p_3(x)....p_m(x) = q_2(x)\,q_3(x)....q_n(x). \qquad ....(1)$$

Now we can repeat the above argument on the relation (1) with $p_2(x)$. If $n > m$, then

after m steps the left hand side becomes 1 while the right hand side reduces to a product of a certain number of $q(x)$ (the excess of n over m). But the $q(x)$ are irreducible polynomials so they are not units of $F[x]$ i.e., they are not polynomials of zero degree.

So their product will be a polynomial of degree ≥ 1. So it cannot be equal to 1. Therefore n cannot be greater than m. Then $n \leq m$. Similarly interchanging the roles of $p(x)$ and $q(x)$, we get $m \leq n$. Hence $m = n$.

Also in the above process we have shown that every $p(x)$ is equal to some $q(x)$ and conversely every $q(x)$ is equal to some $p(x)$. Hence the theorem has been completely established.

Thus we can say that the ring of polynomials over a field is a unique factorization domain.

Remainder Theorem.

Theorem.15. If $f(x) \in F[x]$ and $a \in F$, for any field F, then $f(a)$ is the remainder when $f(x)$ is divided by $(x-a)$.

Proof. By division algorithm there exist polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)(x-a) + r(x)$, where either $r(x) = 0$ or $\deg r(x)$ is less than the degree of $x-a$. But the degree of $(x-a)$ is 1. Therefore $r(x)$ has degree 0 or no degree. Hence $r(x)$ is a cannot polynomial i.e., $r(x)$ is simply an element, say, r in F. Thus $f(x) = q(x)(x-a) + r$. Putting $x = a$ in this relation, we get $f(a) = q(a)(a-a) + r \Rightarrow f(a) = r$.

Example.7. Show that the polynomial $x^2 + x + 4$ is irreducible over F, the field of integers modulo 11.

Solution. The field F is $(\{0,1,...,10\}, +_{11}, \times_{11})$. Let $f(x) = x^2 + x + 4$.

If $a \in F$, then by a^n we shall mean $a \times_{11} a \times_{11} a \times_{11} a.....$ up to n times.

Now $f(0) = 0^2 +_{11} 0 +_{11} 4 = 4$, $f(1) = 1^2 +_{11} 1 +_{11} 4 = 6$,

$f(2) = 2^2 +_{11} 2 +_{11} 4 = 10$, $f(3) = 3^2 +_{11} 3 +_{11} 4 = 5$, $f(4) = 2$,

$f(5) = 1$, $f(6) = 6^2 +_{11} 6 +_{11} 4 = 2$, $f(7) = 5$, $f(8) = 10$, $f(9) = 6$, $f(10) = 4$.

Since $f(a) \neq 0 \nvdash a \in F$, therefore by factor theorem $x-a$ does not divide

$f(x) \nvdash a \in F$. Therefore $f(x)$ has no proper divisors in $F[x]$. Hence $f(x)$ is irreducible over F.

11.10 Quotient Rings

Suppose R is an arbitrary ring and S is an ideal (two sided ideal) in R. Then S is a subgroup of the additive abelian group of R. We can form the cosets (right as well as left) of S in R .Since R is an abelian additive group, therefore if $a \in R,$ then the right coset $S+a$ will be equal to the corresponding left coset $a+S$. Thus we shall call $S+a$ as simply a coset of S in $R.$ We remember from our study of cosets in group theory , that if $a,b \in R,$ then

$$S+a=S+b \Leftrightarrow a-b \in S \text{ .}$$

The cosets of S in R are called the residue classes of S in R. We denote the set of all residue classes of S in R by the symbol R/S. Thus

$$R/S=\{S+a : a \in R\} \text{ .}$$

We shall now impose a ring structure on the set R/S by defining addition and multiplication of residue classes.

Theorem.16. If S is an ideal of a ring $R,$ then the set $R/S=\{S+a : a \in R\}$ Or all residue classes of S in S forms a ring for the compositions in R/S defined as follows:

$(S+a)+(S+b)=S+(a+b)$ **[Addition of residue classes]**

$(S+a)(S+b)=S+ab$ **[Multiplication of residue classes]**

Proof. Since $S+(a+b)$ and $S+ab$ are also residue classes of S in $R,$ therefore R/S is closed

with respect to addition and multiplication of residue classes. First of all, we shall show

that both addition and multiplication in R/S are well defined. For this we are to show that if $S+a=S+a'$ and $S+b=S+b',$ then

$$(S+a)+(S+b)=(S+a')+(S+b')$$

And $$(S+a)(S+b)=(S+a')(S+b')$$

We have $S+a=S+a' \Rightarrow a' \in S+a$

And $S+b=S+b' \Rightarrow b' \in S+b$

Therefore there exist $\alpha, \beta \in S$ such that $a'=\alpha+a, b'=\beta+b$.

Now we have $a'+b'=(\alpha+a)+(\beta+b)=(a+b)+(\alpha+\beta)$.

$\therefore (a'+b')-(a+b)=\alpha+\beta \in S$.

$\therefore S+(a'+b')=S+(a+b)$

$\Rightarrow (S+a')+(S+b')=(S+a)+(S+b)$.

Thus addition in R/S is well defined.

Again we have $a'b'=(\alpha+a)(\beta+b)=\alpha\beta+\alpha b+a\beta+ab$

$=ab+\alpha\beta+\alpha b+a\beta$.

$\therefore a'b'-ab=\alpha\beta+\alpha b+\alpha\beta \in S$. [Since S is an ideal therefore $\alpha, \beta \in S$ and

$a, b \in R \Rightarrow \alpha b \in S, a\beta \in S, \alpha\beta \in S$ and finally $\alpha\beta+\alpha b+a\beta \in S$].

Now since $a'b'-ab \in S$, therefore $S+a'b'=S+ab$

$\Rightarrow (S+a')(S+b')=(S+a)(S+b)$.

Hence multiplication in R/S is also well defined.

Associativity of addition in R/S. We have

$(S+a)+[(S+b)+(S+c)]=(S+a)+[S+(b+c)]$

$=S+[a+(b+c)]=S+[(a+b)+c]=[S+(a+b)]+(S+c)$

$= \left[(S+a)+(S+b) \right] + (S+c).$

Commutativity of addition in R/S. We have

$(S+a)+(S+b) = S+(a+b) = S+(b+a) = (S+b)+(S+a).$

Existence of additive identity. We have $S = S+0 \in R/S$. If $S+a \in R/S$, then

$(S+0)+(S+a) = S+(0+a) = S+a.$

$\therefore S$ is the additive identity.

Existence of additive inverse. Let $S+a \in R/S$.

The $S+(-a) \in R/S$. Also we have

$\left[S+(-a) \right] + \left[S+a \right] = S+\left[(-a)+a \right] = S+0 = S.$

$\therefore \ S+(-a)$ or $S-a$ is the additive inverse of $S+a$.

Associativity of multiplication . We have

$\left[(S+a)(S+b) \right](S+c) = (S+ab)(S+c) = S+(ab)c$

$= S+a(bc) = (S+a)(S+bc) = (S+a)\left[(S+b)(S+c) \right].$

Distributivity of multiplication with respect to addition.

We have $(S+a)\left[(S+b)+(S+c) \right] = (S+a)\left[S+(b+c) \right]$

$= S+a(b+c) = S+(ab+ac) = (S+ab)+(S+ac)$

$S+a(b+c) = S+(ab+ac) = (S+ab)+(S+ac).$

Similarly, we can prove that

$\left[(S+b)+(S+c)\right](S+a)=(S+b)(S+a)+(S+c)(S+a)$.

Hence R/S is a ring with respect to the two compositions

The residue class $S+0$ or S is the zero element of this ring.

11.11 Homomorphism of Rings

Homomorphism into

A mapping f from a ring R into a ring R' is said to be a homomorphism of R into R' if

$f(a+b)=f(a)+f(b) \forall a,b \in R$.

$f(ab)=f(a)\,f(b)$ for all $a,b \in R$.

Homomotphism onto

A mapping f from a ring R onto a ring R' is said to be a homomorphism of R onto R' if

$f(a+b)=f(a)+f(b) \forall a,b \in R$.

$f(ab)=f(a)\,f(b)$ for all $a,b \in R$.

Also then R' is said to be a homomorphism image of R.

Theorem.17. If f is a homomorphism of a ring R into a ring R', then $f(0)=0'$, where 0 is the zero element of the ring R and $0'$ is the zero element of R'.

$f(-a)=-f(a) \forall a \in R$.

Proof. (i) Let $a \in R$. Then $f(a) \in R'$. We have

$f(a)+0'=f(a)$ [$\because 0'$ is the additive identity of R']

$= f(a+0) = f(a) + f(0)$

Now R' is a group with respect to addition. Therefore

$f(a) + 0' = f(a) + f(0)$

$\Rightarrow 0' = f(0).$ [by left cancellation law].

(ii) Let a be any element of R. Then $-a \in R$.

We have $0' = f(0) = f\left[a + (-a)\right] = f(a) + f(-a)$.

$\therefore f(-a)$ is the additive inverse of $f(a)$ in the ring R'. Thus $f(-a) = -f(a)$.

11.12 Kernel of a Ring Homomorphism

If f is a homomorphism of a ring R into a ring R', then the set S of all those elements of R which are mapped onto the zero element of R' is called the kernel of the homomorphism f.

Thus if f is a homomorphism of R into R', then S is the kernel of f if $S = \{x \in R : f(x) = 0'$ where $0'$ is the zero element of $R'\}$.

Note: If f is a homomorphism of a ring R into a ring R' with kernel S, then S is an ideal of R.

11.13 Maximal Ideals

An ideal $S \neq R$ in a ring R is said to be a maximal ideal of R if whenever U an ideal of R such that $S \subseteq U \subseteq R$, then either $R = U$ or $S = U$.

Check your progress

Q.1. What do you mean by Greatest Common Divisor?

Q.2. Define the ring of polynomials.

Q.3. State the Unique Factorization Domain Theorem.

Q.4. State the Reminder Theorem.

Q.5. Define the maximal ideals.

11.14 Prime Ideals and Euclidean Rings

Let R be a ring and S an ideal in R. Then S is said to be a prime ideal of R if $ab \in S, ab \in R$ implies that either a or b is in S.

Let R be an integral domain i.e., let R be a'commutative ring without zero divisors. Then R is said to be Euclidean ruing if to every non-zero element $a \in R$ we can assign a non-negative integer $d(a)$ such that for all $a, b \in R$, both non-zero, $d(ab) \geq d(a)$.

For any $a, b \in R$ and $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

The second part of the above definition is known as division algorithm. Also we do not assign a value to $d(0)$. Thus $d(a)$ will remain undefined when $a = 0$. Also $d(a)$ will be called $d-$value of a and $d(a)$ must be some non-negative integer for every non-zero element $a \in R$.

Example.8. The ring of integers is a Euclidean ring.

Solution. Let $(\mathrm{I}, +, .)$ be the ring of integers where

$$\mathbf{I} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Let the d function on the non-zero elements of **I** be defined as

$d(a) = |a| \vee 0 \neq a \in \mathrm{I}$.

Now if $0 \neq a \in \mathrm{I}$, then $|a|$ is a non-negative integer. Thus we have assigned a non-negative integer to every non-zero element $a \in \mathrm{I}$.

$\left[d(-5) = |-5| = 5, d(-1) = |-1| = 1, d(4) = |4| = 4 \text{ etc} \right]$

Further if $a, b \in \text{I}$ and are both non zero, then

$$|ab| = |a||b|$$

$$\Rightarrow |ab| \geq |a| \qquad \left[\because \ |b| \geq 1 \text{ if } 0 \neq \text{b} \in \text{I} \right]$$

$$\Rightarrow d(ab) \geq d(a).$$

Finally we know that if $a \in \text{I}$ and $0 \neq b \in \text{I}$, then there exist two integers q and r such that

$$a = qb + r \text{ where } 0 \leq r < |b|$$

i.e., where either $r = 0$ or $1 \leq r < |b|$

i.e., where either $r = 0$ or $d(r) < d(b)$.

It should be noted that $d(b) = |b|$ and if r is a positive integer then $r = |r| = d(r)$. Therefore the ring of integers is a Euclidean ring.

Example.9. Let $f(x) = 2x^4 + 3x^3 + 2$ **and** $g(x) = 3x^5 + 4x^3 + 2x + 3$ **be two polynomials over the field** $Z_5 = \left(\{0,1,2,3,4\}, +_5, \times_5 \right)$. **Determine (i)** $(d/dx) f(x)$, **(ii)** $f(x).g(x)$.

Sol. (i) We have

$$\frac{d}{dx} f(x) = 4(2)x^3 + 3(3)x^4$$

$$= (2 +_5 2 +_5 2 +_5 2)x^3 + (3 +_5 3 +_5 3)x^4$$

$$= 3x^3 + 4x^3.$$

(ii) We have $f(x)g(x)$

$$= \left(2 + 3x^3 + 2x^4\right)\left(3 + 2x^2 + 4x^3 + 3x^5\right)$$

$$= \left(2 \times_5 3\right) + \left(2 \times_5 2\right)x^2 + \left[\left(2 \times_5 4\right) +_5 \left(3 \times_5 3\right)\right]x^3 + \left(2 \times_5 3\right)x^4$$

$$+ \left[\left(2 \times_5 3\right) +_5 \left(3 \times_5 2\right)\right]x^5 + \left[\left(3 \times_5 4\right) +_5 \left(2 \times_5 2\right)\right]x^6$$

$$+ \left(2 \times_5 4\right)x^7 + \left(3 \times_5 3\right)x^8 + \left(2 \times_5 3\right)x^9$$

$$= 1 + 4x^2 + 2x^3 + x^4 + 2x^5 + x^6 + 3x^7 + 4x^8 \mid + x^9.$$

11.15 Summary

A non-empty subset S of a ring R is said to be a left ideal of R if: (i) S is a subgroup of R with respect to addition, and (ii) $rs \in S \forall r \in R$ and $\forall s \in S$.

A non-empty S of a ring R is said to be a right ideal of R if: (i) S is a subgroup of R under addition, and (ii) $sr \in S \forall r \in R$ and $\forall s \in S$.

A non-empty subset S of a ring R is said to be an ideal of R if: (i) S is a subgroup of R under addition *i.e.,* S is a subgroup of the additive group of R, and (ii) $rs \in S$ and $sr \in S$ for every $r \in R$ and every $s \in S$.

The intersection of any two left ideals of a ring is again a left ideal of the ring. A commutative ring with unity is a field if it has no proper ideals. The intersection of two ideals of R is an ideal of R.

An ideal S of a ring R is said to be a principal ideal if there exists an element $a \in S$ such that any ideal T of R containing a also contains S i.e., $S = (a)$.

A commutative ring R without zero divisors and with unity element is a principal ideal ring if every ideal S in R is a principal ideal i.e., if every ideal S in R is of the form $S = (a)$ for some $a \in S$.

The ring of integers is a principal ideal ring. Every field is a principal ideal ring.

Suppose $0 \neq a$ is an element of a commutative ring R. Then a is said to divide $b \in R$, if there exists an element $c \in R$ such that $b = ac$.

Let R be a commutative ring. If $a, b \in R$ then $0 \neq d \in R$ is said to be a greatest common divisors of a and b if (i) $d \mid a$ and $d \mid b$. (ii) Whenever $c \mid a$ and $c \mid b$ then $c \mid d$.

A mapping f from a ring R into a ring R' is said to be a homomorphism of R into R' if

$$f(a+b) = f(a) + f(b) \forall a, b \in R.$$

$$f(ab) = f(a)\, f(b) \text{ for all } a, b \in R.$$

A mapping f from a ring R onto a ring R' is said to be a homomorphism of R onto R' if

$$f(a+b) = f(a) + f(b) \forall a, b \in R.$$

$$f(ab) = f(a)\, f(b) \text{ for all } a, b \in R.$$

Also then R' is said to be a homomorphic image of R.

If f is a homomorphism of a ring R into a ring R', then the set S of all those elements of R which are mapped onto the zero element of R' is called the kernel of the homomorphism f.

An ideal $S \neq R$ in a ring R is said to be a maximal ideal of R if whenever U an ideal of R such that $S \subseteq U \subseteq R$, then either $R = U$ or $S = U$.

Let R be a ring and S an ideal in R. Then S is said to be a prime ideal of R if $ab \in S, ab \in R$ implies that either a or b is in S.

11.16 Terminal Questions

Q.1. Define Ideals.

Q.2. Distinguish between subrings and ideals in a ring. Show that the 2-rowed matrices of the form $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, where a, b, c c are integers form a subring of the ring of all 2-rowed matrices with integral entries. Is this subring an integral domain?

Q.3. Show that the set M of all matrices of the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ a, b integers is a left ideal but not a right ideal in the ring of all 2×2 matrices with elements as integers.

Q.4. If U, V are ideals of a ring R, let $U + V = \{u + v : u \in U, v \in V\}$. Prove that $U + V$ is also an ideal of R.

Q.5. Show that an arbitrary intersection of ideals of a ring is an ideal of the ring.

Q.6. Consider the ring R of all 3×3 matrices of the type $\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}$, where a, b, c, d, e, f are real numbers. Show that the set I of all matrices of the form $\begin{bmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is a left ideal of R, which is not a right ideal.

Q.7. Verify the following for being true or false:

(i) The set of all positive rationals is a subring of the ring of all rational numbers.

(ii) A subring of any field is a field.

(iii) Any subring of the ring of integers, Z is an ideal of Z.

Ans. (i) and (ii) are false; (iii) is true.

Q.8. Show that if a ring R has no zero divisors, then the ring $R[x]$ has also no zero divisors.

Q.9. Show that the polynomial $x^3 - 9$ is reducible over the ring of integers modulo 11.

Q.10. Resolve x^4+4 into factors over the field $\left(\{0,1,2,3,4\},+_5,\times_5\right)$.

Q.11. Find the solution of the equation $3x=2$ in the field $\left(Z_7,+_7,\times_7\right)$.

Q.12. If $f(x)=3x^7+2x+3, g(x)=5x^3+2x+6$ be two polynomials over the field $Z_7=\left(\{0,1,2,3,4,5,6\},+_7,\times_7\right)$. Determine

(i) $(d/dx)f(x)$, (ii) $f(x).g(x)$, and (iii) $f(x)+g(x)$.

Q.13. Let $f(x)=x^6+3x^5+4x^2-3x-2$ and $g(x)=x^2+2x-3$ be in $Z_7[x]$. Find

(i) Sum and product of $f(x)$ and $g(x)$ in $Z_7[x]$.

(ii) Two polynomials' $q(x)$ and $r(x)$ in $Z_7[x]$ such that $f(x)=q(x)g(x)+r(x)$ with degree of $r(x)<2$.

Q.14. Defined a prime field. Prove that the field of rational numbers is a prime field. Give an example of a field which is not a prime field.

Q.15. What do you mean by Quotient Rings?

Q.16. Explain the homomorphism on rings.

Q.17. Define kernel of a ring homomorphism.

Q.18. Define maximal ideal.

Answers

---

2. No.

7. (i) and (ii) are false; (iii) is true.

10. $x^4+4=(x+1)(x+2)(x+3)(x+4)$.

11. $x = 3$ because $3 \times_7 3 = 2.$

12. (i) $2.$ (ii) $4 + 4x + 4x^2 + x^3 + 3x^6 + 4x^7 + 6x^8 + x^{10}$ (iii) $3x^7 + 5x^3 + 4x + 2.$

13. (i) $f(x) + g(x) = x^6 + 3x^5 + 5x^3 + 6x + 6;$

$$f(x)g(x) = 1 + 6x + 5x^2 + 5x^3 + 4x^4 + 5x^5 + 3x^6 + 5x^7 + x^8.$$

Note that in Z_7, we have $-3 = 4, -1 = 6$ etc.

