Bachelor of Science
(FOURTH SEMESTER)

MT(N)-202
ABSTRACT ALGEBRA

DEPARTMENT OF MATHEMATICS
SCHOOL OF SCIENCES
UTTARAKHAND OPEN UNIVERSITY
HALDWANI, UTTARAKHAND
263139

COURSE NAME: ABSTRACT ALGEBRA

COURSE CODE: MT(N)-202

Department of Mathematics
School of Science
Uttarakhand Open University
Haldwani, Uttarakhand, India,
263139

BOARD OF STUDIES 2023

Editor

Dr. Deepa Bisht
Assistant Professor (AC)
Department of Mathematics,
School of Sciences, Uttarakhand Open University

Unit Writer	Blocks	Units
Dr. Kamlesh Bisht Assistant Professor (AC) Department of Mathematics Uttarakhand Open University	**I, II, III**	**01 to 14**

Course Title and Code : Abstract Algebra (MT(N)-202)

ISBN :

Edition : 2024

Contents

Course: Abstract Algebra **Course code: MT(N)-202**

Credit: 4

COURSE INFORMATION

The present self-learning material **"Abstract Algebra"** has been designed for B.Sc. (Fourth Semester) learners of Uttarkhand Open University, Haldwani. This self learning material is writing for increase learner access to high-quality learning materials. This course is divided into 14 units of study. The first six units are devoted to basic concepts of set, group, different types of group, subgroup and various applications of groups to solve the real life problem. Unit 7 and Unit 8 are focussed on the topic of group homomorphism and isomorphism. The aim of Unit 9 to introduce the various application of group in terms of class equations. Unit 10 to 11 explain the further extension of group theory in terms of ring theory and integral domain. Unit 12 and Unit 13 explain the most essential too in abstract algebra name as ideal, factor ring and ring homomorphism. Unit 14 will explain the theory of field which is very useful to understand the primary concept of linear algebra. This material also used for competitive examinations. The basic principles and theory have been explained in a simple, concise and lucid manner. Adequate number of illustrative examples and exercises have also been included to enable the leaners to grasp the subject easily.

Course Name: Abstract Algebra **Course Code: MT(N)-202**

Credit: 4

SYLLABUS

Sets, Groups and Subgroups

Sets, Some basic concept of sets: Cartesian product; Binary operation; Relations; Partitions, Definition and examples of different groups, Permutation and quaternion groups, Elementary properties of groups. Subgroups and examples of subgroups, Cyclic groups, Properties of cyclic groups, Lagrange's theorem, Euler phi function.

Normal Subgroups, Permutation Group and Group Homomorphism

Properties of cosets, Normal subgroups, Simple groups, Factor groups, Cauchy's theorem for finite abelian groups; Centralizer, Normalizer, Center of a group, Product of two subgroups; Classification of subgroups of cyclic groups.

Cycle notation for permutations, Properties of permutations, Even and odd permutations, alternating groups, Cayley's theorem and its applications, Group homomorphisms, Properties of homomorphisms, Group isomorphisms, Properties of isomorphisms; First, second and third isomorphism theorems for groups, Class equation.

Rings, Ideal, Integral domain and Field

Ring, Elementary properties of a ring, ring with or without zero divisor, Isomorphism of ring, subring, Characteristic of ring, Imbedding of ring into another field, Ring of endomorphism of an abelian group, Ideal, Principle ideal, Unit, Associate, Prime elements, Greatest common divisor, Polynomial ring, Homomorphism of ring, Kernel of ring homomorphism, Maximal ideal, Prime ideal, Euclidean ring, Integral domains and fields.

BLOCK- I

SETS, GROUPS AND SUBGROUPS

UNIT 1: BASIC CONCEPTS OF SETS

CONTENTS:

1.1 *INTRODUCTION*

Set theory, branch of mathematics that deals with the properties of well-defined collections of objects, which may or may not be of a mathematical nature, such as numbers or functions. The theory is less valuable in direct application to ordinary experience than as a basis for precise and adaptable terminology for the definition of complex and sophisticated mathematical concepts.

Between the years 1874 and 1897, the German mathematician and logician Georg Cantor created a theory of abstract sets of entities and made it into a mathematical discipline. This theory grew out of his investigations of some concrete problems regarding certain types of infinite sets of real numbers. A set, wrote Cantor, is a collection of definite, distinguishable objects of perception or thought conceived as a whole. The objects are called elements or members of the set.

1.2 *OBJECTIVES*

After studying this unit, learner will be able to

i. To analyze and predict the behavior of these systems over time.

ii. To provide solutions to problems that cannot be solved using other mathematical techniques.

iii. To understand the definition of differential equation.

1.3 *SETS*

A set is a well - defined collection of distinct objects.

By a 'well – defined' collection of objects we mean that there is a rule by means of which it is possible to say, without ambiguity, whether a particular object belongs to the collection or not. The objects in a set are **'distinct'** means we do not repeat an object over and over again in a set.

Each object belonging to a set is called an element of the set. Sets are usually denoted by capital letters A, B, N, Q, S etc. and the elements by lower case letters a, b, c, x etc.

The symbol $\in$ is used to indicate 'belongs to'. Thus $x \in A \Longrightarrow x$ is an element of the set A.

The symbol $\notin$ is used to indicate 'does not belong to'. Thus $x \notin A \Longrightarrow x$ is not an element of the set A.

Example: Let A = {1, 2, 3, 4, 5} be a set then we say $1 \in A$, $2 \in A$, $3 \in A$, $4 \in A$, $5 \in A$ but $6 \notin A$, $7 \notin A$, $8 \notin A$.

1.4 *METHODS OF DESCRIBING A SET*

There are two methods of describing a set.

(1) Roster Method.

In this method, a set is described by listing all its element, separating by commas and enclosing within curly brackets.

For Example. (i) If A is the set of odd natural numbers less than 10, then in roster form.

$$A = \{1, 3, 5, 7, 9\}$$

(ii) if B is the set of letters of the world FOLLOW, then in roster form.

$$B = \{F, O, L, W\}$$

(2) Set Builder Method.

Listing the element of a set is sometimes difficult and sometimes impossible. We do not have a roster form of the set or rational number or the set of real numbers. In set builder method, a set is described by means of some property which is shared by all the element of the set.

For Example. (i) If P is the set of all prime numbers, then

$$P = \{x : x \text{ is a prime number}\}$$

(ii) if A is the set of all natural numbers between 5 and 50, then

$$A = \{x : x \in N \text{ and } 5 < x < 50\}$$

1.5 *TYPES OF SETS*

(i) Finite set. A set is said to be finite if the number of its elements is

Finite i.e. its elements can be counted, by one by one, with counting

coming to end.

For Example. (a) the set of letters in the English alphabet is finite set since it has 26 elements.

(b) Set of all multiples of 10 less than 10000 is a finite set.

(ii) Infinite set. A set is said to be infinite if the number of its elements is infinite i.e. we count its elements, one by one, the counting never comes to an end.

For Example. (a) the set of all points in a straight line is an infinite set.

(b) the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ all are infinite sets.

(iii) Null Set. A set having no element is known as a null set or void set or an empty set and is denoted by $\emptyset$ or {}.

For Example. (a) $\{x : x \text{ is an integer and } x^2 = 3\} = \emptyset$, because there is no integer whose square is 3.

(iv) Singleton Set. A set having only one element is called a singleton set.

For Example. (a) {a} is a singleton set.

(b) {x: $x^3 + 1 = 0$ and x∈ $\mathbb{R}$} = { -1 } is a singleton set.

1.6 *SUBSET, SUPERSET AND POWER SET*

Set A is said to be a subset of Set B if all the elements of Set A are also present in Set B. In other words, set A is contained inside Set B. Example: If set A has {X, Y} and set B has {X, Y, Z}, then A is the subset of B because elements of A are also present in set B.

Subset Symbol

In set theory, a subset is denoted by the symbol ⊆ and read as 'is a subset of'.

Using this symbol we can express subsets as follows:

A ⊆ B; which means Set A is a subset of Set B.

Note: A subset can be equal to the set. That is, a subset can contain all the elements that are present in the set.

All Subsets of a Set

The subsets of any set consists of all possible sets including its elements and the null set. Let us understand with the help of an example.

Example: Find all the subsets of set A = {1,2,3,4}

Solution: Given, A = {1,2,3,4}

Subsets are {},{1}, {2}, {3}, {4}, {1,2}, {1,3}, {1,4}, {2,3}, {2,4}, {3,4},{1,2,3}, {2,3,4}, {1,3,4}, {1,2,4},{1,2,3,4}.

Superset Definition

In set theory, set A is considered as the superset of B, if all the elements of set B are the elements of set A. For example, if set A = {1, 2, 3, 4} and set B = {1, 3, 4}, we can say that set A is the superset of B. As the elements of B [(i.e.,)1, 3, 4] are in set A. We can also say that B is not a superset of A.

Superset Symbol

The superset relationship is represented using the symbol "⊃". For instance, the set A is the superset of set B, and it is symbolically represented by A ⊃ B.

Consider another example,

X = {set of polygons}, Y = {set of irregular polygons}

Then X is the superset of Y (X⊃Y). In other words, we can say that Y is a **subset** of X (Y⊂X).

Proper Superset

The proper superset is also known as a strict superset. The set B is the proper superset of set A, then all the elements of set A are in B, but set B must contain at least one element which is not present in set A.

For example, let us take four sets.

A = {a, b, c}, B = {a, b, c, d}, C = (a, b, c}, D = {a, b, e}

From the sets given above,

B is the proper superset of A, as B is not equal to A

C is a superset of set A, but the set C is not a proper superset of set A, as C = A

D is not a superset of A, as the set D does not contain the element "c" which is present in set A.

Power Set

The set of all subsets of a set A is called the power set of A and denoted by P(A).

i.e. P(A) = {S: S ⊂ A }.

For Example. (i) if A = {a}, then P(A) = {∅, A}

(ii) If B = {1, 2} then P{B} = {∅,{1}, {2}, B}

Theorem 1. Every set a subset of itself.

Proof. Let A is any set. Since x ∈ A ⟹ x ∈ A, therefore A ⊂ A.

Theorem 2. Empty set is a subset of every set.

Proof. Given two sets A and B, let A=∅.
By definition, A is a subset of B if and only if every element in A is also in B.
This means that A would not be a subset of B if there exists an element in A that is not in B.
However, there are no elements in A. This means there cannot exist an element in A that is not in B. Thus, A is a subset of B.
Since A = ∅ and B is an arbitrary set, the ∅ must be a subset of all sets.

Theorem 3. The empty set is unique.
Proof. Let $\emptyset_1 and\ \emptyset_2$ be two empty sets.

Since empty set is a subset of every set .

Therefore $\emptyset_1 \subset \emptyset_2$ and $\emptyset_2 \subset \emptyset_1$

$\Longrightarrow \emptyset_1 = \emptyset_2$ that proves the uniqueness of $\emptyset$.

Note: if a set has n elements, then the number of subsets is 2^n.

1.7 *OPERATIONS ON A SETS*

1. Union of Sets. The union of two sets X and Y is equal to the set of elements that are present in set X, in set Y, or in both the sets X and Y. This operation can be represented as;

X ∪ Y = {a: a ∈ X or a ∈ Y}

Let us consider an example, say; set A = {1, 3, 5} and set B = {1, 2, 4}
Then A ∪ B = {1, 2, 3, 4, 5}

Properties of Union of Sets

(i) For any two Sets A and B, A ⊂ $A \cup B$ or B ⊂ $A \cup B$

Proof. Let x be any element of A. then

x ∈ A $\Longrightarrow$ x ∈ $A \cup B$

therefore A ⊂ $A \cup B$

similarly, we can prove B ⊂ $A \cup B$

(ii) For any set A, $A \cup \emptyset$ = A.

Proof. $A \cup \emptyset$ = {x: x ∈ A or x ∈ ∅ }

= {x: x ∈ A } [$\because$ ∅ has no element]

= A

(iii) Union of sets is idempotent i.e. foe any set A, A∪ A = A.

Proof. A ∪ A = {x: x ∈ A or x ∈ A}

= {x: x ∈ A }

= A

(iv) Union of sets is commutative.

Proof. A ∪ B = {x: x ∈ A or x ∈ B}

= {x: x ∈ B or x ∈ A }

= B ∪ A

Note: Union of sets is Associative.

2. Intersection of Sets. The intersection of two sets X and Y is the set of all elements which belong to both X and Y. This operation can be represented as;

X ∩ Y = {a: a ∈ X and a ∈ Y}

Let us consider an example, say; set A = {1, 3, 5} and set B = {1, 2, 4}
Then A ∩ B = {1}

Properties of Intersection of Sets

(i) For any two sets A and B, $A \cap B \subset A$ and $A \cap B \subset B$.

Proof. Let x be any element of $A \cap B$. then

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

$\Rightarrow x \in A$ (in particular)

Therefore $A \cap B \subset A$

Similarly, we can prove $A \cap B \subset B$.

(ii) Intersection of sets is idempotent i.e. foe any set A, $A \cap A = A$.

Proof. $A \cap A = \{x: x \in A \text{ and } x \in A\}$

$= \{x: x \in A\}$

$= A$

(iii) Intersection of sets is commutative.

Proof. $A \cap B = \{x: x \in A \text{ and } x \in B\}$

$= \{x: x \in B \text{ and } x \in A\}$

$= B \cap A$

Note: Intersection of sets is Associative.

3. Difference of Sets. The difference of two sets A and B is the set of all elements which are in A but not in B.

The difference of sets A and B is denoted by A – B.

i.e. $A - B = \{x: x \in A \text{ and } x \notin B\}$

For example. (i) if $A = \{1, 2, 3, 4, 5\}$ and $B \{2, 4, 6, 8\}$, then $A - B = \{1, 3, 5\}$, $B - A = \{6, 8\}$.

Clearly, $A - B \neq B - A$

Note. The difference of sets is not commutative.

4. Complement of a Set. Let U be the universal set and $A \subset U$. then complement of A is the set of those elements of U which are not in A. the complement of A is denoted by A^c.

Symbolically, $A^c = U - A = \{x: x \in U \text{ and } x \notin A\} = \{x: x \notin A\}$

For example. If U is the set of all natural numbers and A is the set of even natural numbers, then

$A^c = U - A$

= the set of those natural numbers which are not even

= the set of odd natural numbers.

5. Symmetric Difference of Sets. If A and B are any two sets, then the sets $(A - B) \cup (B - A)$ is called the symmetric difference of A and B.

The symmetric difference of A and B is denoted by $A \Delta B$ and read as 'A symmetric difference B'.

For Example. If $A = \{a, b, c, d, e\}$ and $B = \{c, d, e, f, g\}$, then

$A - B = \{a, b\}$, $B - A = \{f, g\}$

Therefore A Δ B = (A – B) ∪ (B − A)

= {a, b} ∪ {f, g} = {a, b, f, g}.

1.8 *DE MORGAN'S LAWS*

For any two sets A and B, prove that

(a) $(\mathbf{A \cup B)^c = A^c \cap B^c}$ **(b)** $\mathbf{(A \cap B)^c = A^c \cup B^c}$

Proof. (a) We need to prove, $(A \cup B)^c = A^c \cap B^c$

Let X = $(A \cup B)^c$ and Y = $A^c \cap B^c$

Let p be any element of X, then p ∈ X ⇒ p ∈ $(A \cup B)^c$

⇒ p ∉ (A ∪ B)

⇒ p ∉ A or p ∉ B

⇒ p ∈ A' and p ∈ B'

⇒ p ∈ A' ∩ B'

⇒ p ∈ Y

∴ X ⊂ Y . . . (i)

Again, let q be any element of Y, then q ∈ Y ⇒ q ∈ A' ∩ B'

⇒ q ∈ A^c and q ∈ B^c

⇒ q ∉ A or q ∉ B

⇒ q ∉ (A ∪ B)

⇒ q ∈ $(A \cup B)^c$

⇒ q ∈ X

∴ Y ⊂ X . . . (ii)

From (i) and (ii) X = Y

$(A \cup B)^c = A^c \cap B^c$

(b) We need to prove, $(A \cap B)^c = A^c \cup B^c$

Let X = $(A \cap B)^c$ and Y = $A^c \cup B^c$

Let p be any element of X, then p ∈ X ⇒ p ∈ $(A \cap B)^c$

⇒ p ∉ (A ∩ B)

$\Rightarrow p \notin A$ and $p \notin B$

$\Rightarrow p \in A^c$ or $p \in B^c$

$\Rightarrow p \in A^c \cup B^c \Rightarrow p \in Y$

$\therefore X \subset Y$ ————(i)

Again, let q be any element of Y, then $q \in Y \Rightarrow q \in A^c \cup B^c$

$\Rightarrow q \in A^c$ or $q \in B^c$

$\Rightarrow q \notin A$ and $q \notin B$

$\Rightarrow q \notin (A \cap B)$

$\Rightarrow q \in (A \cap B)^c$

$\Rightarrow q \in X$

$\therefore Y \subset X$ ————(ii)

From (i) and (ii) X = Y

$(A \cap B)^c = A^c \cup B^c$

1.9 *CARTESIAN PRODUCT OF TWO SETS*

Given two non-empty sets A and B. The Cartesian product A × B is the set of all ordered pairs of elements from A and B,

i.e., $A \times B = \{(p, q): p \in A, q \in B\}$

If either P or Q is the null set, then A × B will also be an empty set,

i.e., $A \times B = \varphi$

For Example: if A = {1, 2} and B = {3, 4, 5}, then the Cartesian Product of A and B is A × B = {(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)}.

Cardinality of Cartesian Product?

The cardinality of Cartesian products of sets A and B will be the total number of ordered pairs in the A × B.

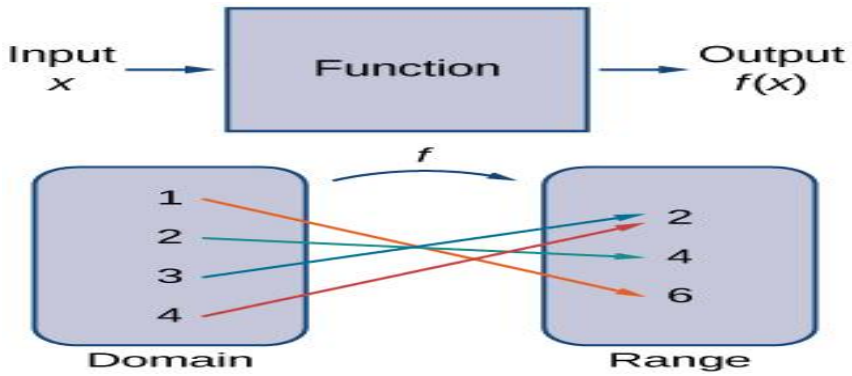
Let p be the number of elements of A and q be the number of elements in B.

So, the number of elements in the Cartesian product of A and B is pq.

i.e. if n(A) = p, n(B) = q, then $n(A \times B) = pq$.

1.10 *FUNCTIONS OR MAPPINGS*

A function can be visualized as an input/output device.



Let A & B be any two non-empty sets. If there exists a rule 'f ' which associates to every element x ∈ A, a unique element y ∈ B, then such rule 'f ' is called a function or mapping from the A to the set A to the
set B.
We write f: A ⟶ B read 'f ' is a function from X to Y.
The set **A** is called the domain of f and the set **B** is called the Co-domain of f.
Range of f = f(A) = {f(x): x ∈ A} , clearly f(A) ⊂ B.

1.11 KINDS OF *FUNCTIONS*

(1) Equal Functions. Let A and B be sets and f: A ⟶ B and f: B ⟶ A be functions. We say that f and g are equal and write f = g if f(a) = g(b) for all a ∈ A. If f and g are not equal, we write f ≠ g.

(2) One – One Function (Injective Function). A function f is one-to-one if every element of the range of g corresponds to exactly one element of the domain of f. One-to-one is also written as 1-1.
Formally, it is stated as, if f(x) = f(y) implies x=y, then f is one-to-one mapped, or f is 1-1.

Example. Show that f: R⟶ R defined as f(a) = $3a^3 - 4$ is one to one function?

Solution: Let f (a_1) = f (a_2) for all a_1 , $a_2 \in$ R

so $3a_1^3 - 4 = 3a_2^3 - 4$

$a_1^3 = a_2^3$

$a_1^3 - a_2^3 = 0$

$(a_1 - a_2)(a_1 + a_1a_2 + a_2^2) = 0$

$a_1 = a_2$ and $(a_1^2 + a_1a_2 + a_2^2) = 0$

$(a_1^2 + a_1a_2 + a_2^2) = 0$ is not considered because there are no real values of a_1 and a_2.

Therefore, the given function f is one-one.

(3) Onto Function (Surjective Function). Onto function could be explained by considering two sets, Set A and Set B, which consist of elements. If for every element of B, there is at least one or more than one element matching with A, then the function is said to be **onto function** or surjective function.

Note: To show that a function f is an onto function, put y = f(x), and show that we can express x in terms of y for any y ∈ B.

Example 1. Let A = {1, 5, 8, 9) and B {2, 4} And f ={(1, 2), (5, 4), (8, 2), (9, 4)}. Then prove f is a onto function.

Solution: From the question itself we get,

A={1, 5, 8, 9), B = {2, 4} & f={(1, 2), (5, 4), (8, 2), (9, 4)}

So, all the element on B has a domain element on A or we can say element 1 and 8 & 5 and 9 has same range 2 & 4 respectively.

Therefore, f: A → B is a surjective function.

Example 2. How to tell if this function is an onto function? g: R → R defined by $g(x) = 1 + x^2$

Solution: Given the function $g(x) = 1 + x^2$.
For real numbers, we know that $x^2 > 0$. So $1 + x^2 > 1$. $g(x) > 1$ and hence the range of the function is $(1, \infty)$. Whereas, the second set is R (Real Numbers). So the range is not equal to codomain and hence the function is not onto.

Example 3. If f: R → R defined as f(x) = 2x.

Solution. Let y = 2x then $x = \frac{y}{2}$

Thus, for every y R, we have $x = \frac{y}{2} \in R$ such that f(x) = y.

Thus, f is onto.

Example 4. Consider the function f: R → R defined as $f(x)= x^2$.

Solution. Let $y = x^2$ therefore $x = \pm \sqrt{y}$

The square of any real number is non-negative.

It means that $y \geq 0$.

Thus, for $y \leq 0$, we cannot find an element x such that f(x) = y.

Thus, the range of f(x) is the set of non-negative real numbers and the negative real numbers are not in the image of f(x).

As a result, f(x) is not onto.

Note: If you restrict the co-domain to $\mathbb{R}^{+} \cup \{0\}$, which is the set of non-negative real numbers, the function becomes onto.

1.12 *INVERSE FUNCTION*

Let f: A → B be a one – one and onto function. Then the function
g: B → A which associates to each element b ∈ B the unique element
a ∈ A such that f(a) = b is called the inverse function of f. the inverse function of f is denoted by f^{-1}.
Note: every function does not have an inverse. A function f: A → B has inverse iff f is one – one and onto. If f has inverse, then f is said to be invertible and f^{-1}: B → A. also if a ∈ A, then f(a) = b where b ∈ B
⟹ a = $f^{-1}(b)$.

1.13 *COMPOSITE OF FUNCTION*

Let f : A → B and g : B → C be two functions. Then the composition of f and g, denoted by g ∘ f, is defined as the function g ∘ f : A → C given by g ∘ f (x) = g(f (x)), ∀ x ∈ A.
Domain: f(g(x)) is read as f of g of x. In the composition of (f o g) (x) the domain of function f becomes g(x). The domain is a set of all values which go into the function.

Example: If f(x) = 3x+1 and g(x) = x^2, then f of g of x,

f(g(x)) = f(x^2) = $3x^2$+1.

If we reverse the function operation, such as f of f of x,

g(f(x)) = g(3x+1) = $(3x+1)^2$

Check your progress

True or false Questions

Problem 1. function f: R→ R, then f(x) = 2x is injective.

Problem 2. function f: R→ R, then f(x) = 2x+1 is not injective.

Problem 3. The onto function is also called the surjective function.

Problem 4. function f: R→ R, f(x) = |x| is an onto function.

Problem 5. In the surjective function, the range of the function "f" is equal to the codomain.

1.14 *SUMMARY*

1. A set is a well - defined collection of distinct objects.

2. $A \subseteq B$; which means Set A is a subset of Set B.

3. For any two sets A and B, $A \cap B \subset A$ and $A \cap B \subset B$.

4. (a) $(A \cup B)^c = A^c \cap B^c$ (b) $(A \cap B)^c = A^c \cup B^c$

5. Let f: $A \rightarrow B$ and g: $B \rightarrow C$ be two functions. Then the composition of f and g, denoted by $g \circ f$, is defined as the function $g \circ f$: $A \rightarrow C$ given by $g \circ f(x) = g(f(x))$, $\forall x \in A$.

1.15 GLOSSARY

- Numbers
- letters
- Collections of objects

1.16 *REFERENCES*

- T. M. Apostol, Mathematical Analysis (2nd Edition), Narosa Publishing House, 2002.
- R.G. Bartle and D.R. Sherbert, Introduction of real analysis (3rd Edition), John Wiley and Sons (Asia) P. Ltd., Inc. 2000.
- W. Rudin, Principles of Mathematical Analysis (3rd Edition), McGraw-Hill Publishing, 1976.

1.17 *SUGGESTED READING*

- S.C. Malik and Savita Arora, Mathematical Analysis (6th Edition), New Age International Publishers, 2021.
- Shanti Narayan, A course of Mathematical Analysis (29th Edition), S. Chand and Co., 2005.
- K. A. Ross, Elementary Analysis**,** The Theory of Calculus (2nd edition), Springer, 2013.

1.18 *TERMINAL AND MODEL QUESTIONS*

Q 1. Prove that the function f:$\mathbb{N} \longrightarrow \mathbb{N}$ is given by f(x) = x^2 is one – one function.

Q 2. Prove that the function f:$\mathbb{N} \longrightarrow \mathbb{N}$ is given by f(x) = x^2 is not onto function.

Q 3. Let A = [– 1, 1]. Then, discuss whether the following functions defined on A are one-one, onto or bijective.

(a) f(x) = $\frac{x}{2}$. (b) f(x) = x^2

Q 4. If f(x) = $3x^2$, then find (f ∘ f)(x).

Q 5. If f (x) = 2x and g(x) = x+1, then find (f ∘ g)(x) if x = 1.

1.19 *ANSWERS*

CHECK YOUR PROGRESS

CYQ 1. True

CYQ 2. False

CYQ 3. True

CYQ 4. False

CYQ 5. True

TERMINAL QUESTIONS

TQ 3. (a) One - One but not Onto.

(b) Not One - One and not Onto.

TQ 4. 27 X^2

TQ 5. 4

Unit-2: GROUPS

CONTENT:

2.1 *INTRODUCTION*

The founder of group theory is generally considered to be **Évariste Galois** (1811–1832), a French mathematician who developed the foundational concepts of the theory in the early 19th century. Galois introduced the idea of a group as a way to study the symmetries of the roots of polynomial equations, leading to what is now called **Galois theory**. This work laid the groundwork for understanding the solvability of polynomials and provided a deep connection between algebra and geometry.

Although Galois is credited with formalizing group theory, earlier contributions to the concept of groups were made by mathematicians such as **Joseph-Louis Lagrange**, who studied permutations in his work on equations, and **Carl Friedrich Gauss**, who considered

groups in the context of number theory. However, it was Galois who first explicitly defined and used the structure of a group as we understand it today.

Group theory is a fundamental branch of abstract algebra that studies algebraic structures known as groups, which consist of a set of elements combined with an operation that satisfies four core properties: closure, associativity, the existence of an identity element, and the existence of inverses. Groups serve as a unifying framework to explore and formalize the concept of symmetry in mathematics, science, and engineering, appearing naturally in diverse contexts such as geometry, number theory, and physics. They describe transformations that preserve structure, like rotations, reflections, or permutations, and provide a systematic way to study these transformations. Groups are categorized into different types, such as finite and infinite groups, abelian (commutative) and non-abelian (non-commutative) groups, and specific subtypes like cyclic, dihedral, and permutation groups. The study of group theory has profound applications, ranging from solving polynomial equations and analyzing crystal symmetries in chemistry to underpinning quantum mechanics, cryptography, and coding theory. Its abstract nature and wide applicability make group theory a cornerstone of modern mathematics.

2.2 *OBJECTIVES*

The main objectives of studying group theory are tailored to provide students with a foundational understanding of the subject and prepare them for advanced studies or applications. These objectives include:

1. **Understand the Basics of Group Theory**: Introduce students to the fundamental concepts of groups, including their definitions, properties, and examples, such as cyclic groups, permutation groups, and symmetry groups.
2. **Develop Problem-Solving Skills**: Teach students how to apply group-theoretic methods to solve mathematical problems, such as verifying group properties, analyzing subgroups, and working with cyclic and normal subgroups.
3. **Explore Group Structure**: Familiarize students with the structural aspects of groups, including Lagrange's theorem, order of elements, cosets, and the concept of normality and quotient groups.
4. **Connect with Other Areas of Mathematics**: Establish connections between group theory and other areas, such as linear algebra, number theory, and abstract algebra, to demonstrate its interdisciplinary nature.
5. **Develop Logical and Abstract Thinking**: Enhance students' ability to think logically and abstractly by analyzing and proving theorems within the framework of group theory.

These objectives align with the goal of equipping learners with both theoretical understanding and practical tools to analyze and apply permutation groups in various mathematical contexts.

By achieving these objectives, students in a B.Sc. course gain a strong foundation in group theory, which is essential for pursuing higher studies in mathematics or applying the concepts in related scientific fields.

2.3 *BINARY OPERATION*

A **binary operation** is an operation that combines two elements (operands) from a set to produce another element of the same set. Formally, if S is a set, a binary operation on S is a function:

$$*: S \times S \to S$$

Here, $*$ is the binary operation, and for any $a, b \in S, a * b \in S$. Here, we can also say that S is closed with respect to the binary operation $*$.

Examples 1: Addition on integers (*Z*): Let Z denotes the set of integers then "+" denote binary operation if,

$$+: Z \times Z \to Z$$

i.e., for all $a, b \in Z$ we should have $a + b \in Z$. Then we called "+" is the binary operation on Z.

e.g., if $3,5 \in Z$ then 3 + 5 = 8

Example 2: Multiplication on real numbers (*R*): Let R denotes the set of real numbers then "$\times$" or "." denote binary operation if,

$$\times: R \times R \to R$$

i.e., for all $a, b \in R$ we should have $a \times b \in R$. Then we called "." is the binary operation on R.

e.g., 2·3 = 6

Note 1: Throughout the book we will use multiplication by ".".

Note 2: If $|A| = n$, then $|A \times A| = n^2$. Hence, the number of elements from $A \times A$ to A are $(n)^{n^2}$.

Note 3: In general, we will say, $*$ is the binary operation on any set X if and only $a * b \in X$, for all $a, b \in X$.

Remarks 1: Every function from $A \times A$ to A defines a binary operation on A and conversely.

Remarks 2: Binary operation is always a function.

Some more examples on binary operation:

(i) On the set of natural number (N):

(i) $a * b = \min\{a, b\}$

(ii) $a * b = \max\{a, b\}$

(iii) $a * b = LCM(a, b)$

(iv) $a * b = GCD(a, b)$

(v) $a * b = a^b$

All, from (i) to (v) are binary operation on the set of natural numbers.

(B) On the set of real number (R):

(vi) $a * b = a + b$

(vii) $a * b = a.b$

(viii) $a * b = a + b + a.b$

(ix) $a * b = \frac{a+b}{2}$

(x) $a * b = a^b$

All, from (vi) to (ix) are binary operation on the set of real numbers (R) except (x) because $(-1)^{1/2} \notin R$

(C) On the set of positive real number (R^+): As we know that set of positive real number is $R^+ = \{x \in R \mid x > 0\}$

(xi) $a * b = a + b$

(xii) $a * b = a.b$

(xiii) $a * b = a^{\log_e b}$

(xiv) $a * b = \frac{a+b}{2}$

(xv) $a * b = a^b$

All, from (xi) to (xv) are binary operation on the set of positive real numbers.

(D) On the set of power set of natural number *P(N)*: As we know that power set of natural number is the collection of all the subset of natural number i.e., $P(N) = \{X \mid X \subset N\}$.

(xvi) $X * Y = X \cup Y$

(xvii) $X * Y = X \cap Y$

(xviii) $X * Y = X - Y$

(xix) $X * Y = (X - Y) \cup (Y - X)$

All, from (xvi) to (xix) are binary operation on the set of power set of natural number.

2.4 *GROUP*

To define the group we first need to focus some other important definitions and concepts related to group which will helpful to understand the concept of group more easily.