(ii) $q(x) = x^4 + x^3 + x^2 + x + 5, r(x) = 4x + 3.$

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

U. P. Rajarshi Tandon
Open University

Master of Science

PGMM -106/MAMM-106
Advanced Algebra

Block

5 Extension Fields and Galois Theory

Unit- 12 **Extension Fields**
Unit- 13 **Galois Theory-I**
Unit- 14 **Galois Theory-II**

Block-5

Extension Fields and Galois Theory

Extension fields and Galois theory are fundamental in modern algebra, offering powerful methods for analyzing field structures and solving polynomial equations. By extending a base field, certain equations that were previously unsolvable can be solved, making extension fields vital in areas such as number theory, algebraic geometry, and coding theory. Building on this, Évariste Galois developed Galois theory, which forges a deep link between field extensions and group theory, demonstrating how the symmetries of polynomial roots determine their solvability by radicals.

The applications are extensive: in pure mathematics, it proves the impossibility of solving general quantic equations by radicals; in cryptography and error-correcting codes, it underpins secure communication systems; and in physics, it provides insight into symmetries and conservation laws. Owing to these diverse contributions, extension fields and Galois theory occupy a central place in both theoretical exploration and practical applications.

In this Block we have to study about Extension Fields, Galois theory which is fixed field to a group of automorphisms, Galois Group G(K/F) of a field extension K/F. We also study about fundamental theorem of Galois Theory as well as automorphisms group fixing F, field of H.We have to study in this chapter about finite field or Galois field. This block divided into three units. Unit Twelve discusses field extensions, including finite extensions, algebraic extensions, and simple extensions, as well as the root field and decomposition field of a polynomial. It also covers the solution of algebraic equations, multiple roots, separable and inseparable polynomials, and the simplicity of finite separable extensions. Units Thirteen and Fourteen focus on Galois theory, introducing its key elements such as fixed fields, normal extensions, Galois groups, and the fundamental theorem of Galois theory.

Unit: 12 EXTENSIONS FIELDS

Structure

12.19 Separable polynomials, separable elements and separable field extensions

12.20 Multiple roots

12.21 Separable and inseparable polynomials

12.22 Characterization of Separability

12.23 Condition for multiple roots

12.24 Separable elements

12.25 Separable extensions generated by separable elements

12.26 Simplicity of finite separable extensions

12.27 Summary

12.28 Terminal Questions

12.1 Introduction:

This Unit will be devoted to a study of the theory of finite field extensions involving the introduction of the concepts of Algebraic extensions and of the special types of the same, viz., Normal and Separable extensions. It is intended to lead to the Galois Theory of finite, normal and separable field extensions.

This study had originated with that of polynomial equations and in the following Unit will be developed the criteria for the solvability of polynomial equations by radicals as an application of Galois Theory. The theory of finite fields as finite field extensions of prime fields of non-zero characteristic will also be taken up as an application of the theory of finite field extensions.

12.2 Objectives

After study in this unit one will be able to understand the

- field extensions and roots of polynomial.
- Finite field extensions, Algebraic field extensions and simple field extensions.
- Root field and decomposition field of a polynomial
- Solution of algebraic equations and multiple root
- Separable and inseparable polynomials.
- Simplicity of finite separable extensions

12.3 Field extensions

Let L be any given field and K any sub-field of the same. We then say that L is an extension field or simply an extension of K. Consider any field L and the family of all its sub-fields. Let Γ denote the intersection of this family of sub-fields. Then Γ is obviously a prime field in the sense that it possesses no proper sub-field. A prime field is either isomorphic to the field Q of rational numbers or to the residue class field Jp for some prime p.

Thus we see that every field L can be thought of as an extension of a field Γ isomorphic to the field Q or Jp according as the characteristic of L is zero or the prime p.

12.4 Roots of a polynomial

Let L be any given field and let

$f(x) = a_0 + a_1x + \cdots \ldots + a_nx^n \in K[x]$, $a_0, a_1, a_2, \ldots\ldots a_n \in K$

And let $\alpha \in K$. Then the element

$$a_0 + a_1\alpha + \cdots \ldots + a_n\alpha^n$$

of K is denoted by the symbol $f(\alpha)$.

It may be easily seen that if

$$f(x) \in K[x], \psi(x) \in K[x]$$

And if we write

$$\varphi_1(x) = f(x) + \psi(x), \qquad \varphi_2(x) = f(x)\psi(x),$$

Then

$$\varphi_1(\alpha) = f(\alpha) + \psi(\alpha), \qquad \varphi_2(\alpha) = f(\alpha)\psi(\alpha),$$

If α is such that $f(\alpha) = 0$, we say that α is a root of the polynomial $f(x)$ or of the polynomial equation $f(x) = 0$.

Suppose that $\alpha \in K$ is a root of $f(x) \in K[x]$. Now there exist two polynomials $q(x)$ and $r(x)$ which $\in K[x]$ and are such that

$$f(x) = (x - \alpha)q(x) + r(x),$$

Where $r(x) = 0$ or deg $r(x) <$ deg $(x - \alpha)$. Thus r(x) is necessarily a member of K, say β. We have thus

$$f(x) = (x - \alpha)q(x) + \beta,$$

So that

$$f(\alpha) = \beta$$

We thus see that

$$f(\alpha) = 0 \leftrightarrow (x - \alpha)|f(x)$$

It may thus be seen that if $f(x) \in K[x]$ has a root $\alpha \in K$, then $f(x)$ is not an irreducible member of K[x] in as much as $(x - \alpha) \in K[x]$ is a factor of the same. The converse, however, is not true so that a reducible member of K[x] may have no root in K.

for example

$$x^4 - 5x^2 + 6 \in Q[x],$$

is reducible without having any root in Q.

12.5 Polynomial equations and field extensions:

The field C of complex numbers is known to be such that the only irreducible members of the polynomial ring C[x] over the same are those of degree one. In other words, every polynomial of the nth degree over the field C of complex number has n roots belonging to the field. This property is, however, not true of arbitrary fields. As an example, we may see that

$$x^3 - 2 \in Q[x]$$

is an irreducible member of the same and has no root lying in Q and

$$x^2 + 1 \in R[x]$$

is also an irreducible member of the same and has no root lying in R.

While $x^2 + 2$ is an irreducible member of the ring Q[x] over the field Q of rational numbers, it is reducible as a member of the polynomial ring over the extension field $Q(\sqrt{2})$ of Q. Similarly while $x^2 + 1$ is an irreducible member of the ring R[x] over the field R of real numbers, it is reducible as a member of the polynomial ring over the extension field $R(\sqrt{-1}) = C$ of complex numbers.

It has thus to be emphasized that the problem of the reducibility and irreducibility of polynomials and of the solution of polynomials equations is intrinsically related to the field in question and the answer to the problem changes on a change of the field.

To solve an equation $f(x) = 0$ where $f(x) \in K[x]$ amounts to constructing an extension field L of K such that $f(x)$ thought of as a member of L[x] is expressible as a product of linear factors and as such has as many roots in L as is the degree of the same.

12.6 Finite field extensions:

An extension field L of a field can K be thought of as a* vector space over K relative to the field addition in L and the field multiplication of the elements of L with those of K as the two vector space compositions. As a vector space over K, the dimension of L may be finite or infinite. We say that L is a finite field extension of the field K or briefly that L is finite over K, if the vector space L over K is finite dimensional and this finite dimension is known as the degree of L over K and is denoted by the symbol' (L : K).

Illustrations.1. The field C of complex numbers is a finite extension of the field R of real numbers and

(C : R) = 2 i.e. degree of C over R is 2.

2. The field $Q\sqrt{2}$ consisting of the numbers

$$a + b\sqrt{2}, \qquad a \in Q, b \in Q$$

If finite over Q and

$$(Q\sqrt{2}: Q) = 2$$

3. the field $Q(\sqrt{2}, \sqrt{3})$ consisting of the numbers

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3},$$

Where a, b, c, d $\in Q$, is finite over Q and

$$\left(Q\left(\sqrt{2},\sqrt{3}\right): Q\right) = 4$$

4. The field $Q(\pi)$ is not a finite field extension of Q.

12.7 Transitivity of finite extensions:

Theorem. If K, L, M are three fields such that

$$K \subseteq L \subseteq M$$

Then M is a finite extension of K if and only if M is a finite extension of L and L a finite extension of K. Moreover, then,

$$(M: K) = (M: L)(L: K).$$

Proof: Let M be of finite degree over K.

Let L, being a sub-space of the finite dimensional vector space M over K, is itself finite dimensional. Further the finite set of elements constituting a basis of M over K is clearly a generating system of M over L and accordingly M is also finite dimensional over L.

Now suppose that

$$(M: L) = m\ , (L: K) = n$$

Let $\alpha_i, 1 \leq i \leq m,\ is\ a\ basis\ of\ M\ over\ L,\ \ \beta_j, 1 \leq j \leq n, is\ a\ basis\ of\ L\ \ over\ K,$ respectively then $\beta_j \in M$ as L is a subset of M ,it means mn elements belong to M. It will be shown that the set of mn elements $(\alpha_i\beta_j)$ constitutes a basis of M over K.

To show $(\alpha_i\beta_j)$ generates M over K $(a_1, a_2, \ldots\ldots, a_m)$ is a basis of $M\ \ over$ L

Let $\gamma \in M$. we have

$$\gamma = \sum_{i=1}^{m} l_i\alpha_i\ , l_i \in L \ldots\ldots\ \ (1)$$

$l_i \in L$ and $(\beta_1, \beta_2, \ldots\ldots\ldots\beta_n)$ is a basis of L over K , we have

$$l_i = \sum_{j=1}^{n} f_{ij}\beta_j, \qquad f_{ij} \in K \ldots\ldots\ \ (2)$$

Thus

$$\gamma = \sum_{i=1}^{m}\sum_{j=1}^{n} f_{ij}\,\alpha_i\beta_j \qquad (from\ (1)\ and\ (2))$$

So that $\gamma \in M$ is a linear combination over K of the set of mn elements $\alpha_i\beta_j$.

Thus the set of *mn* elements $\alpha_i\beta_j$ generates the vector space M over K.

To show $(\alpha_i\beta_j)$ is linearly independent

Suppose that

$$\sum_{j=1}^{n}\sum_{i=1}^{m} f_{ij}\,\alpha_i\beta_j = 0$$

We have

$\supset \sum_{i=1}^{m}\left(\sum_{j=1}^{n} f_{ij}\,\beta_j\right)\alpha_i = 0$ as $(a_1, a_2, \ldots\ldots, a_m)$ is a basis of M *over* L

$$\supset \sum_{j=1}^{n} f_{ij}\,\beta_j = 0 \ \ for\ each\ j,$$

$\supset f_{ij} = 0\ for\ each\ i\ and\ j$ *as* $(\beta_1, \beta_2, \ldots\ldots\ldots\beta_n)$ is a basis of L over K

Thus we see that the set of *mn* elements $(\alpha_i\beta_j) \in M$ is linearly independent over K.

Hence the set of *mn* elements $\alpha_i\beta_j$ constitute a basis of M over K so that

$$(M : K) = mn$$

Hence the theorem.

12.8 Algebraic field extensions:

Let L be any finite extensions field of degree n over K. Let α be any arbitrary element of L. then the (n + 1) elements

$$1, \alpha, \alpha^2, \ldots\ldots\ldots\ldots, \alpha^{n-1}, \alpha^n$$

of the vector space L of finite dimension n over the field K from a linearly dependent system and accordingly there exists a system of (n+1) members

$$a_0, a_1, a_2, \dots\dots\dots, a_{n-1}, a_n,$$

not all zero, of K such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots \dots \dots + a_{n-1}\alpha^{n-1} + \ a_n\alpha^n = 0.$$

This shows that, α, is a root of a non-zero polynomial equation

$$a_0 + a_1x + a_2x^2 + \cdots \dots \dots + a_{n-1}x^{n-1} + \ a_nx^n = 0,$$

over K[x].

thus we see that if L is a finite field extension over K, each element of L is a root of some non-zero polynomial equation over K[x].

Definition: An extension field L of a field K is said to be algebraic over K, if each element of L satisfies a non-zero polynomial equation over k.

From the preceding discussion, we deduce that every finite field extension L of K is algebraic over K.

The converse of this result is, however not true in as much as there exist algebraic extensions which are not finite. Also an infinite extension may not be algebraic.

12.9 Simple field extension:

Definition: A field extension L of a field K obtainable on adjunction of a single element to K is known as a simple extension of K. thus a simple extension L of a field K is expressible as

$$L = K(\alpha)$$

Where α is an element of L.

Illustrations 1. The field C is a simple extension of the field R in as much as we have

$$C = R\left(\sqrt{-1}\right).$$

2. The field K(x) of rational functions of an indeterminate x is a simple extension of the field K.

For example, Show that $Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$ and deduce that $Q(\sqrt{2},\sqrt{3})$ is a simple extension of the field Q.

Note. The reader should carefully distinguish between finite and simple extensions in as much as a simple extension may not be finite. Thus for example, the field Q(x) of rational functions is a simple but not a finite extension of Q. Moreover, later on we shall obtain conditions under which a finite extension may be simple.

12.10 Structure of simple field extensions:

Let L = K(α) be a simple field extension of K. it is proposed here to study the structure of K(α).

The symbol K(α) denotes the ring obtained on adjoins α to K. clearly

$$K[\alpha] \subseteq K(\alpha)$$

It may be easily seen that K[α] consists of the elements

$$a_0 + a_1x + a_2x^2 + \cdots \ldots \ldots + a_nx^n \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where n is a non-negative integer and $a_0, a_1, a_2, \ldots\ldots\ldots, a_{n-1}, a_n$ range over K.

The field K(α) is the quotient field of the integral domain consisting of the elements (1).

We proceed first to answer the following question:

'Is the representation of elements of $K[\alpha]$ by expressions of the form

$$f(\alpha) = a_0 + a_1\alpha^2 + \cdots \ldots \ldots + a_n\alpha^n$$

Unique?'

Let, if possible,

$$f(\alpha) = \varphi(\alpha) where\ f(x) \neq \varphi(x).$$

Then, we see that α satisfies a non-zero polynomial equation

$$\psi(x) = f(x) - \varphi(x) = 0;\ \psi(x) \in K[x].$$

We have thus two cases to distinguish in respect of α, according as there exists or does not exist a non-zero polynomial $\psi(x) \in K[x]$ such $\psi(\alpha) = 0$.

In case there does not exist a non-zero polynomial $\in K[x]$ with α as a root, we see that

$$f(x) \to f(\alpha)$$

Is a one-one mapping K[x] onto K[α].

Also we may see that if

$$f(x) \to f(\alpha), \varphi(x) \to \varphi(\alpha)$$

Then

$$f(x) + \varphi(x) \to f(\alpha) + \varphi(\alpha), f(x)\varphi(x) \to f(\alpha)\varphi(\alpha)$$

We thus have

$$K[\alpha] \cong K[x]$$

And accordingly also

$$K(\alpha) \cong K(x)$$

Thus in this case the simple field extension $K(\alpha)$ is isomorphic to the field $K(x)$ of rational function over K; an isomorphism being given by $\alpha \to x, \alpha \to a$ where $a \in K$.

Now suppose that there does exist a non-zero polynomial $\psi(x) \in K[x]$ such that

$$\psi(\alpha) = 0$$

It may be easily seen that in this case the set I of all those polynomials which $\in K[x]$ and which have α as a root is a o-zero ideal in K[x].

In fact, if

$$\psi_1(x) \in I, \psi_2(x) \in I, f(x) \in K[x],$$

So that, we have

$$\psi_1(\alpha) - \psi_2(\alpha) = 0, f(\alpha)\psi_1(\alpha) = 0,$$

So that

$$\psi_1(x) - \psi_2(x) \in I, f(x)\psi_1(x) \in I.$$

As K[x] is a principal ideal ring, there exists a non-zero polynomial $\varphi(x) \in K[x]$ such that

$$\varphi(x) = I$$

Thus the polynomials which $\in K[x]$ and which have α as a root are given by f(x), $\varphi(x)$; f(x) being an arbitrary member of K[x].

It may be seen that $\varphi(x)$ is the lowest degree polynomial which $\in K[x]$ and which has α as a root. Also $\varphi(x)$ is irreducible over K[x].

In fact, if

$$\varphi(x) = \varphi_1(x)\varphi_2(x),$$

Where each of $\varphi_1(x)\varphi_2(x)$ is of positive degree, we have

$$\varphi(\alpha) = 0 \; either \; \varphi_1(\alpha) = 0, or \; \varphi_2(\alpha) = 0$$

So that α is a root of a polynomial equation over K[x] with degree smaller than that of $\varphi(x)$. We thus arrive at a contradiction.

If a be any non-zero member of K, we have

$$\varphi(x) = \big(a\varphi(x)\big),$$

So that we may suppose that $\varphi(x)$ is monic, i.e., the co-efficient of the highest degree term is unity. Then $\varphi(x)$ is uniquely characterized as follows:

- **(i)** $\varphi(x) \in K[x]$
- **(ii)** $\varphi(x) = 0$
- **(iii)** $\varphi(x)$ is irreducible over K[x],
- **(iv)** $\varphi(x)$ is monic.

This polynomial $\varphi(x)$ is usually described as the monic minimal polynomial over K belonging to α.

Consider now any element

$$f(\alpha) = a_0 + a_1\alpha + \cdots \ldots + a_m\alpha^m \in K[\alpha].$$

There exist polynomials q(x) and r(x) such that

$$f(x) = \varphi(x)q(x) + r(x),$$

Where r(x) = 0 or deg r(x) < deg $\varphi(x)$

$$f(\alpha) = r(\alpha)$$

Thus f(α) is expressible as r(α) where the degree of r(x) is less than that of $\varphi(x)$. Also clearly no two elements $r_1(\alpha), r_2(\alpha)$ such that

$$degr_1(x) < deg\varphi(x), degr_2(x) < deg\varphi(x)$$

can be equal. Thus we see that each element of the integral domain K[α] is uniquely expressible as

$$b_0 + b_1\alpha + \cdots \ldots \ldots + b_{n-1}\alpha^{n-1} \qquad \ldots\ldots \qquad (2)$$

Where $b_0, b_1, \ldots \ldots \ldots, b_{n-1} \in K$ and n is the degree of $\varphi(x)$.

Consider now any element

$$F(\alpha)/G(\alpha) \in K(\alpha)$$

Since $G(\alpha) \neq 0$, G(α) is not a multiple of the irreducible $\varphi(x)$. Thus the greatest common divisor of G(x) and $\varphi(x)$ is unity.

Accordingly, there exist polynomials

$$G_1(x), \varphi_1(x) \in K[x],$$

Such that

$$G(x)G_1(x) + \varphi(x)\varphi_1(x) = 1$$

$$G(\alpha)G_1(\alpha) = 1$$

So that

$$\frac{F(\alpha)}{G(\alpha)} = F(\alpha)G_1(\alpha),$$

Where $F(\alpha)G_1(\alpha)$ is a polynomial in α.

Proceeding as before, we may now express $F(\alpha)G_1(\alpha)$ in the form (2). This shows that each element of the field K(α) is as well expressible in the form (2) so that we have, in this case,

$$K(\alpha) = K[\alpha]$$

Also since each element of K(α) is uniquely expressible as

$$b_0 + b_1\alpha + \cdots \ldots \ldots + b_{n-1}\alpha^{n-1}$$

Where $b_0, b_1, \ldots\ldots\ldots, b_{n-1} \in K$ and n is the degree of the minimal polynomial $\in K[x]$ with α as a root, we see that the n elements

$$1, \alpha, \ldots\ldots\ldots\ldots\ldots, \alpha^{n-1}$$

Constitute a basis of the vector space K(α) over K and accordingly

$$[K(\alpha): K] = n$$

We have thus proved the following:

(i) If α is not a root of any non-zero polynomial $\in K[x]$, then the simple field extension K(α) is isomorphic to the field K(x) of rational functions so that K(α) is an infinite non-algebraic extension of K. in this case α is said to be transcendental over K.

(ii) If α is a root of some non-zero polynomial $\in K[x]$ and the minimal polynomial $\varphi(x)$ belonging to α is of degree n, then the simple field extension K(α) is of finite degree n over K and each element of the same is uniquely expressible as

$$b_0 + b_1\alpha + \cdots\ldots\ldots\ldots + b_{n-1}\alpha^{n-1}$$

Where $b_0, b_1, \ldots\ldots\ldots, b_{n-1} \in K$.

Thus $[K(\alpha): K] = n$ =degree of the minimal polynomial of α over K.

In this case α is said to be algebraic over K of degree n.

It follows that each element of a finite field extension L of degree n over K is algebraic over K; degree of each element being <n. in fact the degree of each element of L is a divisor of n. if $\beta \in L$, we have

$$K \subseteq K(\beta) \subseteq L$$

So that

$$(L: K) = \big(L: K(\beta)\big)(K(\beta): K),$$

And accordingly $(K(\beta): K)$ is a divisor of (L : K) which is n.

Another presentation: We shall now investigate the structure of simple field extensions in a comparatively more advanced manner making use of the Homomorphism theorem for rings.

The mapping

$$f(x) \to f(\alpha)$$

of K[x] onto K[α] is, as may be easily seen, a homomorphism.

Let, I, denote the kernel of this homomorphism so that it is an ideal of K[x] consisting of all those members of the same which have α as a root. As K is a field, K[x] is a principal ideal ring and accordingly I is a principal ideal of K[x].

Three cases are conceivable:

(i) I = 0), **(ii)** I = (1) **(iii)** I ≠ (0), I ≠ (1).

Case I. Let I = (0) In this case, the kernel I consists of only the zero of K[x] so that there is no non-zero polynomial having α as a root.

Thus the mapping $f(x) \to f(\alpha)$ is in this case one-one so that we have

$$K[x] \cong K[\alpha]$$

From this it follows that

$$K(x) \cong K(\alpha)$$

So that the field K(α) is, in this case, isomorphic to the field K(x) of rational functions of x over K.

Case II. Let I = (1) This case is not possible for this implies that the kernel consists of all the members of K[x] and , in particular, the unity I of K is mapped on zero.

Case III. Let I ≠ (0), I ≠ (1). There then exists a polynomial $\varphi(x) \in K[x]$ of positive degree such that

$$I = (\varphi(x))$$

We have

$$K[\alpha] \cong K[x]/(\varphi(x))$$

Where α is mapped on [x].

The polynomial $\varphi(x)$ is necessarily on irreducible member of K[x], for K[α] is an integral domain.

Thus $\varphi(x)$ is a maximal ideal of the principal ideal ring K[x] and accordingly the residue class ring

$$K[x]/(\varphi(x))$$

is a field. Therefore K[α] is in this case already a field, and we have

$$K(\alpha) = K[\alpha]$$

Thus the field K(α) is, in this case, isomorphic to the residue class field $K[x]/(\varphi(x))$; the ideal $(\varphi(x))$ consisting of all those polynomial member of K[x] which have α as a root.

Canonical representation of the members of K[α]: In case α is not algebraic over K, each element of K(α) is uniquely expressible as

$$f(\alpha)/g(\alpha)$$

Where f(x) and $0 \neq$ g(x) are arbitrary polynomials of K[x].

Consider now the case when α is algebraic over K and $(\varphi(x))$ is the ideal consisting of all those polynomials of K[x] which have α as a root. Since

$$\big(\varphi(x)\big) = \big(a\varphi(x)\big),$$

Where a is any arbitrary non-zero member of K, we may regard $(\varphi(x))$ as monic.

Consider any member [f(x)] of $K[x]/(\varphi(x))$

There exist two polynomials q(x) and r(x) $\in K[x]$ such that

$$f(x) = \varphi(x)q(x) + r(x),$$

Where r(x) = 0 or deg r(x) < deg $\varphi(x)$

Since

$$f(x) - r(x) = \varphi(x)q(x) \in (\varphi(x))$$

We have

$$[f(x)] = [r(x)]$$

Thus we see that each member of $K[x]/\varphi(x)$ is representable as [r(x)],

Where deg r(x) < n; n being the degree of $\varphi(x)$. This representation is unique in as much as

$$[r_1(x)] = [r_2(x)] \supset r_1(x) = r_2(x),$$

If $\deg r_1(x) < n, \deg r_2(x) < n.$

Thus each element of the field $K[x]/\varphi(x)$ is representable as

$$[b_0 + b_1x + \cdots \ldots + b_{n-1}x^{n-1}] \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where n being the degree of $\varphi(x)$. The member of K[α] corresponding to (1) in the isomorphic mapping of K(α) onto $K[x]/\varphi(x)$ referred to above is

$$b_0 + b_1 x + \cdots \ldots . + b_{n-1} x^{n-1}$$

Thus we arrive at the result in another manner.

It should be remembered that we compute with the members of K(α) as we do with the polynomials modulo the ideal $\varphi(x)$.

12.11 Existence of simple field extensions:

In the preceding section, we have investigated the structure of any arbitrary simple field extension K(α) of a field K on the assumption that the same exists. We have seen that a simple field extension may be

(i) Transcendental or **(ii)** algebraic

We may note also that any two simple transcendental field extensions of a field K are isomorphic in as much as each is isomorphic to the field K(x) of rational functions of an indeterminate x over the field K. thus we may say that there exists only one abstract simple transcendental extension of a given field.

In the following, we shall make reference to the question of existence of the simple algebraic extensions and see as to what can said in respect of the same.

It will be shown below that every field K such that there exist irreducible members of K[x] of degree greater than one admit of simple algebraic extensions.

Solution of algebraic equations:

From an abstract point of view, the problem of solving an equation $\varphi(x) = 0$ where

$$\varphi(x) \in K[x]$$

Amounts to constructing an extension field L of K such that $\varphi(x)$ as which also $\in L[x]$ so that $\varphi(x) = 0$ has as many roots in L as in the degree of $\varphi(x)$.

In this connection, we prove the following fundamental theorem.

Theorem: If $\varphi(x)$ be any irreducible member of K[x] then there exists an extension field L of K such that $\varphi(x) = 0$ has a root in L.

It has been seen in that if $\varphi(x)$ is an irreducible member of K[x] then the field K(α) obtained on adjoining a root α of $\varphi(x) = 0$ to the field K is such that

$$K(\alpha) \cong K[x]/[\varphi(x)].$$

This result provides a clue for the construction of the field L as stipulated in the theorem.

We write

$$L = K[x]/(\varphi(x))$$

And proceed to show that this L can be made into the required field.

Firstly, we see that $\varphi(x)$ being an irreducible member of the principal ideal ring K[x], the residue class ring L is actually a field.

Secondly, we show that L contains a sub-field isomorphic to the field K.

Consider the mapping

$$a \to [a],$$

of K into L.

Denoting by K' the sub-set of the elements [a] of L where $a \in K$, we see that

$$a \to [a]$$

Is a mapping of K onto K'. This mapping is one-one. In fact

$$[a] = [b] \supset a - b \in (\varphi(x))$$

And since the degree of each non-zero member of $(\varphi(x))$ is positive we see that a – b = 0 and accordingly a = b.

Thus $[a] = [b] \supset a = b$

Also we have

$$a + b \to [a + b] = [a] + [b]$$

$$ab \to [ab] = [a][b]$$

Thus the mapping in question, is an isomorphism and we have

$$K \cong K'.$$

As a result of this isomorphism, we identify each element [a] of K' with the corresponding element a of K so that we may regard K actually as a sub field of L, i.e., the field L as an extension of K.

As a second step, we show that

$$[x] \in L,$$

is a root of $\varphi(x) = 0$ where we now regard $\varphi(x)$ as belonging to L[x].

Let $\varphi(x) = a_0 + a_1x + \cdots \ldots + a_nx^n.$

We have

$$\varphi(x) = a_0 + a_1[x] + \cdots \ldots + a_n[x]^n$$

$$= [a_0] + [a_1][x] + \cdots \ldots + [a_n][x]^n$$

$$= [a_0 + a_1x + \cdots \ldots + a_nx^n] = [\varphi(x)] = [0] = 0$$

So that [x] is a root of $\varphi(x) = 0$.

Thus we have proved the theorem as stated.

Note. By virtue of the result established, each element of the field K([x]) obtained on adjoining a root [x] of

$$a_0 + a_1x + \cdots \ldots + a_nx^n = 0$$

To the field K is uniquely expressible as

$$b_0 + b_1[x] + \cdots \ldots + b_{n-1}[x]^{n-1},$$

Where

$$b_0, b_1, \ldots \ldots \ldots \ldots b_{n-1} \in K,$$

And we manipulate with the same in respect of addition and multiplication as we do with polynomials modulo $\varphi(x)$.

12.12 Root Field:

A simple extension field of a field K containing a root of an irreducible member of K[x] is called a root field of the polynomial.

Illustration: Consider

$$x^2 - 2x + 2 \in J_3[x]$$

The three elements of J_3 may be taken as 0, 1, 2.

Since neither 0 nor 1 is a root of $x^2 - 2x + 2 = 0$, we see that $x^2 - 2x + 2$ is an irreducible member of $J_3[x]$.

Denoting a root of $x^2 - 2x + 2 = 0$ by α, we see that the elements of the field $J_3(\alpha)$ are given by

$$a + b\alpha$$

Where a, b range over the elements of J_3. Thus $J_3(\alpha)$ is a finite field with 9 elements, viz.

$$0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha$$

It would be a good exercise for the reader to compute the inverses of the non-zero elements of the field.

12.13 Decomposition field of a polynomial:

An extension field L of a field K is said to be a decomposition field of $\varphi(x) \in K[x]$, if $\varphi(x) \in K[x]$ is expressible as

$$\varphi(x) = a(x - \alpha_1) \dots\dots\dots\dots (x - \alpha_n),$$

Where

$$a \in K, \alpha_1 \dots\dots\dots\dots\dots, \alpha_n \in L$$

And if

$$L = K(\alpha_1 \dots\dots\dots\dots\dots, \alpha_n).$$

12.14 Existence of a decomposition field:

Theorem: There exists a decomposition field for every$\varphi(x) \in K[x]$.

The theorem will be proved by induction in respect of the degree of a polynomial.

Let the degree of $\varphi(x)$ be n.

The theorem is obviously true for polynomials of degree 1. Suppose that the theorem is true for polynomials of degree less than n.

Let

$$\varphi(x) = \varphi_1(x)\varphi_2(x) \dots\dots\dots \varphi_i(x)$$

Where each of the polynomials on the right is an irreducible member of K[x]. clearly K itself is a decomposition field of $\varphi(x)$ if each of $\varphi_1(x)\varphi_2(x) \dots\dots\dots \varphi_i(x)$ is of first degree. Suppose that at least one of them say $\varphi_1(x)$, is of degree ≥2. There then exists an extension field K(α_1) containing a root α_1 of $\varphi_1(x) = 0$. Thus in the field K(α_1), we have a relation of the form

$$\varphi(x) = (x - \alpha_1)\psi(x),$$

Where the degree of $\psi(x) \in K(\alpha_1)[x]$ is n – 1.

By our supposition there exists a decomposition field

$$K(\alpha_1)(\alpha_2 \dots\dots\dots\dots, \alpha_n) = K(\alpha_1 \dots\dots\dots\dots, \alpha_n)$$

of $\psi(x) \in K(\alpha_1)[x]$. Clearly then,

$$L = K(\alpha_1 \dots\dots\dots\dots, \alpha_n),$$

is a decomposition field of $\varphi(x) \in K[x]$.

12.15 Uniqueness of the decomposition field

It will now be shown that the decomposition field of a polynomial is unique a part from isomorphism, i.e., any two decomposition fields of a polynomial are abstractly identical.

Theorem: Any two decomposition fields of a polynomial $\varphi(x) \in K[x]$ are isomorphic.

Proof: Also the isomorphic mapping can be so chosen that each element of K is mapped on itself i.e., remains invariant and the set of roots of $\varphi(x)$ in one decomposition field is mapped one-one onto the set of roots of $\varphi(x)$ in the other.

For the proof of this theorem, we need to introduce the notion of continuation of isomorphic mappings and to prove a lemma.

12.16 Continuation of an isomorphic mapping

If

$$K \subset L, K' \subset L'$$

Then an isomorphic mapping

$$g: L \to L'$$

is said to be a continuation of the isomorphic mapping

$$f: K \to K'$$

If g(a) = f(a) for each $a \in K$

Lemma: If f is isomorphic mapping of K onto K' and if

$$p(x) = a_0 + a_1 x + \cdots \ldots + a_n x^n$$

is an irreducible member of K[x] so that

$$f[p(x)] = f(a_0) + f(a_1)x + \cdots \ldots + f(a_n)x^n$$

is also an irreducible member of K'[x], then the mapping f can be continued to an isomorphism of the simple extension fields L and L' obtained on adjoining a root α of p(x) = 0 and a root α' of $f[p(x)] = 0$ to K and K' respectively such that α is mapped on α'.

It may be easily seen that if p(x) is an irreducible member of K[x], then $f[p(x)]$ is also an irreducible memberK'.

We have

$$\tau: L = K(\alpha) \cong K[x]/[p(x)],$$

$$\tau': L' = K'(\alpha') \cong K'[x]/[p(x)]$$

Also we have the isomorphic mapping

$$\eta: K[x]/[p(x)] \cong K'[x]/[f(p(x))]$$

Given by

$$\eta: [p(x)] = [f(p(x))]$$

Here

$$p(x) \in K[x]$$

Then, as will be shown the mapping

$$(\tau')^{-1}\eta\tau$$

is the required continuation of f.

Firstly it is an isomorphic mapping of L onto L'. if a be any member of K, we have

$$[(\tau')^{-1}\eta\tau](a) = [(\tau')^{-1}\eta][\tau(a)] = (\tau')^{-1}\{\eta[a]\} = (\tau')^{-1}[f(a)] = f(a)$$

So that $(\tau')^{-1}\eta\tau$ is a continuation of f.

Finally, we have

$$[(\tau')^{-1}\eta\tau](\alpha) = [(\tau')^{-1}\eta][\tau(\alpha)] = (\tau')^{-1}\{\eta[x]\} = (\tau')^{-1}[f(x)] = \alpha'$$

Hence the Lemma.

Cor. If L_1 and $L_2$are two simple extensions of a field K each containing a root of p(x) which is an irreducible member of K[x], then L_1 and L_2 are isomorphism may be so chosen that each element of K is mapped on itself and one root is mapped on the other.

This follows from the preceding lemma on taking K' and K as the same field f as the identity automorphisms of K.

This corollary shows that any two root fields of the same irreducible member $\varphi(x) \in K[x]$ are isomorphic so that we may say that apart from isomorphism there exists only one root field of an irreducible polynomial.

It should be noted that this result holds good only for irreducible polynomials, the fields $Q(\sqrt{2}), Q(-\sqrt{2})$ being the simple field extensions of Q each containing a root of the irreducible member $x^2 - 2$ of Q[x] are isomorphic. On the other hand the simple field extensions $Q(\sqrt{2}), Q(\sqrt{3})$ each containing a root of $(x^2 - 2)(x^3 - 3) \in Q[x]$ are not isomorphic.

Proof of the main theorem

Let $\phi(x) \in K[x]$ and let $L = K(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$, $M = K(\beta_1, \beta_2, \ldots\ldots, \beta_n)$

Let $\varphi_1(x)$ be any irreducible factor of $\phi(x)$ in K[x] of degree ≥2.

Then someone of $\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ is a root of $\varphi_1(x) = 0$ lying in L and some one of $\beta_1, \beta_2, \ldots\ldots, \beta_n$ is a root of the same lying in M. without any loss of generality, we suppose that α_1, β_1 are root of $\varphi_1(x) = 0$ lying in L and M respectively.

By the lemma, we have an isomorphic mapping, being a continuation of the identity mapping of K.,

$$\sigma_1 : K(\alpha_1) \cong K(\beta_1)$$

Where for α_1 is mapped on β_1 and each element of K is mapped on itself. In fact σ_1 is a continuation of the identity automorphism of K.

Let

$$\phi(x) = (x - \alpha_1)g_1(x) where\ \ g_1(x) \in K(\alpha_1)[x]$$

This gives

$$\phi(x) = \big(x - \sigma_1(\alpha_1)\big)\sigma_1(\alpha_1(x))$$

$$= (x - \beta_1)\sigma_1\big(g_1(x)\big) where\ \ \sigma_1\big(g_1(x)\big) \in K(\beta_1)[x]$$

Let $h_1(x)$ be any irreducible factor of $g_1(x)$ over $K(\alpha_1)[x]$ and $h_2(x)$ the corresponding irreducible factor of $\sigma_1\big(g_1(x)\big)$ over $K(\beta_1)[x]$. Some one of the $\alpha_1, \alpha_2, \dots\dots\dots, \alpha_n$ is a root of $g_1(x) = 0$ and some one of $\beta_1, \beta_2, \dots\dots\dots, \beta_n$ is a root of $\sigma_1\big(g_1(x)\big) = 0$.

Again without loss of generality we may suppose, that α_2 is a root of $g_1(x) = 0$ and β_2 of $\sigma_1\big(g_1(x)\big) = 0$. Then by the lemma, there exists an isomorphic mapping σ_2 of

$$K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2)\ onto\ K(\beta_1)(\beta_2) = K(\beta_1, \beta_2)$$

Which is a continuation of the mapping σ_1 of $K(\alpha_1)$ onto $K(\beta_1)$ and which is such that

$$\sigma_2(\alpha_2) = \beta_2$$

Proceeding in this manner, we shall arrive at an isomorphic mapping σ_n of

$$K(\alpha_1, \alpha_2, \dots\dots\dots, \alpha_n)\ onto\ \ K(\beta_1, , \dots\dots\dots, \beta_n)$$

of the requisite type

Note 1. The decomposition field of a polynomial is also sometimes referred to as its splitting field.

Note 2. If L, L' be two field extensions of the same field K and there exists an isomorphic mapping σ of L onto L' such that $\sigma(a) = a$ for each $a \in K$, then we say that L and L' are K-isomorphic and that σ is a K-isomorphism of L onto L'. thus if α, β are two roots of an irreducible $\phi(x) \in K[x]$, there exists a K-isomorphism of K(α) onto K(β).

Note 3. Taking M the same as L in the theorem, we see that if L is a decomposition field of $\phi(x)$ over K and if α, β are two roots of an irreducible divisor $\psi(x)$ of $\phi(x)$ over K, then the K-isomorphism of $K(\alpha)$ onto $K(\beta)$ which maps α on β can be continued to a K-automorphism of the L.

In fact we can think of M as the decomposition field of $\phi(x)$ as belonging to $K(\alpha)[x]$ as well as to $K(\beta)[x]$ and the σ of the lemma as the K-isomorphism of K(α) onto K(β) which maps α on β.

12.17 Solution of Algebraic Equations

In the foregoing, it has been shown that there exists a decomposition field for every given polynomial $\phi(x) \in K[x]$ and the same, apart from isomorphism, is unique. From a pure algebraic point of view, the study of any given polynomial equation over a field K amounts to that of the structure of the decomposition field L of the same. In the following, when we come to the discussion of Galois theory, it will be seen that this study is intimately related to the study of intermediate fields between K and L. this algebraic study is, however, to be carefully distinguished from that we meet in Analysis.

In Analysis, we have a special field C of complex numbers with a special role such that every number field can be thought of as a sub-field of the same and the study of polynomial equations consists in developing methods for approximating to the individual roots of the same.

Normal extension fields

We shall now introduce the notion of a particular type of algebraic extensions known as Normal Extension

An algebraic extension field L over K is said to be normal over K, if the decomposition field of the minimal polynomial $\phi(x) \in K[x]$ for each element $\alpha \in L$ is contained in L.

This means that if L is normal over K and if $\alpha \in L$ and if $\phi(x)$ is the minimal polynomial of x over K[x] then $\phi(x)$ can be expressed as a product of linear factors in L[x] or in other words every polynomial $\phi(x) \in K[x]$ having one root in the field L has all its roots in L.

12.18 Structure of finite normal extensions

Theorem: Every decomposition field extension is a normal extension.

Proof: Let

$$L = K(\alpha_1, \dots\dots\dots, \alpha_n)$$

be the decomposition field of $\psi(x) \in K[x]$; $\alpha_1 \dots\dots\dots\dots, \alpha_n$ being the roots of $\psi(x)$

Let $\alpha \in L$ and let $\phi(x)$ be the minimal polynomial of x over K[x].

Regarding $\phi(x)$ as a member of L[x], we denote by M the decomposition field of the same so that we have

$$K \subset L \subseteq M.$$

Let α, β be any two roots of $\phi(x)$ in M. there exists a K-isomorphism, σ, say, of K(α) onto K(β) mapping α on β.