Algebraic Structure: A set equipped with one or more binary operation on it is called an algebraic structure.

e.g., $(R, +, .)$ is an algebraic structure because set of real number (R) is closed with respect to both the operation addition and multiplication.

Groupoid: A set equipped with one binary operation is defined as a groupoid.

e.g., (N, +), (N, .), (R, +), (R, .), (Z, +), (Z, .) are groupoid because these are closed with respect to their mentioned operation.

Semi-group: A groupoid with associative binary operation is called semi-group.

i.e., A set G along with the binary operation $*$ is called semi-group if it satisfies the following conditions.

(i) For all $a, b \in G$, $a * b \in G$. [Name as closed property]

(ii) For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$ [Name as associative property]

Example 3: (R, +) is semi group because for each $a, b, c \in R$, we always get

(i) $a + b \in R$
(ii) $a + (b + c) = (a + b) + c$

For e.g., $1, \frac{3}{2} \in R$ then $1 + \frac{3}{2} = \frac{5}{2}$, which is also an element of R i.e, $\frac{5}{2} \in R$.

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

Again, $1, \frac{3}{2}, \frac{-5}{4} \in R$ then $1 + \left(\frac{3}{2} + \left(\frac{-5}{4}\right)\right) = 1 + \left(\frac{3}{2} - \frac{5}{4}\right) = 1 + \frac{1}{4} = \frac{5}{4}$

And $\left(1 + \frac{3}{2}\right) + \left(\frac{-5}{4}\right) = \frac{5}{2} - \frac{5}{4} = \frac{5}{4}$

So, we can say that $1+\left(\frac{3}{2}+\left(\frac{-5}{4}\right)\right)=\left(1+\frac{3}{2}\right)+\left(\frac{-5}{4}\right)$

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

Similarly, we can check for any other elements of *R*.

Hence, we can say that (*R*, +) is semi group.

Monoid: A semi group $(G,*)$ is called monoid if there exist an element $e \in G$ such that for all $a \in G$, $a*e=a=e*a$. Such element (*e*) in a group *G* is called the identity element.

i.e., A set *G* along with the binary operation $*$ is called monoid if it satisfies the following conditions.

(i) For all $a,b \in G$, $a*b \in G$. [Name as closed property]

(ii) For all $a,b,c \in G$, $a*(b*c)=(a*b)*c$ [Name as associative property]

(iii) For all $a \in G, \exists\ e \in G$ such that $a*e=a=e*a$ [Name as existence of identity property]

Example 4: (*R*, +) is monid because for each $a,b,c \in R$, we always get

(i) $a+b \in R$
(ii) $a+(b+c)=(a+b)+c$
(iii) In *R*, there exist $0 \in R$ such that $a+0=a=0+a$ for all $a \in R$

We can understand (i) and (ii) from example 3.

For (iii), we know that in a set of real number the element "0" is such element which on addition with any real number always give the same element.

For e.g., $1+0=1=0+1$, $(-1)+0=-1=0+(-1)$, $\sqrt{2}+0=\sqrt{2}=0+\sqrt{2}$, $(-\sqrt{2})+0=-\sqrt{2}=0+(-\sqrt{2})$

Similarly, we can check these three properties for any other elements of *R*.

Hence, we can say that (*R*, +) is monoid.

Group: A monoid $(G,*)$ is called group if and only if each element of *G* possess its inverse with respect to the operation $*$.

i.e., A set *G* along with the binary operation $*$ is called group if it satisfies the following conditions.

(i) For all $a,b \in G$, $a * b \in G$. [Name as closed property]

(ii) For all $a,b,c \in G$, $a*(b*c) = (a*b)*c$ [Name as associative property]

(iii) For all $a \in G, \exists\ e \in G$ such that $a*e = a = e*a$ [Name as existence of identity property]

(iv) For all $a \in G, \exists\ b \in G$ such that $a*b = e = b*a$ [Name as existence of inverse property]

Here such element *b* is called the inverse of *a* 'OR' Most of the time, we denote inverse of the element *a* as a^{-1} (notation).

Note: If we say *a* is the inverse of *b* then we can also say that *b* is the inverse of *a*.

Example 5: (*R*, +) is group because for each $a,b,c \in R$, we always get

(i) $a+b \in R$

(ii) $a+(b+c) = (a+b)+c$

(iii) In *R*, there exist $0 \in R$ such that $a+0 = a = 0+a$ for all $a \in R$

(iv) In *R*, for each $a \in R$ we always get $-a \in R$ such that $a+(-a) = 0 = (-a)+a$

For e.g., $1+(-1) = 0 = (-1)+1 \Rightarrow$ Inverse of 1 is -1 i.e. $1^{-1} = -1$

Similarly, $\sqrt{2}+(-\sqrt{2}) = 0 = (-\sqrt{2})+\sqrt{2} \Rightarrow$ Inverse of $\sqrt{2}$ is $-\sqrt{2}$ i.e. $(\sqrt{2})^{-1} = -\sqrt{2}$

So, we can say that every element $a \in R$, we can always find $-a \in R$ such that on operation we get the identity element.

i.e., $a+(-a) = (-a)+a = 0$

Hence, we can say that (*R*, +) is group.

Abelian group: A group $(G,*)$ is called abelian group if it satisfies the commutative property.

i.e., A group $(G,*)$ is called abelian group if $\forall\ a,b \in G,\ a*b = b*a$.

e.g., (*R*, +) is abelian group, (*Z*, +) is abelian group

Note 1: Similarly, we can prove that $(Z,+),(Q,+),(C,+)$ are abelian group.

2: If the group is not abelian then we referred it as non-abelian group.

Note: Throughout this book, whenever we say G^* it means the set without zero element.

i.e., $G^* = G - \{0\}$.

e.g., $R^* = R - \{0\}$, $Q^* = Q - \{0\}$, $C^* = C - \{0\}$ etc.

Here, we can easily check that $(R^*,.),(Q^*,.),(C^*,.)$ are form group.

Example 6: Show that set of natural number *N* is not group with respect to addition.

Solution: As we know that set of natural number is closed with respect to addition i.e., addition of any two natural number is again a natural number. But in the set of natural we did not get any number $e \in N$ such that $a + e = a = e + a, \forall a \in N$. Generally, for addition 0 is the identity element because $a + 0 = a = 0 + a, \forall a \in N$ but $0 \notin N$.

Hence (*N*, +) does not satisfies the existence of identity property that why *N* is not group with respect to addition.

Example 7: Show that the set $G = \{..-3m, -2m, -m, 0, m, 2m, 3m, ...\}$ of multiples of integers by a fixed integer *m* is a group with respect to addition.

Solution: We can also define *G* as, $G = \{mz \mid m\, is\ fixed\, and\, z \in Z\}$

We will said the given set *G* is group with respect to the operation addition if it satisfies the following properties.

Closure property: Let $a, b \in G \Rightarrow a = rm, b = sm$ where, $r, s \in Z$.

Then $a + b = rm + sm = (r + s)m$

As we know that, $(Z,+)$ is group with respect to addition then $\forall r, s \in Z \Rightarrow r + s = l \in Z$

So, $a + b = (r + s)m = lm \in G$

Hence, *G* is closed with respect to addition.

Associative property: Since the element of *G* are all integers and we know that the $(Z,+)$ is group. Hence it will also satisfy the associative property.

Existence of identity: $0 \in G$ and we have $0 + a = a = a + 0, \forall a \in G$.

Existence of inverse: Let rm be any arbitrary element of *G*, where $r \in Z$. Since Z is closed with respect to addition then $-r \in Z$.

Then $(-r)m + rm = (-r + r)m = 0m = 0 \in G$

Similarly, $rm + (-r)m = (r - r)m = 0m = 0 \in G$

Hence, $-rm$ is the additive inverse of rm.

Thus every element of G possesses additive inverse of rm.

Hence G is a group with respect to addition.

Example 8: Show that the set of all positive rational numbers forms an abelian group under the composition defined by, $a*b=\frac{ab}{2}$

Solution: Let Q_+ denote the set of all positive rational number. If we define the operation $*$ such as $a*b=\frac{ab}{2}$, then we have to prove that pair $(Q_+,*)$ is a group.

Closure Property: As we know that in the set of positive rational number, $\forall a,b\in Q_+$, we have always $\frac{ab}{2}\in Q_+$. Hence Q_+ is closed with respect to the operation $*$.

Associative property: Let $a,b,c\in Q_+$ then,

$$(a*b)*c=\left(\frac{ab}{2}\right)*c=\left(\frac{ab}{2}\right)\frac{c}{2}=\frac{a}{2}\left(\frac{bc}{2}\right)=a*(b*c)$$

Existence of identity: Let us consider e be the identity element of Q_+ then $\forall a\in Q_+$, we have $a*e=a$ i.e., $\frac{ae}{2}=a\Rightarrow e=2$.

Similarly we can prove, $e*a=a$ i.e., $\frac{ea}{2}=a\Rightarrow e=2$.

So, $a*e=a=a*e\,\forall a\in Q_+$, here obviously we get $e=2$. Since $2\in Q_+$, thus we can say that $(Q_+,*)$ possess the identity element.

Existence of inverse: Let us consider a be the arbitrary element of Q_+. We say the element b be the inverse of a then we have $a*b=e$ i.e., $\frac{ab}{2}=e=2\Rightarrow b=\frac{4}{a}$. Now, $a\in Q_+$, then $\frac{4}{a}\in Q_+$ such that $(4/a)*a=2=a*(4/a)$. As a is the arbitrary element then we can say that each element of Q_+ possess its inverse element.

Hence, $(Q_+,*)$ is a group.

Commutativity: Let $a,b\in Q_+$. Then, $a*b=\frac{ab}{2}=\frac{ba}{2}=b*a$.

Hence, $(Q_+,*)$ is an abelian group.

2.5 *SOME GENERAL PROPERTIES OF GROUP*

Let us consider a non-empty subset equipped with a binary operation denoted by multiplication. Throughout this book, we assume the operation of multiplication (.) unless specified otherwise. The theorems and corollaries that hold true for the operation of multiplication will also be valid for other operations. Therefore, learners should not be confused by statements and theorems with respect to the operations.

Theorem 1: (Uniqueness of identity): The identity element in a group is unique.

Proof: To prove that identity element is unique we have to first consider the group *G* has two identity elements e and e'. Since *G* is group, then obviously $ee' \in G$ (by closure property).

If e is the identity then, $ee' = e'$ … (1)

If e' is the identity then, $ee' = e$ … (2)

But ee' is the unique element of G.

Therefore by (1) and (2) $ee' = e'$ and $ee' = e$

$\Rightarrow e' = e$

Hence, we now confirmed that identity element will be unique.

Theorem 2: (Uniqueness of inverse): The inverse of each element in a group is unique.

Proof: To prove that inverse of each element is unique we have to first consider the element '*a*' of a group *G* has two inverse elements b and c. Let *e* is the identity element of *G*.

If b is the inverse of *a* then $ab = e = ba$ … (1)

If c is the inverse of *a* then $ac = e = ca$ … (2)

Now, from (1) and (2)

$b(ac) = b(e) = be = b$ [As *e* is the identity element then, $be = b$]

Also, $(ba)c = (e)c = ec = c$ [As *e* is the identity element then, $ec = c$]

As *G* is group so it will be satisfy associative property with respect to composition multiplication.

Therefore, $(ba)c = b(ac) \Rightarrow b = c$

Hence inverse is unique.

Theorem 3: If the inverse of a is a^{-1}, then the inverse of a^{-1} is a *i.e.*, $(a^{-1})^{-1} = a$

Proof: Let *G* be the group and e be the identity element of the group. Also we have assumed that a^{-1} is the inverse element of any arbitrary element *a*. Then for any arbitrary element of $a \in G$. $a\,a^{-1} = e$ [By the concept of inverse in G]

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

$\Rightarrow a[(a^{-1})^{-1}a^{-1}] = (a^{-1})^{-1}$ [Group always satisfies the associative property]

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

Hence, $(a^{-1})^{-1} = a$

Note 1: The inverse of identity element is itself *i.e.*, $ee^{-1} = e = e^{-1}e$.

2: In the additive group inverse of any arbitrary element $a \in G$ is $-a$.

3: Generally in the additive group 0 is the identity element.

4: Generally in the multiplicative group 1 is the identity element.

Example 9: In a group *G*, show that $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$.

Solution: Let $a, b \in G$ and a^{-1}, b^{-1} are their inverse respectively. Then,

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

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

Now, $(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1}$ [composition is associative]

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

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

$= aa^{-1} = e$

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

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

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

Hence we have, $(ab)^{-1} = b^{-1}a^{-1}$.

Note 1: In additive notation the statement of this theorem will be, $-(a+b) = (-b) + (-a)$.

Note 2: It can be generalized by induction as follows:

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

Theorem 4: (Cancellation laws hold good in a group) If a,b,c are elements of *G*, then

$a\,b = a\,c \Rightarrow b = c$ (Left cancellation law)

and $b\,a = c\,a \Rightarrow b = c$ (Right cancellation law)

Proof: Let *G* be a group and $a \in G \Rightarrow a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$, where *e* is the identity element.

Now, $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$ [Multiplying both sides on the left by a^{-1}]

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

$\Rightarrow eb = ec$

$\Rightarrow b = c$

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

$\Rightarrow b(aa^{-1}) = c(aa^{-1}) \Rightarrow be = ce \Rightarrow b = c$

Note 1: In additive notation these results can be written as $a + b = a + c \Rightarrow b = c$

Example 10: If a,b,c are any two elements of a group *G*, then the equation $ax = b$ and $ya = b$ have unique solutions in *G*.

Solution: Let *G* be a group and $a \in G \Rightarrow a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$, where *e* is the identity element.

Since, $a \in G, b \in G \Rightarrow a^{-1} \in G, b \in G$

$\Rightarrow a^{-1}b \in G$ [By closure property]

Now, substitute $a^{-1}b$ for x in the left hand side of the equation $ax = b$, we have

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

Thus, $x = a^{-1}b$ is a solution in G of the equation $ax = b$.

Now, we have to show that the solution is unique. For it suppose that $x = x_1$ and $x = x_2$ are two solution of the equation $ax = b$.

Then, $ax_1 = b$ and $ax_2 = b$

$\Rightarrow ax_1 = ax_2$, then by left cancellation law,

$\Rightarrow x_1 = x_2$

Therefore, the solution is unique.

Similarly, we can prove that the equation $ya = b$ have unique solutions in *G*.

2.6 *SPECIAL GROUP*

In this section we will define some special types of group which are more roughly used in many units and are more useful to understand the similarities and dissimilarities of many groups.

Addition modulo *n*: We shall now define a new type of addition known as 'addition modulo *m*' and written as $a +_m b$, where *a* and *b* are any integer and *m* is a fixed positive integer.

Thus by definition we have, $a +_m b = r, 0 \le r < m$.

Where *r* is the least non-negative remainder when $a + b$ is divided by *m*. Which is read as "*a* is congruent to b modulo *m*"

e.g., $5 +_2 2 = 1$, since $5 + 2 = 7 = 2(3) + 1$ and when we divide (5+2) by 2 we get the remainder 1. Thus, we say $5 +_2 2 = 1$.

e.g., $15 +_4 3 = 2$, since $15 + 3 = 18 = 4(4) + 2$ and when we divide $(15 + 3)$ by 4 we get the remainder 2. Thus, $15 +_4 3 = 2$.

Note 1: $a +_m b = b +_m a$

2: When a and b are two integer such that $(a-b)$ is divisible by a fixed positive integer m, then we write $a \equiv b \pmod{m}$. Which is read as "a is congruent to b modulo m".

3: $a +_m (b +_m c) = a +_m (b + c)$

e.g., $15 +_4 (3 +_4 1) = 3 = 15 +_4 (3+1)$

Multiplication modulo *n*: Now define a new type of multiplication known as 'multiplication modulo m' and written as $a \times_m b$, where a and b are any integer and m is a fixed positive integer.

Thus by definition we have, $a \times_m b = r, 0 \le r < m$.

Where r is the least non-negative remainder when $a \times b$ is divided by m.

e.g., $5 \times_2 2 = 0$, since $5 \times 2 = 10 = 2(5) + 0$ and when we divide (5×2) by 2 we get the remainder 0. Thus, we say $5 \times_2 2 = 0$.

e.g., $15 \times_4 3 = 1$, since $15 \times 3 = 45 = 4(11) + 1$ and when we divide (15×3) by 4 we get the remainder 1. Thus, $15 \times_4 3 = 1$

Note 1: $a \times_m b = b \times_m a$

2: $a \times_m (b \times_m c) = a \times_m (b \times c)$

Example 11: (Additive group of integers modulo *m*) The set $G = \{0, 1, 2, ..., m-1\}$ of first m non-negative integer is a group, the composition being addition reduced modulo m.

Proof: Closed property: As we know by definition of addition modulo m.

$a +_m b = r$ where, $0 \le r \le m-1$. Therefore for all $a, b \in G$ we get $(a +_m b) \in G$. Hence G is closed with respect to the operation addition modulo m.

Associative property: Let $a, b, c \in G$ and m is fixed positive integer.

Then, $a +_m (b +_m c) = a +_m (b + c)$

$=$ The least non-negative remainder when $a + (b + c)$ is divided by m

$=$ The least non-negative remainder when $(a+b)+c$ is divided by m

$=(a+b)+_m c$

$=(a+_m b)+_m c$

Thus, $a+_m (b+_m c)=(a+_m b)+_m c$

Existence of identity: We have $0 \in G$, also if we have any $a \in G$ then, $0+_m a = a = a+_m 0$. Therefore, 0 is the identity element of *G*.

Existence of inverse: As 0 is the identity element so inverse of 0 is 0 itself. Also if *a* is any non-identity element of *G* then $m-a$ is also an element of G.

Now, $a+_m (m-a)=0$. Hence we can say that every non-identity element of G has inverse in G.

Commutative: $a+_m b =$ The least non-negative remainder when $a+b$ is divided by m

$=$ The least non-negative remainder when $b+a$ is divided by m

$=b+_m a$

i.e., $a+_m b = b+_m a$

Hence, $(G,+_m)$ is abelian group.

Note: In general, we denote $Z_m=\{0,1,2,...,m-1\}$ and say Z_m is abelian group with respect to the operation (w.r.t.) addition modulo *m i.e.*, $(Z_m,+_m)$ is abelian group.

e.g., $(Z_6,+_5)$, $(Z_2,+_2)$, $(Z_3,+_3)$ etc. are the abelian group.

***U*(*n*):** We will define an important group most commonly used in this book. Here, *U*(*n*) is the collection of all natural number less than *n* and relatively prime to *n* i.e.,

$U(n)=\{x \in N \mid x<n \text{ and } \gcd(x,n)=1\}$

e.g. $U(4)=\{x \in N \mid x<4 \text{ and } \gcd(x,4)=1\}=\{1,3\}$

e.g., $U(5)=\{1,2,3,4\}$

e.g., $U(8)=\{1,3,5,7\}$

Example 12: $U(n)$ is always an abelian group with respect to the operation multiplication modulo n ($\times_n$) for all $n \in N$.

Solution: As we know, $U(n)=\{x \in N \mid x<n \text{ and } \gcd(x,n)=1\}$.

Here, obviously if $a,b \in U(n)$ then $\gcd(ab,n)=1$

$\Rightarrow a \times_n b \in U(n)$ or in general we can say $ab \in U(n)$. Thus, $U(n)$ is closed w.r.t. operation $\times_n$.

As multiplication modulo *n* is associative and commutative both hence $U(n)$ will also.

Since, $1 \in U(n) \forall n \in N$ then 1 will be the identity of $U(n)$ i.e., $\forall a \in U(n)$,

$1 \times_n a = a \times_n 1 = a$

Now consider, $U(n)=\{a_1, a_2, ..., a_k\}$ for any $n \in N$

Let $a \in U(n)$ then, $\{aa_1, aa_2, ..., aa_k\}$ are also element of $U(n)$ as it is closed and none of the two elements of $\{aa_1, aa_2, ..., aa_k\}$ are same (Here it should be remember always that $aa_i = a \times_n a_i$).

If it is then, $a \times_n a_i = a \times_n a_j$ or $aa_i = aa_j$

$\Rightarrow aa_i \equiv aa_j \pmod{n}$

$\Rightarrow n \mid (aa_i - aa_j) \Rightarrow n \mid a(a_i - a_j)$

Since, $a \in U(n)$ and $\gcd(a,n)=1 \Rightarrow n \nmid a$

$\Rightarrow n \mid (a_i - a_j) \Rightarrow a_i - a_j \equiv 0 \pmod{n}$

$\Rightarrow a_i \equiv a_j \pmod{n}$

Hence all $\{aa_1, aa_2, ..., aa_k\}$ are distnict.

$\Rightarrow \exists a_r \in U(n)$ such that $a \times_n a_r = 1 = a_r \times_n a$

Which means a_r is the inverse of *a*. So, we can say every element of $U(n)$ has its inverse in $U(n)$. Thus, $U(n)$ is abelian group with respect to the operation multiplication modulo *n*.

Quaternion group (Q_8): An another important non-abelian group name as quaternion group and denoted by Q_8 and defined as,

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, which satisfies the rule,

$ij = k$ and $ji = -k$; $jk = i$ and $kj = -i$; $ki = j$ and $ik = -j$

Also, $i^2 = j^2 = k^2 = -1$ and $kj = -i$

Note: Q_8 is non-abelian group with respect to the operation multiplication.

2.7 *ORDER OF A GROUP*

The **order of a group** is the number of elements it contains, denoted by |*G*|. Sometime we name it as the cardinality of the group. A group may have finite element, countable element or uncountable elements. If any group *G* has finite element say *n* then we say group of order *n* otherwise we called group of infinite order.

e.g., (*R*, +) is infinite group.

Euler ϕ – function: A function from natural number (*N*) to natural number (*N*) such that

$\phi(n) =$ Collection of all natural number less than *n* and relatively prime to *n*. The mean of relatively prime is that whose g.c.d with *n* is 1.

If n is any natural number and $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ is the prime factorisation of *n*, then

$\phi(n) = (p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1})...(p_k^{n_k} - p_k^{n_k-1})$

e.g., $\phi(24) = \phi(2^3.3) = (2^3 - 2^2)(3-1) = 4.2 = 8$

Example 13: Find the order of the group $U(2^5)$.

Answer: Since order of $U(2^5)$ is $\phi(2^5)$.

We know that, $\phi(2^5) = 2^5 - 2^{5-1} = 32 - 16 = 16$

Note: If p is prime then, $\phi(p) = p - 1$

Check your progress

If $Z_5 = \{0,1,2,3,4\}$ and the operation $+_5$ then find the following problems.

Problem 1: Is $(Z_5, +_5)$ a group?

Problem 2: Find the order of the group $(Z_5, +_5)$.

Problem 3: Find the identity element of $(Z_5, +_5)$

Problem 4: Find the inverse element of the element of 4 in $(Z_5, +_5)$.

2.8 *SUMMARY*

This unit on group theory introduces the concept of a group, a fundamental structure in abstract algebra defined by a set and a binary operation satisfying closure, associativity, identity, and inverse properties. Key topics include examples of groups such as integers under addition and symmetric groups, classifications like Abelian and non-Abelian groups. On the basic of this we further study Subgroups, Lagrange's theorem (relating subgroup order to group order), normal subgroups, and quotient groups in upcoming units. The chapter explores the applications of group theory in understanding symmetry, transformations, and mathematical structures in various domains, providing tools for solving problems in geometry, physics, and beyond. Group theory has applications in diverse fields such as geometry, number theory, physics, and cryptography, making it a cornerstone of modern mathematics.

2.9 *GLOSSARY*

- Binary operation.
- Algebraic structure.
- Group.
- Semi group.
- Monoid.
- Abelian group.
- Order of the group.
- Euler ϕ – function.

- Addition modulo *n*.
- Multiplication modulo *n*.

2.10 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975),*Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.

2.11 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

2.12 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Show that the set of all positive rational numbers forms an abelian group under the composition defined by, $a*b=\frac{a+b+ab}{2}$.

2. Show that set of all matrices of order $n\times n$ with respect to the operation multiplication is form non-abelian group when $n\geq 3$.

3. Show that power set of natural number is form group with respect to the operation $*$ defined by, $X*Y=(X-Y)\cup(Y-X)$ where $X,Y\in P(N)$.

4. Show that set of natural number is form group with respect to the operation $*$ defined by, $a*b=GCD(a,b)$ where $a,b\in N$.

5. Show that set of natural number is form group with respect to the operation $*$ defined by, $a*b=LCM(a,b)$ where $a,b\in N$

6. Prove that Z_n is form group with respect to the operation addition modulo *n*.

Short Answer Type Question:

1. Prove that the Quaternion group Q_8 is group with respect to operation multiplication.

2. Find the order of the group $U(5^{99})$.

3. Prove that $U(8)$ is a group with respect to the operation multiplication modulo 8.

4. Prove that Z_5 is a group with respect to the operation addition modulo 5.

5. Prove that cancellation laws hold good in a group.

6. Is set of natural number forms a group with respect to operation addition? If No, then why?

Fill in the blanks:

1. A group *G* is a set equipped with a binary operation that satisfies four properties: closure, associativity, the presence of an ……. element, and the existence of ……. for each element.

2. A group *G* is called ……. if $ab = ba \forall a, b \in G$.

3. The identity element *e* of a group *G* satisfies the property …….

4. In any group *G*, the inverse of an element *a* is denoted by a^{-1} and satisfies ……..

5. A ……. is a non-empty set *G* with a binary operation that satisfies closure, associativity, identity, and inverse properties.

6. The …… of a group *G* is the total number of elements in *G*.

7. In a group *G*, $(ab)^{-1}$ = ……

Objective type questions:

1. **Which of the following is a necessary property of a group?**
a) Associativity
b) Commutativity
c) Distributivity
d) Reflexivity

2. **A group G is called Abelian if:**
a) *G* is finite
b) *G* has an identity element
c) *G* is commutative
d) *G* is cyclic

3. The identity element of a group *G*:
a) Is unique
b) Has no inverse
c) May not exist
d) Is not required to satisfy associativity

4. Which of the following is not a group under the usual operation?
a) The set of integers under addition
b) The set of rational numbers under multiplication
c) The set of natural numbers under addition
d) The set of real numbers under addition

5. A group with a finite number of elements is called:
a) Infinite group
b) Cyclic group
c) Finite group
d) Symmetric group

6. Which of the following groups is cyclic?
a) The set of integers under addition
b) The set of rational numbers under multiplication
c) The set of even integers under addition
d) The set of real numbers under multiplication

7. If *G* is a group, and $a, b \in G$, then $(ab)^{-1}$ equals:
a) ab^{-1}
b) $b^{-1}a^{-1}$
c) $a^{-1}b^{-1}$
d) $b^{-1}a$

8. In a group *G*, the identity element *e* satisfies:
a) $e^2 = e$
b) $e.g = g = g.e \forall\, g \in G$
c) $e^{-1} = e$
d) All of the above

True and False questions:

1. Every group has a unique identity element.
2. In a group, every element has a unique inverse.
3. The set of natural numbers under addition forms a group.
4. A group G is called Abelian if $ab = ba$ for all $a,b \in G$.
5. If G is a group, then the equation $ax = b$ always has a unique solution for x in G.
6. The identity element of a group G is always equal to 1.
7. The set of all even integers under addition forms a group.
8. A finite group cannot have an infinite subgroup.

9. The set of real numbers under multiplication forms a group.

10. The set of matrices under matrix multiplication always forms a group.

11. If G is a group and $a \in G$, then $(a^{-1})^{-1} = a$.

2.13 *ANSWERS*

Answer of check your progress:

Problem 1: Yes

Problem 2: 5

Problem 3: 0

Problem 4: 1

Answer of short answer type question:

2. 4×5^{98}

6. Set of natural number is not form a group with respect to operation addition because additive identity $0 \notin N$.

Answer of the objective type question:

1.	a)	**2.**	c)	**3.**	a)	**4.**	c)
5.	c)	**6.**	c)	**7.**	b)	**8.**	d)

Answer of the fill in the blanks:

1.	Identity, Inverses	**2.**	Abelian	**3.**	$e.a = a.e = a \forall a \in G$
4.	$a.a^{-1} = a^{-1}.a = e$	**5.**	Group	**6.**	Order
7.	$b^{-1}a^{-1}$				

Answer of True and False:

1.	True	**2:**	True	**3:**	False	**4:**	True
5:	True	**6:**	False	**7:**	True	**8:**	True
9:	False	**10:**	False	**11:**	True		

Unit-3: SUBGROUP

CONTENT:

3.1 *INTRODUCTION*

The concept of subgroups emerged as a part of the development of group theory in the 19th century. Group theory originated from the study of algebraic equations, particularly the work of **Évariste Galois** in the early 1830s. Galois introduced the idea of groups to analyze the solvability of polynomial equations, leading to what is now known as **Galois theory**. His work hinted at the importance of subsets of groups that retain group structure, laying the groundwork for subgroups.

Later, **Arthur Cayley** in the mid-1800s formalized the concept of groups and explored their properties systematically. Subgroups became an essential tool in understanding

the structure of larger groups. **Camille Jordan** and **Sophus Lie** further advanced the study of subgroups in the context of finite groups and continuous transformation groups, respectively.

By the late 19th and early 20th centuries, mathematicians like **Emmy Noether** and **Élie Cartan** expanded the application of subgroups to abstract algebra and geometry. The study of subgroups has since become a cornerstone of modern algebra, with applications in number theory, geometry, cryptography, and physics.

By studying subgroups, mathematicians gain a deeper understanding of the structure and behavior of groups, enabling them to explore more advanced concepts in abstract algebra and its applications.

3.2 *OBJECTIVES*

The objectives of studying **subgroups** in group theory are as follows:

1. **Understand Structural Hierarchies**: To analyze how a smaller subset of a group inherits the group properties and interacts with the larger group.
2. **Identify Symmetries**: Subgroups help in identifying specific symmetries or transformations within a group that hold unique significance.
3. **Simplify Problem-Solving**: By focusing on subgroups, problems involving complex groups can often be reduced to simpler components.
4. **Explore Properties**: To study properties like closure, associativity, identity, and inverses within smaller subsets and verify their subgroup status.
5. **Classify Groups**: Subgroups help in classifying groups by revealing internal structures, such as normal subgroups, cyclic subgroups, or center subgroups.
6. **Understand Generators**: Subgroups often arise from generators of a group and help in exploring cyclic structures.
7. **Applications in Science and Engineering**: Subgroups are used in symmetry analysis, cryptography, quantum mechanics, and other fields to isolate specific behaviors or properties of larger systems.

3.3 *SUBGROUP*

A **subgroup** is a subset of a group that itself forms a group under the same binary operation as the parent group. To qualify as a subgroup, the subset must satisfy the group axioms: closure, associativity, identity, and inverses. Subgroups are fundamental in understanding the internal structure of groups and play a key role in simplifying and solving problems in group theory. For example, the set of even integers is a subgroup of the integers under addition. Subgroups are used to explore the symmetries of objects, simplify complex group operations, and form the basis for advanced concepts like normal subgroups and quotient groups.

Definition: Let $(G,*)$ be a group and $H \subset G$, we say H is a subgroup of G if $(H,*)$ is group itself. **Generally, we *denoted* it as $H < G$.**

Throughout this book whenever we use the symbol $H < G$ it always mean that H is subgroup of G.

Note 1: The operation on group and its subgroup are always same. For e.g. as we know that set of integer (Z) is group with respect to the operation addition and $Z_5 = \{0,1,2,3,4\}$ is subset of Z but Z_5 is not subgroup of Z because the operation used in Z_5 is addition modulo 5 *i.e.*, operation on Z_5 and Z are not same.

Some useful subgroup corresponds to their respective group

(i) $(R,+) < (C,+)$

(ii) $(Q,+) < (R,+) < (C,+)$

(iii) $(mZ,+) < (Z,+) < (Q,+) < (R,+) < (C,+)$

(iv) $(Q^*,.) < (R^*,.) < (C^*,.)$

Note 1: For any $(G,*)$ the subset of i.e., $\{e\}$ and G itself are always subgroups of the group $(G,*)$. Here, $\{e\}$ is called **trivial subgroup** of $(G,*)$ and G itself called **improper subgroup** of $(G,*)$.

2: If $H < G$ such that $H \neq G$ then H is called **proper subgroup** of $(G,*)$. So, we can say that $\{e\}$ is also a proper subgroup of $(G,*)$.

Example 1: Find all the subgroup of the quaternion group (Q_8).

Solution: In the previous unit we have studied about the quaternion group form a non-abelian group with respect to the operation multiplication. As we know that $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, which satisfies the rule.