This can be extended to an isomorphic mapping

$$K(\alpha)[x] \cong K(\beta)[x].$$

Regarding $\psi(x)$ as belonging to K(α)[x] and to K(β)[x], we can continue the K-isomorphism of K(α) onto K(β), to the K-isomorphism σ', say, of the decomposition fields

$$K(\alpha, \quad \alpha_1, \dots\dots\dots, \alpha_n), K(\beta, \quad \alpha_1, \dots\dots\dots, \alpha_n)$$

In this latter isomorphism, α is mapped on β and the set $\alpha_1, \dots\dots\dots, \alpha_n$ is mapped one-one onto itself. As

$$\alpha \in L \; and \; \alpha_1, \dots\dots\dots, \alpha_n \in L,$$

We see that α is a rational combination of a finite number of elements of K and of $\alpha_1, \dots\dots\dots, \alpha_n$. Subjecting this relation to the isomorphism σ', we see that β is as well a rational combination of a finite number of elements of K and of $\alpha_1, \dots\dots\dots, \alpha_n$. This shows that $\beta \in L$.

Hence the result.

Converse of the preceding theorem: Every finite normal extension field is a decomposition field.

Let

$$L = K(\beta_1, \dots\dots\dots.., \beta_r)$$

be a finite normal, extension of K. each $\beta_1, \dots\dots\dots.., \beta_r$ is algebraic over K. Let $\varphi_1(x), \dots\dots\dots, \varphi_r(x)$ be the minimal polynomials over K belonging to $\beta_1, \dots\dots\dots.., \beta_r$ respectively. As L is normal over K and contains one root of each of $\varphi_1(x), \dots\dots\dots, \varphi_r(x)$, we see that the decomposition field of each of these polynomials is contained in K. thus L is the decomposition field of

$$\varphi(x) = \varphi_1(x), \dots\dots\dots, \varphi_r(x)$$

Over K.

Note. From the preceding we see that so long as we deal with finite extension fields of a field K, the totality of normal extensions coincides with that of the decomposition fields of the polynomials over K so that the concept of finite normal extension field turns out to be equivalent to that of a decomposition field.

Theorem: If L is a normal extension of K and M is an intermediate field so the

$$K \subset M \subset L,$$

Then L is also normal over M.

Proof: Let $\alpha \in L$ and let $\phi(x), \psi(x)$ be the minimal polynomials belonging to α over the fields K and M respectively.

Now

$$\phi(x) \in K[x] \sqsupset \phi(x) \in M[x],$$

$\phi(x)$and $\psi(x)$ is the minimal polynomial over M satisfied by α, so that we see that

$$\psi(x) \parallel \phi(x)$$

So that each root of $\psi(x)$ in L is as well a root $\phi(x)$ in L. also each root of $\phi(x)$ belongs to L. thus each root of $\psi(x)$ belongs to L. Thus L is normal over M.

Hence the theorem.

Note. It should be seen that in the preceding case, M may not be a normal extension field of K.

12.19 Separable polynomials, separable elements and separable field extensions

A slight complication arises in the course of the development of the theory of algebraic field extensions on account of the existence of what are known as inseparable polynomials over a field and accordingly the concepts of separable and inseparable polynomials over a field will now be introduced.

12.20 Multiple roots

Let $\phi(x) \in K[x]$ and let L be the decomposition field of $\phi(x)$ or any extension field of K over the decomposition field L. Now, if $\alpha \in L$ is a root of $\phi(x)$, we have

$$(x - \alpha)/\phi(x) \; in \; L[x]$$

It may, however, happen that a higher power of (x – α) than one is a factor of $\phi(x)$ in L[x]. Suppose that r > 1 is a positive integer such that $(x - \alpha)^r$ but not $(x - \alpha)^{r+1}$ is a factor of $\phi(x)$. We then say that α is a multiple root of multiplicity, r, of $\phi(x)$. A non-multiple root is known as a simple root.

12.21 Separable and inseparable polynomials

An irreducible $\phi(x)$ over afield K is s to be separable over K, if the roots of $\phi(x)$ in its decomposition field are all simple. Also any arbitrary polynomial over K is said to be separable over K if each of its irreducible factors over K is separable. A polynomial which is not separable is known as inseparable.

It is not correct to say that a polynomial over K is separable if it has only simple roots. Thus if $\psi(x)$ is irreducible and separable over K, $[\psi(x)]^2$ is also separable over K.

12.22 Characterization of Separability

To find the condition for separability or otherwise of a polynomial, we have to introduce a linear transformation in a polynomial domain which formally is the same as that of Derivation in Analysis.

Thus if

$$\phi(x) = a_0 + a_1x + \cdots..+a_nx^n \in K[x]$$

Then, by def., we write

$$\phi'(x) = a_1 + 2a_2x + \cdots..+na_nx^{n-1},$$

So that $\phi'(x)$ is also a member of K[x]. we say that $\phi'(x)$ is the derivative of $\phi(x)$. The mapping

$$\phi(x) \to \phi'(x)$$

may be easily seen to be a linear transformation in K[x]. In fact, we may show that

$$f(x) = \phi(x) + \psi'(x) \sqsupset f'(x) = \phi'(x) + \psi'(x),$$

$$g(x) = a\phi(x) \sqsupset g'(x) = a\phi'^{(x)}, \qquad a \in K.$$

Further, if

$$h(x) = \phi(x)\psi(x)$$

we may show that

$$h'^{(x)} = \phi'^{(x)}\psi'(x) + \psi(x)\psi'(x).$$

Since the product of $\phi(x)$ with $\psi(x)$ is a linear combination of power of x, we need only prove the result for products of two powers of x. thus consider

$$\phi'(x) = x^r, \qquad \psi(x) = x^8$$

So that

$$h(x) = x^{r+8}$$

$$h'(x) = (r+8)x^{r+8-1}$$

$$h'(x) = (r\,x^{r-1})x^8 + (8x^{8-1})x^r$$

$$h'(x) = \phi'(x)\psi(x) + \psi'(x)\phi(x).$$

This proves the result.

12.23 Condition for multiple roots:

Theorem. If α is a multiple root of $\phi'(x)$, then it is also a root of $\phi'(x)$. Conversely, if α is a simple root of $\phi(x)$, then $\phi'(x) \neq 0$.

Proof: Let, α, be a multiple root of $\phi(x)$. Then we have a relation

$$\phi(x) = (x-\alpha)^r \psi(x),$$

Where $\psi(x) \in K(\alpha)[x]\ and\ r > 1$

$\therefore$ $$\phi'(x) = r(x-\alpha)^{r-1}\psi(x) + (x-\alpha)^r \psi'(x)$$

So that

$$\phi'(\alpha) = 0$$

Now suppose that α is a simple root of $\phi(x)$, so that we have

$$\phi(x) = (x-\alpha)\psi(x)$$

Where $\psi(x) \in K(\alpha)[x] and\ \psi(\alpha) \neq 0$

$\therefore$ $$\psi'(x) = \psi(x) + (x-\alpha)\psi'(x),$$

So that

$$\phi(\alpha) = \psi(\alpha) \neq 0$$

Hence the result.

Condition for separability:

Theorem: Let $\phi(x)$ be irreducible over K. then

(i) If the characteristic of K is zero, $\phi(x)$ is separable over K;

(ii) If the characteristic of K is $p \neq 0$, $\phi(x)$ is separable over K except when it is expressible as $\phi(x^p)$.

Proof: Let $\phi(x) = a_0 + a_1 x + a_2 x^2 + \cdots \ldots \ldots + a_n x^n,\ a_n \neq 0$

$$\phi'(x) = a_1 + 2a_2 x + \cdots \ldots \ldots + a_n x^{n-1}$$

Let α be a multiple root of $\phi(x) \in K[x]$ so that α is also a root of $\phi'(x) \in K[x]$. As $\phi(x)$ is the minimal polynomial belonging to α, $\phi'(x)$ is necessarily a product of $\phi(x)$ with some member of K[x]. Since, however, the degree of $\phi'(x)$ is smaller than that of $\phi(x)$ we must have

$$\phi'(x) = 0$$

Thus we have $a_1 = 0, 2a_2 = 0, \ldots \ldots \ldots \ldots, na_n = 0$

For a field K of characteristic zero, this can only happen, if

$$a_1 = 0, a_2 = 0, \ldots \ldots \ldots \ldots, a_n = 0$$

i.e., if the degree of $\phi(x)$ is non-positive.

Thus no irreducible polynomial over a field of characteristic zero can have multiple roots and accordingly every polynomial over a field of characteristic zero is separable.

Suppose now that the characteristic of K is p. from (1), we deduce that $a_k = 0$ if k is not a multiple of p

So the $\phi(x)$ is of the form

$$a_0 + a_1x^p + a_2x^{2p} + \cdots \ldots \ldots$$

i.e., it is a polynomial in x^p.

It may very well happen that $\phi(x)$ is a polynomial in x^{p^2}. For the sake of generality, we suppose that $\phi(x)$ is a polynomial in $x^{(p^e)}$ but not in $x^{(p^{e+1})}$. Let

$\phi(x) = \psi\left(x^{p^e}\right) = \psi(y)$, where we write $y = x^{p^e}$.

We cannot have $\psi(y) = 0$ for it it were so, we would have

$$\psi(y) = x(y^p) = x\left(x^{p^{e+1}}\right),$$

Which would be a contradiction of the hypothesis.

Thus $\psi(y) \in K[y]$ would have only simple roots in an extension field of K. suppose that M is the decomposition field of $\psi(y)$ over K.

Let

$$\psi(y) = (y - \beta_1) \ldots \ldots \ldots (y - \beta_t)$$

Where $\beta_1 \ldots \ldots \ldots \ldots \ldots, \beta_t$ are all distinct members of M.

$$\phi(x) = \left(x^{p^e} - \beta_1\right) \ldots \ldots \ldots \ldots \left(x^{p^e} - \beta_t\right)$$

in the decomposition field L of $\phi(x)$, there will exist roots $\alpha_1 \ldots \ldots \ldots \ldots \ldots, \alpha_t$ of

$$x^{p^e} - \beta_1, \ldots \ldots \ldots \ldots, x^{p^e} - \beta_t$$

respectively. We have

$$\alpha_1^{p^e} = \beta_1, \ldots \ldots \ldots, \alpha_t^{p^e} = \beta_t$$

$$x^{p^e} - \beta_1 = x^{p^e} - \alpha_1^{p^e} = (x - \alpha_1)^{p^e}, etc$$

$$\phi(x) = (x - \alpha_1)^{p^e} \ldots \ldots \ldots \ldots (x - \alpha_t)^{p^e}$$

This shows that $\phi(x) = 0$ has only t distinct roots and each root has multiplicity p^e. Thus

$$n = tp^e;$$

n being the degree of $\phi(x)$. The natural number e is known as the exponent of $\phi(x)$. We have thus proved the following:

For a field K of characteristic p > 0, an irreducible $\phi(x)$ over K has multiple roots if and only if it is a polynomial in x^p. Also if $\phi(x)$ is a polynomial in x^p, each root is of the same degree of multiplicity $p^e; e$ being some natural number. This e is such that $\phi(x)$ is a polynomial in $x^{p^{e+1}}$.

12.24 Separable elements

An element α algebraic over K is said to be separable over K, if the minimal polynomial over K belonging to α is separable.

Separable extensions:

An algebraic extension L of K is said to be separable if each element of L is separable over K.

In case an element or a field extension is not separable, we say that the same is inseparable.

It follows from the preceding that every algebraic extension of a field of characteristic zero is necessarily separable over the same so that inseparable extensions can occur only for fields of non-zero characteristic.

Thus in respect of number fields, the concept of inseparability becomes trivial.

Theorem: If $K \subset M \subset L$ and L is a separable extension of K, then L is a separable extension of M and M is a separable extension of K.

The proof which is very simple is left to the reader.

Characterization of Separable elements:

We have already obtained a characterization of separable polynomials over a field and shall here obtain that of separable elements over a field.

Theorem: If α is separable over K. then the field K(α) has precisely [K(α); K] distinct K-isomorphic images in the decomposition field L of the minimal polynomial $\phi(x)$ over K belonging to α and conversely.

Proof: Let n be the degree of $\phi(x)$ so that

$$[K(\alpha): K] = n$$

Let, α be over the field K then

$$\alpha = \alpha_1, \alpha_2, \dots\dots\dots, \alpha_n$$

of $\phi(x) = 0$ are all distinct.

The field $K(\alpha) = K(\alpha_1)$ is K-isomorphic to each of the n field.

$$K(\alpha_1) = K(\alpha_n)$$

The isomorphism's being determined by

$$\alpha \to \alpha_1, \alpha \to \alpha_2, \dots\dots\dots\dots\dots\dots\dots, \alpha \to \alpha_n$$

Thus these K-isomorphism's are all distinct.

Now suppose that some field $K_1 \in L$ is K-isomorphic to K(α) and as a result α mapped on some $\alpha' \in L$. We then have

$$0 = \phi(\alpha) \to \phi(\alpha') = 0$$

So that α' is itself a root of $\phi(x)$ in L and as such it coincides with some one of $\alpha_1, \alpha_2, \dots\dots\dots \alpha_n$.

Thus we have the first part of the theorem.

Conversely suppose that n distinct sub-fields.

$$K_1, \dots\dots\dots\dots\dots\dots K_n$$

Are just the sub fields of L which are K-isomorphic to K(α) and let, as a result, α be mapped on

$$\alpha_1, \alpha_2, \dots\dots\dots \alpha_n$$

Then $\alpha_1, \alpha_2, \dots\dots\dots \alpha_n$ are the n distinct roots of $\phi(x) = 0$ The degree of $\phi(x)$ being n, we deduce that the same is separable over K.

Thus we have proved the complete theorem.

Note 1. It is useful to note that if $M \supset L$, then the number of distinct K-isomorphic images of K(α) in M is the same as that in L.

Note 2. From the above, we deduce that α will be inseparable over K; if and only if the number of distinct K-isomorphic image of K(α) L falls short of the degree of α over K which, by def., is the same as the degree of K(α) over K.

12.25 Separable extensions generated by separable elements

Theorem: If α is separable over K, then so is K(α) separable over K.

Proof: We have to show that every element β of K(α) is separable over K.

Let L be the decomposition field of the minimal $\phi(x)$ over K belonging to α.

Since L is normal over K and $\beta \in L$, it contains the decomposition field of the minimal polynomial for β say $\psi(x)$, over K. we have

$$K \subset K(\beta) \subset K(\alpha) \subset L.$$

Let K(β) have in all b distinct K-isomorphic images in L and let β be thus mapped on

$$\beta = \beta_1, \beta_2, \ldots\ldots\ldots \beta_b$$

Which are b distinct elements of L.

Also let K(α) have in all a distinct K(β)-isomorphic images in L and let α be thus mapped on

$$\alpha = \alpha_1, \alpha_2, \ldots\ldots\ldots\ldots\ldots\ldots \alpha_a$$

Which are a distinct elements of L. Then the mappings

$$\beta \to \beta_i \;\; \alpha \to \alpha_j, \qquad 1 \le i \le b; \;\; 1 \le j \le a$$

Determine ab distinct K-isomorphic images of K(α) in L. also clearly every K-isomorphic images of K(α) in L is thus describable.

As α is separable over K, we have

$$[K(\alpha): K] = ab$$

Also $a \le [K(\alpha): K(\beta)], b \le [K(\beta): K].$

Since

$$[K(\alpha): K(\beta)][K(\beta): K] = [K(\alpha): K] = ab$$

We deduce that, we must have

$$[K(\alpha): K(\beta)] = a, \qquad [K(\beta): K] = b$$

Thus β is separable over K and hence K(α) is a separable extension of K.

Cor. The decomposition field of a separable polynomial $\phi(x) \in K[x]$ is a separable extension of the field K.

12.26 Simplicity of finite separable extensions

Theorem of the primitive element

Theorem: Let α, β be separable over K. then K (α, β) is a simple extension of K.

We shall, in the following, assume that K is a field with an infinite number of elements. The case of a field with a finite number of elements will be taken up a little later in this chapter when we come to the consideration of finite fields.

Let $\phi(x), \psi(x)$ be the minimal polynomials for α and β respectively over K and let L be the decomposition field of the polynomial

$$\phi(x), \psi(x)$$

We suppose that

$$\deg \phi(x) = m, \qquad deg\psi(x) = n$$

$$\alpha = \alpha_1, \alpha_2, \dots\dots\dots, \alpha_i \dots\dots\dots, \alpha_m$$

$$\beta = \beta_1, \beta_2, \dots\dots\dots, \beta_j \dots\dots\dots, \beta_n$$

Be the roots of $\phi(x)$ and $\psi(x)$ in L. these roots are all distinct as α and β are given to be separable over K.

Consider now the m(n – 1) linear equations

$$\alpha_i + x\beta_j = \alpha_1 + x\beta_1, \qquad 1 \leq i \leq m, 2 \leq j \leq n$$

over L. for each i and each j ≠ 1, this equation has a single root in L so that we obtain m(n – 1) elements of L, being the roots of these m(n – 1) equations. Some of these elements may belong to K. As K is assumed to contain an infinite of elements, there exists an element $c \in K$ different from those referred to here. We write

$$\theta = \alpha_1 + c\beta_1 = \alpha + c\beta$$

And see that

$$K(\theta) \subseteq K(\alpha, \beta)$$

Consider

$$\psi(x) \in K(\theta)[x], \phi(\theta - cx) \in K(\theta)[x]$$

It may be easily seen that the only root common to

$$\psi(x) = 0, \phi(\theta - cx) = 0$$

is β so that $x - \beta$ is the greatest common divisor of $\psi(x)\ and\ \phi(\theta - cx)$. Since

$$\psi(x) \in K(\theta)[x], \phi(\theta - cx) \in K(\theta)[x]$$

We see that

$$x - \beta \in K(\theta)[x]$$

Thus

$$\beta \in K(\theta)$$

Thus also

$$\alpha = \theta - c\beta \in K(\theta)$$

$$K(\alpha, \beta) \subseteq K(\theta)$$

Thus

$$K(\alpha, \beta) = K(\theta)$$

Cor. Every finite separable extension is simple. This follows from the preceding as a result of a finite number of successive applications.

12.27 Summary

One can say that L is an extension field or simply an extension of K. Consider any field L and the family of all its sub-field. Let Γ denote the intersection of this family of sub-fields. Then Γ is obviously a prime field in the sense that it possesses no proper sub-field. A prime field is either isomorphic to the field Q of rational numbers or to the residue class field Jp for some prime p.

The field C of complex numbers is known to be such that the only irreducible members of the polynomial ring C[x] over the same are those of degree one. In other words, every polynomial of the nth degree over the field C of complex number has n roots belonging to the field.

If K, L, M are three fields such that

$$K \subseteq L \subseteq M$$

Then M is a finite extension of K if and only if M is a finite extension of L and L a finite extension of K.

An extension field L of a field K is said to be algebraic over K, if each element of L satisfies a non-zero polynomial equation over k.

Let L = K(α) be a simple field extension of K. it is proposed here to study the structure of K(α).

Every decomposition field extension is a normal extension.

12.28 Terminal Questions

1. Define the field extensions.

2. Explain the simple field extension.

3. Write a short note on decomposition field of a polynomial.

4. What do you mean by separable and inseparable polynomials?

5. Show that a polynomial of the second or third degree is a reducible member of K[x] if and only if the same has a root in K.

6. Show directly from definition that $Q(\sqrt{2})$, $Q(\sqrt{2},\sqrt{3})$ are algobraic over Q.

7. Show that $Q(\pi)$ is an infinite non-algebraic extension of Q.

8. Show that the field C of complex numbers is incapable of algebraic extension.

9. Show that every field extension L of degree 2 over K is necessarily normal over K.

10. Show that $Q(\sqrt{2},\sqrt{3})$ is a decomposition field of $(x^2-2)(x^2-3) \in Q[x]$ and verify by considering the elements $\sqrt{2}, +\sqrt{3}$, $(\sqrt{2}-\sqrt{3})$ that the same is a normal extension of Q.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

Unit 13: Galois Theory-I

Structure

13.1 Introduction

The Portals are now reached and Galois Theory is introduced in unit in the setting of the theory of finite field extensions. This unit is devoted to developing criteria for Solvability by radicals and Constructability by Ruler and Compass the vindicating the rise of Galois Theory. This theory which arose in an attempt to solve a type of problems in connection with the theory of algebraic equations will be taken up now. The actual problems will be taken up in the following unit.