$ij = k$ and $ji = -k$; $jk = i$ and $kj = -i$; $ki = j$ and $ik = -j$

Also, $i^2 = j^2 = k^2 = -1$ and $kj = -i$

Now, we can easily check that the following subset of Q_8 like,

$H_1 = \{1\}$

$H_2 = \{1,-1\}$

$H_3 = \{1,-1,i,-i\}$

$H_4 = \{1,-1,j,-j\}$

$H_5 = \{1,-1,k,-k\}$

$H_6 = \{\pm 1,\pm i,\pm j,\pm k\} = Q_8$

Here, all $H_i, i = 1\ to\ 6$ are proper and improper subset of Q_8 and also these $H_i, i = 1\ to\ 6$ are form itself group with respect to the operation multiplication. Hence we can say these $H_i, i = 1\ to\ 6$ are subgroup of Q_8.

3.4 *ONE-STEP SUBGROUP TEST (OST)*

The **one-step subgroup test** is a straightforward technique used in group theory to check whether a given subset *H* of a group *G* is a subgroup of *G*.

Theorem 1: If $H \subset G$ such that $H \neq \phi$ then $H < G$ if and only if $\forall a,b \in H, a * b^{-1} \in H$. Where $*$ is the binary operation on *G*.

Proof: Let we assume that $\forall a,b \in H, a * b^{-1} \in H$.

Given $H \neq \phi \Rightarrow$ there exist an element $a \in H$.

$\Rightarrow a * a^{-1} \in H$, since we know that $a * a^{-1} = e$, which means identity element $e \in H$. So, we can say existence of identity element in *H*.

If $H = \{e\}$ only, then the theorem done because we know that $\{e\}$ is always a subgroup of any group called trivial subgroup of *G*.

But if $H \neq \{e\}$ then there exist $a(\neq e) \in H$ then by definition,

$a, e \in H \Rightarrow e * a^{-1} = a^{-1} \in H$, which means every non-identity element possesses its inverse in *H*. Therefore we can say that if $a \in H$ then $a^{-1} \in H$. So, we can say existence of inverse element in *H*.

Now, let $a,b \in H$ then obviously by definition $a^{-1}, b^{-1} \in H$

Now again $a \in H$ and $b^{-1} \in H$ then $a * (b^{-1})^{-1} \in H$ i.e., $a * b \in H$. So, we can say H is closed with respect to the operation $*$.

Since G is a group so it will satisfies the associativity property and hence its each subset will also the satisfies the associative property with respect to the operation $*$.

Conversely, Let we assume that $H \subset G$ is a subgroup of $(G,*)$. It means H itself is a group with respect to the operation $*$. So, if any elements $a, b \in H$ then there inverse will also belongs to the group i.e., $a^{-1}, b^{-1} \in H$. Now if $a, b^{-1} \in H$, then by closure property on group $a * b^{-1} \in H, \forall\, a, b \in H$.

Note 1: If G is a group with respect to the operation multiplication and $H \subset G$ such that $H \neq \phi$ then $H < G$ if and only if $\forall\, a, b \in H, ab^{-1} \in H$.

2: If G is a group with respect to the operation addition and $H \subset G$ such that $H \neq \phi$ then $H < G$ if and only if $\forall\, a, b \in H, a + (-b) \in H$ i.e., $a - b \in H$.

Algorithm for OST: To claim $H < G$ for given $H \subset G$.

Step 1: Show $H \neq \phi$

Hint: Think about the identity element $e \in H$

Step 2: Choose arbitrary $x, y \in H$ and write the property of $x \& y$ as member of *H*.

Step 3: Evaluate $x . y^{-1}$ and using step-2 show that $x . y^{-1} \in H$.

Example 2: Prove that set of integer is subgroup of set of real number with repsct to the operation addition.

Solution: To prove that the set of integers *Z* is a subgroup of the set of real numbers *R* under the operation of addition, we use the **subgroup criteria**. Specifically, we check that:

1. *Z* is non-empty.
2. *Z* is closed under addition.
3. *Z* is closed under taking inverses.

Step 1: *Z* is non-empty

The set of integers *Z* contains at least one element, e.g., 0∈Z. Hence, *Z* is non-empty.

Step 2: Closure under addition

If $a,b \in Z$, then their sum $a+b$ is also an integer *i.e.*, $(a+b \in Z)$. Since the integers are closed under addition, this property holds.

e.g., $1,-2 \in Z$ then $1+(-2)=1-2=-1 \in Z$

Step 3: Closure under inverses

For any integer $a \in Z$, its additive inverse $-a$ is also an integer ($-a \in Z$). Hence, *Z* is closed under taking inverses i.e., $a-(-a)=a+a=2a \in Z$ as $a \in Z$

e.g., $1,-2 \in Z$ then $1-(-2)=1+2=3 \in Z$

3.5 *TWO-STEP SUBGROUP TEST (TST)*

The **two-step subgroup test** is a two-step based technique used in group theory to check whether a given subset *H* of a group *G* is a subgroup of *G*.

Theorem 2: 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: If part: Let H be a subgroup of G then H must be closed with respect to the operation multiplication i.e., the composition in G. Therefore $a \in H, b \in H \Rightarrow ab \in H$.

Now, let $a \in H$ then $a^{-1} \in H$ as H is subgroup hence group itself. It means each element of H possesses its inverse in *H*.

Only if part: Since $a \in H, b \in H \Rightarrow ab \in H$, it means H is closed with respect to multiplication.

Associativity: Since *G* is a group so it will satisfies the associativity property and hence its each subset will also the satisfies the associative property with respect to the operation multiplication.

Existence of identity: Since the identity of the subgroup is the same as the identity of the group. Now, $a \in H \Rightarrow a^{-1} \in H$ [According to the condition]

Further, $a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H$

$\Rightarrow e \in H$ [From the given condition]

i.e., the identity *e* is an element of *H*.

Existence of inverse: Since $a \in H \Rightarrow a^{-1} \in H$, it means each element of *H* possesses its inverse. Hence *H* itself is a group for the composition in *G*. So *H* is a subgroup of *G*.

3.6 *ALGEBRA OF COMPLEXES OF A GROUP*

Any non-empty subset (*H*) of a group (*G*) is called the **complexes of the group**. IF H is closed with respect to the given operation then we say that the complex *H* is stable for the composition in the group *G* and that the composition in *G* has induced a composition in *H*. If for this induced composition H itself is a group, then *H* is called a subgroup of the group.

If H and K are two complexes of the group G then multiplication of complexes defined as,

$HK = \{hk \mid h \in H, k \in K\}$.

Obviously, $HK \subseteq G$. Thus *HK* is a complex of *G* consisting of the elements of *G* obtained on multiplying each member of *H* with each member of *K*.

Note: As we know that complex *H* is always a subset of the group *G* then the associativity and commutativity will always hold on complex *H*.

Example 3: Multiplication (Addition) of complexes is associative.

Solution: We have to prove that $(HK)L = H(KL)$.

Let *h, k, l* are arbitrary element of *H, K* and *L* respectively, so that $(hk)l \in (HK)L$

But, $(hk)l = h(kl) \in H(KL)$

$\Rightarrow (HK)L \subseteq H(KL)$ … (1)

Similarly, we can show that $H(KL) \subseteq (HK)L$ …. (2)

Hence, by (1) and (2) we get $(HK)L = H(KL)$.

Note: Whenever we say $HK = KH$, then it does not mean that we should have $hk = kh \forall h \in H \text{ and } \forall k \in K$. What we require is that each element of the set *HK* should be present in *KH* and each element of *KH* should be present in *HK*.

Inverse of a complexes: Let *H* be any complex of *G*. Then we define,

$H^{-1} = \{h^{-1} : h \in H\}$ *i.e.,* H^{-1} is the complexes of *G* consisting of the inverses of the element of *H*.

Theorem 3: If *H* and *K* are any two complexes of a group *G*, then $(HK)^{-1} = K^{-1}H^{-1}$.

Proof: Let x be any arbitrary element of $(HK)^{-1}$. Then,

$x = (hk)^{-1}, h \in H, k \in K$

$\Rightarrow x = k^{-1}h^{-1} \in K^{-1}H^{-1}$ $[h^{-1} \in H^{-1}, k^{-1} \in K^{-1}]$

$\therefore (HK)^{-1} \subseteq K^{-1}H^{-1}$ … (1)

Again let y be any arbitrary element of $K^{-1}H^{-1}$

Then $y = k^{-1}h^{-1}, k \in K, h \in H$

$y = (hk)^{-1} \in (HK)^{-1}$

Hence, $K^{-1}H^{-1} \subseteq (HK)^{-1}$ … (2)

By, (1) and (2) we get, $(HK)^{-1} = K^{-1}H^{-1}$

Theorem 4: If *H* is any subgroup of a group *G*, then $(H)^{-1} = H$. Also show that 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 $H^{-1} \subseteq H$

Again, $h \in H \Rightarrow h^{-1} \in H$

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

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

$\therefore H \subseteq H^{-1}$

Thus, we can say that $H = H^{-1}$

Note: If H is a complex of a group G and $H = H^{-1}$, then it is not necessary that H is a subgroup of G. For example, $H = \{-1\}$ is a complex 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 the multiplication.

Theorem 5: 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 subgroup of G, therefore $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$

$HH \subseteq H$

Now let h be any element of H. Then we can write $h = he$, where e is the identity element of G. Now, $he \in HH$, since $h \in H, e \in H$

Thus $H \subseteq HH$.

Hence, $H = HH$

3.7 *PROPERTIES OF SUBGROUPS*

Theorem 6: A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that $HH^{-1} \subseteq H$.

Proof: The condition is necessary: It is given that H is a subgroup of G. Let ab^{-1} be any arbitrary element of HH^{-1}. Then $a \in H, b \in H$.

Since H itself is a group, therefore $b \in H \Rightarrow b^{-1} \in H$.

Thus $a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Hence, $HH^{-1} \subseteq H$.

The condition is sufficient: It is given that $HH^{-1} \subseteq H$.

Let $a \in H, b \in H \Rightarrow ab^{-1} \in HH^{-1}$. Since $HH^{-1} \subseteq H$, therefore $ab^{-1} \in HH^{-1} \Rightarrow ab^{-1} \in H$. Thus $a \in H, b \in H \Rightarrow ab^{-1} \in H$. Since H is a subgroup of G.

Corollary 1: : A necessary and sufficient condition for a non-empty subset *H* of a group *G* to be a subgroup is that $HH^{-1} = H$.

Proof: The condition is necessary: Suppose *H* is a subgroup of *G***,** then by theorem $HH^{-1} \subseteq H$.

Now *H* is a subgroup of *G*. Therefore $e \in H$. If *h* is any arbitrary element of *H*, then

$h = he = he^{-1} \in HH^{-1}$ $[\because h \in H, e^{-1} \in H^{-1}]$

$\therefore H \subseteq HH^{-1}$

Hence, $HH^{-1} = H$

The condition is sufficient: It is given that $HH^{-1} = H$.

$\therefore HH^{-1} = H$

Hence by theorem, *H* is subgroup of *G*.

Theorem 7: If *H*, *K* are two subgroup of a group G, then *HK* is a subgroup of G, iff $HK = KH$.

Proof: Let us consider *H*, *K* are two subgroup of a group G and $HK = KH$ then we have to prove that *HK* is a subgroup of G. So, we have only to show that $(HK)(HK)^{-1} = HK$ (By corollary 1)

We have, $(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1}) = H(KK^{-1})H^{-1}$

$= (HK)H^{-1}$ $[\because K \text{ is a subgroup} \Rightarrow KK^{-1} = K]$

$= (KH)H^{-1}$ $[HK = KH]$

$= K(HH^{-1})$

$= KH$ $[\because H \text{ is a subgroup} \Rightarrow HH^{-1} = H]$

$\because HK = KH \Rightarrow HK$ is a subgroup of *G*.

Conversely, suppose that *HK* is a subgroup.

Then, $(HK)^{-1} = HK$

$\Rightarrow K^{-1}H^{-1} = HK$ [$\because K$ is a subgroup $\Rightarrow K^{-1} = K$ and similarly, $\Rightarrow H^{-1} = H$]

Note: If *H, K* are subgroups of an abelian group *G*, then *HK* is a subgroup of *G*.

Theorem 9: If H_1 and H_2 are two subgroup of a group *G*, then $H_1 \cap H_2$ is also a subgroup of *G*.

Proof: Let H_1 and H_2 are two subgroup of a group *G* then we have to show that $H_1 \cap H_2$ is also a subgroup of G. To prove this we will use the one step subgroup test.

For it let, $a, b \in H_1 \cap H_2$ then we have only to show that $ab^{-1} \in H_1 \cap H_2$.

Now if $a, b \in H_1 \cap H_2 \Rightarrow a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$

$\Rightarrow a \in H_1$ and $a \in H_2$, Similarly, $b \in H_1$ and $b \in H_2$.

Further, $a \in H_1, b \in H_1 \Rightarrow ab^{-1} \in H_1$ [As H_1 is subgroup then by one step subgroup test]

Similarly, $b \in H_1, b \in H_2 \Rightarrow ab^{-1} \in H_2$ [As H_2 is subgroup then by one step subgroup test]

So, we have $ab^{-1} \in H_1$ and $ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Hence, we achieved that if $a, b \in H_1 \cap H_2$ then $ab^{-1} \in H_1 \cap H_2$. So, we can claim that $H_1 \cap H_2$ is also a subgroup of *G* if H_1 and H_2 are two subgroup of the group *G*.

Corollary 2: Arbitrary intersection of subgroups of a group is also a subgroup of the group.

Proof: Let G be a group and $\{H_t \mid t \in T\}$ be the family of subgroups H_t of the group G, where *T* be the indexed set. We have to show that $H = \cap\{H_t \mid t \in T\}$ is also the subgroup of G.

For it let, $a, b \in \cap\{H_t \mid t \in T\} \Rightarrow a \in H_t$ and $b \in H_t \; \forall \, t \in T$

Now, $a, b \in H_t \Rightarrow ab^{-1} \in H_t$ for all $t \in T$. As H_t is arbitrary subgroup from the family of subgroup $\{H_t \mid t \in T\}$ hence we get,

$a, b \in \cap\{H_t \mid t \in T\} \Rightarrow ab^{-1} \in \cap\{H_t \mid t \in T\}$ [Because H_t are subgroups for all $t \in T$]

Thus, arbitrary intersection of subgroups of a group is also a subgroup of the group.

Example 4: Show by suitable example that the union of two subgroup is not necessarily a subgroup while intersection of subgroup is a subgroup.

Solution: As we know that set of integer (Z) is a group with respect to the operation addition. Also, we know that mZ, m is fixed integer is a subgroup of Z. So, we can say that

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

And $3Z = \{0, \pm 3, \pm 6 \pm 9, ...\} = \{...-9, -6, -3, 0, 3, 6, 9, ...\}$ are two subgroup of Z.

Now, $2Z \cup 3Z = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9...\}$.

Now, $2 \in 2Z \cup 3Z$ and $3 \in 2Z \cup 3Z$ but $3+2=5 \notin 2Z \cup 3Z$. Hence, $2Z \cup 3Z$ is not closed with respect to the operation addition. So, we can say that union of two subgroup is not necessarily a subgroup.

$2Z \cap 3Z = \{0, \pm 6, \pm 12, \pm 18, ...\}$

Theorem 10: Union of two subgroups is a subgroup if and only if one is contained in the other.

Proof: Let H_1, H_2 are two subgroups of a group G and also we consider that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. Then obviously,

If $H_1 \subseteq H_2$ then $H_1 \cup H_2 = H_1 \Rightarrow H_1 \cup H_2$ is subgroup as H_1 is subgroup;

And if $H_2 \subseteq H_1$ then $H_1 \cup H_2 = H_2 \Rightarrow H_1 \cup H_2$ is subgroup as H_2 is subgroup.

Thus, if one subgroup is contained in the other subgroup then union of two subgroups is a subgroup.

Conversely, suppose that $H_1 \cup H_2$ is subgroup where H_1, H_2 are two subgroups. So, we have to prove that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

For it, let we suppose that H_1 is not subset of $H_2 \Rightarrow \exists a \in H_1$ and $a \notin H_2$ … (1)

And if, H_2 is not subset of $H_1 \Rightarrow \exists b \in H_2$ and $b \notin H_1$ … (2)

Now, from (1) and (2), we get $a \in H_1 \cup H_2$ and $b \in H_1 \cup H_2$.

Since we have $H_1 \cup H_2$ is subgroup, therefore $ab = c$ (say) is also an element of $H_1 \cup H_2$.

But $ab = c \in H_1 \cup H_2 \Rightarrow c \in H_1$ or $c \in H_2$

Suppose $ab = c \in H_1$ then $b = a^{-1}c \in H_1$ [$\because H_1$ is a subgroup, therefore $a \in H_1 \Rightarrow a^{-1} \in H_1$]

But from (2), we have $b \notin H_1$. Thus we get a contradiction.

Again suppose $ab = c \in H_2$ then $a = cb^{-1} \in H_2$ [$\because H_2$ is a subgroup, therefore $b \in H_2 \Rightarrow b^{-1} \in H_2$]

But from (1), we have $a \notin H_2$. Thus here also we get a contradiction.

Hence either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Hence the theorem proved.

Example 5: Can an abelian group have a non-abelian subgroup?

Solution: Since every subgroup of an abelian group is abelian. If *G* is an abelian group and *H* is a subgroup of *G*, then the operation on *H* is commutative because it is already commutative in *G* and *H* is a subset of *G*. Hence an abelian group cannot have a non-abelian subgroup.

Example 6: Can a non-abelian group have a abelian subgroup?

Solution: A non-abelian group can have [an abelian subgroup]. For example the quaternian group Q_8 is non-abelian while its subgroup $H = \{1, -1, i, -i\}$ is abelian subgroup.

Example 7: Can a non-abelian group have a non-abelian subgroup?

Solution: A non-abelian group can have a non-abelian subgroup. For example, as we know that every group *G* has *G* and $\{e\}$ are its two ready-made subgroup. Similary, the quaternian group Q_8 has Q_8 and $\{e\}$ are two its subgroup where Q_8 is non-abelian. So we can say that a non-abelian group have a non-abelian subgroup.

Check your progress

If $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is a group with respect to the operation multiplication then find the following problems.

Problem 1: Is $H_1 = \{1, -1\}$ a subgroup group of Q_8 ?

Problem 2: Is $H_2 = \{1, -1, j, -j\}$ a subgroup group of Q_8 ?

Problem 3: Is $H_2 = \{1, -1, k, -k\}$ a subgroup group of Q_8?

Problem 4: Find the abelian and non-abelian subgroup of Q_8?

3.8 *SUMMARY*

The unit on subgroups explores the concept and properties of subgroups within the context of group theory. It begins by defining a subgroup as a subset of a group that itself satisfies the group axioms: closure, associativity, the existence of an identity element, and inverses. The unit introduces key criteria like the **subgroup test**, which states that a non-empty subset is a subgroup if it is closed under the group operation and inverses. Examples of subgroups, including trivial and improper subgroups, are discussed to illustrate the concept. The unit also delves an important role to learn about Lagrange's Theorem, which relates the order of a subgroup to the order of the parent group, and the concept of cyclic subgroups generated by a single element, which we will learned later. Overall, this unit emphasizes the utility of subgroups in analyzing the structure and symmetry of groups.

3.9 *GLOSSARY*

- Subgroup.
- One-step subgroup test.
- Two-step subgroup test.
- Complexes of the group.

3.10 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975),*Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.

3.11 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

3.12 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Show that a necessary and sufficient condition for a non-empty subset H of a finite group G to be a sub-group is that $a \in H, b \in H \Rightarrow ab \in H$.

2. If G is a group, the centre of G, $Z(G)$ is defined by, $Z(G) = \{z \in G \mid zx = xz \forall\, x \in G\}$. Prove that $Z(G)$ is a subgroup of G.

3. If $a \in G$ we define $N(a) = \{x \in G \mid xa = ax\}$. Prove that $N(a)$ is a subgroup of G.

4. Let G be a group, H is a subgroup of G. Let for $x \in G$, $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$. Prove that xHx^{-1} is a subgroup of G.

5. Show that integral multiple of 5 form a subgroup of the additive group of integers.

6. Show that all those element of an abelian group G which satisfy the relation $a^2 = e$ constitute a subgroup of G.

Short Answer Type Question:

1. Let H be a subgroup of a group G and define $T = \{x \in G : xH = Hx\}$ then prove that T is a subgroup of G.

2. Define a subgroup with examples. What is the difference between a complex and a subgroup of a group.

3. Give an example of a non-abelian group G which has the property that every proper subgroup of G is abelian.

4. Show that a group can never be expressed as the union of two of its proper subgroup.

Fill in the blanks:

1. A subset H of a group G is a subgroup if it is _____ under the group operation and contains the _____ of G.

2. The identity element of a subgroup H is the same as the _____ element of the parent group G.

3. A subgroup H is called a _____ subgroup if it only contains the identity element.

4. If a is an element of a group G, the set of all powers of a, $\{a^n \mid n \in Z\}$, forms a _____ subgroup of G.

5. A non-empty subset H of a group G is a subgroup if $a, b \in H$ implies _____ in H, and $a^{-1} \in H$.

6. The subgroup generated by an element $g \in G$ is called the _____ subgroup of G.

7. The _____ subgroup of any group G is G itself.

Objective type questions:

1. Which of the following is **NOT** a requirement for a subset H of a group G to be a subgroup?
- a) H is non-empty.
- b) H is closed under the group operation.
- c) H contains all elements of G.
- d) H is closed under inverses.

2. The set of integers under addition forms a group. Which of the following subsets is a subgroup?
- a) The set of all odd integers.
- b) The set of all even integers.
- c) The set of all positive integers.
- d) The set of all negative integers.

3. If H is a subgroup of a group G, then:
- a) H must be finite.
- b) H must contain at least two elements.
- c) The identity element of G is in H.
- d) H must be equal to G.

4. If H is a subgroup of G, which of the following must hold?
- a) H is closed under addition.
- b) H contains the identity element of G.
- c) H is closed under multiplication.
- d) H contains the inverse of each of its elements.

5. Which of the following is not a criterion for $H \subseteq G$ to be a subgroup?
- a) $H \neq \varphi$
- b) H is closed under the group operation
- c) For all $a, b \in H, ab^{-1} \in H$
- d) H is commutative

6. The intersection of two subgroups of a group *G*:
- a) Is always a subgroup of *G*
- b) Is never a subgroup of *G*
- c) Depends on the group *G*
- d) Is equal to *G*

7. If *H* and *K* are subgroups of a group **G**, then $H \cap K$
- a) Is always a subgroup of *G*
- b) Is a subgroup only if $H \subseteq K$ or $K \subseteq H$
- c) Is never a subgroup of *G*
- d) Is a subgroup if $H \cap K = \varphi$

8. A subgroup *H* of *G* is called proper if:
- a) $H = G$
- b) $H \neq G, H \neq \{e\}$
- c) $H \neq G$
- d) $H \subseteq G$

9. A nonempty subset *H* of a group *G* is a subgroup if and only if:
- a) *H* is closed under the group operation
- b) *H* is closed under inverses and the group operation
- c) *H* is closed under scalar multiplication
- d) *H* satisfies $gh^{-1} \in H \; \forall \, g, h \in H$

10. If *G* is a finite group and *H* is a subgroup of *G*, then the order of *H*:
- a) Divides the order of *G*
- b) Equals the order of *G*
- c) Must be prime
- d) Is always odd

11. If *H* is a subgroup of *G* and $g \in G$, gHg^{-1}:
- a) Is always a subgroup of *G*
- b) Is never a subgroup of *G*
- c) Is equal to *H*
- d) Is equal to *G*

12. A subgroup *H* of a group *G* is normal if and only if:
- a) $gH = Hg$ for all $g \in G$
- b) *H* is abelian
- c) *H* is cyclic
- d) *H* is finite

True and False questions:

1. Every group has exactly one trivial subgroup.

2. The identity element of a group does not necessarily belong to its subgroups.

3. The union of two subgroups is always a subgroup.

4. A non-empty subset of a group is a subgroup if it is closed under the group operation and inverses.

5. If *H* is a subgroup of *G*, then *H* must also be a normal subgroup.

6. The center of a group *G* is always a normal subgroup of *G*.

7. If *G* is a finite group and *H* is a subgroup of *G*, then the order of *H* divides the order of *G*.

8. The intersection of any two subgroups of a group is always a subgroup.

9. A group with no proper non-trivial subgroups is called a simple group.

10. The union of all subgroups of a group *G* forms a subgroup of *G*.

11. If *H* is a proper subgroup of *G*, then *H* must be finite.

3.13 *ANSWERS*

Answer of check your progress:

Solution 1: Yes.

Solution 2: Yes.

Solution 3: Yes.

Solution 4: The abelian subgroup of Q_8 are $H_1 = \{e\}, H_2 = \{1,-1\}, H_3 = \{1,-1,i,-i\}$, $H_4 = \{1,-1,j,-j\}$, $H_5 = \{1,-1,k,-k\}$

The non-abelian subgroup of Q_8 are Q_8.

Answer of the objective type question:

1.	c	**2.**	b	**3.**	c	**4.**	b, c, d
5.	d	**6.**	a	**7.**	c	**8.**	c
9.	d	**10.**	a	**11.**	a	**12.**	a

Answer of the fill in the blanks:

1.	Closed, Identity element	**2.**	Identity	**3.**	Trivial
4.	Cyclic	**5.**	*ab*	**6.**	Cyclic
7.	Improper				

Answer of True and False:

1.	True	**2.**	False	**3.**	False	**4.**	True
5.	False	**6.**	True	**7.**	True	**8.**	True
9.	True	**10.**	False	**11.**	False		

Unit-4: CYCLIC GROUP AND LAGRANGE'S THEOREM

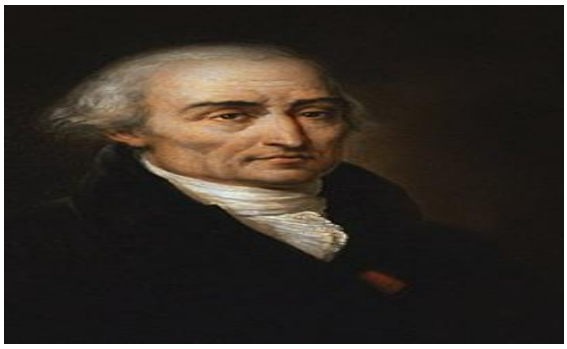
CONTENT:

4.1 *INTRODUCTION*

Joseph-Louis Lagrange made significant contributions to **abstract algebra**, particularly in **group theory** and **permutation theory**. His most famous result, **Lagrange's Theorem**, established that the order of a subgroup divides the order of a finite group, laying

the groundwork for later developments in group theory. His work in **permutation groups** influenced Évariste Galois, leading to the foundation of **Galois theory**, which connects group theory with field theory and polynomial equations. Lagrange also studied **resolvents in algebraic equations**, contributing to the understanding of polynomial roots and their symmetries. His insights into number theory and modular arithmetic played a key role in the development of modern algebraic structures, influencing later mathematicians like Cauchy and Galois.

Joseph-Louis Lagrange (born Giuseppe Luigi Lagrangia or Giuseppe Ludovico De la Grange Tournier; 25 January 1736 – 10 April 1813), also reported as Giuseppe Luigi Lagrange or Lagrangia, was an Italian mathematician, physicist and astrono mer, later naturalized French. He made significant contributions to the fields of analysis, number theory, and both classical and celestial mechanics.



Joseph-Louis Lagrange

25 January 1736 – 10 April 1813

https://images.app.goo.gl/Goewxm3NQYvFwhrP7

Lagrange's theorem provides crucial insights into the possible sizes of subgroups within a given group and serves as a foundational tool for further studies in algebra, such as in the classification of groups and the study of cosets. However, it does not guarantee the existence of subgroups of every divisor of |G|, only that such sizes are possible.

In this unit we will also learn about the cyclic group. The concept of **cyclic groups** has its roots in the early development of **group theory**, which emerged in the 18th and 19th centuries. The origins of cyclic groups can be traced back to the work of **Joseph-Louis Lagrange (1736–1813)**, who studied permutations and the structure of algebraic equations. However, the formal definition and deeper exploration of cyclic groups came later with **Évariste Galois (1811–1832)**, whose work on **Galois theory** introduced the idea of groups associated with polynomial equations.

In the 19th century, **Augustin-Louis Cauchy (1789–1857)** and **Camille Jordan (1838–1922)** further developed group theory, formalizing concepts like group order, generators, and cyclic subgroups. Cyclic groups were recognized as fundamental building blocks of **finite groups**, playing a crucial role in **modular arithmetic** and number theory, as seen in the works of **Carl Friedrich Gauss (1777–1855)**. Over time, cyclic groups became central in **abstract algebra**, influencing **ring theory, field theory, and cryptography**. Today, they are one of the most basic and widely used algebraic structures in mathematics.

4.2 *OBJECTIVES*

The **objectives** of studying the unit on **cyclic groups and Lagrange's theorem** in abstract algebra are as follows:

1. **Understanding the Concept of Cyclic Groups** – Define cyclic groups and explore their properties, including generation by a single element.

2. **Classification of Cyclic Groups** – Differentiate between **finite and infinite cyclic groups** and understand their structures.

3. **Exploring Generators** – Identify generators of cyclic groups and determine the conditions under which an element can generate the entire group.

4. **Subgroups of Cyclic Groups** – Prove that every subgroup of a cyclic group is also cyclic and characterize the subgroups of finite cyclic groups.

5. **Order of Elements** – Understand the relationship between the order of an element and the order of the group, including how to compute element orders.

6. **Lagrange's theorem**- Understand the concept of Lagrange's theorem and its implementation.

By the end of the chapter, students should have a strong foundational understanding of cyclic groups and their significance in algebra and applied mathematics.

4.3 *ORDER OF GROUP*

Definition: Let $(G,*)$ be a group then we say G is finite or infinite group, as number of elements in G are finite or infinite.

When G is finite set say n, then we denote cardinality i.e., $Card(G) = |G| =$ The order of $G = O(G) = n$.

Else, we say G is infinite group instead of saying G is infinite order group.

For e.g., $O(Q_8) = 8$, $O(Z_5) = 5$, $Card(U(8)) = Card(\{1,5,7,11)\}, \times_{12}\} = 4$.

4.4 *GENERATION OF ELEMENT*

Let $(G,*)$ be a group then, if $a \in G \Rightarrow a^{-1} \in G$ and $\forall m \in N, a^m \in G, (a^{-1})^m \in G$

i.e., $a^m, a^{-m} \in G$

Note: We will write $a^0 = e$ *i.e.,* $a^m.a^{-m} = e \Rightarrow a^0 = e$

Then define, $S = \{a^m \mid m \in Z\} \subset G$

Then S is called the subset generated by *a* and denoted by $< a >$

i.e., $< a >= S = \{a^m \mid m \in Z\}$

$\Rightarrow \forall a \in G, < a >= S = \{a^m \mid m \in Z\} \subset G$

e.g., If $G = Q_8$ and $a = i$, then $< i >= \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$

e.g., If $G = U(15) = \{1, 4, 5, 7, 8, 11, 13, 14\}$ is a group with respect to the operation $\times_{15}$. As $4 \in U(15)$ then

$< 4 >= \{4, 4^2, 4^3, ...\} = \{4, 1, 4, 1, ...\} = \{1, 4\}$

4.5 *ORDER OF AN ELEMENT*

Let *G* be a group and $a \in G$, then the order of element a is defined as the cardinality of the set $S =< a >$ and denoted by $O(a)$.

i.e., for $a \in G$, $O(a) = |< a >| = | S |$

if $< a >$ is infinite set then we say a is an element of infinite order.

Observation: If $a \in G$ such that $| S | = |< a >| = m$

$\Rightarrow < a >= \{a, a^2, a^3, ..., a^m = e\}$

i.e., $a, a^2, a^3, ..., a^n, a^{n+1}, ... \in < a >$

claim as, $|< a >| = m$

$< a >= \{a, a^2, a^3, ..., a^m = e\}$.

Let $n \in Z$ then $n = mq + r, 0 \le r < m$

$a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q . a^r = e^a . a^r = a^r \in \{a, a^2, a^3, ..., a^m\}$

Note: If $a \in G$, then the smallest $m \in N$ is said to be order of a if $a^m = e$ and denoted by $O(G)$. If no such m exist, then a is of infinite order.

Result and properties:

(i) For any G, the identity element is the only element of order 1 in G i.e., $O(e)=1$

Hence, for any element $a \in G, O(a)=1 \Leftrightarrow a=e$

(ii) We know that $e^{-1}=e$ i.e., we can say that e is the self-inverse element.

Moreover, if $a \neq e \in G$ such that $a^{-1}=a$

As $a \neq e \Rightarrow O(a) \neq 1$

As $a * a^{-1}=a \Rightarrow a * a=e$

$\Rightarrow a^2=e \Rightarrow O(a)=2$

Hence, every element of order 2 is self-inverse.

(iii) A non-identity element is of order 2 *iff* it is self-inverse.

(iv) $< a >=\{a^m \mid m \in Z\}=\{(a^{-1})^{-m} \mid -m \in Z\}$

$=\{(a^{-1})^r \mid r \in Z\}$

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

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

Hence, we can say that order of any element in a group is same as its inverse 'OR' in any group order of element is equal to the order of inverse element.

(v) Let $a \in G$ then $\forall x \in G$, $O(xax^{-1})=O(a)$

Proof: $O(a)=m \Rightarrow a^m=e$

$a \neq e, 1<r<m$

$(xax^{-1})^2=(xax^{-1})(xax^{-1})=xa^2x^{-1}$

Then by induction, $(xax^{-1})^n=xa^nx^{-1}$

If $n=m$ then, $(xax^{-1})^m=xa^mx^{-1}$

If $r<m$ then we say $O(xax^{-1})=r$

Such that $(xax^{-1})^r=e$

$\Rightarrow xa^r x^{-1} = e$

$\Rightarrow a^r = x^{-1}ex = e$

$\Rightarrow a^r = e$, which is a contradiction because $r < m$

$\Rightarrow O(xax^{-1}) = m \forall\, x \in G \,\&\, \forall a \in G$

Hence, $O(xax^{-1}) = O(a)$

Example 1: Find the order of each element of the group Q_8?

Solution: As we know that $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

Since 1 is the identity element of Q_8 therefore $O(1) = 1$.

Now, $(-1)^1 = -1$ and $(-1)^2 = (-1)(-1) = 1$. So $O(-1) = 2$.

$(i)^1 = i$, $(i)^2 = (i)(i) = -1$, $(i)^3 = (i)(i)(i) = -i$, $(i)^4 = (i)(i)(i)(i) = 1$. So $O(i) = 4$

$(-i)^1 = -i$, $(-i)^2 = (-i)(-i) = -1$, $(-i)^3 = (-i)(-i)(-i) = i$, $(-i)^4 = (-i)(-i)(-i)(-i) = 1$. So $O(-i) = 4$

$(j)^1 = j$, $(j)^2 = (j)(j) = -1$, $(j)^3 = (j)(j)(j) = -j$, $(j)^4 = (j)(j)(j)(j) = 1$. So $O(j) = 4$

$(-j)^1 = -j$, $(-j)^2 = (-j)(-j) = -1$, $(-j)^3 = (-j)(-j)(-j) = j$,
$(-j)^4 = (-j)(-j)(-j)(-j) = 1$. So $O(-j) = 4$

Similarly, we can evaluate that $O(k) = 4 = O(-k)$.

Hence in Q_8, $O(1) = 1, O(-1) = 2, O(i) = O(-i) = O(j) = O(-j) = O(k) = O(-k) = 4$.

Example 2: Find the order of each element of the group Z_6?

Solution: As we know that $Z_6 = \{0,1,2,3,4,5\}$ is a group with respect to the operation addition modulo 6.

Since 0 is the identity element of Z_6 therefore $O(0) = 1$

Now, $(1)^1 = 1, (1)^2 = 1 +_6 1 = 2, (1)^3 = 1 +_6 1 +_6 1 = 3, (1)^4 = 1 +_6 1 +_6 1 +_6 1 = 4$,

$(1)^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5, (1)^6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0 \Rightarrow O(1) = 6$.

Again, $(2)^1 = 2, (2)^2 = 2 +_6 2 = 4, (2)^3 = 2 +_6 2 +_6 2 = 0 \Rightarrow O(2) = 3$,

$(3)^1 = 3, (3)^2 = 3 +_6 3 = 0 \Rightarrow O(3) = 2$

$(4)^1 = 4, (4)^2 = 4 +_6 4 = 2, (4)^3 = 4 +_6 4 +_6 4 = 0 \Rightarrow O(4) = 3$,

And, $(5)^1 = 5, (5)^2 = 5 +_6 5 = 4, (5)^3 = 5 +_6 5 +_6 5 = 3, (5)^4 = 5 +_6 5 +_6 5 +_6 5 = 2$,

$(5)^5 = 5 +_6 5 +_6 5 +_6 5 +_6 5 = 1, (5)^6 = 5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0 \Rightarrow O(5) = 6$

Note 1: In the infinite multiplicative group of non-zero rational numbers, the order of every element except the element 1 and -1 is infinite.

2: In the additive group of integers the order of every element except 0 is infinite.

3: In an infinite group elements may be of finite as well as of infinite order.

Theorem 1: The order of every element of a finite group is finite and less than or equal to the order of the group.

Proof: Let us consider *G* be a finite group with respect to the operation multiplication. Let $a \in G$ then all positive integral powers of a i.e., $a, a^2, a^3, \ldots$. All these are element of G, by closure axioms. Since G has a finite number of elements, therefore all these integral power of a cannot be distinct element of G. Let us suppose that $a^r = a^s \ (r > s)$.

Now, $a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s}$

$\Rightarrow a^{r-s} = a^0 \Rightarrow a^{r-s} = e$

- where $m = r - s$

Since $r > s$, therefore m is a positive integer. Thus there exists a positive integer *m* such that $a^m = e$.

Now we know that every set of positive integers has a least member. Therefore the set of all those positive integers m such that $a^m = e$ has least member, 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 by closure property $a, a^2, a^3, \ldots, a^n$ are element of *G* and no two of these are same. If it is possible, let $a^r = a^s, 1 \le s < r \le n$.

Then $a^{r-s} = e$. Since $0 < r - s < n$, therefore $a^{r-s} = e$ implies that the order of a is less than *n*. This is a contradiction. Hence $a, a^2, a^3, ..., a^n$ 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 of a group is the same as that of its inverse a^{-1}.

Proof: Let *n* and *m* be the orders of a and a^{-1} respectively. We have $O(a) = n \Rightarrow a^n = e$ (Identity element)

$\Rightarrow (a^n)^{-1} = e^{-1} \Rightarrow (a^{-1})^n = e$

$\Rightarrow O(a^{-1}) \le n \Rightarrow m \le n$

Also, $O(a^{-1}) = m \Rightarrow (a^{-1})^m = e$

$\Rightarrow (a^m)^{-1} = e \Rightarrow a^m = e \qquad [\because b^{-1} = e \Rightarrow b = e]$

$\Rightarrow O(a) \le m \Rightarrow n \le m$

Now, $m \le n$ and $n \le m \Rightarrow m = n$.

If the order of a is infinite, then the order of a^{-1} cannot be finite. Because $O(a^{-1}) = m \Rightarrow O(a)$ is finite. Therefore, if the order of a is infinite, then the order of a^{-1} must also be infinite.

Theorem 3: The order of any integral power of an element *a* cannot exceed the order of a.

Proof: Let a^k be any integral power of a. Let $O(a) = n$.

Now, $O(a) = n \Rightarrow a^n = e$ (identity element)

$\Rightarrow (a^n)^k = e^k \Rightarrow a^{nk} = e$

$\Rightarrow (a^n)^k = e^k \Rightarrow a^{nk} = e$

$\Rightarrow (a^k)^n = e \Rightarrow O(a^k) \le n$

Theorem 4: If the element a of a group G is of order *n*, then $a^m = e$ *iff n* is a divisor of *m*.

Proof: Let n be a divisor of m. Then there exists an integer q such that $nq = m$.

Now, $\Rightarrow a^m = a^{nq} = (a^n)^q = e^q = e$.

Conversely, let $a^m = e$.

Since m is an integer and n is a positive integer, therefore by division algorithm there exist integers q and r such that

$m = nq + r$, where $0 \le r < n$.

Now, $a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r \qquad [\because a^n = e]$

$\because a^m = e \Rightarrow a^r = e$.

Since $0 \le r < n$, therefore $a^r = e \Rightarrow r$ 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 $a^r = e$.

$\therefore m = nq \Rightarrow n$ is a divisor of m.

Some properties of order of an elements:

1: If a, x are the elements of any group then a and $x^{-1}ax$ are the same.

2: Order of ab is the same as that of ba where a and b are any elements of a group.

3: If a is an element of order n and p is prime to n, then a^p is also of order n.

4: If a and b are any elements of a group G, then $(bab^{-1})^n = ba^n b^{-1}$ for any integer n.

5: If G is an abelian group then, then for all $a, b \in G$ and all integers n, $(ab)^n = a^n b^n$.

6: For every element a in a group G, $a^2 = e$, then G is an abelian group.

7: A group G is abelian if every element of G except the identity element is of order two.

8: Every element of a group G is its own inverse then G is abelian.

9: If a, b are any two elements of a group G, then $(ab)^2 = a^2 b^2$ *iff* G is abelian.

10: If G is a group of even order then it has an element $a \ne e$ satisfying $a^2 = e$.

Example 3: Let G be a group and let $a \in G$ be of finite order n. Then for any integer k, we have

$O(a^k) = \dfrac{O(a)}{\gcd(n,k)} = \dfrac{n}{\gcd(n,k)}$, where gcd = Greatest common divisor.

Solution: Let $\gcd(n,k)=m$. Then obviously, $n=pm, k=qm$ for some integers p and q such that $\gcd(p,q)=1.$

Let $O(a^k)=l \Rightarrow (a^k)^l=e \Rightarrow a^{kl}=e$

$\Rightarrow n \mid kl$ $[\because O(a)=n; \therefore a^{kl}=e \Rightarrow n \mid kl]$

$\Rightarrow pm \mid qml \Rightarrow p \mid ql$

$\Rightarrow p \mid l$

Again $(a^k)^p=(a^{qm})^p=a^{qmp}=a^{qn}=(a^n)^q=e^q=e$

Therefore, $O(a^k) \mid p$ i.e., $l \mid p$

Now again, $l \mid p$ and $p \mid l \Rightarrow l=p$.

$$\therefore O(a^k)=p=\frac{n}{m}=\frac{n}{\gcd(n,k)}$$

4.6 *CYCLIC GROUP*

Definition: A group *G* with respect to the operation multiplication is **cyclic** if there exists an element $g \in G$ such that every element in *G* can be written as:

$G=\{g^n \mid n \in Z\}$.

It means every element of the group *G* is of the form g^n i.e., if $a \in G$ then *a* can be written as $a=g^m$, where m is some integer.

- The element *g* is called a **generator** of the group.
- If the group is finite of order *n*, then:

  $G=\{g^0, g^1, g^2, ..., g^{n-1}\}$

- In terms of additive group the cyclic group *G* is defined as $G=\{ng \mid g \in G, n \in Z\}$

Note: Any group *G* is said to be cyclic if there exist an element $a \in G$ which have order equal to the order of that group. Such element $'a'$ will called the generator of that group.

Examples:

4. **Integers under addition**: Z=⟨1⟩, because every integer is a multiple of 1 (i.e., Z = {…,−2,−1,0,1,2,… })

5. **Modulo arithmetic**: $Z_n = \{0,1,2,...,n-1\}$ under addition mod n is cyclic.
   For example, $Z_5 =< 1 >= \{0,1,2,3,4\}$.

6. **Multiplicative group of units modulo *n***: The group $Z_7^* = \{1,2,3,4,5,6\}$ under multiplication mod 7 is cyclic since $< 3 >= \{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3,2,6,4,5,1\} = Z_7^*$.

   Since, $3^0 = 1, 3^1 = 3, 3^2 = 9 \pmod 7 = 2, 3^3 = 27 \pmod 7 = 6, 3^4 = 81 \pmod 7 = 4$

   $3^5 = 3^4.3 \pmod 7 = 4.3 = 5, 3^6 = 3^5.3 \pmod 7 = 5.3 = 1$.

7. Set of cube root of unity i.e., $\{1, \omega, \omega^2\}$ is form cyclic group with respect to operation multiplication.

Key Properties:

- Every cyclic group is **abelian** (commutative).
- Every subgroup of a cyclic group is also cyclic.
- A cyclic group of order *n* has $\phi(n)$ generators, where ϕ is Euler's totient function.

Some properties of cyclic group:

Theorem 5: Every subgroup of a cyclic group is abelian group.

Proof: Let *G* be a cyclic group. Then there exists an element $g \in G$ such that:

$G = \{g^n \mid n \in Z\}$

Take any two elements $a, b \in G$. Since *G* is cyclic, there exist integers *m* and *n* such that:

$a = g^m, b = g^n$

We want to show that $ab = ba$.

Now compute:

$ab = g^m.g^n = g^{m+n}$. Similarly, $ba = g^n.g^m = g^{n+m}$

Since addition of integers is commutative so, $g^{m+n} = g^{n+m}$

Now, $ab = ba$

Therefore, *G* is abelian.

Theorem 6: If *a* is the generator of a cyclic group then its inverse is also an generator of the group.

Proof: Let *G* be a cyclic group such that:

$G =< a >= \{a^n \mid n \in Z\}$

So every element of *G* is of the form a^n for some integer *n*.

Now consider the element a^{-1}. We want to show that: $< a^{-1} >= G$.

That is, the powers of a^{-1} also generate all elements of *G*.

Take any element $a^n \in G$. We can write: $a^n = (a^{-1})^{-n}$

So every $a^n \in G$ is also in $< a^{-1} >$.

Similarly, the powers of a^{-1} are of the form:

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

But $a^{-n} \in G$ because *G* contains all powers of *a*, including negative ones.

So: $< a^{-1} >= \{(a^{-1})^n = a^{-n} \mid n \in Z\} = \{a^m \mid m \in Z\} = G$

Example 7: Find the generator of Z_6.

Solution: Step 1: Find a generator:

Check if 1 is a generator. We compute $<1>$ under addition mod 6:

1 mod 6=1; 1+1=2 mod 6=2; 1+1+1=3 mod 6=3
4, 5, 0 (eventually you get all elements)
So, $<1>=\{0,1,2,3,4,5\} = Z_6$

⇒ 1 is a **generator**.

Step 2: Find the inverse of 1 mod 6

In Z_6, the inverse of 1 (under addition) is 5 because:

$1+5 \equiv 0 \bmod 6$. So, $-1 \equiv 5 \bmod 6$

Step 3: Check if 5 is also a generator

Now compute $< 5 >$ (adding 5 repeatedly mod 6):

$5 \bmod 6 = 5$; $5+5 = 10 \bmod 6 = 4$; $4+5 = 9 \bmod 6 = 3$; $3+5 = 8 \bmod 6 = 2$; $2+5 = 7 \bmod 6 = 1$; $1+5 = 6 \bmod 6 = 0$

So: $\langle 5 \rangle = \{0,1,2,3,4,5\} = Z_6$

⇒ **5 is also a generator**.

4.7 *LAGRANGE'S THEOREM*

In group theory, one of the foundational results is **Lagrange's Theorem**, named after the mathematician **Joseph-Louis Lagrange**. It explores a beautiful relationship between a group and its subgroups — specifically, how the size (or **order**) of a subgroup relates to the size of the entire group.

In essence, **Lagrange's Theorem tells us that in a finite group, the number of elements in any subgroup divides evenly into the number of elements in the group**.

This result is powerful because:

- It **restricts the possible sizes** of subgroups.
- It helps us **understand the structure** of a group.
- It leads to deeper results in algebra, such as **Cauchy's Theorem** and **the classification of finite groups**.

Theorem 7 (Statement of Lagrange's theorem): The order of each subgroup of a finite group is divisor of the order of that group.

Proof: Let we consider *G* be a finite group of order *n* and also *H* be any subgroup of *G* such that order of *H* is *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, $Ha = \{h_1 a, h_2 a, ..., h_m a\}$.

Here, Ha has m distinct member members, since $h_i a = h_j a \Rightarrow h_i = h_j$ (But we have given all $h_i's$ are different)

Therefore each right coset of *H* in *G* has *m* distnict members. Any two distinct right cosets of *H* in *G* are disjoint, it means they have no common element. Since *G* is a finite group then the number of distinct right coset of *H* in *G* will be finite, say equal to *k*. The union of these *k* distinct right coset of *H* in *G* is equal to *G*. Thus if, $Ha_1, Ha_2, ..., Ha_k$ are the *k* distnict right coset of *H* in *G*, then $G = Ha_1 \cup Ha_2 \cup ... \cup Ha_k$

$\Rightarrow$The number of element of in G = The number of element in $Ha_1 +$ The number of element in $Ha_2 + \ldots +$ The number of element in Ha_k (Because we know that two distinct right cosets are mutually disjoint).

$\Rightarrow O(G) = km \Rightarrow n = km$

$\Rightarrow k = \frac{n}{m} \Rightarrow m$ is divisor of n

$\Rightarrow O(H)$ is a divisor of $O(G)$.

Hence the theorem proved.

Note 1: Here *k* is called the **index of *H* in *G* denoted by** $[G:H]$ or $i_G(H)$. We have here, $m = n/k$. Thus *k* is divisor of *n*.

2: The index of every subgroup of a finite group is divisor of the order of the group.

3: If H is a subgroup of a finite group *G*, then the index of H in G = The number of distinct right (or left) coset of *H* in *G*. Hence, $[G:H] = i_G(H) = \frac{O(G)}{O(H)}$.

4: The converse of Lagrange's theorem need not to be true. In later unit we get an important example that 12 is divisor of the *Alternating group* A_4 but A_4 does not possesses any subgroup of order 12.

Corollory 1: The order of every element of a finite group is a divisor of the order of the group.

Proof: Let *G* be a finite group with |*G*| = *n*. Let $a \in G$, with order *m* then $< a >$ is the subgroup generated by *a*. Then by **Lagrange's Theorem**, the order of any **subgroup** of a finite group divides the order of the group.

So, $|< a >| = m \,||\, G| = n$

Therefore, $Order\, of\ a \,|\, Order\, of\ G$.

Corollary 2: If *G* be a finite group of order *n* and $a \in G$, then $a^n = e$.

Example 8: Group $Z_8 = \{0,1,2,3,4,5,6,7\}$ under addition mod 8

- The group order is |G|=8.
- Possible orders of subgroups (by Lagrange): divisors of 8 → {1,2,4,8}

Let's look at the element $2 \in Z_8$.
What is the order of 2?

$2 \cdot 1 \equiv 2 \bmod 8$; $2 \cdot 2 \equiv 4 \bmod 8$; $2 \cdot 3 \equiv 6 \bmod 8$; $2 \cdot 4 \equiv 0 \bmod 8$

So order of 2 = 4, and it divides 8 ⇒ □ Lagrange's Theorem holds.

Example 9: Multiplicative group $Z_7^* = \{1,2,3,4,5,6\}$

This is the group of integers modulo 7 under multiplication (excluding 0).

- |G|=6
- Possible orders of subgroups: {1,2,3,6}

Check the order of $3 \in Z_7^*$:

$3^1 \cong 3 (\mathrm{mod}\, 7)$; $3^2 \cong 2 (\mathrm{mod}\, 7)$; $3^3 \cong 6 (\mathrm{mod}\, 7)$; $3^4 \cong 4 (\mathrm{mod}\, 7)$; $3^5 \cong 5 (\mathrm{mod}\, 7)$;
$3^6 \cong 1 (\mathrm{mod}\, 7)$

So order of 3= 6, which divides 6 ⇒ □ Lagrange's Theorem holds.

Theorem 8: Every group of prime order s cyclic.

Proof: Let *G* be a group and let |*G*| = *p*, where *p* is a **prime number**.

Let *e* be the identity element of *G*.

Take any element $a \in G$ such that $a \neq e$.

By **Lagrange's Theorem**, the **order** of an element $a \in G$ divides the order of the group.
So the order of *a*, denoted order of *a*, divides *p*.

Since $a \neq e$, the only possible divisors of *p* are 1 and *p*, and it can't be 1 (that would mean $a = e$).

Thus, order of *a* is *p*.

This means: $< a >= \{e, a, a^2, ..., a^{p-1}\}$

has *p* distnict elements ⇒ ⟨a⟩=G

So, *G* is generated by *a* ⇒ **G is cyclic.**

Theorem 9 (Cauchy's theorem): Let *G* be a **finite group**, and let *p* be a **prime number** that divides the order of *G*. Then *G* contains an element of order *p*.

'OR'

If |*G*| = *n* and $p \mid n$, where *p* is prime, then $\exists a \in G$ such that $O(a) = p$.

Proof: Let *G* be a finite abelian group, and let $p \mid\mid G \mid$, where *p* is prime. We proceed by **induction** on |G|.

If $\mid G \mid = p$**,** then *G* is a group of prime order ⇒ *G* is cyclic ⇒ Every non-identity element has order *p*.

Now assume the theorem holds for all finite abelian groups of order less than *n*. Let |*G*|=*n*, and suppose $p \mid n$. Let *e* be the identity in *G*

If **every non-identity element has order not divisible by *p***, consider let $a \in G$, $a \neq e$, and let $< a >$ be the cyclic subgroup generated by *a*. Then $|< a >| = m$ and since *G* is abelian, the quotient group $G / < a >$ is also abelian.

But now $|< a >| = m < n|$, and if $p \mid n$ but $p \nmid m$ then $p \mid\mid G / < a >|$.

By induction $G / < a >$, has an element of order *p*, which lifts to an element in *G* whose order is a multiple of *p*, a contradiction.

Therefore, there exists an element in *G* whose order is divisible by *p*, and in fact we can find one of **order exactly *p***.

□ This completesthe theorem.

Theorem 10: Every finite group of composite order has a proper subgroup.

Proof: What does this mean?

- A **composite number** is a positive integer **greater than 1** that is **not prime** — i.e., it has divisors other than 1 and itself.
- A **proper subgroup** of a group G is a subgroup $H \subset G$ such that $H \neq \{e\}$ and $H \neq G$

So the theorem says:
If *G* is a finite group and |*G*| is a **composite number**, then *G* has **at least one nontrivial proper subgroup**.

Now, let *G* be a finite group and let |*G*| = *n*, and suppose *n* is **composite**. So $n = ab$, where $1 < a < n$ and $1 < b < n$. In particular, $a \mid n$

We want to **show that *G* has a proper subgroup**.

Step 1: Use Lagrange's Theorem

- Lagrange's Theorem says:
  If $H \leq G$, then $|H| \mid |G|$
- Let *a* be a **proper divisor** of *n* (i.e. $1 < a < n$).
- Then by **Cauchy's Theorem** (or sometimes just structure of groups), in many standard proofs, we can say:

There **exists an element** $g \in G$ such that $O(g) = d$, for some $d \mid n$, and then the cyclic subgroup $< g >$ has order *d*.

But even without invoking Cauchy's Theorem, we can say:

- There must exist a **cyclic subgroup** of order *d*, where $d \mid n$, $1 < d < n$, due to the **structure of finite groups**.

So *G* has a subgroup of order *d*, and since $1 < d < n$, this subgroup is:

→ **Nontrivial** (more than identity)

→ **Proper** (smaller than the whole group)

Conclusion:

Every finite group of **composite order** must have a **proper nontrivial subgroup**, because the order of the group has at least one proper divisor, and **Lagrange's Theorem** ensures that a subgroup of that order (or at least one dividing |*G*|) can exist.

Theorem 11: Every subgroup of a cyclic group is cyclic**.**

Proof: We'll prove this for infinite cyclic group and finite cyclic group.

Case 1: Infinite Cyclic Group

Let $G =< a >$, and suppose $G \cong Z$ (the integers under addition). Let $H \leq G$ be any subgroup.

Every subgroup of Z is of the form $mZ = \{mk \mid k \in Z\}$, for some non-negative integer *m*.

So:

- $H =< a^m >$, where *m* is the **smallest positive integer** in *H*.
- Therefore, *H* is cyclic, generated by a^m.

Done for infinite cyclic groups.

Case 2: Finite Cyclic Group

Let $G =< a >$ be a **finite cyclic group** of order *n*, so $G = \{e, a, a^2, ..., a^{n-1}\}, a^n = e$.

Let $H \leq G$ be a subgroup. We want to show that *H* is also cyclic.

Step 1: Use element orders and divisors

Let $H \neq \{e\}$. Then *H* contains some powers of *a*, say:

$H = \{a^{k_1}, a^{k_2}, ...\}$

Let *m* be the **smallest positive integer** such that $a^m \in H$. We claim $H =< a^m >$

Step 2: Show that $< a^m > \subseteq H$

Since $a^m \in H$ and *H* is a subgroup, all powers of a^m are in *H*, so:

$< a^m > \subseteq H$

Step 3: Show that every element of *H* is a power of a^m

Let $a^k \in H$. Use the **division algorithm** $k = mq + r$,where $0 \leq k < m$

Then $a^k = a^{mq+r} = (a^q)^m a^r$

Since $a^k, (a^q)^m \in H$, and *H* is a group ⇒ their product inverse:

$a^r = a^k.(a^m)^{-q} \in H$

But $0 \leq r < m$, and *m* was the **smallest** positive exponent such that $a^m \in H$ so:

- If $r > 0$, it contradicts the minimality of *m*
- So $r = 0$, and $a^k = (a^m)^q$

Hence $a^k \in < a^m > \Rightarrow H \subseteq < a^m >$

Step 4: Combine both inclusions

Since $< a^m > \subseteq H$ and $H \subseteq < a^m > \Rightarrow H = < a^m >$

Thus, ***H* is cyclic**, generated by a^m.

Hence the theorem proved that Every subgroup of a cyclic group (finite or infinite) is itself cyclic.

Corollary 3: If $G = < a >$ has order *n*, then for every divisor $d \mid n$, there exists exactly one subgroup of order *d*- namely $< a^{n/d} >$.

Check your progress

Let *G* be a finite group of order 20. Answer the following problems with proper reasoning and justification:
Problem 1: List all possible orders of subgroups of *G*. Justify your answer using Lagrange's Theorem**.**
Problem 2: Can *G* be a cyclic group? If yes, give an example and discuss the number of generators.
Problem 3: If *G* is cyclic, find the number of elements of order 4 in *G*.
Problem 4: Let $G = < a >$ be a cyclic group of order 20. Find the order of the elements a^2, a^5 and a^{10}.

4.8 *SUMMARY*

This unit on **Cyclic Groups, Lagrange's Theorem, and Order of an Element** explores fundamental concepts in group theory. A **cyclic group** is a group generated by a single element, meaning every element in the group can be written as a power (or multiple) of that generator. These groups are always abelian and can be finite or infinite. **Lagrange's Theorem** states that in a finite group, the order (number of elements) of any subgroup divides the order of the group, leading to important consequences such as constraints on possible subgroup sizes and element orders. The **order of an element** is the smallest positive integer *n* such that $a^n = e$, where *e* is the identity element. This order always divides the order of the group. Together, these concepts help classify groups, analyze subgroup structure, and understand the behavior of elements within algebraic systems.

4.9 *GLOSSARY*

- Order of group.
- Generation of an element.

- Order of an element.
- Cyclic group.
- Generating element
- Index of a subgroup
- Lagrange's theorem

4.10 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975),*Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.

4.11 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

4.12 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Define a cyclic group. Prove that every cyclic group is abelian. Also, give one example each of a finite and an infinite cyclic group. Discuss whether every abelian group is cyclic.

2. State and prove that every subgroup of a cyclic group is cyclic. Also, determine the number of subgroups in a cyclic group of order 30 and list their orders.

3. State and prove Lagrange's Theorem for finite groups.

4. Using the Lagrange's theorem, explain why a group of order *p*, where *p* is a prime number, must be cyclic and has no proper nontrivial subgroups.

5. Define the order of an element in a group. Prove that the order of an element $a \in G$ is equal to the order of the cyclic subgroup generated by *a*. Also, prove that if $a^n = e$, then the order of *a* divides *n*.

6. Let *G* be a finite group**,** and let $a \in G$. Prove that the order of the element *a* divides the order of the group G. Give an example to support your result.

Short Answer Type Question:

1. Define a cyclic group with an example.
2. What is the difference between a finite cyclic group and an infinite cyclic group?
3. List all the generators of Z_8.
4. Is every cyclic group abelian? Justify your answer.
5. How many subgroups does a cyclic group of order 15 have?
6. State Lagrange's Theorem.
7. If a group has order 20, what are the possible orders of its subgroups?
8. Can a group of order 10 have a subgroup of order 3? Why or why not?
9. If *G* is a group of prime order, prove that it has no proper non-trivial subgroups.
10. Give an example of a group where not every divisor of the group order corresponds to a subgroup.
11. Define the order of an element in a group.
12. What is the order of the element 3 in the group Z_7?
13. Prove that the order of any element divides the order of the group.
14. If the order of an element *a* is 6, what is the order of a^2?
15. In a cyclic group of order 10, how many elements are there of order 5?

Fill in the blanks:

1. A group *G* is called cyclic if there exists an element $g \in G$ such that every element of *G* can be written as a _____ of *g*.
2. The number of generators of a cyclic group of order *n* is equal to _____.
3. Every subgroup of a cyclic group is _____.
4. A cyclic group of order 6 has _____ generators.

5. Lagrange's Theorem states that the order of any subgroup of a finite group divides the _____ of the group.
6. If a group *G* has order 20, then the possible orders of its elements are the _____ of 20.
7. In a finite group, the order of an element always _____ the order of the group.
8. A group of prime order is always _____.

9. The **order** of an element $a \in G$ is the smallest positive integer *n* such that a^n _____.
10. If the order of a group is 8, then no element can have order _____.
11. In a cyclic group of order 10, the order of the element a^2 is _____.

12. The identity element of any group has order _____.

Objective type questions:

1. Which of the following is always true for a cyclic group *G*?
A) *G* is always infinite
B) Every element of *G* has the same order
C) Every subgroup of *G* is cyclic
D) *G* has no proper subgroups

2. If a group *G* has order 20, what are the possible orders of its subgroups?
A) 1, 2, 4, 5, 10, 20
B) 1, 2, 3, 4, 5, 10, 20
C) 1, 5, 10, 20
D) Any positive integer less than 20

3. In a group *G*, if an element a has order 5, what is the smallest positive integer n such that $a^n = e$ (identity)?
A) 0
B) 1
C) 5
D) 10

4. How many generators does a cyclic group of order 7 have?
A) 1
B) 2
C) 6
D) 7

5. What is the order of the identity element in any group?
A) 0
B) 1
C) Depends on the group
D) Cannot be determined

6. If $G =< a >$ is a cyclic group of order 8, what is the order of the element a^2?
A) 4
B) 8
C) 2
D) 1

7. Let *G* be a group of order 15. What are the possible orders of elements in *G*?
A) 1, 3, 5, 15

B) 1, 5, 15
C) 1, 3, 15
D) Any divisor of 15

8. How many subgroups does a cyclic group of order 10 have?
A) 5
B) 10
C) 4
D) 6

9. If an element *a* in a group has order 7, what is the order of a^{-1}?
A) 1
B) 7
C) 6
D) Cannot be determined

10. A group *G* is cyclic if:
A) It has only one element
B) It has a finite number of elements
C) Every element is the identity
D) There exists an element $g \in G$ such that every element of *G* is a power of *g*

True and False questions:

1. Every cyclic group is abelian.
2. If a group has only one generator, then it must be cyclic.
3. Every abelian group is cyclic.
4. A cyclic group of order *n* has $\phi(n)$ generators.

5. Lagrange's Theorem states that the order of a subgroup divides the order of the group.
6. If an element $a \in G$ has order 6, then the order of *G* must be 6.
7. Every divisor of the group's order corresponds to a subgroup.
8. If a group has order 9, then it cannot have an element of order 6.
9. The order of any element in a finite group divides the order of the group.
10. In a group of order 11, every non-identity element has order 11.
11. The identity element is the only element of order 1.

12. If $a^k = e$, then the order of *a* is *k*.

4.13 *ANSWERS*

Answer of check your progress:

Problem 1: Possible orders of subgroups are the divisors of 20**:**
Divisors of 20 = 1, 2, 4, 5, 10, 20
By Lagrange's Theorem**,** the order of any subgroup must divide the order of the group.

Problem 2: Yes, *G* can be cyclic.
Example: The group Z_{20} (integers modulo 20 under addition) is a cyclic group of order 20.
Number of generators = $\phi(20) = 8$

Problem 3: In a cyclic group of order 20, the number of elements of order *d* is $\phi(d)$ if *d* divides 20. Since 4 divides 20, the number of elements of order 4 = $\phi(4) = 2$.