Let L be a finite, separable and normal extension of a field K. Then the group of $K-$ automorphisms of L is called the Galois group of L over K and will be denoted by the symbol $G(L/K)$. It will be seen that we are here defining Galois Theory groups of Extensions which are finite, separable as well as normal. Galois Theory for field extensions which do no satisfy this condition is beyond the scope of this unit. While for each element of the Galois group $G(L/K)$, each element of K is necessarily invariant, it is conceivable that some elements which do not belong to K are also left invariant by the members of the group G. it will, however, be shown in the following that this possibility cannot actually arise for the types of extensions under consideration.

13.2 Objectives

After studying this unit, the learner will be able to understand the:

- Galois theory
- Galois Extensions
- Fundamental theorem on Galois Theory

13.3 Galois Theory:

When we can find the solutions for a polynomial with rational coefficients using only rational numbers and the operations of addition, subtraction, division, multiplication and finding n^{th} roots, we say that $p(x)$ is soluble by radicals.

Using Galois Theory, you can prove that if the degree of $p(x) < 5$ then the polynomials is soluble by radicals, but there are polynomial of degree 5 and higher not soluble by radicals. Galois Theory is concerned with symmetries in the roots of a polynomial $p(x)$. For example, if $p(x) = x^2 - 2$ then the roots are $\pm\sqrt{2}$.Galois Theory has applications in classic problems such as squaring the circle and the determining solvability of polynomials as well as in number theory, differential equations and algebraic geometry. Galois Theory, originally introduced by Evariste Galois, provides a connection between field theory and group theory.

In other words, Galois Theory uncovers a relationship between the structure and the structures of fields. It then uses this relationship to describe how the roots of a polynomial related to one another. More specifically, we start with a polynomial $f(x)$. Its root lives in a field called the splitting field of $f(x)$. These roots display a symmetry which is seen by letting a certain group called the Galois group of $f(x)$ act on them. And we can gather information about the group structure from the field structure and vice versa via the Fundamental theorem of Galois.

Galois Theory is a showpiece of mathematical unification bringing together several different branches of the subject and creating a powerful machine for the study of problems of considerable historical and mathematical importance.

13.4 Galois Extensions:

An extension E of F is called a Galois extension if (i) E/F is finite (ii) F is the fixed filed to a group of automorphisms of E.

We first find a necessary and sufficient condition for a finite extension to be Galois.

Theorem 1: Let E/F be a finite extension. Then E/F is a Galois Extension if an only if it is both normal and separable.

Proof: Let E/F be a Galois extension. Then F is the fixed Filed of a group G of automorphisms of E. By Artin's theorem, Since E/F is finite, G is also finite.

Let G = { σ_1 = I, σ_2, ... , σ_n}

Let a ∈ E. Let $\sigma_i(a)$ =a_i, i = 1, 2, ..., n.

Suppose a_1 = σ_1, σ_2, ...σ_r are distinct element of {a_1, a_2,.....a_n}.

Let S = { a_1, a_2....., a_r}. Then S ⊆ E.

Now $\sigma_J(a_i)$ = $\sigma_J\sigma_i$(a) =$\sigma_k(a)$= σ_k ∈ S.

So , σ_J : S→S for all j = 1, 2 ....., n. Since σ_J : E →E is one- one, So is σ_J : S→S. Also, S is finite ⟹ σ_J : S→S is onto .Therefore, σ_J is a permutation of S for all j.

Let f(x) = (x - a_1) ... (x - a_r)

= x^r + $\propto_1 x^{r-1}$ + ... + $\propto_1 x^r$

Now $\sigma_t(f(x))$ = (x - σ_t (a_1)) .....(x - $\sigma_t(a_r)$)

= (x - a_1) ..... (x - a_r) = f(x) for all t.

So, x^r + σ_t ($\propto$)x^{r-1}+.....+ $\sigma_t(\propto)$ = x^r + $\propto_1 x^{r-1}$ + ….+ $\propto_r$

⇒ $\sigma_t(\alpha_i)$ = α_i for all t and i

⇒ α_i belongs to the fixed field of G

⇒ α_i ∈ F, for all i

$\Rightarrow$ f(x) $\in$ F[x].

Let g(x) be a monic irreducible factor of f(x) in F[x].

Let α_i be zero of g(x) in E. Now $\alpha_j = \sigma_j(a) = \sigma_j\sigma_\propto^{-1}(a_i) = \propto_t (a_i)$. So a_i is a zero of g(x) in E.

$\Longrightarrow \sigma_t(a_i)$ is a zero of $\sigma_t(g(x))$ = g(x) in E

$\Longrightarrow a_j$ is a zero of g(x) in E for all j

$\Longrightarrow$ g(x) = f(x)

$\Longrightarrow$ f(x) = Irr (F,a).

Since a is a simple zero of f(x), a is separable over F. So, E/F is separable. Also f(x) splits in E[x].

$\Longrightarrow$ E/F is normal.

Conversely, let G be the group of all F-automorphisms of E. Let F^r be the fixed field of G.

Then F $\subseteq$ F' $\subseteq$ E and o (G) = [E : F].

Since E/F is separable normal $\Longrightarrow$ E/F' is separable, normal.

Therefore, there are exactly n = [E : F] F- automorphisms of E.

$\Rightarrow$ o(G) = n $\Longrightarrow$ [E : F'] = n $\Rightarrow$ [F' : F] = 1 $\Rightarrow$ F' = F.

$\Rightarrow$ F is the fixed field of G $\Rightarrow$ E/F is Galois.

Cor. 1: Let E/F be finite extension. Then E/F is Galois if and only if F is the fixed field of the group of all F-automorphisms of E.

Proof: Let E/F be Galois. Then from above E/F is finite, normal, separable. Again by converse part of the above result, F is the fixed filed of the group of all F-automorphisms of E. Converse, follows by definition.

Cor. 2: Let char k = 0 Then k is contained in some Galois extension of k.

Proof: Let f(x) be non-constant polynomial in k[x]. Let E be minimal splitting field of f(x) over k. Then E/K is finite normal. Since char k = 0, k is perfect $\Rightarrow$ E/K is separable. So, E/K is Galois.

Note: When E/F is Galois, the group of all F- automorphisms of E is denoted by Gal (E/F) or G(E/F) called the Galois group of E/F.

Theorem 2: Let E/F be a finite extension. Then E/F is contained in a Galois extension if and only if it is separable.

Proof: Let E/F be a contained in a Galois extension E'/F. Then F ⊆ E ⊆ E'.

Now E'/F is Galois ⇒ E'/F is separable ⇒ E/F' is separable.

Conversely, let E/F be separable. Since E/F is finite, E = F (α_1, α_2,....., α_n).

Let P_i = Irr (F, α_i), $\alpha_i \in$ E

$\alpha_i \in$ E ⇒ α_i is separable over F

⇒ α_i is simple zero of p_i for all i

⇒ each zero of p_i in a splitting field is simple

Let f = $\prod_{i=1}^{n} p_i$ Then F ∈ k[x] ⊆ E[x], and f splits in some extension of E.

Let L be a minimal splitting field of f(x) over F

Then L = F (zero of f in an extension of E)

= F ($\alpha_1, \alpha_2, \ldots\ldots\ldots \alpha_n$, zero of f other than $\alpha_i's$ in an extension of E)

= E (zero of f other than $\alpha_i's$ in an extensin of E)

⇒ = F ⊆ E ⊆ L

Also, L is generated by separable elements over F (as each zero of f in an extension of E is simple and is a zero of an irreducible polynomial of $p_i \in$ F[x]) ⟹ L/F is separable ⟹ E/F is contained in a separable extension L/F.

Theorem 3: Let E/k be Galois and F be any extension of k. Then EF/F is Galois and G(EF/F) is isomorphic to a subgroup of G(E/k).

Proof : Since E/k is Galois, E/k is finite normal. So, E is a minimal splitting field of some polynomial f(x) ∈k [x].

Let f(x) = $\propto$ (x- α_1) (x - α_2)..... (x - α_n), $\alpha_i \in$E, $\alpha \in$k.

Then E = k(α_1, α_2 ... . , α_n).

Also, E/k is separable $\Rightarrow$ each α_i is separable over k. Now k $\subseteq$ F $\subseteq$ EF and α_i is separable over k $\Rightarrow$ α_i is separable over F.

Again, E = k (α_1, α_2, ... α_n)

$\Rightarrow$ EF = FE = Fk (α_1, α_2, ... α_n) = F (α_1, α_2, ... α_n) as k $\subseteq$ F

$\Rightarrow$ EF is a minimal splitting field of f(x) over F

$\Rightarrow$ EF/F is finite normal.

Also, EF is generated by separable elements over F $\Rightarrow$ EF/F is separable .

So, EF/F is Galois.

Let $\sigma \in$ G (EF/F).

Let f = $\propto f_1 f_2$.....f_r where each f_i is monic irreducible polynomial in k [x].

So, each α_i is zero for some $f_j \in$ k [x].

Since $\alpha_i$is separable over k, α_i is a simple zero.

Let S = {α_1, α_2, ... α_n} . Then α_i is a zero of f in E $\subseteq$ EF

$\Rightarrow \sigma(\alpha_i)$ is a zero of σ(f) = f in EF $\Rightarrow \sigma(\alpha_i) \in$ S.

So, { $\sigma(\alpha_1)$, $\sigma(\alpha_2)$, ... $\sigma(\alpha_n)$} = {α_1, α_2, ... α_n}

$\Rightarrow \sigma$ (E) = k ($\sigma(\alpha_1)$, $\sigma(\alpha_2)$, ... $\sigma(\alpha_n)$) = k (α_1, α_2, ... α_n) = E

$\Rightarrow \sigma$ restricted to E belongs to G(E/k)

Define θ : G (EF|F) $\rightarrow$ G(E/k) s.t.,

$\theta(\sigma) = \sigma|$E

Then θ is a homomorphism.

Also θ is one-one as $\sigma|E = I \Rightarrow \sigma(\alpha_i)$ for all i $\Rightarrow \sigma(a)$ = a for all a $\in$ EF as EF = F(α_1, α_2, ...α_n) and σ fixes each element of F $\Rightarrow \sigma$ I on EF.

So, G(EF/F) $\cong \theta$ (G(EF/F)) $\leq$ G(E/F).

Cor. 3 If E/k is Galois and F, an Extension of k, then [EF : F] divides [E ; K].

Proof . By above theorem, EF/F is Galois

$\Longrightarrow$ [EF : F] = o(G(EF/F))

Also, [E : k] = o(G(E/k))

But θ (G(EF/F))$\leq$ G (E/F)

$\Longrightarrow$ o($\theta(G(EF/F)$) divides o (G(E/F))

$\Longrightarrow$o(G(EF/F)) divides o (G(E/F)

$\Longrightarrow$[EF : F] divides [E : k]

Remark : The above corollary need not be true if E/K is not Galois. For example, let k = Q let α be the real cube root of 2. Then , $\alpha\omega$, $\alpha\omega^2$ are roots of f(x) = x^3 -2 in C.

Let E = Q ($\alpha\omega$), F = Q (α)

Then EF = Q($\alpha\omega$) Q (α) = Q ($\alpha, \alpha\omega$) = Q ($\alpha, \sqrt{3}i$)

So [EF : F] [F($\sqrt{3}i$) : F] = 2

while [E : k] = [Q ($\alpha\omega$) : Q] = deg Irr (Q, $\alpha\omega$)

= deg f(x) = 3.

13.5 Fundamental Theorem of Galois Theory:

The Fundamental Theorem of Galois Theory is one of the most elegant theorems in mathematics. Look at Figures 5.1 and 5.2 Figure 5.1 pictures the lattice of subgroup of the group of field automorphisms of Q($\sqrt[4]{2}$. i). The integer along an upward lattice line form a group H_1 to a group H_2 is the index of H_1 in H_2 . Figure 5.2 shows the lattice of subfields of Q($\sqrt[4]{2}$. i). The integer along an upward line from a field K_1

to a field K_2 is the degree of K_2 over K_1. Notice that the lattice in Figure 5.2 is the lattice of Figure 5.1 turned upside down. This is only one of many relationships between these two lattices. The Fundamental Theorem of Galois Theory relates the lattice of subfields of an algebraic extension E of a Field F to the subgroup structure of the group of automorphisms of E that send each element of F to itself. This relationship was discovered in the process of attempting to solve a polynomial equation $f(x) = 0$ by radicals.

Before we can give a precise statement of the fundamental Theorem of Galois Theory, we need some terminology and notation.

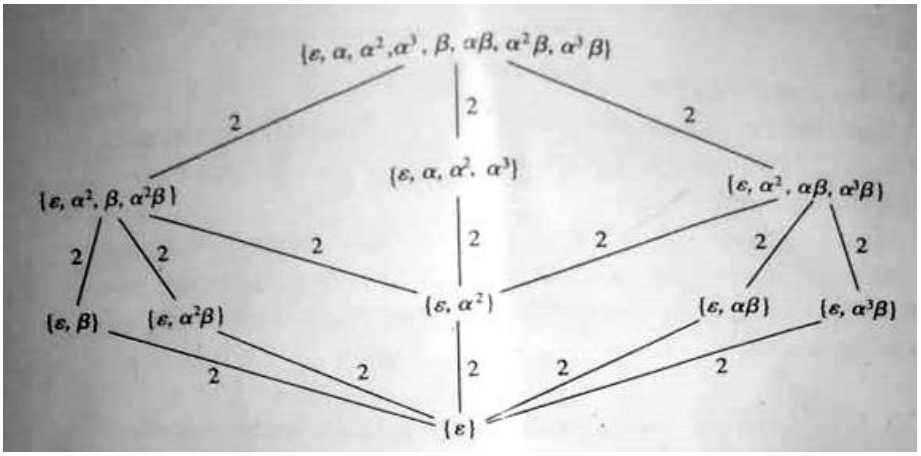


Figure 5.1

Figure 5.1 Lattice of subgroups of the group of field automorphisms of $Q(\sqrt[4]{2}. i)$, where a : i→ i and $\sqrt[4]{2} \rightarrow$ -i $\sqrt[4]{2}$; β : i → -i and $\sqrt[4]{2} \rightarrow \sqrt[4]{2}$.

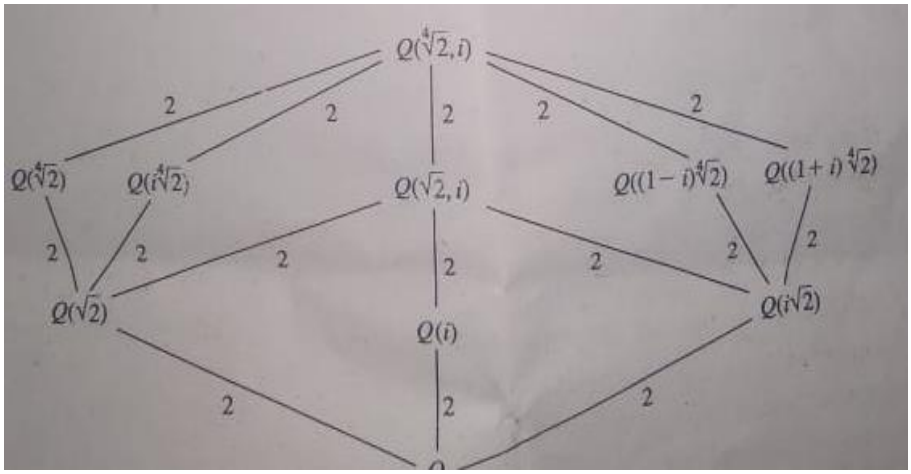


Figure 5.2 Lattices of subfields of $Q(\sqrt[4]{2}. i)$.

Check your progress

Q.1. Write a short note on Galois theory.

Q.3. Define the Galois extensions.

Q.3. State the fundamental theorem of Galois theory.

Theorem 4: (The fundamental theorem of Galois Theory). **Let E/k be Galois Let G= G(E/k) be the group of all k-automorphisms of E. Then**

(i) **There is one-one correspondence between the sets $\mathcal{A}$ = {F\F = field, k ⊆ F ⊆ E $\mathcal{B}$ = {H\ H ≤G} which is an order inverting bijection.**

(ii) **F ∈ $\mathcal{A}$ is the fixed field of the subgroup H ∈ $\mathcal{B}$ corresponding to F and H ∈ $\mathcal{B}$ is the group H* automorphisms of E, Where H* is the fixed field of H.**

(iii) **If H is the subgroup of $\mathcal{B}$ corresponding to the field F in $\mathcal{A}$ then o(H) = [E : F] and [G : H] = [F : k].**

(iv) **If H_1 , H_2∈ $\mathcal{B}$ corresponding to F_1, F_2∈ A respectively, then F_1, F_2 are conjugate under an automorphism σ ∈ G if and only σ^{-1} H_1 σ = H_2.**

(v) **If H ∈ $\mathcal{B}$ corresponds to F ∈ $\mathcal{A}$ then F/k is normal if and only if H is normal subgroup of G and in that case, G(F/k) ≅ $\frac{G}{H}$.**

Proof : Define $\theta : \mathcal{A} \to \mathcal{B}$s.t.,

θ (F) = F*

Where F* = {σ ∈ G | σ(x) = x for all x ∈ F}. Then F* ∈ $\mathcal{B}$

Similarly, define θ : $\mathcal{B} \to \mathcal{A}$ s.t.,

θ (H) = H*

Where H* = {x ∈ E | σ(x) = x for all σ ∈ H}

Then H* ∈ $\mathcal{A}$, is the fixed field of H.

Let F_1, F_2∈ $\mathcal{A}$, such that $F_1 \subseteq F_2$

Let σ ∈ F_2*Then σ(x) = x for all x ∈ F_2

$\Longrightarrow \sigma(x) = x$ for all $x \in F_1$ as $F_1 \subseteq F_2$

$\Longrightarrow \sigma \in F_1^* \Longrightarrow F_2^* \subseteq F_1^* \Longrightarrow \theta(F_2) \subseteq \theta(F_1) \Longrightarrow \theta$ is an order inverting map.

Similarly, φ is an order inverting map.

Let $H \in \mathcal{B}$ Then $\sigma \in H \Longrightarrow \sigma(x) = x$ for all $x \in H^* \Longrightarrow \sigma \in H^{**} \Longrightarrow H \subseteq H^{**}$

Also $x \in F(F \in \mathcal{A}, ,) \Longrightarrow \sigma(x) = x$ for all $\sigma \in F^*$

$\Longrightarrow$ x belongs to the fixed filed of F^*

$\Longrightarrow x \in F^{**} \Longrightarrow F \subseteq F^* = H$ Then $H^{**} = F^{***}$

Now $H \subseteq H^{**} \Longrightarrow F^* \subseteq F^{***}$ for all $F \in \mathcal{A}$, ,

Also, $F \subseteq F^{**} \Longrightarrow \theta(F^{**}) \subseteq \theta(F) \Longrightarrow F^{***} \subseteq F^*$ for all $F \in \mathcal{A}$, So, $F^* = F^{**}$ Similarly $H^* = H^{***}$ for all $H \in \mathcal{B}$.

Now θ is one-one onto if and only if $\theta\varphi$ = Identity if and only if $H = H^{**}$ for all $H \in B$ and $F = F^{**}$ for all $F \in \mathcal{A}$

Let $H \in \mathcal{B}$ Then $H^* = F$ is the fixed field of H.

By Artin theorem $o(H) = [E : F]$;

Also $o(H^{**}) = [E : H^{***}] = [E : H^*] = [E : F]$

So, $o(H) = o(H^{**})$. But $H \subseteq H^{**}$. Therefore, $H = H^{**}$

Let $F \in \mathcal{A}$ Then $k \subseteq F \subseteq E$.

Now E/k is Galois $\Longrightarrow$ E/F is Galois $\Longrightarrow$ F is the fixed field of the group H of all F- automorphisms of E.

$\Longrightarrow H \leq G \Longrightarrow H \in \mathcal{B}$.

Now H^* = Fixed field of $H = F \Longrightarrow H^{***} = F^{**} \Longrightarrow H^* = F^{**} \Longrightarrow F = F^{**}$ for all $F \in \mathcal{A}$

Thus, θ one-one onto.

This proves (i),

(ii) Let F ∈ $\mathcal{A}$ Let θ(F) = H Then F* = H ⟹ F**= H* ⟹ F is the fixed field of H.

Let H ∈ $\mathcal{B}$ Then there exists F ∈ $\mathcal{A}$, Such that θ (F) = H⟹ H = F*

Let σ ∈ H Then σ ∈ F* ⟹ $\sigma(x)$ = x for all x ∈ F ⟹ σ is an F-automorphisms of E.

Conversely, let σ be an F- automorphisms of E.

Then $\sigma(x)$ = x for all x ∈ F⟹ σ ∈ F*= H.

So, H is the group of all F = H*-automorphisms of E.

(iii) By Artin theorem

$\sigma(H)$ = [E : H*] = [E : F]

[G: H] = $\frac{o(G)}{o(H)}$ = $\frac{[E: k]}{[E: F]}$ = [F: k]

(iv) Suppose $F_1, F_2 \in \mathcal{A}$ are conjugate under σ ∈ G. Then $\sigma(F_1) = F_2$

Let y ∈ F_2 Then y = σ(z), z ∈ F_1 Therefore σ^{-1} (y)= z

⟹ $\tau\,\sigma^{-1}$(y) = τ(z), for all τ ∈ H_1

⟹ $\sigma\tau\sigma^{-1}$ (y) = $\sigma\tau(z) = \sigma(z)$ for all τ ∈ H_1

⟹ $\sigma\tau\sigma^{-1}$ (y) = y, for all τ ∈ H_1, y ∈ F_2

⟹ $\sigma\tau\sigma^{-1}$ ∈ H_2, for all τ ∈ H_1

⟹ σ H_1 $\sigma^{-1} \subseteq H_2$

Let a ∈ F_1 Then σ(a) = b ∈ F_2

⟹ $\eta\sigma$(a) =η(b) , for all η ∈ H_2

⟹ $\eta\sigma$(a) =(b), for all η ∈ H_2

⟹ σ^{-1} $\eta\sigma$(a) = σ^{-1}(b) = a, for all η ∈ H_2,a ∈ F_1

⟹ σ^{-1} $\eta\sigma$ ∈ H_1, for all η ∈ H_2

⟹ σ^{-1} $H_2\sigma \subseteq H_1$

$\Longrightarrow H_2 \subseteq \sigma H_1 \sigma^{-1}$

So, $H_2 = \sigma H_1 \sigma^{-1}$

conversely, let $H_2 = \sigma H_1 \sigma^{-1}$ for $\sigma \in G$.

Let $y \in F_2$, Now $\sigma\tau\sigma^{-1} \in H_2$ For all $\tau \in H_2$

$\Longrightarrow \sigma\tau\sigma^{-1}(y) = y$

$\Longrightarrow \tau\sigma^{-1}(y) = \sigma^{-1}(y) = z$

$\Longrightarrow \tau(z) = z,$ for all $\tau \in H_1$

$\Longrightarrow z \in F_1$

$\Longrightarrow y = \sigma(z) \in \sigma(F_1)$

$\Longrightarrow F_2 \subseteq \sigma(F_1)$

Let $x \in F_1$ Now $\sigma^{-1}\eta\sigma \in H_1$ For all $\eta \in H_2$

$\Longrightarrow \sigma^{-1}\eta\sigma(x) = x$

$\Longrightarrow \eta\,\sigma(x) = \sigma(x)\, x'$

$\Longrightarrow \eta\,(x') = x'$ for all $\eta \in H_2$

$\Longrightarrow x' \in F_2$

$\Longrightarrow \sigma(x) \in F_2$

$\Longrightarrow \sigma(F_1) \subseteq F_2$

So, $\sigma(F_1) = F_2 \Longrightarrow F_2$ are conjugate under σ.

(v) Suppose F/k is normal. Since E/k is finite, So is F/K Therefore, F/K is finite normal

$\Longrightarrow$ F is a minimal splitting field of some $f \in k[x]$.

Let $f = \alpha(x - \alpha_1) .....(x - \alpha_n)$, $\alpha_i \in E$, $\alpha \in k$.

Then $F = k(\alpha_1, \alpha_2, ... \alpha_n)$.

Let $\sigma \in G$. Then σ is k-automorphisms of E$\Longrightarrow \sigma$(f) = f.

$\Longrightarrow$ f= α(x - $\sigma(\alpha_1)$)..... (x - $\sigma(\alpha_n)$)

$\Longrightarrow \sigma(\alpha_1)$, ... $\sigma(\alpha_n)$ are zeros of f in E

$\Longrightarrow \{ \alpha_1, \alpha_2, \ldots \ldots \ldots, \alpha_n\} = \{ \sigma(\alpha_1), \ldots\ldots \sigma(\alpha_n)\}$.

$So,$ σ(F) = k ($\sigma(\alpha_1), \ldots . \sigma(\alpha_n)$)

= k(α_1,...., α_n) = F for all $\sigma \in G$.

By (iv), $\sigma^{-1}H\sigma = H$ for all $\sigma \in G$

$\Longrightarrow$ H is a normal subgroup of G.

Conversely, let H = F* be normal subgroup of G. Then $\sigma^{-1} H\sigma = \sigma$ for all $\sigma \in G$.

$\Longrightarrow \sigma(F) = F$ by (iv) for all $\sigma \in G$

Let $\alpha \in F$, p(x) = Irr (k, α)

Since E/k is normal and $\alpha \in E$, we find p(x) splits in E.

Let β be a zero of p(x) in E.

Then α, β are zeros of p(x) in E.

$\Longrightarrow$ there is an isomorphism θ : k(α)$\rightarrow$ k(β) s.t.,

θ (α) = β, θ(a) = a for all a $\in$ k.

Since $\beta \in E$, k (β) $\subseteq$ E. So θ is a k-homorphisms from k(α) to E.

Since E/K is finite normal, θ can be extended to k-automorphisms σ of E. So, $\sigma \in G$.

Now $\sigma(\alpha) = \theta(\alpha) = \beta$ and $\sigma(\alpha) \in \sigma$(F)= F$\Longrightarrow \beta \in F$.

Thus, p(x) splits in F$\Longrightarrow$F/K is normal.

Let H be a normal subgroup of G. Then the corresponding field F is normal over k from above. Since E/k is Galois, So is F/k, Let N = Gal (F/k)

Define Ψ : G$\rightarrow$ N s.t.,

$\Psi(\sigma) = \bar{\sigma}$, where $\bar{\sigma}$ is the restriction of σ on F.

(Since H $\leq$ G,σ^{-1} H σ= H $\Longrightarrow$ $\sigma(F) = F$)

Let $\sigma, \eta \in$ G.

Then $\overline{\sigma\eta}\ (\alpha) = (\sigma\eta)\ (\alpha)$, $\alpha \in$ F

$= \sigma\ (\eta(\alpha))$, $\eta(\alpha) \in$ F

$= \bar{\sigma}(\eta(\alpha))$

$= \bar{\sigma}(\bar{\eta}(\alpha))$

$= (\bar{\sigma}\bar{\eta})\ (\alpha)$, for all $\alpha \in$ F

$\Longrightarrow \overline{\sigma\eta} = \bar{\sigma}\bar{\eta}$

$\Longrightarrow \Psi\ (\sigma\eta) = \Psi\ (\sigma)\ \Psi(\eta)$

$\Longrightarrow$ Ψ is a homomorphism

Let$\theta \in$ N. Then $\in$ N. Then θ can be extended to k-automorphisms σ of E $\Longrightarrow$ $\sigma \in$ G

$\Longrightarrow \Psi\ (\sigma) = \bar{\sigma} = \theta$. So Ψ is onto. Now $\sigma \in$ Ker $\Psi \Leftrightarrow \Psi\ (\sigma)$ = Identity of N $\Leftrightarrow \bar{\sigma}$ Identity of F $\Leftrightarrow \bar{\sigma}(\alpha) = \alpha$ for all $\alpha \in$ F.

The result now follows by using fundamental theorem of homomorphism.

Example 1: (i)Let *E* be aminimal splitting field of f(x) = x^3 -2 over Q.

Solution. Let α be the real cube root of 2.

Then E = $Q(\alpha, \alpha\omega, \alpha\omega^2) = Q(\alpha, \sqrt{3}, i) = Q\ (\alpha, \alpha\omega) = Q\ (\alpha, \omega)$

Also, [E :Q] = 6 Since char Q= 0, E/Q is separable (as Q is perfect$\Longrightarrow$ every algebraic extension of Q is separable.)

Also, E is a minimal splitting field of f(x) over Q $\Longrightarrow$ E/Q is finite normal.

So, E/Q is Galois

Let G = G(E/Q) be the group of all Q-automorphisms of E.

Then Q is the fixed field of G, By Artin's theorem o(G)= [E : Q]=6

Since α, αw are roots of f(x) there exists Q-isomorphisms

σ_0 : Q(α) → Q($\alpha\omega$) s.t., $\sigma_0(\alpha) = \alpha\omega$

Let g(x) = x^2 +x+ 1 , then g(x) is irreducible over Q(α) ⊆ R and σ_0 (g(x)) = g(x) is irreducible over Q(αw)

Since w, w are roots of g(x) there exists an isomorphism

σ : Q (α, ω) = E → Q($\alpha\omega$, α) = E s.t.,

σ (w) = ω, $\sigma(\alpha) = \sigma_0(\alpha) = \alpha\omega$, $\sigma(\alpha) = \sigma_0(\alpha) = a \forall$ a ∈ Q

Thus σ is Q-automorphism of E, $\sigma \neq$ I.

Also ω, ω^2 are roots of g(x) which is irreducible over Q (α) and ∃ Q (α) is isomorphism

τ : Q (α, ω) = E → Q (α, ω^2) = E, s.t.,

$\tau(\omega) = \omega^2$, $\tau(\alpha) = \alpha$

and so τ is Q-automorphism of E, $\tau \neq$ I

Now $\sigma^2(\alpha) = \alpha\omega^2$, $\sigma^2(\omega) = \omega$

($\sigma\ \tau$) (α) = $\alpha\omega$, ($\sigma\tau$) (ω^2) = ω^2

($\sigma^2\tau$) (α) = $\alpha\ \omega^2$, ($\sigma^2\tau$) (ω^2) = ω^2

Since o(G) = 6, G = {I, σ, σ^2, τ, $\sigma\tau$, $\sigma^2\tau$}

Also ($\sigma\tau$) (α) = $\tau(\alpha\omega) = \alpha\ \omega^2$, $\tau\sigma \neq \sigma\tau$

So G is a non-abelian group of order 6 and so G ≅ S_3

Denote $\alpha\omega$ by 1, $\alpha\omega^2$ by 2 and $\alpha\omega^3$ by 3 and we get

τ = (12), σT = (13), σ^2T = 23, σ = (123), σ^2 = (132)

Write$\tau = \sigma_2, \sigma = \sigma_3$, σT = σ_4, $\sigma^2 = \sigma_5$ and $\sigma^2 T = \sigma_6$

Then G = { I, $\sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6$}

Subgroup of G are: H_1 = {I, σ_2}, H_2 = {I, σ_4}, H_3 = {I, σ_6}, H_4 = {I, σ_3, σ_5}, H_5 = G, H_6 = {I}.

Let F_1 = H_1 *, the fixed field of H_1 .

Now H_1 fixes $\alpha \Longrightarrow$ Q $\subseteq$ Q (α) $\subseteq$ $F_1 \subseteq$ E.

But [Q(α) : Q] = 3, [E : F_1] = [E : H_1*] = o(H_1) = 2 and [E : Q] = 6 $\Longrightarrow$ F_1 = Q (α).

Let F_2 = H_2* the fixed field of H_2

Then F_2 = Q (αw^2) and F_3, The fixed field of H_3 is Q(αw)

Let F_4 = H_4* the fixed field of H_4Now H_4 fixes $\sqrt{3}i \Longrightarrow$ Q$\subseteq$ Q ($\sqrt{3}i$) $\subseteq$ $F_4 \subseteq$ E.

Since [E : F_4] = 3[Q$\sqrt{3}i$:Q] = 2 [E : Q] = 6, F_4 =Q ($\sqrt{3}i$).

Clearly, F_5, = Fixed field of G =Q and F_6 Fixed Field of H_6 = E.

So, we have 6 intermediate fields between Q and E corresponding to 6 subgroup of G. Since H_1, H_2, H_3 are not normal, F_1 /Q, F_2 /Q, F_3 /Q are nor normal. also H_4, H_5, H_6 are normal subgroup of G, and thus F_4 /Q, F_5 /Q, F_6 /Q are normal subgroup of G.

(ii) Let E be a minimal splitting field of f(x) = x^4 +1 over Q.

Solution. Then α, α^3, α^5, α^7 are roots of f(x) where α = cos $\frac{\pi}{4}$ + i sin $\frac{\pi}{4}$

and E = Q(α) = Q(α^3) = Q(α^5) = Q(α^7)

Then [E : Q] = [Q(α) : Q] = deg Irr (Q, α) = deg f(x) = 4.

Char Q = 0 $\Longrightarrow$ E/Q is separable.

Also E is minimal splitting field of f(x) over Q implies E/Q is normal.

Hence E/Q is Galois

Let G = G(E/Q) be the Galois group of E/Q.

By Artin's theorem, o(G) = [E : Q] = 4.

Since α and α^3 are roots of an irreducible polynomial f(x) over Q, there exists Q-automorphism

σ_3 : Q(α) = E → Q (α^3) = E, s.t.,

$\sigma_3(\alpha) = \alpha^3$

Similarly, there exists Q-automorphisms

σ_5 : Q(α) = E → Q (α^5) = E, s.t.,

$\sigma_5(\alpha) = \alpha^5$

σ_7 : Q(α) = E → Q (α^7) = E, s.t.,

$\sigma_7(\alpha) = \alpha^7$

So G = {I, σ_3, σ_5, σ_7}

Also $\sigma^2{}_3 = \sigma^2{}_5 = \sigma^2{}_7$ = I

Thus G is an abelian non cyclic group of order 4 and so it the Klein's four group.

Subgroups of G are H_1 = {I, σ_3}, H_2 = {I, σ_5}, H_3 = {I, σ_7}, H_4 = G, H_5 = {I}.

Now $\sigma \in G \Longrightarrow \sigma(\sqrt{2})^2 = \sigma(2) = 2 \Longrightarrow (\sigma(\sqrt{2})^2 = 2 = 0 \Longrightarrow \sigma(\sqrt{2})$ is a zero of $x^2 + 2$ in $E \subseteq C \Longrightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$. Similarly σ(i) = $\pm$ i.

So, $\sigma_3(\alpha) = \alpha^3 \Longrightarrow \sigma_3\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

$\Longrightarrow \sigma_3(\sqrt{2}) = -\sqrt{2}$, σ_3(i) = -i

$\Longrightarrow \sigma_3(\sqrt{2}i) = -\sqrt{2}i$

$\Longrightarrow H_1$ = Fixes $\sqrt{2}i$

Let $F_1 = H_1^*$ the fixed field of H_1

Then $Q \subseteq Q(\sqrt{2}i) \subseteq F_1 \subseteq E$

But $[Q(\sqrt{2}i) : Q] = 2, [E : F_1] = 2, [E : Q] = 4$

So, $F_1 = Q(\sqrt{2}i)$

Also, $\sigma_5(\alpha) = \alpha^5 \Longrightarrow \sigma_5\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \frac{-1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$

$\sigma_5(\sqrt{2}) = -\sqrt{2}$ and σ_5 (i)= i $\Longrightarrow$ H_2 Fixes i.

Let $F_2 = H_2^*$ the fixed field of H_2.

Then $Q \subseteq Q(i) \subseteq F_2 \subseteq E$ and $[E : F_2] = 2, [Q(i) : Q] = 2, [E : Q] = 4 \Longrightarrow F_2 = Q(i)$.

Now $\sigma_7(\alpha) = \sigma^7 \Longrightarrow \sigma_5\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}} \Longrightarrow \sigma_5(\sqrt{2}) = \sqrt{2} \Longrightarrow H_3$ Fixes $\sqrt{2}$. Let $F_3 = H_3^*$.

Then $Q \subseteq Q\sqrt{2} \subseteq F_3 \subseteq E$ and $[E : F_3] = 2, [Q(\sqrt{2}) : Q] = 2, [E : Q] = 4$

$\Longrightarrow F_3 = Q(\sqrt{2})$.

Clearly F_4 = fixed field of H_4 (=G) is Q and F_5 = Fixed field of H_5 =E.

So, F_1, F_2, F_3, F_4, F_5, are intermediate fields lying between Q and E.

Since F_1, F_2, F_3, are quadratic extension of Q, F_1 /Q, F_2 /Q, F_3 /Q, are normal. Also F_4 /Q, F_5 /Q, are normal. But G being abelian all subgroup of G normal subgroups of G.

13.6 Summary

Galois Theory is a remarkable example of mathematical unification, linking various branches of mathematics and providing a powerful framework for addressing problems of great historical and mathematical significance. An extension E of F is called a Galois extension if (i) E/F is finite (ii) F is the fixed filed to a group of automorphisms of E.

(The fundamental theorem of Galois Theory). Let E/k be Galois Let G= G(E/k) be the group of all k-automorphisms of E. Then

(vi) There is one-one correspondence between the sets $\mathcal{A}$ = {F\F = field, k $\subseteq$ F $\subseteq$ E $\mathcal{B}$ = {H\ H $\leq$G} which is an order inverting bijection.

(vii) $F \in \mathcal{A}$ is the fixed field of the subgroup $H \in \mathcal{B}$ corresponding to F and $H \in \mathcal{B}$ is the group H* automorphisms of E, Where H* is the fixed field of H.

(viii) If H is the subgroup of $\mathcal{B}$ corresponding to the field F in $\mathcal{A}$ then o(H) = [E : F] and [G : H] = [F : k].

(ix) If H_1 , $H_2 \in \mathcal{B}$ corresponding to F_1, $F_2 \in A$ respectively, then F_1, F_2 are conjugate under an automorphism $\sigma \in G$ if and only $\sigma^{-1} H_1 \sigma = H_2$.

(x) If $H \in \mathcal{B}$ corresponds to $F \in \mathcal{A}$ then F/k is normal if and only if H is normal subgroup of G and in that case, $G(F/k) \cong \frac{G}{H}$.

13.6 Terminal Questions

Q.1. What do you mean by Galois theory?

Q.2. Explain the Galois extensions.

Q.3. State and prove the fundamental theorem of Galois theory.

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.

Unit 14: Galois Theory-II

Structure

14.1 Introduction

Galois theory, together with the ideas of fixed fields and normal extensions, holds great significance in modern algebra as it connects field theory with group theory. It helps determine whether polynomial equations can be solved by radicals and reveals the deep link between field extensions and symmetry. The notion of a fixed field, which remains unchanged under a group of automorphisms, provides clarity about the structure of extensions, while normal extensions ensure the inclusion of all polynomial roots, making them vital in studying solvability. These concepts are not only central to pure mathematics but also have wide applications in number theory, coding theory, cryptography, and the study of symmetries in physics. Collectively, they offer a unifying framework that advances both theoretical understanding and practical problem-solving. In this unit discuss the element from Galois theory, fixed field, normal extension.

14.2 Objectives

After studying this unit, the learner will be able to understand the:

- Automorphism, Group Fixing F, Field of H
- Finite field

14.3 Automorphism, Group Fixing F, Field of H:

Let E be an extension field of the field F. An automorphism of E is a ring isomorphism form E onto E. The automorphism group of E fixing F, Gal(E/F), is the set of all automorphism of E that take every element of F to itself. If H is a subgroup of Gal (E/F), the set every element of F itself. If H is a subgroup of Gal (E/F), the set

$E_H = \{x \in E \,!\, \emptyset(x) = x \text{ for all } \emptyset \in H\}$ is called the fixed field of H.