Problem 4: Use the formula, Order of $a^k = \frac{n}{\gcd(n,k)}$, here $n = 20$

Order of $a^2 = \frac{20}{\gcd(20,2)} = \frac{20}{2} = 10$

Order of $a^5 = \frac{20}{\gcd(20,5)} = \frac{20}{5} = 4$

Order of $a^{10} = \frac{20}{\gcd(20,10)} = \frac{20}{10} = 2$

Answer of the fill in the blanks:

1. power **2.** Euler's totient function *ϕ(n)* **3.** *cyclic*

4. 2 (*since ϕ(6)=2\phi(6) = 2ϕ(6)=2*) **5.** order

6. divisors **7.** divides **8.** Cyclic

9. identity element **10.** 3 *(*because 3 does not divide 8*)*

11. 5 (since $\frac{10}{\gcd(2,5)} = 5$) **12.** 1

Answer of the objective type question:

1.	C	**2.**	A	**3.**	C	**4.**	C
5.	B	**6.**	A	**7.**	D	**8.**	A
9.	B	**10.**	D				

Answer of True and False:

1.	True	**2.**	True	**3.**	False	**4.**	True
5.	True	**6.**	False	**7.**	False	**8.**	True
9.	True	**10.**	True	**11.**	True	**12.**	False

BLOCK- II

NORMAL SUBGROUP, PERMUTATION GROUP AND GROUP HOMOMORPHISM

Unit-5: NORMAL SUBGROUP

CONTENT:

5.1 *INTRODUCTION*

Évariste Galois was a French mathematician born in Bourg-la-Reine who possessed a remarkable genius for mathematics. Among his many contributions, Galois **founded abstract algebra and group theory**, which are fundamental to computer science, physics, coding theory and cryptography.

Évariste Galois

25 October 1811 – 31 May 1832

It is tribute to the genius of Galois that he recognized that those subgroups for which the left and right cosets coincide are distinguished ones. Very often in mathematics the crucial problem is to recognize and to discover what the relevant concepts are.

In the previous sessions, we have already learned that how any set *G* can be formed a group with respect to (*w.r.t.*) the given operation. We have also learned about various types of groups and their properties. Some applications of group like subgroup, cyclic group, order of the group, permutation group, homomorphism, isomorphism, center of the group, cosets and Lagranges theorem are already studies in previous classes. In this unit we will learn about the Normal subgroups and its use to construct the quotient group.

As we know that, in a group *G*, it is not always true that $gH = Hg$ for all $g \in G$ where, *H* is a subgroup of a group *G*.

Example 1: Let *G* be a permutation group of degree 3 on three symbol 1, 2, 3 and $H = \{I, (1\ 2)\}$ is a subgroup of *G*. Since $a = (2, 3) \in G$ then the left coset of *a* in *G* i.e.,

$aH = \{(2\ 3)I, (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\}$

And the right coset of *a* in *G* is,

$Ha = \{\mathrm{I}(2\ 3), (1\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2\ 3)\}$

Here clearly, we can see that $aH \neq Ha$

In other words, right cosets are not always the same as left cosets. Group theory depends heavily on the subgroups for which this characteristic holds because they enable the creation of a new class of groups known as factor or quotient groups. Homomorphisms, a generalisation of isomorphisms, can be used to study factor groups.

5.2 *OBJECTIVES*

After reading this unit learners will be able to

- Understand the basic definition of normal subgroup and quotient group.
- Implement the application of theorems into various problem
- Construction of various types of quotient groups

5.3 *NORMAL SUBGROUP*

Definition: A subgroup *H* of a group *G* is normal in *G* if $gH = Hg$ for all $g \in$ G. In other words, the right and left cosets of a group *G* must be exactly the same for a subgroup *H* to be considered normal subgroup.

If *H* is a normal subgroup of the group *G* then symbolically it is represented as $H \trianglelefteq G$.

Example 2: Let G be a permutation group of degree 3 on three symbol 1, 2, 3 and $H=\{I,(1\,2\,3),(1\,3\,2)\}$ is a subgroup of G. Since $a=(1,2)\in G$ then the left coset of a in G i.e.,

$aH=\{(1\,2)I,(1\,2)(1\,2\,3),(1\,2)(1\,3\,2)\}=\{(1\,2),(2\,3),(1\,3)\}$

And the right coset of a in G is,

$Ha=\{\mathrm{I}(1\,2),(1\,2\,3)(1\,2),(1\,3\,2)(1\,2)\}=\{(1\,2),(1\,3),(2,3)\}$

Similarly, we can see that $aH=Ha\ \forall a\in G$

So, we can say that H is the normal subgroup of G.

Note 1: If we are saying that H is a normal subgroup of G i.e., $gH = Hg$ for all $g\in$ G then its mean that there exist $h\in H$ such that gh is any element of gH which will be equal to any element of $h'g$ where $h'\in H$ i.e., $gh=h'g$.

In example 2, $(1\,2)(1\,3\,2)=(1\,2\,3)(1\,2)$

Proper subgroup: A subgroup H of a group G is called proper subgroup of G if $H\neq G$ and it is represented as $H<G$ and it is read as "H is a proper subgroup of G".

Since, $G\subseteq G$ *i.e.*, G is subset of itself so G, is called improper subgroup of G.

A subgroup H which contains only identity element *i.e.*, $H=\{e\}$ is called the trivial subgroup of G.

5.3.1 *SIMPLE GROUP*

Definition: If a group has no proper normal subgroup is called a simple group.

Theorem 1: If G be a group and H is the subgroup of G. Then the following statement are equivalent.

1. The subgroup H is normal in G
2. For all $a\in G$, $aHa^{-1}\subseteq H$
3. For all $a\in G$, $aHa^{-1}=H$

Proof: $(1)\Rightarrow(2)$. We have given H is the normal subgroup of G then $aH=Ha\ \forall a\in G$. It means for a given $h\in H$, $a\in G$ there exist $h'\in H$ such that $ah=h'a$. Since $a\in G$ and G is the group then $a^{-1}\in G$.

$\Rightarrow (ah)a^{-1}=(ha)a^{-1}$

$\Rightarrow aha^{-1}=h\in H$

So, $aHa^{-1} \subseteq H \ \forall a \in G$

$(2) \Rightarrow (3)$ Let $a \in G$ and H is normal subgroup of G, then we have already prove that $aHa^{-1} \subseteq H$. Now we have only to show that $H \subseteq aHa^{-1} \ \forall a \in G$.

Since $a \in G \Rightarrow a^{-1} \in G$

Therefore we have $a^{-1}H\left(a^{-1}\right)^{-1} \subseteq H \ \forall a \in G$

$\Rightarrow a^{-1}Ha \subseteq H \ \forall a \in G$

$\Rightarrow a\left(a^{-1}Ha\right)a^{-1} \subseteq aHa^{-1} \ \forall a \in G$

$\Rightarrow a\left(a^{-1}Ha\right)a^{-1} \subseteq aHa^{-1} \ \forall a \in G$

$\Rightarrow H \subseteq aHa^{-1} \ \forall a \in G$

Now again for each $a \in G$, $aHa^{-1} \subseteq H$ and $H \subseteq aHa^{-1}$

So, for all $a \in G$, $H = aHa^{-1}$

$(3) \Rightarrow (1)$ Suppose that $H = aHa^{-1} \ \forall a \in G$ then we have to prove that H is normal in G.

Since, for all $a \in G$, $H = aHa^{-1}$

$\Rightarrow Ha = \left(aHa^{-1}\right)a \ \forall a \in G$

$\Rightarrow Ha = aH \ \ \forall a \in G$

$\Rightarrow$ each left coset of H in G is a right coset of H in G.

$\Rightarrow H$ is normal subgroup of G.

Theorem 2: A subgroup H of a group G is normal in G iff the product of two right or left coset of H in G is again a right or left coset of H in G.

Proof: Suppose H is a normal subgroup in G and Ha, Hb are two right coset of H in G where, $a, b \in G$. Then

$(Ha)(Hb) = H(aH)b$

$= H(Ha)b$ $[\because H \text{ is normal } \Rightarrow Ha = aH]$

$= HHab$ $[\because HH = H]$

$= Hab$ $[a \in G, b \in G \Rightarrow ab \in G]$

Therefore, Hab is also a right coset of H in G.

Conversely, we will suppose that the product of two right cosets of H in G is again a right coset of H in G. Let x be any arbitrary element of G then x^{-1} will also an element of G. So,

Hx and Hx^{-1} are two distinct right cosets of H in G. Thus, $HxHx^{-1}$ is also a right coset of H in G. Therefore we must have,

$HxHx^{-1} = H \; \forall x \in G$

$\Rightarrow h_1 xhx^{-1} \in H \; \forall x \in G$ and $\forall h_1, h \in H$

$\Rightarrow h_1^{-1}\left(h_1 xhx^{-1}\right) \in h_1^{-1} H \; \forall x \in G$ and $\forall h_1, h \in H$

$\Rightarrow xhx^{-1} \in H \; \forall x \in G$ and $\forall h \in H$ $[\because h_1^{-1} H = H$ as $h_1^{-1} \in H$ since $h_1 \in H]$

$\Rightarrow H$ is a normal subgroup of G.

Theorem 3: Intersection of two normal subgroup of a group is also a normal subgroup of the group.

Solution: Let G be a group and H, K are of its two normal subgroup of G. Now, we have to prove that $H \cap K$ is also a normal subgroup of G. Let a be any element of $H \cap K$ *i.e.*,

$x \in H \cap K \Rightarrow x \in H$ *and* $x \in K$

Since, H and K are both normal in G. Therefore, $a \in G, h \in H \Rightarrow axa^{-1} \in H$

Similarly, $a \in G, x \in K \Rightarrow axa^{-1} \in K$

Now, again $axa^{-1} \in H$, $axa^{-1} \in K \Rightarrow axa^{-1} \in H \cap K$

Hence $H \cap K$ is a normal subgroup of G.

Corollary: Arbitrary collection of normal subgroup is also a normal subgroup of the group i.e., let G be a group and let $\{H_n : n \in \wedge\}$ be the family of normal subgroup of G where $\wedge$ is the index set then $\underset{n\in\wedge}{\cap} H_n$ is the arbitrary intersection of the family of normal subgroups which is also a normal subgroup of G.

Solved Examples

Example 3: Show that each subgroup of the Abelian group G is a normal subgroup of the group.

Solution: Let G be a Abelian group and H is a subgroup of the group. Suppose that $h \in H$ and $x \in G$.

Now consider, $xhx^{-1} = x(x^{-1}h)$

$= (xx^{-1})h$

$= eh = h \in H$

So, $\forall x \in G, h \in H, xhx^{-1} \in H \Rightarrow H$ is a normal subgroup of G.

Example 4: Prove that the alternating subgroup A_n is the normal subgroup of the symmetric group S_n

Solution: Suppose that $\alpha \in S_n$ and $\beta \in A_n$. As we know that A_n is collection of all even permutation of S_n so, β is a even permutation. Now, there are two cases arises,

Case I: If α is odd permutation then α^{-1} is also an odd permutation. As we know that product of odd and even permutation is odd permutation, it means $\alpha\beta$ is odd permutation. Similarly, product of two odd permutation is even permutation *i.e.*, $\alpha\beta\alpha^{-1}$ is even permutation.

So, for $\alpha \in S_n, \beta \in A_n, \alpha\beta\alpha^{-1} \in A_n$. Thus, A_n is normal subgroup.

Case II: If α is even permutation then α^{-1} is also an even permutation. As we know that product of two even permutation is even permutation, it means $\alpha\beta$ is even permutation. Similarly, product of two even permutation $\alpha\beta$ and α^{-1} is even permutation *i.e.*, $\alpha\beta\alpha^{-1}$ is even permutation.

So, for $\alpha \in S_n, \beta \in A_n, \alpha\beta\alpha^{-1} \in A_n$. Thus, A_n is normal subgroup.

From the both cases we have conclude that A_n is normal subgroup of S_n.

Example 5: If *H* is a subgroup of index 2 in *G* then *H* is a normal subgroup of *G*.

Solution: If H is a subgroup of index 2 in G, it means, number of distinct right (left) coset of H in G are 2. So, *G* can be written in the union of two of its distinct right (left) cosets *i.e.*, $G = H \cup Hx = H \cup xH$, here $x \notin H$ because if it is $xH = H = Hx$.

As we know that no element common to H and xH therefore, we must have $xH = Hx \forall x \in G$

Hence *H* is normal subgroup of *G*.

e.g. Index of alternating subgroup A_n in the symmetric group S_n is 2. So, A_n is the normal subgroup in the symmetric group S_n**.**

Example 6: If *H* is normal in *G* and *K* is a subgroup of *G* such that $H \subseteq K \subseteq G$. Then, show that *H* is also a normal subgroup of *K*.

Solution: We have given that *H* is normal in *G* so, *H* will also a subgroup of *G*. Since, $H \subseteq K$ where, *K* is a subgroup of *G*. So we have only to show that *H* is also a normal subgroup of *K*. Let *x* be any arbitrary element of *K* then *x* will also belong to *G* therefore we

have $Hx = xH$. Since, H is a subgroup of G and $\forall x \in K$ we have $Hx = xH$. Thus, H is normal subgroup of K.

Example 7: If N is normal in G and H is subgroup of G then show that $H \cap N$ is normal subgroup of H.

Solution: As we know that intersection of two subgroup of G is also a subgroup of G then $H \cap N$ will be subgroup of G. Similarly, since $H \cap N \subseteq H$ so, $H \cap N$ will also subgroup of H. Now, only to prove that $H \cap N$ is normal in H.

Let x be any element of H and a be any element of $H \cap N$ then a will belong in both H and N. Since, N is normal in G then $axa^{-1} \in N$. Again,

$x, a \in H \Rightarrow axa^{-1} \in H$

Thus, we can say that $axa^{-1} \in H \cap N$

i.e., $H \cap N$ is normal subgroup of H.

Example 8: Prove that every complex is commutative with normal subgroup.

Solution: Let N is a normal subgroup and H is any complex of the group G. Then we have to prove that $NH = HN$.

Let $nh \in NH \; where \; n \in N, h \in H$. We can rewrite $nh = hh^{-1}nh = h(h^{-1}nh)$. Since, N is normal subgroup therefore, $h^{-1}nh \in N$. Hence $nh \in HN$ which means, $NH \subseteq HN$.

Again, let $hn \in HN \; where \; n \in N, h \in H$. We can rewrite $hn = hnh^{-1}h = \left(hnh^{-1}\right)h$. Since, N is normal subgroup therefore, $hnh^{-1} \in N$. Hence $hn \in NH$ which means, $HN \subseteq NH$.

Hence $NH = HN$.

Example 9: If N is normal subgroup of G and H is subgroup of G, Prove the following

- **(i)** HN is a subgroup of G
- **(ii)** N is a normal subgroup of HN.

Solution: As, we know by theorem that if H, K are subgroup of G, then HK is subgroup of G *iff* $HK = KH$. Using the previous example, HN will also a subgroup because N and H both are subgroup of G such that $NH = HN$.

Now HN is subgroup of G and N is normal subgroup of G also $N \subseteq HN$. Therefore, N is subgroup of HN. We have only to prove that N is a normal in HN. Let h_1n_1 be arbitrary element of HN and n be any element of N. Then $h_1 \in H, n_1 \in N$ and we have $(h_1n_1)n(h_1n_1)^{-1} = h_1(n_1nn_1^{-1})h_1^{-1} \in N$. Since N is normal in G and $n_1nn_1^{-1} \in N, h_1 \in G$. Therefore N is a normal subgroup of HN.

Example 10: If *N* and *M* are two normal subgroups of *G* such that $N \cap M = \{e\}$. Then show that each element of *N* commutes with each element of *M*.

Solution: Since *N* and *M* are two normal subgroups of *G* such that $N \cap M = \{e\}$. Then to prove that for any element $n \in N, m \in M$

$\Rightarrow nm = mn \forall m, n$

Consider the element $nmn^{-1}m^{-1}$. As we know $mnm^{-1} \in N$ because *N* is normal and $n \in N$ therefore, $nmn^{-1}m^{-1} \in N$.

Again, as we know $nmn^{-1} \in M$ because *M* is normal and $m \in M$ therefore, $nmn^{-1}m^{-1} \in M$.

Now, $nmn^{-1}m^{-1} \in N$ and $nmn^{-1}m^{-1} \in M \Rightarrow nmn^{-1}m^{-1} \in N \cap M$

$\Rightarrow nmn^{-1}m^{-1} = \{e\}$ [Because, $N \cap M = \{e\}$]

$\Rightarrow nm = mn \ \forall m \in M, n \in N$

i.e., every element of *N* commutes with every element of *M*.

Example 11: If in a group *G*, *H* is the only subgroup of finite order *m* then *H* is normal in *G*.

Solution: We have given *H* is subgroup of *G* such that *O*(*H*) = *m*. To prove this example, first we consider the set $xHx^{-1} = \{xhx^{-1} : h \in H\}$ and we will prove that this set is the subgroup of *G*. As we know by the theorem that any set *H* will subgroup of *G* if $ab^{-1} \in H \ \forall a, b \in H$. Let $h_1, h_2 \in H$ then $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$

Now consider, $xh_1x^{-1}\left(xh_2x^{-1}\right)^{-1} = xh_1x^{-1}\left(xh_2^{-1}x^{-1}\right) = xh_1\left(x^{-1}x\right)h_2^{-1}x^{-1}$

$= xh_1(e)h_2^{-1}x^{-1} = x(h_1h_2^{-1})x^{-1} \in xHx^{-1}$

$\Rightarrow h_1h_2^{-1} \in xHx^{-1} \ \forall h_1, h_2 \in xHx^{-1}$. Hence, xHx^{-1} is subgroup of *G*.

Now we will prove that $O(xHx^{-1}) = m$. Let $H = \{h_1, h_2, h_3, ..., h_m\}$ where all $h_i, i = 1 to m$ are distinct then $xHx^{-1} = \{xh_1x^{-1}, xh_2x^{-1}, xh_3x^{-1}, ..., xh_mx^{-1}\}$. Here, no element in xHx^{-1} are same because if it is,

$xh_ix^{-1} = xh_jx^{-1} \Rightarrow h_i = h_j$, which is not possible. So, $O(xHx^{-1}) = m$.

But we have *H* is the only such subgroup of order *m*. Therefore we must have, $xHx^{-1} = H \ \forall x \in G$. Thus, *H* is normal subgroup of *G*.

Example 12: By an example verify that if *H* is normal in *G* and *K* is normal in *H* then *K* may not be normal in *G*.

Solution: Let us consider the following subgroup of the group S_4 on the four symbols *a, b, c, d.*

$G = \{I, (a\,b\,c), (a\,d\,c\,b), (a\,b)(c\,d), (a\,c)(b\,d), (a\,d)(b\,c), (a\,c), (b\,d)\}$

$H = \{I, (a\,b)(c\,d), (a\,c)(b\,d), (a\,d)(b\,c)\}$

$K = \{I, (a\,b)(c\,d)\}$

As we can easily seen that *H* is a subgroup of *G* and *K* is a subgroup of *H*. Index of *H* in *G* is 2 *i.e.*, $[G:H]=2$, it means *H* is normal in *G*. Similarly, index of *K* in *H* is 2 *i.e.*, $[H:K]=2$, it means *K* is normal in *H*. $[\because [G:H] = O(G)/O(H) = 8/4 = 2]$

Here, K is not normal in G because for the element $(a,b,c,d) \in G$ and the element $(a,b)(c,d) \in K$.

We have $(a\,b\,c\,d)(a\,b)(c\,d)(a\,b\,c\,d)^{-1} = (a\,b\,c\,d)(a\,b)(c\,d)(d\,c\,b\,a) = (a\,d)(b\,c) \notin K$

Thus, *K* is not normal subgroup of *G*.

Example 13: If *H* is subgroup of *G*, let $N(H) = \{x \in G : xhx^{-1} = H\}$ then show that

(1) *N*(*H*) is the largest subgroup of *G* in which *H* is normal.

(2) *H* is normal in *G* iff $N(H) = G$.

Solution 1: In example 11, we have already prove that *N*(*H*) is the subgroup of *G* which is normal in *G*.

First we have to prove that *H* is a normal subgroup of *N*(*H*). Let $h \in H$, therefore $hHh^{-1} = H$. Thus $h \in N(H)$ *i.e.*, $H \subseteq N(H)$. So, *H* is subgroup of *N*(*H*). To show that *H* is normal in *N*(*H*). Let $x \in N(H)$, then $xHx^{-1} = H$

$\Rightarrow xH = Hx \; \forall x \in N(H)$

$\Rightarrow$ *H* is normal in *N*(*H*).

Now, we have to prove that *N*(*H*) is largest such subgroup in which *H* is normal. For it, let *K* is a subgroup of *G* in which *H* is normal then we have only to prove that $K \subseteq N(H)$.

Let $k \in K$, since *H* is normal in *K*, therefore we have $Hk = kH$

$\Rightarrow kHk^{-1} = H \;\; \forall k \in K$

$\Rightarrow k \in N(H)$

$\Rightarrow K \subseteq N(H)$

2: Let *H* is the normal subgroup of *G* and $x \in G$. Then $xH = Hx \; \forall x \in G$

$\Rightarrow xHx^{-1} = H \; \forall x \in G$

$\Rightarrow x \in N(H)$ therefore $G \subseteq N(H)$ but we know $N(H) \subseteq G$.

Thus, $G = N(H)$

Conversely, let $G = N(H)$ then $x \in G \Rightarrow x \in N(H)$

$\Rightarrow xHx^{-1} = H \; \forall x \in G$

$\Rightarrow xH = Hx \forall x \in G$

H is normal in *G*.

5.4 *QUOTIENT GROUP*

Definition: If *H* is a normal subgroup of a group *G*. Then the collection of all distinct cosets of *H* in *G* denoted by *G*/*H* is a group with respect to the operation multiplication of cosets defined as,

$$(aH)(bH) = abH \text{ 'or' } (Ha)(Hb) = Hab \;\; \forall a, b \in G$$

Or

If *H* is a normal subgroup of a group *G*, then the set

$G/H = \{Ha : a \in G\}$ is always form a group under the composition multiplication of cosets such that $(Ha)(Hb) = Hab \;\; \forall a, b \in G$

Note: If *H* is a normal subgroup of the additive group *G*. Then the set G/H is defined as $G/H = \{H + a : a \in G\}$ with respect to the operation addition of cosets such that

$(H + a) + (H + b) = H + (a + b) \forall a, b \in G$

Theorem 13: Set of all distinct cosets of normal subgroup of a group is a group with respect to composition multiplication of cosets.

Proof: Let us consider collection of distinct right (left) cosets of normal subgroup *H* under *G* is

$G/H = \{Ha : a \in G\}$

and the composition multiplication of cosets is

$(Ha)(Hb) = Hab \;\; \forall a, b \in G$

Closure axioms: Let $Ha, Hb \in G/H$ where $a, b \in G$ then

$(Ha)(Hb) = H(aH)b = H(Ha)b = HHab = Hab \in G/H$

Since we know that if *H* is normal subgroup of *G* then

(i) $Ha = aH \; \forall a \in G$

(ii) $HH = H$

And also if G is a group then it will satisfy closure property *i.e.*, if $a, b \in G \Rightarrow ab \in G$

Associativity: Let $Ha, Hb, Hc \in G/H$ where $a, b, c \in G$

Now consider, $(Ha)[(Hb)(Hc)] = (Ha)[H(bH)c] = (Ha)[H(Hb)c] = (Ha)(Hbc)$

$$= Ha(bc) = H(ab)c = H(ab)(Hc) = [(Ha)(Hb)](Hc)$$

[Because G is group so it will satisfy associative property]

Existence of identity: We know that $H = He \in G/H$ where e is the identity element of G, then we have only to prove that H is the identity element of the group G/H.

Let $Ha \in G/H$ then $(He)(Ha) = H(ea) = Ha$

$\Rightarrow H$ is the identity element of the group G/H.

Existence of inverse: Let $Ha \in G/H$. Then $Ha^{-1} \in G/H$ [Because if $a \in G$ then $a^{-1} \in G \Rightarrow Ha^{-1} \in G/H$]

Now, $(Ha)(Ha^{-1}) = H(aa^{-1}) = He = H$

So, coset Ha is the inverse of Ha^{-1} in G/H

Hence, collection of distinct right (left) of normal subgroup H in G is form a group with respect to the operation product of cosets.

Example 14: The alternating group $A_3 = \{I, (123), (132)\}$ is the normal subgroup of the symmetric group $S_3 = \{I, (12), (13), (23), (123), (132)\}$ then $S_3 / A_3 = \{A_3, (23)A_3\}$ is the quotient group.

Example 15: Consider the normal subgroup of $3Z$ of Z. The coset of $3Z$ in Z are,

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

$1 + 3Z = \{..., -5, -2, 1, 4, 7, 10, ...\}$

$2 + 3Z = \{..., -4, -1, 2, , 5, 8, 11...\}$

Here, $Z = (0 + 3Z) \cup (1 + 3Z) \cup (2 + 3Z)$

The composition table of the group $Z/3Z$ is given below.

$+$	$0+3Z$	$1+3Z$	$2+3Z$
$0+3Z$	$0+3Z$	$1+3Z$	$2+3Z$
$1+3Z$	$1+3Z$	$2+3Z$	$0+3Z$
$2+3Z$	$2+3Z$	$0+3Z$	$1+3Z$

In general, the cosets of nZ in Z are

$Z = (0+nZ) \cup (1+nZ) \cup (2+nZ) \cup (3+nZ) \cup ... \cup ((n-1)+nZ)$ then

$G/nZ = \{(0+nZ), (1+nZ), (2+nZ), (3+nZ), ..., ((n-1)+nZ)\}$

The sum of the cosets $k+Z$ and $l+Z$ is $k+l+Z$. Notice that we have written our cosets additively, because the group operation is integer addition.

Example 16: If H is a normal subgroup of the finite group G then $O[G/H] = \frac{O(G)}{O(H)}$.

Solution: As we know that $O[G/H]$ = Number of distinct right coset of H in G.

$\Rightarrow O[G/H]$ = Index of H in G.

$$\Rightarrow O[G/H] = \frac{Number\ of\ element\ in\ G}{Number\ of\ element\ in\ H}$$

$$\Rightarrow O[G/H] = \frac{O(G)}{O(H)}$$

Example 17: Prove that corresponding to every *Abelian* group its quotient group is *Abelian* but their converses need not to be true.

Solution: Let G be a Abelian group and H is its normal subgroup. If elements $a, b \in G$ are such that Ha, Hb are distinct right cosets of quotient group G/H.

Now, $(Ha)(Hb) = H(ab) = H(ba) = (Hb)(Ha)$ [Since G is Abelian $\Rightarrow ab = ba \ \forall a, b \in G$]

$\Rightarrow G/H$ is Abelian group.

But converse is need not be true. Since $S_3/A_3 = \{A_3, (2\,3)A_3\}$ is Abelian group because order of $O[S_3/A_3] = 6/3 = 2$ which is prime and we know that every group of prime order is Abelian while S_3 is not a Abelian group.

Example 18: If H is normal in G and a be any element of order n in G then order of the element Ha in G/H is divisor of n.

Solution: As we know that the identity element of the quotient group G/H is H itself. We have given in a group G, $a \in G$ *s.t.* $O(a) = n$ *i.e.* $a^n = e$. Let us assume $O(Ha) = m$.

Now consider,

$(Ha)^n = (Ha)(Ha)(Ha)....upto\ n\ times = H(aaa...upto\ n\ times) = Ha^n = He = H$

But we have already assume that $O(Ha) = m$ *i.e.*, $(Ha)^m = H$.

$\Rightarrow O(Ha)/O(a)$ [If order of any element a in a group G is n then $a^m = e$ *iff* $n \mid m$]

Check your progress

Problem 1: What will be the order of the group $O\left(\frac{Q_8}{\{1,-1\}}\right)$?

Problem 2: Check the distinct right and left coset of S_3?

Problem 3: Check that A_5 is the normal subgroup of S_5?

5.5 *SUMMARY*

In this unit, we have studied the basic definition of Normal subgroup, Simple group and Quotient group. We have also learn about the above discussed group's related theorems and there implementation in various examples. The overall summarization of this units are as follows:

- Right cosets are not always the same as left cosets
- Alternating subgroup A_n is the normal subgroup of the symmetric group S_n
- If a group has no proper normal subgroup is called a simple group.
- Quotient group always forms a group not a subgroup because identity element of group and subgroup are always same while quotient group and group has always different identity

5.6 *GLOSSARY*

- H is a subgroup of the group G is represented symbolically as $H \leq G$.
- H is a normal subgroup of the group G is represented symbolically as $H \trianglelefteq G$.
- Group with no proper normal subgroup is called a simple group.

5.7 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975),*Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra).*

Krishna Prakashan Media.

5.8 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

5.9 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that alternating group (A_n) is the normal subgroup the symmetric group (S_n).

2. Prove that a factor group of a cyclic group is cyclic.

3. Suppose that a group G has a subgroup of order n. Prove that the intersection of all subgroups of G of order n is a normal subgroup of G.

4. Show that S_4 has a unique subgroup of order 12.

5. Suppose that H is a normal subgroup of a finite group G. If G/H has an element of order n, show that G has an element of order n.

Short Answer Type Question:

6. Give one example each of the following

(a) A subgroup H of a group G which is not normal in G.

(b) A non-abelian subgroup H of a non-abelian subgroup G which is normal in G.

7. If $|G| = 30, |H| = 5$ then what will be $|G/H|$.

8. Prove that each subgroup of cyclic group is normal.

9. Determine the coset decomposition of the subgroup $H = \{I, (12)\}$ corresponding to the symmetric group S_3.

Fill in the blanks:

10. Product of two right coset in a group G is …….. in G.

11. Every subgroup H of index 2 in H is ……. in G.

12. If H is normal subgroup of G then G/H is called ……..

Objective type questions:

1. Which of the following statements is true for a normal subgroup N of a group *G*?

A) N is always the center of G

B) For every $g \in G$, gN = Ng

C) N is always abelian

D) $N \subseteq Z(G)$, where Z(G) is the center of G

2. If *N* is a normal subgroup of *G*, then the quotient group *G*/*N*:

A) Is always abelian

B) Has the same order as G

C) Has an order that divides the order of G

D) Has elements all conjugate to each other

3. A subgroup *N* of a group *G* is normal if and only if:

A) N is the center of G

B) G/N is cyclic

C) $gN=Ng$ for every $g \in G$

D) N is abelian

4. If *G* is a group and *N* is a normal subgroup of *G*, then the elements of *G*/*N* are:

A) Cosets of N in G

B) Conjugates of elements in N

C) Elements of G fixed by N

D) None of the above

5. For a subgroup of *G*, *N* is normal in *G* if:

A) $gNg^{-1}=N$ for all $g \in G$

B) $N \subseteq Z(G)$

C) N is abelian

D) G/N is cyclic

5.10 *ANSWERS*

Answer of self cheque question:

1. 4 **2.** $I, (12), (1,2,3)$ **3.** Yes

Answer of terminal question:

7. $|G/H| = 6$ **10.** Right coset **11.** Normal **12.** Quotient group

Answer of objective questions:

1. B) **2.** C)

3. C) **4.** A)

5. A)

Unit-6: PERMUTATION GROUP

CONTENT:

6.1 *INTRODUCTION*

The concept of permutation groups lies at the heart of group theory, a key area of abstract algebra that studies the symmetry and transformations of mathematical structures. Permutation groups specifically focus on the set of all bijections (permutations) of a set, closed under composition, and their properties. Their origins trace back to the late 18th century when Joseph-Louis Lagrange explored permutations in the context of polynomial equations. Paolo Ruffini made early attempts to link permutations to the solvability of equations, but it was Évariste Galois in the early 19th century who laid the rigorous

foundation. Galois's innovative work demonstrated how permutations could explain the solvability of polynomials, giving rise to what is now known as Galois theory. Since then, permutation groups have become a central tool in mathematics, influencing fields like combinatorics, geometry, and cryptography, while also serving as a gateway to understanding symmetry in nature and theoretical sciences.

6.2 *OBJECTIVES*

The main objectives of studying permutation groups include:

1. **Introduction to Symmetry**: Understanding how permutation groups describe and formalize the concept of symmetry in mathematical structures.
2. **Basic Properties**: Learning the fundamental properties of permutation groups, including closure, associativity, identity, and inverses.
3. **Symmetric and Alternating Groups**: Exploring key examples such as symmetric groups S_n and alternating groups A_n, their orders, and their roles in group theory.
4. **Transpositions and Cycles**: Understanding how permutations can be expressed in terms of disjoint cycles and transpositions, and using these representations to simplify computations.
5. **Group Actions**: Introducing the concept of group actions and their applications in studying orbits, stabilizers, and symmetry.
6. **Applications to Polynomials**: Connecting permutation groups to the roots of polynomials and introducing the basics of Galois theory, highlighting the relationship between group theory and equation solvability.
7. **Problem-Solving**: Developing problem-solving skills by working with examples and exercises involving permutations, compositions, and decompositions.
8. **Foundational Knowledge**: Building a foundation for more advanced topics in algebra, such as automorphisms, abstract groups, and field theory.

These objectives align with the goal of equipping learners with both theoretical understanding and practical tools to analyze and apply permutation groups in various mathematical contexts.