It is easy to show that the set of automorshisms of E forms a group under composition. the automporphism group of E fixing F is a sub group of the automorphism gruop of E and for any subgroup H of Gal (E/F), the fixed field E_H of H is a subfield of E. The group Gal (E/F) is called the Galois group of E over F. Be careful not to misinterpret Gal (E/F) as something having to do with factor rings or factor groups. It does not.

The following examples will help yours assimilate these definitions. In each example, we simply indicate the automorphism are defined. we leave as exercise the verifications that the mappings are indeed automorphisms.

Example.1: Consider the extension $(Q\sqrt{2})$ of Q.

Solution. Since $(Q\sqrt{2}) = \{ a + b\sqrt{2} \,!\, a, b \in Q\}$

and any automorphism of a field containing Q must act as the identity on Q and automorphisms $\emptyset$ of $Q\sqrt{2}$ is completely determined by $\emptyset(\sqrt{2})$. Thus ,

$2 = \emptyset(2) = \emptyset(\sqrt{2}\sqrt{2}) = (\emptyset(\sqrt{2}))^2$

and, therefore, $\emptyset(2) = \pm\sqrt{2}$. This proves that the group Gal $(Q\sqrt{2}/Q)$ has two elements, the identity mapping and the mapping that sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$.

Example.2: Consider the extension $(Q\sqrt[3]{2})$of Q.

Solution. An automorphism $\emptyset$ of Q. An automor phism $\emptyset$ of $Q\sqrt[3]{2}$ is completely determined by $\emptyset(\sqrt[3]{2})$. By an argument analogous to that in we see that $\emptyset(\sqrt[3]{2})$ must be a cube root of 2. Since $(Q\sqrt[3]{2})$ is a subset of the real numbers and $\sqrt[3]{2}$ is the only real cube root of 2, we must have $\emptyset(\sqrt[3]{2}) = \sqrt[3]{2}$. Thus, $\emptyset$ is the

identity automorphism and Gal ($Q\sqrt[3]{2}$/Q) has only one element. Obviously, the fixed field of Gal ($Q\sqrt[3]{2}$/Q) is ($Q\sqrt[3]{2}$).

Example.3: Consider the extension ($Q\sqrt[4]{2}, i$), of Q (i). Any auto morphism $\emptyset$ of ($Q\sqrt[4]{2}, i$) fixing Q(i) is completely determined by $\emptyset$ ($\sqrt[4]{2}$).

Since 2= $\emptyset(2) = \emptyset(\sqrt[4]{2})^4) = (\emptyset(\sqrt[4]{2})^4$

we see that $\emptyset$ ($\sqrt[4]{2}$) must be a fourth root of 2. Thus, there are at most four possible automorphisms of Q ($\sqrt[4]{2}$, i) fixing Q(i). If we define an automorphism α so that α (i)= i and $\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$, then $\alpha\epsilon$ Gal ($Q\sqrt[4]{2}$, i/Q (i)) and α has order 4. Thus, Gal ($Q\sqrt[4]{2}$, i/Q (i)) is a cyclic group of order 4. The fixed field of $\{\varepsilon.\alpha^2\}$ (where ε is the identity automorphism) is Q($\sqrt{2}$, i). The lattice of subgroups of Gal (Q($\sqrt[4]{2}$,i)/Q(i)) and the lattice of subfields of Q ($\sqrt[4]{2}$,i) contain

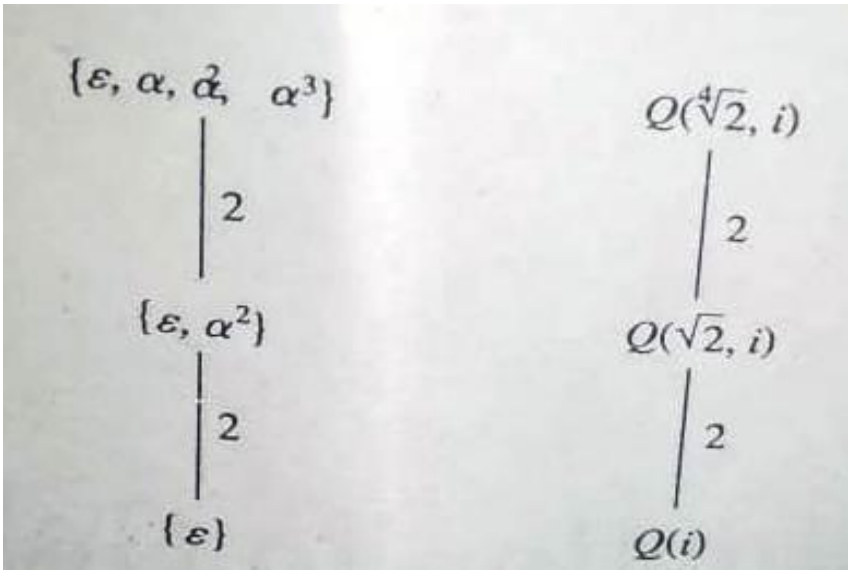


Figure 14.1

Lattice of subgroups of Gal (Q($\sqrt[4]{2}$,i)/Q(i)) and lattice of subfields of (Q($\sqrt[4]{2}$,i) containing Q(i).ing Q(i) are shown in Figure 14.1. As in Figures 13.1 and 13.2, the in tegers along the lines in the group lattice represent the index of a sub group in the group above it, and the integers along the lines of the field lattice represent the degree of the extension of a field over the field below it.

Example.4: Consider the extension Q($\sqrt{3}, \sqrt{5}$) of Q.

Since $Q(\sqrt{3}\sqrt{5}) = (a + b\sqrt{3}+c\sqrt{5} + d\sqrt{3}\sqrt{5}!\ a, b, c, d \in Q\}$, any automorphism $\emptyset$ of $Q(\sqrt{3}, \sqrt{5})$ is completely determined by the two values $\emptyset(\sqrt{3})$ and $\emptyset(\sqrt{5})$. This time there are four automorphisms:

$$\in \alpha\ \beta\alpha\beta$$

$$\sqrt{3} \to \sqrt{3}\sqrt{3} \to -\sqrt{3}\sqrt{3} \to \sqrt{3}\sqrt{3} \to -\sqrt{3}$$

$$\sqrt{5} \to \sqrt{5}\sqrt{5} \to \sqrt{5}\sqrt{5} \to -\sqrt{5}\sqrt{5} \to -\sqrt{5}$$

Obviously, $Gal(Q(\sqrt{3}, \sqrt{5})/Q)$ is isomorphic to $Z_2 \oplus Z_2$. The fixed field of (ε, α) is $Q(\sqrt{5})$, the fixed field of (ε,β) is $Q(\sqrt{3})$, and the fixed field of $(\varepsilon,\alpha\beta)$ is $Q(\sqrt{3}\sqrt{5})$. The lattice of subgroups of Gal $(Q(\sqrt{3}, \sqrt{5})/Q)$ and the lattice of subfields of $Q(\sqrt{3}, \sqrt{5})$ are shown in Figure 14.2.

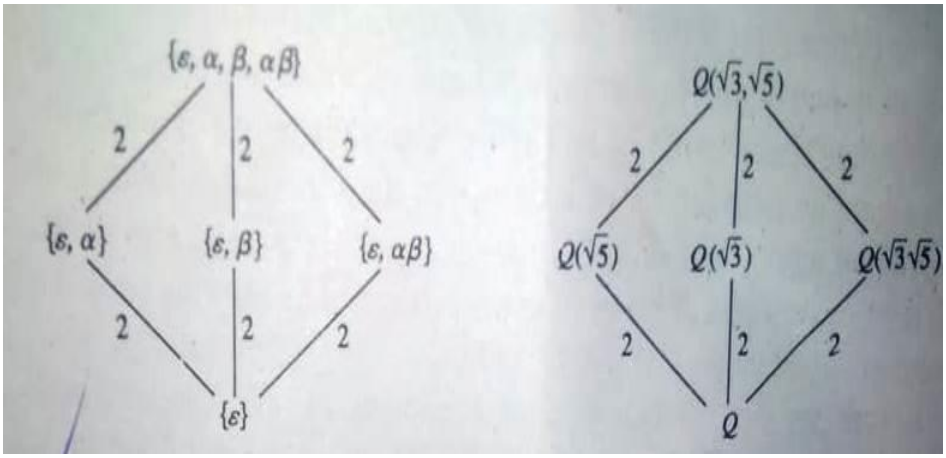


Figure 14.2 Lattice of subgroups of Gal $(Q(\sqrt{3}, \sqrt{3})/Q)$ and lattice of subfields of $Q(\sqrt{3}, \sqrt{5})$.

Example.5: Direct calculations show that $\omega = -1/2 + i\sqrt{3}/2$ satisfies the equations $\omega^3=1$ and $\omega^2 + \omega + 1 = 0$. Now, consider the extension $Q(\omega,\sqrt[3]{2})$ of Q. We may describe the automorphisms of $Q(\omega,\sqrt[3]{2})$ by specifying how they act on ω and $\sqrt[3]{2}$. There are six in all:

$$\in \alpha\ \beta\beta^2\alpha\beta\alpha\beta^2$$

$$\omega \to\ \omega\omega \to \omega^2\omega \to\ \omega \qquad \omega \to\ \omega\omega \to \omega^2\omega \to \omega^2$$

$$\sqrt[3]{2} \to \sqrt[3]{2}\sqrt[3]{2} \to \sqrt[3]{2}\sqrt[3]{2} \to \omega\sqrt[3]{2}\sqrt[3]{2} \to \omega^2\sqrt[3]{2}\sqrt[3]{2} \to \omega^2\sqrt[3]{2}\sqrt[3]{2} \to \omega\sqrt[3]{2}$$

Since $\neq \beta\alpha$, we know that $Gal(Q(\omega, \sqrt[3]{2}/Q)$ is isomorphic to S_3. The lattices of subgroups and subfields are shown in Figure 14.3.

The lattices in Figure 14.3 have been arranged so that the field occupying the same position as some group is the fixed field of that group. For instance, $Q(\omega\sqrt[3]{2})$, is the fixed field of $\{\varepsilon,\alpha\beta\}$.

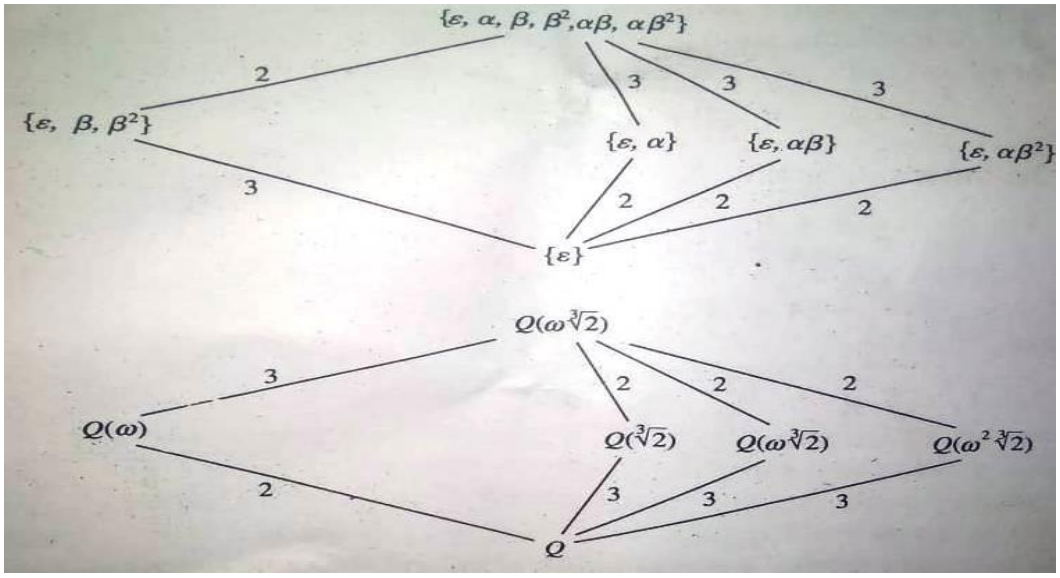


Figure 14.3

Lattice of subgroups of Gal ($Q(\omega, \sqrt[3]{2}/Q)$ and lattice of subfields of Q ($\omega,\sqrt[3]{2}$), where ω =-1/2+ $i\sqrt{3}/2$. The preceding examples show that, in certain cases, there is an initiate connection between the lattice of subfields between E and F and the lattice of subgroups of Gal(E/F). In general, if E is an extension of F, and we let $\mathcal{F}$ be the lattice of subfields of E containing F and $\mathcal{G}$ let be the lattice of subgroups of Gal(E/F), then for each K in $\mathcal{F}$, the group Gal(E/K) is in $\mathcal{G}$ and, for each H in $\mathcal{G}$, the field E_H is in $\mathcal{F}$. Thus, we may define a mapping g: $\mathcal{F} \rightarrow \mathcal{G}$ by g(K) = Gal(E/K) and a mapping f: $\mathcal{G} \rightarrow \mathcal{F}$ by f(H) = E_H. It is easy to show that if K and L be long to $\mathcal{F}$ and K ⊆ L, then g(K) ⊇ g(L). Similarly, if G and H belong to $\mathcal{G}$ and G ⊆ H, then f(G) ⊇ 2 f(H). Thus, fand g are inclusion-revers ing mappings between $\mathcal{F}$ and $\mathcal{G}$. We leave it as an exercise to show that for any K in $\mathcal{F}$, we have (fg)(K) ⊇ K and, for any G in $\mathcal{G}$, we have (gf)(G) ⊇ G. When E is an arbitrary extension of F, these inclusions may be strict. However, when E is a suitably chosen extension of F, the Fundamental Theorem of Galois Theory, Theorem 5.1, says that f and g are inverses of each other so that the inclusions are equalities. In particular, f and g are inclusion-reversing isomorphism's between the lattices $\mathcal{F}$ and $\mathcal{G}$.

14.4 Finite Fields

A field having finite number of elements is called a finite field or a Galois field.

Theorem 5 : If F is a finite field, then o(F) = p^n for some prime p and an integer n ≥ 1.

Proof : Let p be the prime subfield of F.

Since F is finite, so is P≀. There fore, P ≅ $\frac{Z}{<p>}$ for some prime p.

But $\frac{Z}{<p>}$ ≅ {0,1,2,....., p - 1} mod p = F_P ⟹P ≅ F_p

Sine P ⊆ F, we can regard F_P ⊆ F. Now F is a vector space over F_P . Since F is finite [F : F_P] = n= finite.

Let {u_1,.....,u_n} be a basis of F/ F_P

Then F = {$\alpha_1 u_1$ + ...+ $\alpha_n u_n$ | $\alpha_i \in F_P$}.

Now each α_i can be chose in p ways and $\sum \alpha_i u_i = \sum \beta_i u_i \Longrightarrow \alpha_i = \beta_i$, there fore o(F) = p^n.

Theorem 6 : Let P be a prime and n ≥ 1 be an integer. Then there exists a field with p^n elements.

Proof : Let f(x)= x^q-x ∈ F_p [x], q = p^n. Let F be a minimal splitting field of f(x) over F_p.

Then F = F_p (zeros of f in F)

Let S = {zeros of f in F}

Now f ' = qx^{q-1} -1 = -1 as char F = p ⟹ q -1 = p^n -1 =-1.

Therefore , (f, f') = 1

⟹ all zeros of F in F are simple an so distinct.

So, o(S) = q.

Now 0 ∈ S ⟹ S ≠ φ

Also a, b ∈ F_q ⟹ a^q = a, b^q= b⟹ (a ± b)^q = a^q± b^q = a ± b,

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

⟹ a ± b, ab, ab^{-1}(if b≠ 0) ∈ S.

Thus S is a subfield of F.

Let a ∈ F_p Then $a^{p-1} = 1 \Longrightarrow a^p = a \Longrightarrow a^{p^n} = a \Longrightarrow a^q = a$.

$\Longrightarrow$ a is a zero of f in F $\Longrightarrow$ a ∈ S $\Longrightarrow$ $F_p \subseteq S$.

So S is a field containing F_p and S.

But F is the smallest field containing F_p and S.

$\Longrightarrow$ F⊆ S. Also S ⊆ F. So, S = F $\Longrightarrow$ o(F) = o(S) = q.

Lemma 1: Let G be an Aeolian group under multiplication. Let a, b ∈ G be such that o(a) = m, o(b)= n and (m, n)= 1, Then o(ab) = mn

Lemma 2: Let G be an abelian group under multiplication. Let a, b ∈ G be such that o(a) = m, o(b)= n. Then there exists c∈ G such o(c) = l.c.m of m and n.

Proof : Let (m, n).>1

Let $m = p_1^{\alpha_1} \ldots . p_r^{\alpha_r}$

$n = p_1^{\beta_1} \ldots . p_r^{\beta_r}$

where $p_1 \ldots\ldots p_r$ are distinct primes and a_i, β_iarenon negative integers.

Let $l = p_1^{\alpha_1} \ldots\ldots p_s^{\alpha_s} p_{s+1}^{\beta_{s+1}} \ldots\ldots\ldots p_r^{\beta_r}$

where $\alpha_i \geq \beta_i$for i = 1, ...s, and $\beta_j \geq \alpha_j$for j = s +1 ..., r

Then l is the L.C.M of m and n.

Let $x = a^{p_{s+1}{}^{\alpha_{s+1}}} \ldots\ldots Pr^{ar}$, $y = b^{p1\beta1} \ldots\ldots p_s^{\beta_s}$

Then o(x) = $p_1^{\propto_1}, \ldots\ldots p_s^{\propto_s}$

o(y) = $p_{s+1}^{\beta_{s+1}} \ldots\ldots p_r^{\beta_r}$

and (o(x)), o(y)) = 1.

∵ o(xy) = 1.c.m of m and n

$= P_1^{\propto_1} \ldots\ldots p_s^{\propto_s} p_{s+1}^{\beta_{s+1}} \ldots\ldots\ldots p_r^{\beta_r}$

Lemma 3 : With the hypothesis of lemma 2, if n ∤ m, then the l.c.m. l of m and n is greater than m.

Proof : Now m | $l \Longrightarrow m \leq l$. If m = l, then n | $l \Longrightarrow$ n | m, a contradiction So l>m.

Lemma 4 : Let G be a finite abelian group under multiplication. Let $\alpha \in$ G be of maximum order. Then o(β) | o(α) for all $\beta \in$ G.

Proof : Let o(α) = m, o(β) = n.

Suppose n ∤ m. By lemma 3, l = l.c.m of m, n> m. By lemma 2, there is $\gamma \in$ G such that o(γ) = l > m contradicting $\alpha \in$ G is of maximum order. So, n|m $\Longrightarrow$ o (β) | o(α) for all $\beta \in$ G.

Theorem 7 : Let F be a finite field. Then F*, the set of non-zero elements of F forms a cyclic group under multiplication in F.

Proof : Now F* is an abelian group under multiplication.

Let $\alpha \in$ F* be an element of maximum order m.

Then by lemma 4, o(β) | m for all $\beta \in$ F*

So, m = o(β)r$\Longrightarrow \beta^m = \beta^{o(\beta)r} = 1$ for all $\beta \in$ F*.

$\Longrightarrow \beta$ satisfies $x^m - 1$ over F.

Since F can't have more than m zeros of x^m-1, o(F*)≤ m.

But $\alpha \in$ F* and o(α) = m $\Longrightarrow$ 1, α, α^2, ..., α^{m-1} are elements of F*

$\Longrightarrow$ o(F*) ≥ m $\Longrightarrow$ o(F*) = m= o(α) $\Longrightarrow$ F* = <a>

The generators of F* are called primitive elements of F.

Theorem 8 : Let F be finite field of order p^n. ThenF is a minimal splitting field of x^{p^n} -x over F_p.

Proof : We can regard F as an extension of F_p Let q = p^n.

Now F* = <a> , o(α) = o(F*) = q-1. Also $\alpha^{q-1} = 1. \Longrightarrow \alpha^q = \alpha$

$\Longrightarrow$ elements of F are zeros of $f(x) = x^q - x$ over F_p

So, f(x) splits in F.

Therefore, f(x) = x(x- α) .....(x - $\propto^{q-1}$)

$\Longrightarrow$ Minimal splitting filed of f over F_p is $F_p(\alpha, \alpha^2, ..., \alpha^{m-1},1,0) = F_p(F) = F$.