6.3 *PERMUTATION*

Let $X = \{a_1, a_2, ..., a_n\}$ is any finite set.

Define, $S_X = \{ f \mid f : X \to X$, such that f is one-one and on-to$\}$

i.e., $S_X =$ The collection of all one-one and on-to map from X to X .

Then S_X forms a group *w.r.to.* composition of maps as the binary operation given and $O(S_X) = n!$

Note 1: Since, $f \in S_X \Rightarrow f : X \to X$

Defined as, $f(a_i) = b_i$ such that f is one-one and on-to.

i.e., $f(a_1) = b_1$, $f(a_2) = b_2$, $f(a_3) = b_3$, …, $f(a_n) = b_n$

where, $b_i's$ are nothing but $a_i's$ only in some different arrangement.

Then the permutation on X is defined as

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

If we denote it by,

$$\sigma_f = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ f(a_1) & f(a_2) & f(a_3) & ... & f(a_n) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix}$$

Where $b_i = f(a_i)$

2: A permutation on X is a $2 \times n$ matrix where the first row is given by the elements of X and second row is given by their image by some bijection on X. Infact, the second row is an permutation of the first row.

3: If $| X | = n$ then permutation is called of degree n.

4: Let $X = \{a_1, a_2, ..., a_n\}$ define $S_n = \left\{ \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ f(a_1) & f(a_2) & f(a_3) & ... & f(a_n) \end{pmatrix} \middle| f \in S_X \right\}$

Then $| S_n | = n!$

Where, S_n = The set of all the permutation of degree n.

5: On any set X, a bijection is defined as a symmetry on X but if X is finite, it defines a permutation on X of degree equal to cardinality of X i.e., Card (X).

6: Let $f, g \in S_n$, then aby two permutation are said to be equal if $f(a_i) = g(a_i) \forall a_i \in X$

e.g., $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ are two permutation of degree 4,

then by interchanging columns we can write $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

7: Permutation does not affect by rearranging columns.

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

8: If degree is known or *X* is well-known is well-known and $\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ a_1 & a_2 & b_3 & ... & b_n \end{pmatrix}$

Such that $a_r \neq b_r$; $r \neq 1, 2$

Then we can exclude a_1 & a_2 from the permutations

i.e., $\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ a_1 & a_2 & b_3 & ... & b_n \end{pmatrix} = \begin{pmatrix} a_3 & a_4 & a_5 & ... & a_n \\ b_3 & b_4 & b_5 & ... & b_n \end{pmatrix}$

Identity Permutation: If I is a permutation of degree *n* such that *I* replaces each element by the element itself, then I is called the identity permutation of degree *n*.

Thus, $\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix}$ *and* $\begin{pmatrix} 1 & 2 & 3 & ... & 9 \\ 1 & 2 & 3 & ... & 9 \end{pmatrix}$ are identity permutation of degree *n* and 9 respectively.

Product or composition of two permutation: The product or composite of two permutations $f \in S_n$ and $g \in S_n$ of degree *n* denoted by fg, is obtained by second carrying out the operation defined by *g* and then by *f*.

Let $f = \begin{pmatrix} b_1 & b_2 & b_3 & ... & b_n \\ c_1 & c_2 & c_3 & ... & c_n \end{pmatrix}$ and $g = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix}$

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

i.e., $fg = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ c_1 & c_2 & c_3 & ... & c_n \end{pmatrix}$

Here, first *g* replace a_1 by b_1 i.e., $g(a_1) = b_1$ then after that *f* replace b_1 by c_1 i.e., $fg(a_1) = f(b_1) = c_1$.

Obviously $fg \in S_n$ i.e., fg is also a permutation of degree *n*. Thus the product of two permutation of degree *n* is also a permutation of degree *n*.

Example 1: Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two permutation of degree 3. Then

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

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

Clearly, $fg \neq gf$

Note: Product of two permutations is not commutative.

r-Cycle: If $\sigma = \begin{pmatrix} a_1 & a_2 & a_r & a_{r+1}\ldots & a_n \\ a_2 & a_3 & a_1 & a_{r+1}\ldots & a_n \end{pmatrix}$ then σ is called *r*-cycle and written as,

$\sigma = (a_1\, a_2\, a_3 \ldots a_r)$. Where, remaining $a_i; i = r+1 \ \ to\, n$, are unchanged.

e.g., $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \end{pmatrix} = (345)$

Note: If σ is *r*-cycle i.e., $\sigma = (a_1\, a_2\, a_3 \ldots a_r)$ then we say σ is of length *r*.

i.e., Length of cycle = No. of symbols used in that cycle.

e.g., $\sigma = (143)$ is 3-cycle and $\tau = (12)$ is 2-cycle.

Transposition: A cycle of length two is called a transposition.

e.g., $\tau_1 = (12),\ \tau_2 = (13)$

Note 1: A cycle does not change by re-arranging symbols maintaining cyclic order.

e.g., $\sigma = (12345) = (23451) = (34512) = (45123) = (51234)$ but $\sigma = (12345) \neq (24351)$ because here symbols does not maintain the cyclic order.

2: A permutation may not be a cycle.

e.g., $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 5 & 7 & 8 \end{pmatrix} = (1234)(56)$

by σ is not cycle.

Disjoint permutation: Two permutations are said to be disjoint if they have no common symbol. Since every permutation can be written in terms of *r*-cycle. Hence two cycles are said to be disjoint if they have no common symbol.

e.g., $(1234)\&(56)$ are disjoint permutation because they have no common symbol.

Remarks 1: Every permutation can be written as product of two disjoint cycles.

e.g., $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 5 & 7 & 8 \end{pmatrix} = (1234)(56)$

Example 1: If *f* and *g* are disjoint cycles, then $fg = gf$.

Solution: Since the cycles *f* and *g* have no common symbols. Therefore the elements permuted by *f* are left unchanged by *g* and also the elements permuted by *g* remain the same under by *f*. Therefore we shall have $fg = gf$.

e.g., Let $f = (123), g = (45)$

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

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

$\Rightarrow fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ and similarly, $gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Hence, $fg = gf$.

Observation: Let $(12)(13) = (132)$ i.e. cycle (132) can be wriiten as product of transposition.

Similarly, $(12)(13)(14) = (1432)$ i.e., cycle (1432) can be wriiten as product of transposition.

Similarly, ***every cycle can be written as product of transposition***.

Hence, we can say that ***every permutation can be written as product of disjoint cycles and every cycle can be written as product of transposition***.

Hence, ***every permutation can be written as product of transposition***.

e.g., $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 3 & 2 & 7 & 8 & 6 \end{pmatrix} = (14352)(678)$ .... (1)

Since, $(14352) = (12)(15)(13)(14)$ and $(678) = (68)(67)$

Then by (i) we can write,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 3 & 2 & 7 & 8 & 6 \end{pmatrix} = (14352)(678) = (12)(15)(13)(14)(68)(67)$$

Note 1: Every *r*-cycle can be expressed as product of (*r*-1) transposition.

2: Transposition of any cycle are not unique.

e.g., $\sigma = (12345) = (15)(14)(13)(12)$ … (1)

and also, $\sigma = (12345) = (23451)$ (Because cycle does not affect by re-arranging symbols maintaining cyclic order).

$\Rightarrow \sigma = (12345) = (23451) = (21)(25)(24)(23)$ … (2)

By (1) and (2) we can say that transposition is not unique. Similarly we can find other transposition

Cycle decomposition (CD): Let $\sigma \in S_n$ then we can write σ as,

$\sigma = C_1 C_2 ... C_k$, where $C_i's$ are cycle of length n_i (say) and $C_i's; i = 1 to k$, are disjoint.

If $\sum n_i = n =$ The degree of σ

Then the multiset, $\{n_1, n_2, ..., n_k\}$ is defined as the cycle decomposition of σ.

Note: For uniqueness in general we write CD as,

CD of $\sigma = \{n_1, n_2, ..., n_k\};\ n_i \le n_{i+1}$

e.g., $\sigma = (1)(2)(34)(56) \in S_6$

$\sigma = (1)(2)(34)(56) = C_1.C_2.C_3.C_4$

CD of $\sigma = \{1,1,2,2\}$

Example 2: $\sigma = (123)(234)(453)(12) \in S_{10}$, then find the C.D. of σ?

Answer: Here, $\sigma = (123)(234)(453)(12) \in S_{10}$ and it is obvious that σ is not disjoint.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 5 & 4 & 6 & 7 & 8 & 9 & 10 \end{pmatrix} = (1)(2)(3)(45)(6)(7)(8)(9)(10)$$

Then C.D. of $\sigma = \{1,1,1,1,1,1,1,2\}$

Note: If $\sigma \in S_n$ then,

(i) If σ is an r-cycle then C.D. of $\sigma = \{1,1,...,1(n-r)\,times, r\}$

(ii) If σ is a transposition then C.D. of $\sigma = \{1,1,...,1(n-2)\,times, 2\}$

6.4 *SIMILAR PERMUTATION*

Similar Permutation: Two permutations are said to be similar permutation if they have the same cycle decomposition.

e.g., If $\sigma = (12)(34) \in S_4$ then C.D. of $\sigma = \{2,2\}$

If $\tau = (12)(13) \in S_4$ i.e., $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (132)(4)$ then C.D. of $\sigma = \{1,3\}$. Hence the permutation σ, τ are not similar because their cycle decomposition is not unique.

e.g., Permutations $\sigma = (135) \in S_6, \tau = (146) \in S_6$ are similar because their cycle decomposition is {1, 1, 1, 3}.

De-arrangement: If $\sigma \in S_n$ s.t., C.D. of $\sigma = \{n_1, n_2, ..., n_k\}$, a permutation σ is called de-arrangement if $n_i \ne 1 \forall i = 1 to k$. Then σ is called de-arrangement.

e.g., If C.D. of any $\sigma = \{5\}$ and if C.D. of any $\tau = \{2,3\}$ then we called $\sigma \& \tau$ are de-arrangement.

6.5 *GROUP OF PERMUTATION*

In mathematics, a **group of permutations** is a collection of permutations (bijective mappings) on a set that satisfies the axioms of a group. Here's a breakdown of the concept.

Theorem 1: The set S_n of all permutation on n symbols is a finite group of $n!$ with respect to composition of mapping as the operation. For $n \le 2$, this group is abelian for $n > 2$ it is always non-abelian.

Proof: Let $X = \{a_1, a_2, ..., a_n\}$ is any finite set.

Define, $S_n = \{f \mid f : X \to X$, such that f is one-one and on-to$\}$

i.e., $S_n =$ The collection of all one-one and on-to map from X to X.

Clearly, we know that $O(S_X) = n!$ and we have to show S_n forms a group *w.r.to.* composition of maps as the binary operation.

Closed: Let $f = \begin{pmatrix} b_1 & b_2 & b_3 & ... & b_n \\ c_1 & c_2 & c_3 & ... & c_n \end{pmatrix} \in S_n$ *and* $g = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix} \in S_n$ be any two permutation of degree n where $b_i's, c_i's$ are some arrangement of $a_i's$. Then by product or composition of two permutations, denoted multiplicatively, we have

$$fg = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ c_1 & c_2 & c_3 & ... & c_n \end{pmatrix} \in S_n$$

Similarly $\forall\ f, g \in S_n$ we have $fg \in S_n$. Hence, S_n is closed with respect to composition of permutation.

Associativity: Permutations multiplication is associative in general i.e., $\forall\ f, g, h \in S_n$

We have, $(fg)h = f(gh)$.

Existence of Identity: $I = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} \in S_n$ is the identity permutation because for all $f = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix} \in S_n$, we have $fI = If$. Hence S_n contains an identity permutation.

Existence of inverse: Let $f = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix} \in S_n$ be an element of S_n then

$\exists\ f^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 & ... & b_n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} \in S_n$ such that $f^{-1}f = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} = I$

Similarly we get $ff^{-1} = I$

Hence we can say that $\forall\ f \in S_n, \exists\ f^{-1} \in S_n$ such that $ff^{-1} = I = f^{-1}f$.

Hence, S_n is group of order $n!$with respect to the product of permutations as compositions.

Now, If $n=1$, then the set has only one element and every group of order 1 is abelian. If $n=2$, then the set S_n has $2!$ i.e., 2 element and we know every group of order 2 is again abelian group. Now, we have only to show every group of order $n>2$ is non-abelian by giving a suitable example.

Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two permutation of degree 3. Then

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

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

Clearly, $fg \neq gf$

6.6 *EVEN AND ODD PERMUTATION*

In mathematics, an **even permutation** and an **odd permutation** are terms used to describe permutations of a set, based on the number of transpositions (pairwise swaps) required to achieve the permutation.

Even Permutation: A permutation is called even if it can be expressed as a product of an **even** number of transpositions.

Odd Permutation: A permutation is called odd if it can be expressed as a product of an **odd** number of transpositions.

e.g., Every transposition is an odd permutation.

Key Properties:

1. Every permutation is either even or odd, but not both.
2. The identity permutation (where no elements are swapped) is always even because it requires zero transpositions.
3. The parity (even or odd nature) of a permutation does not change when multiplying permutations. For example:

Example 3: The product of two even permutation is an even permutation.

Answer: Suppose *f* and *g* are two even permutation. Further suppose that *f* can be expressed as the product of *r* transposition and *g* can be expressed as the product of s transpositions. Then r and s are both even as given f and g are even. Now *fg* can be expressed as the product of *r+s* transpositions. Since *r+s* is even, therefore *fg* is an even permutation.

Hence we can say that, **Even × Even = Even**

Note: In a similar way we can prove the following:

1: The product of two odd permutation is an even permutation i.e., **Odd × Odd = Even**

2: The product of an even permutation and an odd permutation is an odd permutation i.e., **Even × Odd = Odd** **'OR'** **Odd × Even = Odd**

Example 4: The inverse of an even permutation is an even permutation and the inverse of an odd permutation is an odd permutation.

Answer: Let *f* is an even permutation and f^{-1} is the inverse of *f* such that $ff^{-1} = I$. As we know that identity permutation is an even permutation and also product of two even permutation is an even permutation. On combining these two concepts we assure that f^{-1} should be definitely an even permutation because,

Even (*f* is even) × f^{-1} (unkown permutation) **= Even** **[**By the rule, **Even × Even = Even]**

This is possible only when, f^{-1} should be even.

Theorem 2: Out of the $n!$ permutations on *n* symbols, $\frac{n!}{2}$ are even permutations and $\frac{n!}{2}$ are odd permutations.

Proof: Out of $n!$ permutations on *n* symbols let the even permutation let the even permutations be $e_1, e_2, ..., e_m$ and the odd permutations be $o_1, o_2, ..., o_k$.

Since a permutation is either even permutation or an odd permutation but not both, therefore $m + k = n!$

If S_n is a set of all permutations of degree n, then

$S_n = \{e_1, e_2, ..., e_m, o_1, o_2, ..., o_k\}$. Let $t \in S_n$ and suppose t is a transposition. Since S_n is a group with respect to permutation multiplication, therefore $te_1, te_2, ..., te_m, to_1, to_2, ..., to_k$ are all elements of S_n. Obviously $te_1, te_2, ..., te_m$ are all odd permutations and $to_1, to_2, ..., to_k$ are all even permutations.

Since, no two of the permutations $te_1, te_2, ..., te_m$ are equal because,

$te_i = te_j \Rightarrow e_i = e_j$ (By left cancellation law in the group p_n). Therefore, $e_i \neq e_j$, then $te_i \neq te_j$.

Thus the m odd permutations $te_1, te_2, ..., te_m$ are distnict elements of S_n. But we have supposed that S_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 $to_1, to_2, ..., to_k$ are distnict element of S_n. Therefore, we must have

$$k \leq m \qquad \ldots (2)$$

From (1) and (2), it follows that $m = k = \frac{n!}{2}$

6.7 *ALTERNATING GROUP A_n*

The **alternating group** is a fundamental concept in group theory, a branch of abstract algebra. It is closely related to the symmetric group and consists of all **even permutations** of a finite set.

Definition: If A_n is the set of all even permutation of S_n of degree n i.e.,

$A_n = \{\sigma \in S_n \mid \sigma$ is an even permutation$\}$

Then obviously, cardinality of A_n will be $\frac{n!}{2}$.

Theorem 3: The set of A_n of all even permutation of degree *n* forms a group of order $\frac{n!}{2}$ with respect to the permutation multiplication.

Proof: Let A_n be the collection of all the even permutation of S_n. Also, we know that product of two even permutation is an even permutation, which shows that A_n is closed with respect to the permutation multiplication. So, when we say *f* be any even permutation in S_n.

$\Rightarrow f \in A_n$ [As A_n is the collection of all even permutation]

Since, S_n is associative with respect to the permutation multiplication and $A_n \subset S_n$.

$\Rightarrow A_n$ is also satisfies the associativity with respect to the permutation multiplication.

If I is an identity permutation of degree n then I is an even permutation. Therefore $I \in A_n$. Now we have, $If = f = fI \forall f \in A_n$

$\therefore I$ is an identity element.

Now, let f be any even permutation in S_n. If f^{-1} is the inverse of f in the group of all permutation of degree n, then f^{-1} is also an even permutation because $f^{-1}f = I = ff^{-1} \forall f \in A_n$.

Thus $f \in A_n \Rightarrow \exists f^{-1} \in A_n$ such that

$f^{-1}f = I = ff^{-1}$

i.e., each element of A_n possess inverse.

As we know that number of even permutation in S_n are $\frac{n!}{2}$. Hence, cardinality of A_n is $\frac{n!}{2}$.

Note: As we know that product of two odd permutation is even permutation. Hence, the set of all odd permutation of S_n is not form group with respect to the permutation multiplication as it is not closed.

Example 5: Show that the set S_3 of all permutation on three symbols $\{1,2,3\}$ is a finite non-abelian group of $3!$ order with respect to permutation multiplication.

Solution: We have $S_3 = \{I, (12), (13), (23), (123), (132)\}$. Where I is the identity permutation.

Let we rename elements of S_3 as,

$f_1 = I$, $f_2 = (12)$, $f_3 = (13)$, $f_4 = (23)$, $f_5 = (123)$, $f_6 = (132)$. Then we prepare the composition table as,

Product of permutation	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6

f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

Since all the elements in the composition table are also the elements of S_3. Here, in the composition table $f_1 = I$, is the identity element of S_3 (because for each f_i, $f_i f_1 = f_1 f_i \; \forall i = 1 to 3$)

Also from the composition table we can easily seen that,

The inverse of $f_1 = f_1$

The inverse of $f_2 = f_2$

The inverse of $f_3 = f_3$

The inverse of $f_4 = f_4$

The inverse of $f_5 = f_6$

The inverse of $f_6 = f_5$

So, inverse of each element of S_3 belongs in S_3. Hence, S_3 forms a group.

Now, from table we can easily seen that, $f_2 . f_3 = f_6$ while $f_3 . f_2 = f_5$ i.e., $f_2 . f_3 \neq f_3 . f_2$. So, we can say that S_3 is a non-abelian group.

Example 6: Show that the set S_4 of all permutation on three symbols $\{1,2,3,4\}$ is a finite non-abelian group of order $4!(=24)$ with respect to permutation multiplication.

Solution: We have

$S_4 = \{I, (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143),$
$(234), (243), (12)(34), (23)(14), (23)(14), (31)(24), (1234), (1243), (1324),$.
$(1342), (1423), (1432)\}$.

Where, I is the identity permutation. Similarly, rename the elements of S_4 as in previous example 5, we can prepare the composition table by which we can prove that S_4 is non-abelian group.

Example 7: Show that the set A_4 of all even permutation on three symbols $\{1,2,3,4\}$ is a finite non-abelian group of order $\frac{4!}{2}(=12)$ with respect to permutation multiplication.

Solution: We have

$S_4 = \{I,(12),(13),(14),(23),(24),(34),(123),(132),(124),(142),(134),(143),$
$(234),(243),(12)(34),(23)(14),(23)(14),(31)(24),(1234),(1243),(1324),$.
$(1342),(1423),(1432)\}$.

Then the collection of all even permutation is,

$A_4 = \{I,(123),(132),(124),(142),(134),(143),(234),(243),(12)(34),(23)(14),$
$(23)(14),(31)(24)\}$.

Where, I is the identity permutation. Similarly, rename the elements of A_4 as in previous example 5, we can prepare the composition table by which we can prove that A_4 is non-abelian group.

Theorem 4: A_n is a subgroup of S_n.

Proof: Let $\sigma,\tau \in S_n$ such that $\sigma \& \tau$ are even permutation then obviously $\sigma,\tau \in A_n$. Since inverse of even permutation is also an even permutation. It means, τ^{-1} is even permutation.

Now, since $\sigma \& \tau^{-1}$ are even permutation and product of two even permutation is even permutation. Then obviously, $\sigma.\tau^{-1}$ is even permutation. Hence $\sigma.\tau^{-1} \in A_n$.

Hence by one step subgroup test A_n is a subgroup of $S_n \; \forall n \in N$.

6.8 *ORDER OF PERMUTATION*

The **order of a permutation** refers to the number of times the permutation must be applied to return to the original arrangement of the elements.

Definition: Any permutation σ is called the permutation of order *k* if $\sigma^k = I$, where *k* is the least such natural number.

e.g., Let $\sigma = (123)$ then $\sigma^2 = \sigma.\sigma = (123).(123) = (132)$

then, $\sigma^3 = \sigma^2.\sigma = (132).(123) = I$. Hence order σ is 3.

Note 1: Every cycle of length *r* is an element of order *r*.

2: In mathematical terms, the order of a permutation is the least common multiple (**LCM**) of the lengths of its disjoint cycles.

e.g., Consider the permutation σ = (1 3 5)(2 4) in cycle notation:

- It has two disjoint cycles: (1 3 5) of length 3, and (2 4) of length 2.
- The order of σ is the LCM of the lengths of these cycles:

e.g., Order of σ = LCM(3,2)=6.

2. Identity permutation ϵ = ()
- Contains no cycles (or cycles of length 1).
- The order is 1 because applying it any number of times leaves the elements unchanged.

Steps to Find the Order:

1. Write the permutation in disjoint cycle form.
2. Determine the length of each cycle.
3. Compute the LCM of these lengths.

Example 8: Find the order of the permutation σ = (1 3 5)(2 4).

Solution: Consider the permutation σ = (1 3 5)(2 4) in cycle notation:

- It has two disjoint cycles: (1 3 5) of length 3, and (2 4) of length 2.
- The order of σ is the LCM of the lengths of these cycles:

Example 9: Find the order of the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 3 & 2 & 7 & 8 & 6 \end{pmatrix}$

Solution: Consider the permutation, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 3 & 2 & 7 & 8 & 6 \end{pmatrix} = (14352)(678)$.

It has two disjoint cycles: $c_1 = (14352)$ of length 5 and $c_2 = (678)$ of length 2. Hence the order of the cycle (14352) is 5 and order of the cycle (678) is 3.

Then order of $\sigma = LCM\{O(c_1), O(c_2)\} = LCM(5,3) = 15$.

Note: If the cycles are not disjoint then first make to them disjoint for finding the order of the permutation.

Check your progress

If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 1 & 4 & 6 & 7 & 8 & 9 & 5 & 10 \end{pmatrix}$ then find the following problems.

Problem 1: Partition the given permutation into disjoint cycle including the length one.

Problem 2: Write the cycle decomposition of σ

Problem 3: Find the order of σ.

Problem 4: Find the inverse of σ.

6.9 *SUMMARY*

In this unit, we have studied, a **group permutation** is a mathematical concept involving the set of all permutations (rearrangements) of a given set, typically represented as S_n, the symmetric group of degree n. This group contains all $n!$ permutations of n elements and is equipped with the operation of composition, where two permutations are combined by performing one after the other. The identity permutation leaves all elements unchanged, and every permutation has an inverse that restores the original arrangement. Permutations can be expressed in cycle notation, which simplifies their analysis. The order of a permutation, determined as the least common multiple (LCM) of the lengths of its disjoint cycles, indicates how many times the permutation must be applied to return to the starting arrangement. Symmetric groups are fundamental in abstract algebra, with applications in combinatorics, geometry, and other fields of mathematics.

6.10 *GLOSSARY*

- Permutation group S_n.
- Alternating group A_n
- Cyclic permutation.
- Cycle decomposition.
- Transposition.
- De-arrangement.
- Similar permutation.
- Order of permutation.

6.11 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975),*Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.

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

6.12 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

6.13 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Define the symmetric group S_n. Explain the concept of permutations and their representation in cycle notation. Discuss the significance of disjoint cycles and how they simplify the study of permutations. Provide examples to illustrate your explanation.

2. What is the order of a permutation? Explain the steps to determine the order of a permutation using disjoint cycle notation. Why is the least common multiple (LCM) of cycle lengths significant in this context? Illustrate your answer with detailed examples.

3. Discuss the algebraic structure of the symmetric group S_n. Highlight its key properties, such as closure, associativity, the identity element, and inverses. Explain why S_n is non-abelian for $n \geq 3$and provide examples to support your discussion.

4. Show that S_4 is a non-abelian group of order 24.

5. What is a cyclic permutation? Explain its properties and how it differs from a general permutation. Discuss the role of cyclic permutations in the structure of S_n and give examples to illustrate your explanation.

6. Show that A_4 is a non-abelian group of order 12.

Short Answer Type Question:

1. Prove that S_2 is a finite abelian group.

2. Prove that A_n is subgroup of S_n

3. Prove that number of even and odd permutations in S_n are same.

4. Prove that the set A_n of all even permutation of degree *n* forms a group of order $\frac{n!}{2}$ with respect to the permutation multiplication

5. Prove that the inverse of an even permutation is an even permutation and the inverse of an odd permutation is an odd permutation.

6. Prove that the product of two even permutation is an even permutation.

7. Show that multiplication of permutation is not commutative in general.

Fill in the blanks:

1. The symmetric group S_n consists of all ……. of *n* elements.

2. The alternating group A_n is a subgroup of S_n that contains all ……permutations.

3. A transposition is a permutation that swaps …….. elements and leaves the rest unchanged.

4. The order of the symmetric group S_4 is ……

5. A permutation can be expressed as a product of ……..

6. A *k*-cycle is a permutation that cyclically permutes ……. elements.

7. The sign of a permutation is +1 if the permutation is …….

8. The identity permutation in S_n leaves every element ……

9. In S_3, the total number of permutations is ……

10. The composition of two even permutations results in an …… permutation.

Objective type questions:

1. What is the order of the symmetric group S_n?

a) n!

b) n^2

c) n

d) 2^n

2. Which of the following is true about a permutation group?

a) It is always abelian.

b) It is a subgroup of the symmetric group.

c) It contains only even permutations.
d) It is infinite for $n \geq 3$.

3. The alternating group A_n is defined as:
a) The set of all even permutations of S_n.
b) The set of all odd permutations of S_n.
c) The group of all permutations of size $n-1$.
d) The subgroup of all transpositions in S_n.

4. What is the number of transpositions required to express a permutation in S_n?
a) Exactly 1
b) Equal to the length of the permutation cycle
c) It depends on the permutation
d) Equal to n

5. The identity element in a permutation group S_n is represented by:
a) The permutation that reverses all elements
b) The permutation that leaves all elements unchanged
c) The longest cycle in S_n
d) The product of all transpositions in S_n

6. What is the sign of a permutation if it is an odd permutation?
a) +1
b) −1
c) 0
d) Depends on n

7. If σ and τ are two permutations in S_n, what is στ?
a) The sum of σ and τ.
b) The product of σ and τ.
c) The composition of σ and τ.
d) Always the identity element.

8. Which of the following is not a subgroup of S_3?
a) {e}
b) A_3
c) S_3
d) {(1 2),(1 3)}

9. In the permutation group S_4, the total number of even permutations is:
a) 12
b) 24
c) 6
d) 8

10. A cycle of length k in a permutation group is called a:
a) Transposition
b) k-cycle
c) Simple permutation
d) Subgroup

True and False questions:

1. Every permutation in S_n can be expressed as a product of transpositions.
2. The identity permutation is the only even permutation in S_n.
3. The order of a permutation is the smallest positive integer k such that the permutation raised to the k-th power is the identity.
4. The alternating group A_n is a normal subgroup of S_n.
5. The composition of two odd permutations is always an odd permutation.
6. In the symmetric group S_3, there are six elements, including the identity.
7. A transposition is an even permutation.
8. The alternating group A_4 has 12 elements.
9. The symmetric group S_n is abelian for $n \geq 3$.
10. Any subgroup of a symmetric group is itself a permutation group.

6.14 *ANSWERS*

Answer of check your progress:

Problem 1: $\sigma = (1\,3)(2)(4)(56789)(10)$

Problem 2: Cycle decomposition of $\sigma = \{1,1,1,2,5\}$

Problem 3: Order of $\sigma = 10$

Problem 4: $\sigma^{-1} = (13)(98765)$

Answer of objective question

1.	a)	**2.**	b)	**3.**	a)	**4.**	c)
5.	b)	**6.**	b)	**7.**	c)	**8.**	d)
9.	a)	**10.**	b)				

Answer of fill in the blanks:

1.	Permutation	**2.**	Even	**3.**	Two
4.	24	**5.**	Transposition	**6.**	K
7.	Even	**8.**	Unchanged	**9.**	6
10.	Even				

Answer of True and False

1.	True	**2.**	False	**3.**	True	**4.**	True
5.	False	**6.**	True	**7.**	False	**8.**	True
9.	False	**10.**	True				

Unit-7: GROUP HOMOMORPHISM

CONTENT:

7.1 *INTRODUCTION*

The term "homomorphism" appeared as early as 1892, when it was attributed to the mathematician Felix Klein (1849–1925).

Christian Felix Klein was a German mathematician and mathematics educator, known for his work with group theory, complex analysis, non-Euclidean geometry, and on the associations between geometry and group theory. His 1872 Erlangen program, classifying geometries by their basic symmetry groups, was an influential synthesis of much of the mathematics of the time.

Christian Felix Klein

25 April 1849 – 22 June 1925

A **homomorphism** is a fundamental concept in algebra and mathematics, particularly in the study of structures such as groups, rings, and vector spaces. It refers to a structure-preserving map between two algebraic structures of the same type. Homomorphisms are essential in understanding the relationships and transformations between these structures.

7.2 *OBJECTIVES*

After reading this unit learners will be able to

- Understand the concept of special types of mapping between two groups named as homomorphism which will helpful to deal with isomorphism. It may be possible these groups are under the different binary operations.
- Know that under the homomorphism mapping how the properties of two groups are relate.
- Understand about the other type of mapping like endomorphism and automorphism.
- Understand the basic properties of homomorphism and their related other theorems and definitions.

7.3 *HOMOMORPHISM*

Definition: A mapping f from a group $(G,*)$ into the group $(G',.)$ is said to be a homomorphism if it preserve the composition under f *i.e.*,

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

Or

A mapping $f : G \to G'$ is said to be homomorphism if,

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

where, G and G' are the groups under the operation $'*'$ and $'.'$ respectively.

Note 1: The range of f in G is called the homomorphic image of G'.

2: In general, we take both the groups G and G' under the same operation multiplication and write f is a homomorphism between G to G' if, $f(ab) = f(a)f(b) \ \forall a,b \in G$**,** without the loose of generality.

Example 1: A mapping $f : Z \to E$, from set of integer to the set of even integer such that $f(x) = 2x \forall x \in Z$

is a homomorphism.

Answer: We have given the mapping $f : Z \to E$ such that

$f(x) = 2x \forall x \in Z$

at first, we will check mapping is well defined as $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$

Now, we will check mapping also preserve the composition for it for any $x, y \in Z$

$f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$

$\Rightarrow f$ preserve the composition.

Hence given mapping f is an homomorphism.

Example 2: Show that the Mapping $f : Z \to G$, from set of integer under the operation addition to the group $G = \{1, -1\}$ under the operation multiplication defined as

$$f(x) = \begin{cases} 1, & if\ x\ is\ even \\ -1, & if\ x\ is\ odd \end{cases}$$

is a homomorphism.

Answer: Case I: If $x, y \in Z$ both are even integers. It means $f(x) = 1, f(y) = 1$ then their sum will also an even integer *i.e.*,

$f(x+y) = 1 = 1.1 = f(x) f(y)\ \forall x, y \in Z$

Case II: If $x, y \in Z$ both are odd integers i.e., $f(x) = -1, f(y) = -1$ then their sum will be even integer *i.e.*,

$f(x+y) = 1 = (-1).(-1) = f(x) f(y)\ \forall x, y \in Z$

Case III: If $x, y \in Z$ are such that x is even integer and y is odd integer *i.e.*, $f(x) = 1, f(y) = -1$ then their sum will be odd integer then,

$f(x+y) = -1 = 1.(-1) = f(x) f(y)\ \forall x, y \in Z$

Case IV: If $x, y \in Z$ are such that x is odd integer and y is even integer *i.e.*, $f(x) = -1, f(y) = 1$ then their sum will be odd integer then,

$f(x+y) = -1 = (-1).(1) = f(x) f(y)\ \forall x, y \in Z$

Hence the given mapping f is an homomorphism.

Example 3: Show that the Mapping $f : R^+ \to R$, from set of positive real numbers to the set of real number defined as $f(x) = \log x \forall x \in R^+$ is an homomorphism.

Answer: As we know that set of positive real numbers (R^+) is form group under the operation multiplication and the group R is form group under the operation addition.

Here, clearly the mapping is well-defined since, for

$x = y$

$\Rightarrow \log x = \log y$ [Taking logarithm both side]

$\Rightarrow f(x) = f(y) \; \forall \, x, y \in R^+$

Now, $f(xy) = \log(xy) = \log x + \log y = f(x) + f(y) \; \forall \, x, y \in R^+$

Hence *f* is a homomorphism.

Homomorphism onto: A **onto** mapping from a group $(G,*)$ into the group $(G',.)$ is said to be a homomorphism onto if it preserve the composition under f *i.e.*,

$f(a*b) = f(a).f(b) \; \forall \, a, b \in G$**.**

Endomorphism: A homomorphism from a group G to itself is called an endomorphism.

Example 4: If *G* be a group and a mapping such that, $f : G \to G$ such that $f(x) = x^{-1}$ be a homomorphism then show that *G* is a *A*belian group.

Proof: Since *G* be a group then for any elements $x, y \in G$, *G* will satisfies the closure property *i.e.*, $xy \in G$ and for every element belongs to *G* there exist its inverse in *G*.

Now, $xy = \left(y^{-1}x^{-1}\right)^{-1} = f\left(y^{-1}x^{-1}\right) = f\left(y^{-1}\right)f\left(x^{-1}\right) = yx$

$\Rightarrow G$ is *A*belian group.

Theorem 1: If $f : G \to G'$ be a homomorphism then,

- ***(i)*** If *e* is the identity of *G*, then $f(e)$ is the identity of G'
- ***(ii)*** For any element $a \in G$**,** $f(a^{-1}) = \left[f(a)\right]^{-1}$
- ***(iii)*** If *H* is subgroup of G then $f(H)$ is subgroup of G'
- ***(iv)*** If K is subgroup of G', then $f^{-1}(K) = \left\{k \in G \middle| f(k) \in G'\right\}$ is a subgroup of *G*. Furthermore, if *K* is normal in G' then $f^{-1}(K)$ is normal in *G*.
- ***(v)*** If order of any element $a \in G$ is finite then the order of $f(a)$ is divisor of the order of $a \in G$.

Proof (*i*): Let e and e' are the identity elements of the group *G* and G'. Since f is the mapping from *G* to G' then $f(e)$ will be the elements of G'.

Now, $e' f(e) = f(e) = f(ee) = f(e) f(e)$, then by the right cancellation law

$e' = f(e)$

i.e., $f(e)$ is the identity of G'.

(*ii*): Let *a* be any element of *G* then a^{-1} will be also in *G* because *G* itself a group. Since we have, $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$ … (1)

As we know that if $a \in G \Rightarrow f(a) \in G'$ and G' is also a group then $[f(a)]^{-1} \in G'$

Now multiplying by $[f(a)]^{-1}$ both side in equation (1)

Then, $[f(a)]^{-1}e' = [f(a)]^{-1}[f(a)f(a^{-1})] = ([f(a)]^{-1}f(a))f(a^{-1}) = f(a)$

So, $[f(a)]^{-1} = f(a)$

(*iii*): We have given *H* is subgroup of *G* then to prove that $f(H)$ is subgroup of G'. If $x, y \in H \Rightarrow xy^{-1} \in H$ [By the subgroup test of any nonempty subset of *G*]

Since f is the homomorphism then there exist $a, b \in f(H)$ *s.t.* $a = f(x), b = f(y)$

Now consider, $ab^{-1} = f(x)[f(y)]^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$

Hence we have prove that if $a, b \in f(H)$ then $ab^{-1} \in f(H)$

$\Rightarrow f(H)$ is subgroup of G'.

(*iv*): Let *K* is subgroup of G' and define *H* to be $f^{-1}(K)$; that is *H* is the set of all $g \in G$ such that $f(g) \in K \subseteq G'$. If $a, b \in H$, then $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} \in K$. Since *K* is subgroup of G'. Therefore, $ab^{-1} \in H$ and H is the subgroup of G.

If *K* is normal in G' then we have to show $g^{-1}hg \in H$ for $h \in H, g \in G$

But,

$f(g^{-1}hg) = f(g^{-1})f(h)[f(g)]^{-1} = [f(g)]^{-1}(f(h)[f(g)]) = ([f(g)]^{-1}f(g))f(h) = f(h) \in K$

Since *K* is normal in *G* therefore $g^{-1}hg \in H$

$\Rightarrow H$ is normal subgroup of *G*.

(*v*): Let $a \in G$ and $O(a) = m$ *i.e.*, $a^m = e$

Taking *f*-image both side we get, $f(a^m) = f(e)$

$\Rightarrow f(a)f(a)f(a)....f(a)$ (*m* times) $= f(e)$

$\Rightarrow [f(a)]^m = e'$

If order of $f(a)$ in G' is *n* then $o(f(a)) \mid O(a)$

7.3.1 *IMAGE OR RANGE OF A HOMOMORPHISM*

Definition: If $f : G \to G'$ is a homomorphism then range of homomorphism is defined as,

$Range\ f = f(G) = \{g' \in G \mid f(g) = g'\}$.

We can also say that $f(G) \subseteq G'$. It is also called image of a homomorphism.

Theorem 2: If $f : G \to G'$ is a homomorphism then range of homomorphism is subgroup of G'.

Proof: Let we consider, $x, y \in f(G)$.

$\Rightarrow \exists\ a, b \in G$ s.t., $f(a) = x, f(b) = y$. As we know, $f(G) \subseteq G'$.

Now, $xy^{-1} = f(a)(f(b))^{-1} = f(a)[f(b)]^{-1}$

$= f(ab^{-1}) = f(c)$ [Since f is a homomorphism]

where $c = ab^{-1} \in G$. [By one step subgroup test]

$\Rightarrow xy^{-1} \in f(G)$.

Hence range of homomorphism is a subgroup of co-domain.

Remarks 1: If f is onto homomorphism, then $G' = f(G)$.

2: If f is a homomorphism then we know that the range of homomorphism is a subgroup of co-domain. So, by the Lagrange's theorem $O(f(G)) \mid O(G')$.

Theorem 3: If $f : G \to G'$ is a homomorphism. If G is abelian then image of homomorphism is also an abelian subgroup of G'.

Proof: Let G is an abelian group and $f : G \to G'$ is an homomorphism. Let $x, y \in f(G)$ then $\exists\ a, b \in G$ s.t., $f(a) = x, f(b) = y$.

Now, $xy = f(a)f(b) = f(ab)$ [Since f is an homomorphism]

$= f(ba) = f(b)f(a) = yx$ [Since $a, b \in G$ and G is an abelian group i.e. $ab = ba$]

Hence $f(G)$ is an abelian whenever G is abelian.

Theorem 4: If $f:G\to G'$ is a homomorphism. If G is cyclic then image of homomorphism is also a cyclic subgroup of G'.

Proof: Let $f:G\to G'$ is an homomorphism, which means group operation must be preserved. Let $x,y\in G$ and $f(x)=x_1,\ f(y)=y_1\in f(G)$ be the respective images of x,y.

Now, $f(xy)=f(x)f(y)=x_1y_1$ [Since f is an homomorphism].

Given G be a cyclic and let a be the generator.

$G=<a>=\{a^n:n\in Z\}$. Let us assume that $f(G)$ is a cyclic. Group such that

$f(G)=<b>=\{b^l:l\in Z\}$. Let $x=a^m,\ y=a^n,\ x_1=b^k$ and $x_2=b^r$. It follows that:

$f(a^ma^n)=b^kb^r \Leftrightarrow f(a^{m+n})=b^{k+r}$

We can think we have to demonstrate that an element b may produce the elements in H that are the pictures of G through the homomorphism ϕ.
Since homomorphism transfers identity to identity, the identities may be produced using b by using the same exponent operation to the generator a:
$f(e=a^0=a^{m-m})=b^{m-m}=b^0=e',m\in Z$
Inverse to inverse is sent by homomorphism:
$f(a^{-m})=b^{-m'},m\in Z$
Therefore, as b can generate all the elements of $f(G)$, $f(G)$ is also cyclic.

7.3.2 *KERNEL OF A HOMOMORPHISM*

Definition: If $f:G\to G'$ is a homomorphism then kernel of homomorphism is the collection of all elements of domain set which are mapped into the identity elements of range set.

OR

If $f:G\to G'$ is a homomorphism then,

$\ker f=\{x\in G\mid f(x)=e'\}$

Where e' is the identity element of G'

Theorem 5: If $f:G\to G'$ is a homomorphism then $\ker f$ is the normal subgroup of G.

Proof: Since we have given $f: G \to G'$ is an homomorphism and we know that $\ker f = \{x \in G \mid f(x) = e'\}$ then first we will prove that $\ker f$ is a subgroup of *G*. for it let

$x, y \in \ker f \Rightarrow f(x) = e', f(y) = e'$

Now, $f(xy^{-1}) = f(x) f(y^{-1}) = f(x)[f(y)]^{-1} = e'[e']^{-1} = e'$

$\Rightarrow xy^{-1} \in \ker f$

Hence $\forall x, y \in \ker f$ we have $xy^{-1} \in \ker f$ it means $\ker f$ is the subgroup of *G*.

Now we have to prove that $\ker f$ is the normal subgroup of *G*. For it let g be any element of *G* and k be any element of $\ker f$. Then $f(k) = e'$, we have

$f(gkg^{-1}) = f(g) f(k) f(g^{-1}) = f(g)e' f(g^{-1}) = f(g)[f(g)]^{-1} = e'$

$\Rightarrow xgkg^{-1} \in \ker f$

Hence, $\ker f$ is normal subgroup of *G*.

Theorem 6: A homomorphism $f: G \to G'$ is one-one if and only if $\ker f = \{e\}$.

Proof: We have given $f: G \to G'$ is an homomorphism and let mapping is ono-one. If $x \in \ker f$ be any element

Then $f(x) = e'$ and also $f(e) = e'$

Since f is one-one so, $f(x) = f(e) \Rightarrow x = e \; \forall x \in \ker f$

Hence, $\ker f = \{e\}$.

Conversely, let $\ker f$ contains only the identity element.

For it let, $f(x) = f(y)$

then $f(x)[f(y)]^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \ker f = \{e\}$

$\Rightarrow xy^{-1} = \{e\}$

$\Rightarrow x = y$

$\Rightarrow f$ is one-one.

Check your progress

Problem 1: Is $f: (Z,+) \to (Z,+)$ such that $f(n) = k.n$, where k is fixed, a homomorphism?

Problem 2: Is $f:(Z,+)\to(Z_m,+_m)$ such that $f(n)=n \pmod m$, a homomorphism?

Problem 3: Is $f:(Z,+)\to(G=\{1,-1,i,-i\},.)$ such that $f(n)=i^n$, a homomorphism? Also find this homomorphism is one-one?

7.4 *SUMMARY*

In this unit, we have studied about the mapping like homomorphism which help identify and understand similarities between different algebraic structures by revealing how one structure can be transformed into another while maintaining its core properties. They play a crucial role in classification, simplification, and decomposing mathematical structures. Homomorphisms are ubiquitous in mathematics and serve as the building blocks for more complex concepts like isomorphisms, automorphisms and representations.

A **homomorphism** is a structure-preserving map between two algebraic structures of the same type, such as groups, rings, or vector spaces. It ensures that the operations in one structure correspond to the operations in the other, maintaining their algebraic properties. For example, in a group homomorphism *f*, the relation $f(a*b) = f(a)*f(b)$ holds for all elements *a* and *b*. Homomorphism's are crucial for understanding relationships between mathematical structures, as they reveal how one structure can be transformed into another while preserving its essential characteristics. They are foundational for concepts like kernels, images, isomorphism's, and automorphisms, making them central to algebra and its applications.

7.5 *GLOSSARY*

- Homomorphism
- Kernel of homomorphism mapping *f*.
- Range or Image of homomorphism
- Endomorphism

7.6 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.

- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- https://en.wikipedia.org/wiki/Center_(group_theory)#:~:text=By%20definition%2C%20the%20center%20is,of%20each%20element%20of%20G.

7.7 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

7.8 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that if $f : G \to G'$ is a homomorphism. If G is cyclic then image of homomorphism is also a cyclic subgroup of G'.

2. A homomorphism $f : G \to G'$ is one-one if and only if $\ker f = \{e\}$.

3. If $f : G \to G'$ is an homomorphism then prove that the set $A = \{x \in G \mid f(x) = e'\}$ where e' is the identity element of G' is the normal subgroup of G.

4. Prove that if $f : G \to G'$ is an homomorphism then order of any element $f(a) \in G'$ is divisor of the order of $a \in G$.

5. If two subgroups H, K are normal in G such that $H \subseteq K$, then

$$\frac{G}{K} \cong \frac{G \setminus H}{K \setminus H}$$

Short Answer Type Question:

1. Prove that if $f : G \to G'$ is a homomorphism then range of homomorphism is subgroup of G'.

2. Prove that if $f : G \to G'$ is an homomorphism and H is subgroup of G then $f(H)$ is subgroup of G'.

3. If f is a homomorphism from $f : G \to G'$ then prove that f is one-one if and only if $\ker f = \{e\}$.

4. An endomorphism f in a group G such that $f(x) = x^{-1}$ then G is abelian.

5. Prove that if $f : G \to G'$ is a homomorphism then $\ker f$ is the normal subgroup of G.

Fill in the blanks:

1. If $f : G \to G'$ be a homomorphism then for any element $a \in G$, $f(a^{-1}) = ...$

2. If $f : G \to G'$ be a homomorphism and e is the identity element of G then identity element of G' will be ……

3. …… is the infinite cyclic group

4. A cyclic group of order 123456789 is isomorphic to …….

5. The kernel of a group homomorphism $\phi : G \to H$ is a …… subgroup of G.

6. The …… homomorphism maps every element of G to the identity element of H.

7. If $\phi : G \to H$ is a homomorphism, then $\phi(g^{-1}) = ……$

8. The image of a group homomorphism is a …… of the codomain.

Objective questions:

1. A function $\phi : G \to H$ is a group homomorphism if:

(A) $\phi(a.b) = \phi(a) + \phi(b)$

(B) $\phi(a.b) = \phi(a).\phi(b)$

(C) $\phi(a.b) = a.b$

(D) $\phi(a.b) = \phi(b).\phi(a)$

2. If a function $\phi : G \to H$ is a group homomorphism, which of the following is always true?

(A) $\phi(e_G) = e_H$, where e_G, e_H are identity of G and H respectively.

(B) $\phi(e_G) \neq e_H$

(C) $\phi(e_G)$ is undefined

(D) None

3. The kernel of a group homomorphism $\phi : G \to H$ is defined as:

(A) $Ker(\phi) = \{g \in G \mid \phi(g) = e_G\}$

(B) $Ker(\phi) = \{h \in H \mid \phi(h) = e_H\}$

(C) $Ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$

(D) $Ker(\phi) = \{h \in H \mid \phi(h) = e_G\}$

4. If a function $\phi : G \to H$ is a group homomorphism, which of the following is true about the image of ϕ?

(A) It is a normal subgroup of H

(B) It is a subgroup of H

(C) It is a proper subgroup of H

(D) None of these.

5. Which of the following is NOT preserved under a group homomorphism $\phi : G \to H$?

(A) Identity element

(B) Inverse

(C) Group of individual elements

(D) Closure under the group operation

6. A group homomorphism $\phi : G \to H$ maps an abelian group G to:

(A) An Abelian group H

(B) An non-abelian group H

(C) Either an abelian or non-abelian group H

(D) None

7. Let $\phi : G \to H$ be a homomorphism. The kernel of ϕ:

(A) Is a subgroup of G but not necessarily normal

(B) Is a normal subgroup of G

(C) Is a subgroup of H

(D) May not be a subgroup of G

TRUE (T) and FALSE (F):

1. A homomorphism $\phi : G \to H$ maps every subgroup of *G* to a subgroup of *H*.

2. If $\phi : G \to H$ is a surjective homomorphism and *G* is cyclic, then *H* is cyclic.

3. The image of a group homomorphism is always a normal subgroup of the codomain.

4. A homomorphism $\phi : G \to H$ is a homomorphism and $\phi(G) \neq e_H \; \forall \, g \in G$, then G has no identity element.

7.9 *ANSWERS*

Answer of self cheque question:

1. Yes **2.** Yes **3.** Yes this is homomorphism but not on-to.

Answer of fill in the blanks

1. $[f(a)]^{-1}$ **2.** $f(e)$ **3.** $\boldsymbol{Z}$ **4.** $Z_{123456789}$

5. Normal **6.** Trivial **7.** $(\phi(g))^{-1}$ **8.** Subgroup

Answer of objective type question:

1. (B) **2.** (A) **3.** (C) **4.** (B)
5. (C) **6.** (C) **7.** (B)

Answer of TRUE and FALSE:

1. F **2.** T **3.** F **4.** F

Unit-8: GROUP ISOMORPHISM

CONTENT:

8.1 *INTRODUCTION*

Group isomorphism is a fundamental concept in abstract algebra that formalizes the idea of two groups being structurally identical, even if their elements and operations appear different on the surface. Specifically, an isomorphism between two groups is a bijective (one-to-one and onto) function that preserves the group operation, meaning that the image of the product of any two elements in the first group is equal to the product of their images in the second group. This concept allows mathematicians to classify and study groups by their underlying structure rather than their specific representations, facilitating the identification of groups that are essentially the same in terms of their algebraic properties. Understanding group isomorphism is crucial for exploring deeper relationships within group theory and its applications across various areas of mathematics and science.

8.2 *OBJECTIVES*

The objectives of this unit on isomorphism in group theory are typically focused on understanding and applying the concept of structural equivalence between groups. The key objectives include:

1. **Understanding Isomorphism**: To define group isomorphism formally and explain its significance in identifying groups that are structurally identical, regardless of their representation.
2. **Recognizing Isomorphic Groups**: To develop the ability to determine whether two groups are isomorphic by verifying the properties of an isomorphism, such as bijectiveness and preservation of the group operation.
3. **Exploring Properties**: To examine the properties of groups that are preserved under isomorphism, such as order, group structure, and specific characteristics like commutativity.
4. **Classifying Groups**: To use isomorphism as a tool for classifying groups into equivalence classes, simplifying the study of group theory by focusing on group structures rather than specific examples.
5. **Applications of Isomorphism**: To apply the concept of isomorphism in solving problems in abstract algebra and understanding its implications in other mathematical and scientific contexts.
6. **Building Intuition**: To provide illustrative examples and counterexamples that deepen the conceptual understanding of group isomorphism.

By achieving these objectives, students gain a foundational grasp of isomorphism, enabling them to explore deeper topics in algebra and related fields.

8.3 *ISOMORPHISM*

Two groups are **isomorphic** if there exists a one-to-one correspondence (bijection) between their elements that preserves the group operation. In simpler terms, two groups are isomorphic if they have the same structure, meaning they behave the same mathematically, even if their elements or how they are represented might look different.

Definition: A mapping f from a group $(G,*)$ into the group $(G',.)$ is said to be isomorphism if it satisfies the following condition,

(i) f is ono-one *i.e,* f is injective i.e., distinct element in G have distinct *f*- image in G'

(ii) f is on-to *i.e,* f is surjective.

(iii) $f(a*b) = f(a).f(b)\ \forall a,b \in G$ *i.e.,* f preserve the composition i.e. the image of the product is the product of the images.

Key Properties of Isomorphic Groups:

1. **Bijection**: The mapping ϕ is both injective (one-to-one) and surjective (onto), ensuring every element of *H* corresponds to exactly one element of *G*.

2. **Preservation of Structure**: The group operation is preserved, meaning the result of combining two elements in G is mapped to the combination of their images in H.

Implications:

- If G and H are isomorphic, they are "essentially the same" as groups. Their order (number of elements), subgroup structure, and other group-theoretic properties are identical.
- However, their specific representations or elements may differ.

Example:

1. The additive group of integers modulo 4 (Z_4) and the cyclic group of order 4 are isomorphic because both have the same structure: a single generator that cycles through four elements.

2. The group of rotations of a square and Z_4 are not isomorphic, because the rotation group includes reflections, making it non-cyclic, whereas Z_4 is cyclic.

Example 1: Show that the Mapping $f : R^+ \to R$, from set of positive real numbers to the set of real number defined as $f(x) = \log x \forall x \in R^+$ is an isomorphism.

Answer: In the previous example we have already proved that given mapping is a homomorphism. Now, we are going only to show that mapping (*f*) is a bijective mapping (*i.e.*, *f* is one-one and on-to)

One-One: Let $x, y \in R^+ s.t., \ f(x) = f(y)$

$\Rightarrow \log x = \log y$

$\Rightarrow e^{\log x} = e^{\log y}$

$\Rightarrow x = y$

$\Rightarrow f$ is one-one mapping.

On-to: If $y \in R$ be any real number then clearly $e^y \in R^+$. It means for each $y \in R$ we have $e^y \in R^+$ such that $f(e^y) = \log(e^y) = y \in R$

$\Rightarrow f$ is on-to mapping.

Hence, f is an isomorphism.

Example 2: Show that there is no isomorphism from $f: Q \to Q - \{0\}$ where, Q is set of rational number.

Answer: To prove this example let we assume that $f: Q \to Q - \{0\}$ is an isomorphism. Since f is an isomorphism so f will also a on-to function i.e., for $2 \in Q - \{0\} \exists x \in Q$ s.t.,

$f(x) = 2$

$\Rightarrow f\left[\frac{x}{2} + \frac{x}{2}\right] = 2$

$\Rightarrow f\left(\frac{x}{2}\right) f\left(\frac{x}{2}\right) = 2$ [Since, f preserve the compostion]

$\Rightarrow f\left(\frac{x}{2}\right) f\left(\frac{x}{2}\right) = 2$

$\Rightarrow y^2 = 2$ where, $y = f\left(\frac{x}{2}\right)$, which is a contradiction because there is no rational number which is the solution of quadratic equation $x^2 - 2 = 0$. Hence our assumption is wrong. So, there is no map $f: Q \to Q - \{0\}$ which is an isomorphism.

Some important properties of isomorphic mappings:

Let f be a isomorphic mapping of a group G into a group G' then followings are some properties to be noted.

(i) The f – image of the identity e of G is the identity of G' i.e., $f(e)$ is the identity of G'.

Proof: Let e be the identity of G and e' be the identity of G'. Let a any element of G. Then $f(a) \in G'$.

Now, $e' f(a) = f(a)$ [$\because e'$ is the identity of G']

$= f(ea)$ [$\because e$ is the identity of G]

$= f(e) f(a)$ [$\because f$ is an isomorphic mapping]

Now in the group G', we have

$e' f(a) = f(e) f(a)$

$\Rightarrow e' = f(e)$ [by right cancellation law in G']

$\therefore f(e)$ is the identity of G'

(ii) The $f-$image of the inverse of an element *a* of G is the inverse of the *f*-image of a i.e., $f(a^{-1}) = [f(a)]^{-1}$

Proof: Suppose e is the identity of G and e' is the identity of G'. Then $f(e) = e'$. Now let a be any element of G. Then $a^{-1} \in G$ and $aa^{-1} = e$. We have

$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$ [$\because f$ is a composition preserving]

Therefore $f(a^{-1})$ is the inverse of $f(a)$ in the group G'. Thus $f(a^{-1}) = [f(a)]^{-1}$.

(iii) The order of an element *a* of G is equal to the order of its image $f(a)$.

Proof: Suppose e is the identity of G. Then $f(e)$ is the identity of G'. Let the order of *a* be finite and let it be equal to *n*.

Then $a^n = e \Rightarrow f(a^n) = f(e)$

$\Rightarrow f(aaaaa.....n\,times) = f(e)$

$\Rightarrow f(a)f(a)f(a)....n\,times = f(e)$

$\Rightarrow [f(a)]^n = f(e) \Rightarrow$ order of $f(a) \le n$.

If now the order of $f(a)$ is m, then

$[f(a)]^m = f(e)$

$\Rightarrow f(a)f(a)f(a)....m\,times = f(e)$

$\Rightarrow f(aaaaa.....m\,times) = f(e) \Rightarrow f(a^m) = f(e)$

$\Rightarrow a^m = e$

$\Rightarrow$ order of $a \le m$

Thus $m \le n$ and $n \le m \Rightarrow m = n$

Remarks: If two groups G_1 and G_2 are isomorphic then following points we achieved.

1. G_1 is abelian $\Leftrightarrow G_2$ is abelian.

2. G_1 is cyclic $\Leftrightarrow G_2$ is cyclic.

3. G_1 is non-abelian $\Leftrightarrow G_2$ is non-abelian.

4. Order of G_1 is $n \Leftrightarrow$ Order of G_2 is n.

5. G_1 is countable $\Leftrightarrow G_2$ is countable.

6. G_1 has m element of order k $\Leftrightarrow G_2$ has m element of order k.

7. G_1 has r subgroup of order n $\Leftrightarrow G_2$ has r subgroup of order n.

8. G_1 and G_2 has the same class equation.

9. $Z(G_1) \cong Z(G_2)$.

10. No. of conjugate classes class in G_1 = No. of conjugate classes class in G_2

Infact, G_1 and G_2 are the same group in two different notation for the elements and for the binary operation.

Note 1: If $O(a)$ is finite then, then $O[f(a)]$ can not be finite.

2: While forming such a mapping we should keep in mind the above three facts that an isomorphic mapping must preserve identities, inverse and orders.

Theorem 1: Let N be a normal subgroup of a group G. A mapping f, $f: G \to G/N$ defined as $f(x) = Nx \forall x \in G$ then f is a homomorphism of G onto G/N and $\ker f = N$.

Proof: We have given the mapping $f: G \to G/N$ such that $f(x) = Nx \forall x \in G$. As we know if $x \in G$ then $Nx \in G/N$.

First we will check that f is a onto homomorphism from G to G/N. For it, let $a, b \in G/N$ then,

$f(ab) = Nab = (Na)(Nb) = f(a)f(b)$ [$\because N$ is normal subgroup of G]

$\Rightarrow f$ is a homomorphism from G to G/N.

Since for each element $Nx \in G/N$ there exist an element $x \in G$ such that $f(x) = Nx \forall x \in G$.

Hence, f is on-to mapping.

Let $\ker f$ is the kernel of this homomorphism then, $\ker f = \{x \in G \mid f(x) = N\}$

Now, we have only to prove that $\ker f = N$. Let x be any element of $\ker f$. Then $f(x) = N$, where N is the identity of G/N. But according to mapping $f(x) = Nx = N$ *i.e.*, $Nx = N \Rightarrow x \in N$ [Because if H is normal subgroup of G and $Hx = H$ then $x \in H$]

So, $x \in \ker f \Rightarrow x \in N$. Therefore $\ker f \subseteq N$

Conversely, let y be any element of N. Then $Ny = N$

We have $f(n) = Nn = N$. Therefore $n \in \ker f$

Thus, $n \in N \Rightarrow n \in \ker f$. Therefore $N \subseteq \ker f$

Hence, $\ker f = N$.

8.4 *FUNDAMENTAL THEOREMS*

Theorem 2: Fundamental theorem on group homomorphism: If $f: G \to G'$ is onto homomorphism then $\frac{G}{K} \cong G'$ where $K = \ker f$

OR

In other word, "Every homomorphic image of a group *G* is isomorphic to some quotient group of *G*".

Proof: We have given a on-to homomorphism f from $G \, to \, G'$. Let we define a map

$\phi: \frac{G}{K} \to G'$ s.t. $\phi(Ka) = f(a), a \in G$

First, we have to show that ϕ is an isomorphism. For it initially we shall show the mapping ϕ is well-defined by, $Ka = kb$

$\Rightarrow ab^{-1} \in K = \ker f$

$\Rightarrow f(ab^{-1}) = e'$

$\Rightarrow f(a) f(b^{-1}) = e'$

$\Rightarrow f(a)[f(b)]^{-1} = e'$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \phi(Ka) = \phi(Kb)$

On retracing theses steps backwards, we will get that ϕ is one-one.

Again as $\phi(KaKb) = \phi(Kab) = f(ab) = f(a) f(b) = \phi(Ka)\phi(Kb)$

$\Rightarrow \phi$ is an homomorpshism.

Now we will check ϕ is onto, let $g' \in G'$ be any element. Since $f: G \to G'$ is onto then there exist $g \in G$ such that,

$f(g) = g'$

Now, $\phi[Kg] = f(g) = g'$.

$\Rightarrow \phi$ is on-to

$\therefore \phi$ is an isomorphism.

Hence, $\frac{G}{K} \cong G'$.

Theorem 3: (Second fundamental theorem of Isomorphism). If H and K are two subgroups of the group G where H is normal subgroup of G then,

$\frac{HK}{H} \cong \frac{K}{H \cap K}$.

Proof: By the previous theorems in normal subgroups we can easily seen that $H \cap K$ will be normal subgroup of K because $H \cap K \subseteq H$ *and* $H \cap K \subseteq K$. Similarly, as $H \subseteq HK \subseteq G, H$ will be normal in *HK*.

Now, we define a map $f : K \to \frac{HK}{H}$ s.t.,

$f(k) = Hk$

Then as $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$

Which shows the mapping is well-defined.

Again, $f(k_1 k_2) = Hk_1 k_2 \Rightarrow Hk_1 Hk_2 = f(k_1) f(k_2)$

$\Rightarrow f$ is an homomorphism.

Obviously, the mapping is on-to also then by using the first fundamental theorem we find that

$\frac{HK}{H} \cong \frac{K}{\ker f}$

Since, $k \in \ker f \Leftrightarrow f(k) = H$

$\Leftrightarrow Hk = H$

$\Leftrightarrow k \in H$ [As *H* is normal subgroup of *G*]

$\Leftrightarrow k \in H \cap K$ [$k \in K$ *as* $\ker f \subseteq K$]

So, $\ker f = H \cap K$

Hence the theorem is proved.

Lemma: Let in a group G, if H, K are normal in G such that $H \subseteq K$, then $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and converse of the theorem is also true.

Proof: $\frac{K}{H}$ is a non empty subset of $\frac{G}{H}$, by definition.

Now, for any $Hk_1, Hk_2 \in \frac{K}{H}$

$(Hk_1)(Hk_2)^{-1} = (Hk_1)(Hk_2^{-1}) = Hk_1 k_2^{-1} \in \frac{K}{H}$

$\Rightarrow \frac{K}{H}$ is a subgroup.

Again for any $Hk \in \frac{K}{H}$ and $Hg \in \frac{G}{H}$, we notice that

$(Hg)^{-1}(Hk)(Hg) = Hg^{-1}HkHg = Hg^{-1}kg \in \frac{K}{H}$

as $g \in G, k \in K, K$ is normal in G gives $g^{-1}kg \in K$.

Conversely, let any element $x \in G$ and $k \in K$. In order to prove that K is normal in G we must show that $xkx^{-1} \in K$.

We know that $Hx \in \frac{G}{H} where\, x \in G$ and $Hk \in \frac{K}{H} where\, k \in K$. Since we have given $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$, therefore

$(Hx)(Hk)(Hx)^{-1} \in \frac{K}{H}$

$\Rightarrow Hxkx^{-1} \in \frac{K}{H}$ [As H is normal in G]

$\Rightarrow xkx^{-1} \in K$

$\therefore K$ is normal subgroup of G. Also the quotient group $\frac{K}{H}$ implies that H is normal in G. Therefore, K is normal subgroup of G and $H \subseteq K$.

Theorem 4: (Third isomorphism theorem). If two subgroups H, K are normal in G such that $H \subseteq K$, then

$\frac{G}{K} \cong \frac{G \setminus H}{K \setminus H}$

Proof: By the above lemma we know that if H, K are normal in G such that $H \subseteq K$, then $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and, therefore, we can talk about $\frac{G \setminus H}{K \setminus H}$.

First, we will define a map $f : \frac{G}{H} \to \frac{G}{K}$ s.t.,

$f(Ha) = Ka, a \in G$

Since, H is well defined as

$Ha = Hb$

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

$\Rightarrow Ka = Kb$

$\Rightarrow f(Ha) = f(Hb)$

Now, we will check f is a homomorphism as

$f(HaHb) = f(Hab) = Kab = (Ka)(Kb) = f(Ha)f(Hb)$.