Theorem 9 : Any two finite fields with the same number of elements p^n are F_p isomorphic.

Proof : Let $F_1, F_2,$ be finite field such that $o(F_1) = p^n = o(F_2)$ Then by above F_1, F_2

are minimal splitting fields of f(x) = x^{p^n} - x over $F_p \Longrightarrow F_1, F_2$ are F_p isomorphic.

The above theorem shows that there is unique field of order $q = p^n$ upto an isomorphism. It is denoted by $GF(p^n)$ or GF(q) or Fq.

Example 6 : Show that x^m -1 divides x^n - 1 over a field F if and only if m divides n.

Solution : Let n = km + r, $0 \leq r < m$

The $x^n - 1 = x^r\left(\sum_{i=0}^{k-1} x^{im}\right)(x^m - 1) + (x^r - 1)$

Therefore x^m -1 divides x^n -1 if and only if x^r -1 = 0

Also x^r -1 = 0 if and only if r = 0

So x^m -1 divides x^n -1 if and only if m divides n.

Example 7: Show that x^{p^m} -x divides x^{p^n} - x if m divides n.

Solution : Let n = mu

Then $p^n - 1 = p^{mu} - 1 = (p^m)^u - 1$

$= (p^m) - 1$ (integer)

$\Longrightarrow p^m$ -1 divides p^n -1

By above problem

$x^{p^{m-1}}$ -1 divides $x^{p^{n-1}}$ -1

$\Longrightarrow x^{p^m}$ - x divides x^{p^m} -x

Theorem 10 : Let F be a field with p^n elements . Then F has a subfield k with p^m elements if and only if m divides n.

Proof : suppose k is a subfield of F. Then k can be regarded as an extension of F_p such that $[k : F_p] = m$ Similarly F can be regarded as an extension of F_p such that $[F : F_p] = n$. Now $[F : F_p] = [F : k]\,[k : F_p] = m$ divides n.

Conversely, let F be a field such that $o(F) = p^n$ Suppose m divides n. Now F is a minimal splitting field of x^{p^n} - x over F_p

Let $f(x) = x^{p^n}$ - x and $g(x) = x^{p^m}$ - x

Since m divides n, by above problem g(x) divides f(x).

Consider F' = [zeros of g(x) in F]

Then F' is a subfield of F.

Since g(x) has p^m distinct zeros, F' is a subfield of F with p^m elements.

If k is another subfield of F such that $o(k) = p^m$, then $o(k) = o(F') = p^m$

$\Longrightarrow$ k, F' are F_p-isomorphic

Thus, there is exactly one subfield of F (up to isomorphism) with p^m elements.

Example 8 : Determine the algebraic closure of F_p.

Solution: We know m! divides n! for all positive integers m < n By above theorem F_pm! is a subfield of F_pn! Thus, there is an ascending chain of subfields

$F_p \subseteq F_{p2!} \subseteq F_{p3!} \subseteq$.....

and $F_{P\infty} = \cup_n F_{p^{n!}}$ is a field such that $F_{p^n} \subseteq F_{p^{n!}} \subseteq F_{p^\infty}$ for any positive integer n.

Let S be the set of all polynomials over F_p Let $f \in S$.

Then the minimal splitting field of f over F_p is a finite field F_{p^n}

So, each $f \in S$ splits in F_{p^∞}

Thus the minimal splitting field of S over F_p is

F_p (zeros of f ∈ S in $F_p\infty$) ⊆ $F_p\infty$

Also a ∈ $F_p\infty$ ⟹ a ∈ F_{p^n} for some n ⟹ a is zero of x^{p^n} - x over F_p.

Now f = x^{p^n} - x ∈ S ⟹ a is zero of ∈ S in $F_p\infty$

⟹ $F_p\infty$ ⊆ F_p (zeros of f ∈ S in $F_p\infty$)

⟹ Minimal splitting filed of S over F_p is $F_p\infty$

⟹ $F_p\infty$ is the algebraic closure of F_p.

Theorem 11 : Every finite extension of a finite field is Galois.

Proof : Let k be finite extension finite field k. Then k is also finite field. So char(k)= char K = p, for some prime p. Let o(k) = p^m, o(K) = p^n.

Now K is a minimal splitting field of x^{p^n} - x over F_p⟹ K/ F_p is finite normal.

Also F_p isfinite ⟹ F_p is perfect ⟹ every algebraic extension of F_p is separable ⟹ K/ F_p is separable ⟹ K/ F_p is Galois Now F_p ⊆ k ⊆ K and K/ F_p is Galois ⟹ K/k is Galois .

Cor : F_q/ F_p is Galois, q = p^n,

Theorem 12 : Let F be a finite field. Then there exists an irreducible polynomial of any given degree n over k.

Proof : Let o(F) = p^m, p being prime.

Let q = p^{nm} and let f(x) = x^q - x

The F_q is the minimal splitting field of f(x) over F_p

since m/nm, F_{p^m} = F can be imbedded in F_q

Now F_p ⊆ F = F_{p^m} ⊆ $F_{p^{mn}}$ =E

Then [E : F] = n.

Let E* be the multiplicative group of non-zero elements of E and let E* = <∝>

Then E = F(α) as F ⊆E, $\alpha \in$ E

So, n = [E : F] = [F(α) : F] = deg Irr (F, α)

$\Longrightarrow$ Irr (F, α) is an irreducible polynomial of degree n over F.

Theorem 13 : Let G be the group of F_p automorphisms of F_p . Then G is a cyclic group generated by Fresenius map of order n, where $q = p^n$.

Proof :. let $\theta : F_q \to F_q$ s.t., $\theta(b) = b^p$.

Then θ is called Frobenius map.

Since char F_p = char F_q= p θ is a homomorphism.

Also θ is one-one. Since F_q is finite, θ is onto.

If b ∈ F_q then b^p= b $\Longrightarrow$ θ(b) = b for all b∈ F_p

So, θ is an F_p - automorphisms of $F_q \Longrightarrow \theta \in G$

By Artin theorem, o(G)= [F_q : F_p] as of F_p is the fixed field of G.

$\Longrightarrow$ o(G) = n. We show that o(θ) = n.

Let θ^r = I, let F_q* = <a>

Then $a^{q-1} = 1 \Longrightarrow a^q = a \Longrightarrow x^{p^n}$ =a.

Now θ^r = I $\Longrightarrow \theta^r$(a) = a$\Longrightarrow a^{p^{r-1}}$ = 1.

$\Longrightarrow$ o(a) | p^r-1 $\Longrightarrow$ q -1 | r - 1 $\Longrightarrow$ p^n-1 | p^r-1 $\Longrightarrow$ p^n-1 ≤ p^r-1 ≤ p^r-1 $\Longrightarrow$ n ≤ r.

Also θ^n(b) = b^{p^n} = b for all b ∈ $F_q \Longrightarrow \theta^n$ = I

So, o(θ) = n $\Longrightarrow$ G = < θ>

Example 9 : Prove that every element in a finite field can be written as the sum of two squares.

Solution: Let F be a finite field such that o(F) = p^n

Case 1 : p = 2 Define $\theta : F \to F$ s.t., $\theta(b) = b^2$

Then $\theta(b_1 + b_2) = (b_1 + b_2)^2 = b_1^2 + b_2^2 = \theta(b_1) + \theta(b_2)$

$\theta(b_1 b_2) = (b_1 b_2)^2 = b_1^2 b_2^2 = \theta(b_1)\,\theta(b_2)$

$\Longrightarrow \theta$ is a homorphisms.

Also θ is one-one Since F is finite, θ in onto.

Let $a \in F$ Then there is $b \in F$ such that $\theta(b) = a \Longrightarrow a = b^2 = b^2 + 0^2$ = Sum of two squares in F.

Case 2 : $p \neq 2$. Let $a \in F$. Let $X = \{a - x^2 \mid x \in F\}$

Then $a - x_1^2 = a - x_2^2$, $x_1, x_2 \in F \Longrightarrow x_1^2 = x_2^2 \Longrightarrow x_1 = -x_2$ IF $x_1 \neq x_2$

$\Longrightarrow o(X) = \frac{P^n - 1}{2} + 1 = \frac{P^n + 1}{2}$

Let $Y = \{y^2 \mid y \in F\}$ Then $o(Y) = \frac{P^n + 1}{2}$

Since $X, Y \subseteq F$ and $o(F) = p^n$, $X \cap Y \neq \varphi$

So, $a - x^2 = y^2$ for some $x, y \in F \Longrightarrow a = x^2 + y^2$ = sum of two square in F.

Example 10 : Show that for any integer a and prime p, $a^p \equiv a \pmod p$.

Solution: Let $a = pq + r$, $0 \leq r \leq p$.

Then $a \equiv r \pmod p$

Now $0 \leq r < p \Longrightarrow r \in F_p$.

$\Longrightarrow r_o r_o \ldots_o r = r$

p times

$\Longrightarrow r^p - pu = r$

$\Longrightarrow r^p \equiv r \pmod p$

$\Longrightarrow r^p \equiv a \pmod p$

So, $a \equiv r \pmod{p}$

$\Longrightarrow a^p \equiv r^p \pmod{p}$

$\Longrightarrow a^p \equiv a \pmod{p}$

(The above result is known as Fermat's theorem)

Example 11: Show that every irreducible polynomial f(x) $\in F_p[x]$ is a divisor of $x^{p^n} - x$ for some n.

Solution: Let deg f(x) = d and α be a zero of f(x) in an extension of F_p.

Then $[F_p(\alpha) : F_p]$ = deg Irr (F_p, α) = deg f(x) = d.

So $o(F_p(\alpha)) = p^d$ then $\alpha \in F_p(\alpha) \Longrightarrow \alpha^{p^d} = \alpha \Longrightarrow \propto$ is zero of $x^{p^d} - x \in F_p[x]$

$\Longrightarrow$ f(x) divides $x^{p^d} - x$

Example 12: Show that $x^{p^n} - x$ is the product of monic irreducible polynomials in $F_p[x]$ of degree d, d dividing n.

Solution : Let $f(x) = x^q - x$, $q = p^n$, Let p(x) be a monic irreducible factor of f(x) over F_p Let α be a zero of p(x) in F, where F is a minimal splitting field of f(x) over F_p Then $F = F_p$ and $p(x) = \text{Irr}(F_p, \alpha)$

Now $F_p \subseteq F_p(\alpha) \subseteq F_q$

and $n = [F_q : F_p] = [F_q : F_p(\alpha)]\,[F_q(\alpha) : F_p]$

$= [F_q : F_p(\alpha)]$ deg Irr (F_p, α)

$= [F_q : F_p(\alpha)]$ deg p(x)

$\Longrightarrow$ deg p(x) divides n.

$\Longrightarrow$ any monic irreducible polynomial dividing $x^{p^n} - x$ of degree dividing n.

Example 13: Show that $x^p - x - a$ $(a \neq 0)$ is irreducible over F_p.

Solution: Let $f(x) = x^p - x - a$

Let α be a zero of f(x) in some extension of F_p Then $f(\alpha) = 0$

Consider $f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a$

$= a^p - \alpha - a = f(\alpha) = 0$

$f(\alpha + 2) = (\alpha + 2)^p - (\alpha + 2) - a$

$= (\alpha + 1)^p - (\alpha + 1) - a$

In this way α, α +1, α +2 , ..., α + (p -1) are all zeros of f(x).

Also $f'(x) = p\,x^{p-1} - 1 = -1 \neq 0 \Longrightarrow f'(\beta) = \alpha, \alpha + 1, ..., \alpha + (p - 1)$

$\Longrightarrow \alpha, \alpha + 1, ..., \alpha + (p - 1)$ are distinct zeros of f(x)

now , $F_p(\alpha)$ is a minimal splitting field of f(x) over F_p

Also $[F_p(\alpha) : F_p] = \deg \text{Irr}(F_p, \alpha) \leq p$ as α satisfies f(x) of degree p.

Since F_p is finite, so is $F_p(\alpha)$

Also Char $F_p(\alpha) = p \Longrightarrow o(F_p(\alpha)) = p^m \Longrightarrow [F_p(\alpha) : F_p] = m = \deg \text{Irr}(F_p, \alpha) = \deg g(x) \leq p$.

Now $\alpha^{pm} = \alpha$ but $\alpha^p = \alpha + a \Longrightarrow \alpha^{p^2}$ $(\alpha + a)^2 = \alpha^p + a^p = \alpha + 2a$ as $a \in F_p$

$\Longrightarrow \alpha^p = a$.

In this way $\alpha^{pm} = \alpha + m\alpha \Longrightarrow \alpha = \alpha + ma \Longrightarrow ma = 0 \Longrightarrow p$ divides m as $a \neq 0 \Longrightarrow p \leq m$.

So, $p = m \Longrightarrow \deg g(x) = p$ Also g(x) divides f(x) and deg g(x) = deg f(x)

$\Longrightarrow g(x) = f(x) \Longrightarrow f(x)$ is irreducible over F_p.

Example 14: Construct a field of order 9.

Solution : Let F_9 be the filed of order 9. Let $F_3 = \{0,1,2\}$ mod 3. Then $[F_9 : F_3] = 2$ Let $f(x) = x^9 - x$. Then F_9 is a minimal splitting field of f(x) over F_3 .Let p(x) be an irreducible factor of f(x) over F_3,Let α be a zero of p(x) in F_9. Then α is zero of f(x), If $\alpha \in F_3$, then $p(x) = x - \alpha \Longrightarrow \deg p(x) = 1$. If $\propto \notin F_3$, then $F_3 \subseteq F_3(\alpha) \subseteq F_9 \Longrightarrow [F_9 : F_3] = 2 = [F_9 : F_3(\alpha)]\,[F_3(\alpha) : F_3]$

Since $\alpha \notin F_3$, $[F_3(\alpha) : F_3] \neq 1$

$\Longrightarrow [F_3(\alpha) : F_3] = 2$

But $[F_3(\alpha): F_3] = \deg \text{Irr}(F_3, \alpha)$

$= \deg p(x)$

Thus $\deg p(x) = 2$.

Hence any irreducible factor of $f(x)$ over F_3 hasdegree 1 or 2.

Now $x^9 - x = x(x^8 - 1)$

$= x(x^4 - 1)(x^4 + 1)$

$= x(x - 1)(x + 1)(x^2 + 1)(x^2 - x - 1)(x^2 + x - 1)$

Note $x^2 + 1$, $x^2 - x - 1$, $x^2 + x - 1$ are irreducible over F_3 as none of 0, 1,2, are zeros of these factors.

Let $p(x) = x^2 + 1$. Let α be a zero of $p(x)$

Then $\{1, \alpha\}$ is a basis of $F_9 = F_3(\alpha)$ over F_3

So, $F_9 = \{a + b\propto | a, b \in F_3\}$

$= \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$

Let $u = \alpha + 1$ Then $u^2 = 2\alpha$, $u^4 = -1$, $u^8 = 1$. So, $o(u) = 8 \Longrightarrow F_9^* = \langle u \rangle$

therefore

$F_9 = \{0,1, = u^8, 2 = u^4, \alpha = u^6, \alpha + 1 = u, \alpha + 2 = u^7, 2\alpha = u^2, 2\alpha + 1 = u^3, 2\alpha + 2 = u^5\}$

Now multiplication is defined by element u^i in F_9 we wish to define addition in F_9 with the help of u^i

If $u^n + 1 \neq 0$, Let $u^n + 1 = u^{z(n)}$

Define $u^a + u^b = u^{z(a-b)+b}$ if $u^{a-b} + 1 \neq 0$ where $a \geq b$

$= 0$ if $u^{a-b} + 1 = 0$

Lets find

$u^7 + u^1$

Now $u^6 + 1 = \alpha + 1 = u^1 \neq 0$. So, $z(6) = 1$. Therefore, $u^7 + u^1 = u^{z(6)+1} = u^2$

Also $u^6 + u^2 = 0$ as $u^4 + 1 = -1 + 1 = 0$. In this way addition is defined in terms of u^i

Let $a = u^i$. Then write log a = i . If $b = u^j$, Then $ab = u^{i \oplus j}$, where $\oplus$denotes the addition module 9.

So, log ab = i $\oplus$j = log a $\oplus$b.

Such a logarithm is known as Zech logarithm.

14.5 Summary

An extension E of F is called a Galois extension if (i) E/F is finite (ii) F is the fixed filed to a group of automorphisms of E.

Let E/k be Galois Let G= G(E/k) be the group of all k-automorphisms of E. Then

(i) There is one-one correspondence between the sets $\mathcal{A}$ = {F\F = field, k $\subseteq$ F $\subseteq$ E $\mathcal{B}$ = {H\ H $\leq$G} which is an order inverting bijection.

(ii) F $\in \mathcal{A}$ is the fixed field of the subgroup H $\in \mathcal{B}$ corresponding to F and H $\in \mathcal{B}$ is the group H* automorphisms of E, Where H* is the fixed field of H.

(iii) If H is the subgroup of $\mathcal{B}$ corresponding to the field F in $\mathcal{A}$ then o(H) = [E : F] and [G : H] = [F : k].

(iv) If H_1 , $H_2 \in \mathcal{B}$ corresponding to F_1, $F_2 \in A$ respectively, then F_1, F_2 are conjugate under an automorphism $\sigma \in$ G if and only $\sigma^{-1} H_1 \sigma = H_2$.

(v) If H $\in \mathcal{B}$ corresponds to F $\in \mathcal{A}$ then F/k is normal if and only if H is normal subgroup of G and in that case, G(F/k) $\cong \frac{G}{H}$.

14.6 Terminal Questions

Q.1. Let E be an extension field of Q. Show that any automorphism on E acts as the identity on Q. (This exercise is referred to in this chapter).

Q.2. Let E be a field extension of the field F. Show that the automorphism group of E fixing F is indeed a group. (This exercise is referred to in this chapter.)

Q.3. Let E be a field extension of a field F and let H be a subgroup of Gal(E/F). Show that the fixed field of H is indeed a field. (This exercise is referred to in this chapter.)

Q.4. Let $f(x) \in F[x]$ and let the zeroes of $f(x)$ be $a_1, a_2, \ldots\ldots, a_n$. If $K = (a_1, a_2, \ldots\ldots, a_n)$, show that Gal(K/F) is isomorphic to a group of permutations of the a_i's.[When K is the splitting field of f(x) over F, the group Gal(K/F) is called the Galois Group of f(x).)

Q.5. Show that the Galois group of a polynomial of degree *n* has order dividing$n!$.

Q.6. Let E be the splitting field of $x^4 + 1$ over Q. Find Gal(E/Q). Find all subfields of E. Find the automorphisms of E that have fixed fields $Q(\sqrt{2}), Q(\sqrt{2})$ and $Q(i)$. Is there an automorphism of E whose fixed field is Q.

Q.7. Determine the group of field automorphisms of GF(4).

Q.8. Let E=$Q(\sqrt{2}, \sqrt{5})$. What is the order of the group Gal(E/Q)? What is the order of Gal $Q(\sqrt{2}/Q)$?

Q.9. Given that the automorphism group of $Q(\sqrt{2}, \sqrt{5}, \sqrt{7})$ is isomorphic to $Z_2 \oplus Z_2 \oplus Z_2$, determine the number of subfields of $Q(\sqrt{2}, \sqrt{5}, \sqrt{7})$ that have degree 4 over Q.

Q.10. Let ω be a non-real complex number such that $\omega^5 = 1$. If ϕ is the automorphism of $Q(\omega)$ that carries ω to ω^4, find the fixed field of $\langle\phi\rangle$.

Q.11. Determine the isomorphism class of the group Gal(GF(64)/GF(2)).

Q.12. Determine the isomorphism class of the group Gal(GF(729)/GF(9)).

References

1. Khanna, V. K., & Bhamri, S. K. (2016). A course in abstract algebra. Vikas Publishing House.

2. Vasishtha, A. R., & Vasishtha, A. K. (2006). Modern Algebra (Abstract Algebra). Krishna Prakashan Media.

3. Malik, S. C., & Arora, S. (1992). Mathematical analysis. New Age International.

4. Goyal, J. K., Gupta, K. P. (2023). Advanced Course in Modern Algebra Pragati Prakashan.