Here, ontoness of f is obvious.

Using first fundamental theorem of group homomorphism we can write that,

$\frac{G}{K} \cong \frac{G/H}{\ker f}$, so, we will claim that $\ker f = \frac{K}{H}$.

A member of $\ker f$ will be some member of $\frac{G}{H}$.

Now, $Ha \in \ker f \Leftrightarrow f(Ha) = K$

$\Leftrightarrow Ka = K$

$\Leftrightarrow a \in K$

$\Leftrightarrow Ha \in \frac{K}{H}$

Hence we find $\frac{G}{K} \cong \frac{G/H}{K/H}$

Hence our result is proved. This theorem is also named as "Freshman's Theorem".

Remarks: In the above theorem, since we have put $\frac{K}{H} = \ker f$ because we have notice that $\frac{K}{H}$ is normal in $\frac{G}{H}$ and hence we are talking about $\frac{G/H}{K/H}$. Thus we do not need to prove separately that $\frac{K}{H}$ is normal in $\frac{G}{H}$.

Theorem 5: Let the mapping $f: G \to G'$ be an onto homomorphism with $\ker f = K$. Let the subgroup H' of the group G', define

$H = \{x \in G \mid f(x) \in H'\}$

Then

(i) H is subgroup of G and $K \subseteq H$.

(ii) H' is normal in G' *iff* H is normal in G.

(iii) H' is normal in G' then $\frac{G'}{H'} \cong \frac{G}{H}$

(iv) There exist a one to one association from the from the family S' of all subgroup of G' onto the family S of all subgroup of G, that contain K.

Proof (i): Since, $f(e) = e' \in H' \Rightarrow e \in H$, it means $H \neq \phi$.

Let $x, y \in H \Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x)[f(y)]^{-1} \in H'$

$\Rightarrow f(xy^{-1}) \in H'$

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

Thus H is subgroup of G.

Since $x \in \ker f = K \Rightarrow f(x) = e' \in H'$

Hence for each $x \in K$ we have $x \in H \Rightarrow K \subseteq H$.

(ii): Suppose H is normal subgroup of G. Let the elements $g' \in G', h' \in H'$. Since the given mapping is onto so $\exists g \in G, h \in H$ s.t. $f(g) = g'$, $f(h) = h'$. Since $h \in H, h' \in H'$

Now,

$g^{-1}h'g' = (f(g))^{-1} f(h) f(g)$

$= f(g^{-1}) f(h) f(g) = f(g^{-1}hg) \in H'$ [Because H is normal subgroup in G means $g^{-1}hg \in H$]

Thus H' is normal in G'.

Conversely, assume that H' is normal in G'.

For any elements $h \in H$, $g \in G$,

$f(g^{-1}hg) = (f(g))^{-1} f(h) f(g) \in H'$

as $f(h) \in H', f(g) \in G'$

as $f(h) \in H', f(g) \in G'$ [H' is normal in G']

$\Rightarrow g^{-1}hg \in H$

i.e., H is normal in G

(iii) Let us defining a mapping $\phi : G \to \frac{G'}{H'}$ s.t.,

$\phi(g) = H' f(g)$

Since ϕ is well define as $g_1 = g_2 \Rightarrow f(g_1) = f(g_2)$

$\Rightarrow H' f(g_1) = H' f(g_2)$

$\Rightarrow \phi(g_1) = \phi(g_2)$, which shows mapping is well defined.

Now, we will verify that the mapping ϕ preserve the composition as

$\phi(g_1 g_2) = H' f(g_1 g_2) = H' f(g_1) f(g_2) = H' f(g_1) H' f(g_2) = \phi(g_1)\phi(g_2)$

Again, for any $H'g' \in \frac{G'}{H'}$, since $g' \in G'$ and f is onto $\exists g \in G$ s.t., $f(g) = g'$

Or that $\phi(g) = H' f(g) = H'g'$ showing that ϕ is onto.

By using fundamental theorem then

$$\frac{G'}{H'} \cong \frac{G}{\ker \phi}$$

Now, $x \in \ker\phi \Leftrightarrow \phi(x) = H'$

$\Leftrightarrow H' f(x) = H'$

$\Leftrightarrow f(x) \in H' \Leftrightarrow x \in H$

Hence $\ker\phi = H$

(iv) Define mapping $\psi : S' \to S$, s.t.,

$\psi(H') = H$

Where H is $\{x \in G \mid f(x) \in H'\}$ for any H' in S' by (i) we know that it is subgroup of G, containing K and thus a member of S. ψ is well defined mapping.

Let now $\psi(H') = \psi(T')$ where $H', T' \in S'$

Then $H = T$ where

$H = \{x \in G \mid f(x) \in H'\}$

$T = \{x \in G \mid f(x) \in T'\}$

Now for any $h' \in H' \subseteq G'$, since $f : G \to G'$ is onto, we can find $h \in G$, s.t.,

$f(h) = h' \in H'$

But this shows $h \in H = T$

$\Rightarrow f(h) \in T'$

$\Rightarrow h' \in T' \Rightarrow H' \subseteq T'$

Similarly $T' \subseteq H'$

i.e., $T' = H'$ or ψ is one-one.

We will show now that ψ is onto.

Let $H \in S$ be any member, H is a subgroup of G and $K \subseteq H$.

Consider $f(H) = \{f(h) \mid h \in H\}$

Then $f(H) \neq \phi$ as $e \in H \Rightarrow f(e) = e' \in f(H)$

Again, for any $f(h_1), f(h_2) \in f(H), h_1, h_2 \in H$

And $f(h_1)(f(h_2))^{-1} = f(h_1 h_2^{-1}) \in f(H)$

i.e., $f(H)$ is subgroup of G'.

We show $f(H) = H'$ is the required pre-image of H under ψ,

i.e., we show $\psi(H') = H$,

For it we have to show $H = \{x \in G \mid f(x) \in H'\}$

Let $x \in H$ then $f(x) \in f(H) = H'$

$\Rightarrow x \in \{x \in G \mid f(x) \in H'\}$

Or that $H \subseteq \{x \in G \mid f(x) \in H'\}$

Again, if $x \in \{x \in G \mid f(x) \in H'\}$

Then $f(x) \in H' = f(H)$

$\exists h \in H, s.t.\ f(x) = f(h)$

$\Rightarrow f(xh^{-1}) = e'$

$\Rightarrow xh^{-1} \in \ker f = K$

$\Rightarrow x \in Kh \subseteq H \quad [K \subseteq H]$

Thus $\{x \in G \mid f(x) \in H'\} \subseteq H$

Hence $H = \{x \in G \mid f(x) \in H'\}$

Or that $\psi(H') = H$ and so ψ is onto

Hence the theorem proved.

Example 3: Show that any infinite cyclic group is isomorphic to $G =< Z, + >$ the group of integers.

Solution: Let $G =< a >$ be any infinite cyclic group.

Define, $f : G \to Z$, *s.t.*,

$f(a^i) = i,\ i \in Z$

Since $G =< a >$ is of infinite order, $a^i \in G$ for all $i \in Z$ and $a^i = a^j$ for no $i \neq j$

Thus $a^i = a^j \Rightarrow i = j \Rightarrow f(a^i) = f(a^j)$ or that f is well defined.

Again $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j \Rightarrow f$ is 1-1.

$f(a^i.a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$

Shows that f is a homomorphism.

f is obviously onto and hence the isomorphism is established.

Corollary: Every subgroup of an infinite cyclic group is an infinite cyclic group which is isomorphic to the group itself.

Example 4: Any finite cyclic group of order n is isomorphic to Z_n the group of integers addition modulo n.

Solution: Let $G =< a >$ be a cyclic group s.t.,

$O(G) = O(a) = n$

then $G = \{e, a, a^2, ..., a^{n-1}\}, Z_n = \{0, 1, 2, ..., n-1\}$

Define $f : G \to Z_n$ s.t., $f(a^i) = i$

f is clearly well defined 1-1 onto mapping.

Again $f(a^i.a^j) = f(a^{i+_n j}) = i +_n j = f(a^i) +_n f(a^j)$

Thus f is a homomorphism and hence an isomorphism.

Remark: Any two cyclic groups of same order (finite) are isomorphic and each cyclic group of infinite order is isomorphic to Z (set of integer).

Check your progress

Problem 1: Since $Q_4 \cong Z_2 \times Z_2$, then find whether the identity element 1 of Q_4 map in $Z_2 \times Z_2$?

Problem 2: Is $Z_4 \cong Q_8$ and why?

8.5 *SUMMARY*

In this unit we have learned group isomorphism is a concept in abstract algebra that identifies when two groups are structurally identical. Two groups are isomorphic if there exists a bijective mapping between them that preserves the group operation, ensuring that the algebraic structure of one group corresponds exactly to the other. This equivalence focuses on the underlying structure rather than the specific elements or representations of the groups. Isomorphic groups share properties like order, identity, inverses, and the results of operations, making isomorphism a powerful tool for classifying and studying groups in a simplified and generalized way. On the other manner we can say that if two groups are isomorphic in which one group is completely given then on the basis of given group we can unfold the unknown group completely even these groups are under the different binary operations. We have also learned about the fundamental theorems of isomorphism which are helpful to solve out various problems.

One of the important concept we have learned in this unit that every infinite cyclic group is isomorphic to the set of integers (Z).

8.6 *GLOSSARY*

- $G \cong G'$ represents two groups G, G' are isomorphic to each other.
- Fundamental theorem on isomorphism

8.7 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- https://en.wikipedia.org/wiki/Center_(group_theory)#:~:text=By%20definition%2C%20the%20center%20is,of%20each%20element%20of%20G.

8.8 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

8.9 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that every finite cyclic group of order n is isomorphic to the set of integer under the operation addition modulo *n*.

2. Prove that every infinite cyclic group is isomorphic to Z.

3. Prove that there is no isomorphism from Q to $Q^* = Q - \{0\}$.

4. If two subgroups H, K are normal in G such that $H \subseteq K$, then

$$\frac{G}{K} \cong \frac{G \setminus H}{K \setminus H}$$

5. Prove that relation of isomorphism is an equivalence relation.

6. State and prove the fundamental theorem on group homomorphism.

7. State and prove the second fundamental theorem of Isomorphism.

9. State and prove the third fundamental theorem of Isomorphism.

Short Answer Type Question:

1. If $f : G \to G'$ is an homomorphism and *H* is subgroup of G then $f(H)$ is subgroup of G'.

2. If f is a homomorphism from $f : G \to G'$ then prove that f is one-one if and only if $\ker f = \{e\}$.

3. Prove that any finite cyclic group of order n is isomorphic to the quotient group Z / N, where $N =< n >$

4. An endomorphism *f* in a group *G* such that $f(x) = x^{-1}$ then G is abelian.

Objective type question

1. **What does it mean for two groups *G* and *H* to be isomorphic?**
a) They have the same number of elements.

b) They are structurally identical but may have different element labels.
c) Their multiplication tables are the same in layout.
d) They have the same generators.

2. Which of the following properties is preserved under group isomorphism?
a) Order of the group.
b) Order of an element.
c) Commutativity of the group.
d) All of the above.

3. If two groups *G* and *H* are isomorphic, which of the following statements is true?
a) G and H have the same number of subgroups.
b) G and H have the same order.
c) G and H have the same group operation.
d) Both a) and b).

4. If G and H are isomorphic groups, which of the following is not necessarily true?
a) G and H have the same number of elements of each order.
b) G and H have the same subgroup lattice.
c) G and H are cyclic.
d) G and H have identical presentations.

5. Which of the following groups is isomorphic to Z_4?
a) The Klein four-group V_4
b) The group $\{1,i,-1,-i\}$ under multiplication.
c) $Z_2 \times Z_2$.
d) The group of integers modulo 4 under addition.

6. If G is a group of order 35, then G:
a) Is cyclic.
b) Is isomorphic to Z_{35}.
c) Has a unique group structure.
d) All of the above.

7. How many non-isomorphic groups are there of order 8?
a) 3
b) 5
c) 6
d) 8

8. Which of the following statements is true about isomorphic groups G and H?
a) G and H have the same order of elements.

b) If G is cyclic, H must be cyclic.
c) If G is abelian, H must be abelian.
d) All of the above.

9. If G and H are isomorphic groups, then:
a) They have the same group operation.
b) They have the same multiplication table (up to relabeling).
c) Their elements are exactly the same.
d) They have the same generators but different subgroup structures.

10. Which of the following is a necessary condition for two groups to be isomorphic?
a) They have the same number of generators.
b) They have the same order.
c) They are both abelian or both non-abelian.
d) All of the above.

11. Two groups GGG and HHH are said to be isomorphic if:
a) They have the same number of elements.
b) They have the same algebraic structure.
c) They have the same identity element.
d) They have the same order of elements.

12. Which of the following is *not* preserved under an isomorphism?
a) Order of the group.
b) Commutativity of the group.
c) The specific symbols used for elements.
d) The group operation.

13. If G≅H, which of the following statements is true?
a) G and H have the same number of subgroups.
b) G and H are both finite or both infinite.
c) G and H have the same order of elements.
d) All of the above.

Fill in the blanks:

1. If two groups G, G' are isomorphic then $O(G)$ =.....
2. If two groups G, G' of finite order are isomorphic then number of elements of order n in G are = …….
3. A cyclic group of order 123456789 is isomorphic to …….
4. If G≅H and G has n generators, then H also has …… generators.

5. Two groups G and H are isomorphic if there exists a ……. mapping $\phi : G \to H$ that is a bijective homomorphism.

6. If G and H are isomorphic, then they have the same …… of elements.

7. If G is a cyclic group of order n, then G is isomorphic to ……..

8. Every group of prime order p is …… and isomorphic to Z_p.

9. If two groups are isomorphic, their subgroup …….. are identical.

10. If two groups G and H are isomorphic, their center Z(G) is isomorphic to ……..

11. If G and H are isomorphic, then G is abelian if and only if …….. is abelian.

True and False question:

1. If two groups G and H are isomorphic, then they have identical multiplication tables (up to relabeling).

2. Every group of order 4 is isomorphic to Z_4

3. Every abelian group is isomorphic to a subgroup of Q, the group of rational numbers under addition.

4. The group of real numbers R under addition is isomorphic to the group of positive real numbers R* under multiplication.

5. If G and H are isomorphic groups, every automorphism of G corresponds to an automorphism of H.

6. If G is a group of prime order, then G is isomorphic to Z_p

7. Any two groups of the same order are isomorphic.

8. An infinite cyclic group is isomorphic to Z.

8.10 *ANSWERS*

Answer of objective question:

1.	b)	**2.**	d)	**3.**	d)	**4.**	c)
5.	d)	**6.**	d)	**7.**	b)	**8.**	d)
9.	b)	**10.**	d)	**11.**	b)	**12.**	c)
13.	d)						

Answer of fill in the blanks:

1. $O(G')$ **2.** Number of elements of order n in G' **3.** $Z_{123456789}$

4.	n	**5.**	Bijective	**6.**	Order
7.	Z_n	**8.**	Cyclic	**9.**	Structures
10.	Z(H)	**11.**	H		

Answer of True and False:

1.	True	2.	False	**3.**	True	**4.**	True
5.	True	**6.**	False	7.	False	**8.**	True

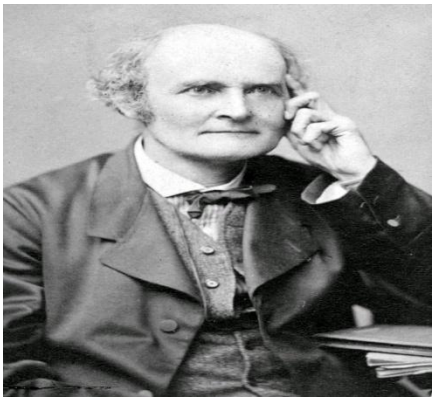
Unit-9: CAYLEY'S THEOREM AND CLASS EQUATION

CONTENT:

9.1 *INTRODUCTION*

British mathematician Arthur Cayley FRS, who lived from 16 August 1821 to 26 January 1895, was very active and focused primarily on algebra. He contributed to establishing the current British school of pure mathematics.

Cayley used to find it amusing to solve challenging arithmetic problems as a kid. He enrolled in Trinity College in Cambridge, where he excelled in mathematics, Greek, French, German, and Italian. He practised law for 14 years.



Arthur Cayley FRS

16 August 1821 – 26 January 1895

https://en.wikipedia.org/wiki/Arthur_Cayley

Theorizing that every square matrix is a root of its own characteristic polynomial, he established what is now known as the Cayley-Hamilton theorem for matrices of orders 2 and 3. He was the first to introduce the contemporary definition of a group as a set with a binary operation that complies with certain rules. Mathematicians used to refer to permutation groups when they used the term "groups." In honour of Cayley, Cayley's theorem, Cayley tables, and Cayley graphs all bear his name.

In this we will also learn about the conjugate element in a group is that to differentiate any group into different conjugate classes by its property of satisfying the condition of equivalence relation. After partition group into different conjugate classes we will learn about the important definition of normalizer of any element in a group and centre of the group which will help us to define the class equation. Various theorems of conjugate element, normalizer and centre of the group and their related application to solve different types of examples are also discussed in this unit.

9.2 *OBJECTIVES*

After reading this unit learners will be able to

- Understand the concept of conjugate element and equivalence relation in cojugacy.
- Understand the application of normalize of an element.

- Understand about the special type of normal subgroup name as center of the group.
- Understand the concept that how we can define an isomorphism from any group to the permutation group which is named as Cayley's theorem.
- Solve more examples on class equation.
- Understand the basic properties of Cayley's theorem and class equation and also their related other theorems.

9.3 *CONJUGATE ELEMENT*

Definition: Two elements *a* and *b* in a group *G* are said to be conjugate to each other or *b* is said to be conjugate to *a* if $\exists x \in G$ *s.t.*

$$b = x^{-1}ax$$

Then *b* is called transform of *a* by *x*. Symbolically, it is denoted by $b \sim a$ and this relation in G is called relation of conjugacy.

Theorem 1: Conjugacy relation is an equivalence relation on *G*.

Proof: Reflexivity: Let *a* be any arbitrary element of a group *G* and *e* is the identity of the group. Then

$a = e^{-1}ae \Rightarrow a \sim a \; \forall \, a \in G$. Therefore the relation is reflexive.

Symmetry: We have to prove if $a \sim b$ then $b \sim a$. Let $a \sim b$ then $\exists x \in G$ *s.t.*

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

$\Rightarrow xax^{-1} = x\left(x^{-1}bx\right)x^{-1} \Rightarrow xax^{-1} = b$

As we know if $x \in G$ then $x^{-1} \in G$

Transitivity: Let $a \sim b$ and $b \sim c$ then $a = x^{-1}bx, b = y^{-1}cy$ for some $x, y \in G$.

Again, $a = x^{-1}\left(y^{-1}cy\right)x$

$\Rightarrow a = x^{-1}y^{-1}cyx = (yx)^{-1}c(yx)$ [Since *G* is a group then $yx \in G, (yx)^{-1} \in G$]

$\Rightarrow a \sim c$ and thus, relation is transitive.

Hence, conjugacy is an equivalence relation.

Classes of conjugate elements: The differences between the classes are follows:

(1) Elements from the same classes will be conjugate.

(2) Different elements from different classes will be not conjugate.

The collection of all elements which are conjugate to $a \in G$ will be denoted by $C(a)$ or $\tilde{a}$ and defined as:

$C(a) = \{x \in G | x \sim a\}$ or $C(a) = \{b \in G | b = x^{-1}ax\}$

For the finite group G, number of distinct element in $C(a)$ will be denoted by c_a.

9.4 *NORMALIZER OF AN ELEMENT OF A GROUP*

Definition: If G is a group and a be any arbitrary element of a group then normalizer of a is the collection of such elements in G which commutes with a. It is denoted by $N(a)$ and defined as:

$N(a) = \{x \in G | ax = xa\}$

Note 1: If e is the identity element of G then $N(e) = G$

2: If G is abelian group and $a \in G$ then $N(a) = G$

Theorem 2: The normalizer of $a \in G$ is the subgroup of G.

Proof: Since, $N(a) = \{x \in G | ax = xa\}$. Let x, y are any element of G then $ax = xa, ay = ya$.

First, we will show that, $y^{-1} \in G$. Since, $y \in G \Rightarrow y^{-1} \in G$ because G is a group.

Now, $y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$ [Pre and post multiply by y^{-1} in $ay = ya$]

$\Rightarrow y^{-1}a(yy^{-1}) = (y^{-1}y)ay^{-1}$ [G satisfied the associativity]

$\Rightarrow y^{-1}ae = eay^{-1}$ [e is the identity element of G]

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

$\Rightarrow y^{-1} \in N(a)$

Now we have to prove that $xy^{-1} \in N(a)$

Consider, $a(xy^{-1}) = (ax)y^{-1}$

$\Rightarrow a(xy^{-1}) = (xa)y^{-1}$ [$ax = xa$]

$\Rightarrow a(xy^{-1}) = x(ay^{-1})$ [G satisfied the associativity]

$\Rightarrow a(xy^{-1}) = x(y^{-1}a)$ [$y^{-1}a = ay^{-1}$]

$\Rightarrow a(xy^{-1}) = (xy^{-1})a$ [G satisfied the associativity]

$\Rightarrow xy^{-1} \in N(a)$

Hence, normalizer of any element $a \in G$ *i.e.*, $N(a)$ is the subgroup of G.

Theorem 3: Any two elements of a group give rise to same conjugate to $a \in G$ *iff* they belong to the same right coset of normalizer of a in G.

Proof: Let us consider, $x, y \in G$ then $x \in N(a)x$ and $y \in N(a)y$. Since x, y are in the same right coset of $N(a)$ in G.

$\Leftrightarrow N(a)x = N(a)y$ [If H is subgroup and $x \in H$ then $Hx = H$]

$\Leftrightarrow xy^{-1} \in N(a)$ [If H is a subgroup of G, then $Ha = Hb \Leftrightarrow ab^{-1} \in H$]

$\Leftrightarrow axy^{-1} = xy^{-1}a$ [By definition of normalizer of an element of G]

$\Leftrightarrow x^{-1}\left(axy^{-1}\right)y = x^{-1}\left(xy^{-1}a\right)y$

$\Leftrightarrow x^{-1}ax(y^{-1}y) = (x^{-1}x)y^{-1}ay$

$\Leftrightarrow x^{-1}axe = ey^{-1}ay$

$\Leftrightarrow x^{-1}ax = y^{-1}ay$

$\Leftrightarrow x, y$ give rise to same conjugate of a.

Theorem 4: If G is a finite group then the number of distinct element in $C(a)$ are $\frac{O(G)}{O(N(a))}$.

Then further prove that $O(G) = \sum \frac{O(G)}{O(N(a))}$, where summation runs over one element of each conjugate class.

Proof: By the previous theorem 6, we know that two elements of a group give rise to same conjugate to $a \in G$ if they belong to the same right coset of normalizer of a in G. In the other sense it means, different conjugate to $a \in G$ belongs to different right coset of $N(a)$ in G. Thus we get a "*one-to-one correspondence between the conjugates of* $a \in G$ *and right cosets of* $N(a)$ *in* G".

Thus, c_a = Number of distnict element in $C(a)$

= Number of distinct right coset of $N(a)$ in G.

= The index of $N(a)$ in G = $\frac{O(G)}{O(N(a))}$

Further, If $C(a_1), C(a_2), ..., C(a_k)$ are k distinct conjugate class in G, Then

$G = C(a_1) \cup C(a_2) \cup ... \cup C(a_k)$

$\Rightarrow$Number of element in G = Number of element in $C(a_1)$ + Number of element in $C(a_2)$ + …+ Number of element in $C(a_k)$

$\Rightarrow O(G) = \sum c_a$, where summation runs over one element of each conjugate class

$\Rightarrow O(G) = \sum \frac{O(G)}{O(N(a))}$

Hence proof the result.

9.4.1 *SELF CONJUGATE ELEMENT*

Definition: An element $a \in G$ is said to be self conjugate if $a = x^{-1}ax \forall\, x \in G\, i.e,\ C(a)$ contains only singleton element $\{a\}$. In other manner, we can say those self conjugate elements are those elements of G which commutes with every element of G. Sometimes self conjugate element is also called invariant element of G.

9.5 *CENTRE OF A GROUP*

Definition: Collection of all self conjugate element of a group is called centre of group G. It is denoted by $Z(G)$ and defined as,

$$Z(G) = \{x \in G | xa = ax \forall a \in G\}$$

e.g.: The centre of the quaternion group $Q_8 = \{1,-1,i,-i,\ j,-j,k,-k\}$ is $Z(Q_8) = \{1,-1,\}$.

Theorem 5: The centre of a group G, $Z(G)$ is the normal subgroup of group.

Proof: First we will prove that $Z(G)$ is subgroup of G. For it, let $x_1, x_2 \in Z(G)$ then be definition $x_1a = ax_1 \forall a \in G$ and $x_2a = ax_2 \forall a \in G$

Since we have, $x_2a = ax_2 \forall a \in G \Rightarrow x_2^{-1}(x_2a)x_2^{-1} = x_2^{-1}(ax_2)x_2^{-1} \forall a \in G$

$\Rightarrow (x_2^{-1}x_2)ax_2^{-1} = x_2^{-1}a(x_2x_2^{-1}) \forall a \in G$

$\Rightarrow eax_2^{-1} = x_2^{-1}ae \forall a \in G$

$\Rightarrow ax_2^{-1} = x_2^{-1}a \forall a \in G$

$\Rightarrow x_2^{-1} \in Z(G)$

Now consider, $(x_1x_2^{-1})a = x_1(x_2^{-1}a)$

$= x_1(ax_2^{-1})$ $[\, x_2^{-1} \in Z(G) \Rightarrow x_2^{-1}a = ax_2^{-1}]$

$= (x_1a)x_2^{-1}$ [By associativity]

$= (ax_1)x_2^{-1}$ $[\, x_1 \in Z(G) \Rightarrow x_1a = ax_1]$

$= a(x_1x_2^{-1})$ [By associativity]

$\Rightarrow x_1x_2^{-1} \in Z(G)$

Hence $Z(G)$ is subgroup of G.

Now we have only to prove that $Z(G)$ is always normal in G. For it let $x \in Z(G), a \in G$ then,

$$axa^{-1} = (ax)a^{-1}$$
$$= (xa)a^{-1}$$
$$= x(aa^{-1})$$
$$= x(e) = x \in Z(G)$$

Thus, $x \in Z(G), a \in G \Rightarrow axa^{-1} \in Z(G)$

Hence, $Z(G)$ is the normal subgroup of group of G.

Theorem 6: Any element, $a \in Z(G)$ *iff* $N(a) = G$.

Proof: Let $a \in Z(G)$ then $xa = ax \forall x \in G$

Also, $N(a) = \{x \in G \mid xa = ax \forall x \in G\}$

So, $a \in Z(G) \Leftrightarrow xa = ax \forall x \in G$

$\Leftrightarrow x \in N(a) \forall x \in G$ [By definition of $N(a)$]

$\Leftrightarrow N(a) = G$

Corollary: If G is finite $a \in Z(G)$ *iff* $O(N(a)) = O(G)$.

Theorem 7: If G be the finite group and $Z(G)$ be the centre of the group G. Then class equation of G can be written as,

$$O(G) = O[Z(G)] + \sum_{a \notin Z(G)} \frac{O(G)}{O[N(a)]}$$

Where, summation runs over one element a in each conjugate class containing more than one element.

Proof: As we know by the previous theorem that class equation of G is

$O(G) = \sum \frac{O(G)}{O(N(a))}$, where, summation runs over one element a in each conjugate class.

By corollary, we know that if G is finite $a \in Z(G)$ *iff* $O(N(a)) = O(G)$.

$\Leftrightarrow a \in Z(G)$ *iff* $\frac{O(G)}{O(N(a))} = 1$

$\Leftrightarrow$ Number of elements in conjugate class of a is one whenever $a \in Z(G)$.

Thus, order of $Z(G)$ will be equal to the number of conjugate classes each having single element which is itself. If we take a such element which belongs any of these conjugate classes, we have $\frac{O(G)}{O(N(a))} = 1$. Hence the class equation can be rewrite as,

$$O(G) = \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))} + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$$

Since, $O(Z(G)) = \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))}$

Hence, $O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$ …(1)

Note: This equation (1) is called the **class equation** of any finite group *G*.

Example 1: Find the class equation for the group S_3.

Answer: We know the symmetric group (S_3) on three symbols 1, 2, 3 is

$S_3 = \{I, (12), (13), (23), (123), (132)\}$.

Then we have,

Z(S_3) = {e} and $C(12)$ = {(12),(23),(13)} because $(12)(13)(12)^{-1} = (23)$ shows that (2 3) is a conjugate of (1 3).

Similarly we can find, $C(123)$ = {(123),(132)}. Hence the class equation of S_3 is,

$|S_3|$ = |Z(S_3)| + $|C(12)|$ + $|C(123)|$ *i.e.*, 3! = 1 + 3 + 2.

Theorem 8: If $O(G) = P^n$, where *P* is a prime number, then $Z(G) \neq \{e\}$.

Proof: As we know for a finite group *G* the class equation of *G* is

$O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$ where, summation runs over those conjugate class which containing more than one element. We have given $O(G) = P^n$ so, the divisor of $O(G)$ are $1, p, p^2, ..., P^k, ...P^n$ i.e., of the form $P^k \ \ where 1 \leq k \leq n$.

Since $\forall a \in G$ we have $N(a)$ is subgroup of *G*. By Lagrange's theorem we know that $O(N(a)) \mid O(G)$.

Also we know that if $a \notin Z(G) \Leftrightarrow N(a) \neq G \Rightarrow O[N(a)] < O(G)$.

Thus if $a \notin Z(G)$ then $O[N(a)]$ will be of the form $P^k \ \ where 1 \leq k < n$.

Let us consider, $O(Z(G)) = m$, where *m* is a positive integer $m < n$. Now by class equation

$$P^n = m + \sum_{a \notin Z(G)} \frac{P^n}{P^k} \Rightarrow m = P^n - \sum_{a \notin Z(G)} \frac{P^n}{P^k} \ \ where 1 \leq k < n \qquad \ldots (1)$$

Since $P \mid P^n$ so, *P* will divide each term of the right hand side of the equation (1)

$\Rightarrow P \mid m$

Therefore centre of G must contain element other then identity. Therefore $Z(G) \neq \{e\}$.

Theorem 9: Every group of order P^2 is *Abelian*.

Proof: We have given order of the group is P^2 *i.e.*, $O(G) = P^2$. So, the positive divisors of P^2 are $1, P, P^2$. By the previous theorem 11 we know that if $O(G) = P^n$, where P is a prime number, then $Z(G) \neq \{e\}$. It means, $O(Z(G)) > 1$. As we know that centre of the group is subgroup of G and by Lagrange's theorem "Order of every subgroup of a finite group is divisor of the order of the group". So either $O(Z(G)) = P$ or $O(Z(G)) = P^2$.

If $O(Z(G)) = P^2$ then we have nothing to prove.

Otherwise, if $O(Z(G)) = P \Rightarrow$ there exist an element $x \in G$ which is not in $Z(G)$ *i.e.*, $x \notin Z(G)$.

Since $N(x)$ is subgroup of G and $x \in N(x)$. Also $a \in Z(G) \Rightarrow ax = xa \forall x \in G$.

$\Rightarrow a \in N(x)$

$\Rightarrow Z(G) \subseteq N(x)$

Since $x \notin Z(G) \Rightarrow O((N(x)) > P$ but $O(N(x))$ must be divisor of P^2

$\Rightarrow O((N(x))$ must be equal to P^2

$\Rightarrow N(x) = G$

$\Rightarrow x \in Z(G)$, thus we get a contradiction.

Hence, $O(Z(G)) = P^2 \Rightarrow G$ is *Abelian* group because $Z(G)$ is always *Abelian* group.

Example 2: Is a group of order 121 is *Abelian*?

Answer: Since, $O(G) = 121 = 11^2$, where 11 is a prime number. Hence G will be Abelian group.

Example 3: Prove that corresponding to every cyclic group its quotient group is cyclic but their converses need not to be true.

Solution: Let G be a cyclic group such that $G = < a >$ *i.e.*, a is the generator of G and H is its subgroup. Then according to theorem every subgroup of G will be normal subgroup of G. If elements $a^n \in G$ then $Ha^n = (Ha)^n$ will be element of quotient group G/H.

Therefore G/H is a cyclic group and Ha will be generator of it.

But converse is need not be true. Since $S_3 / A_3 = \{A_3, (23)A_3\}$ is Abelian group because order of $O[S_3 / A_3] = 6/3 = 2$ which is prime and we know that every group of prime order is cyclic while S_3 is not a Abelian group.

Theorem 10: If $G/Z(G)$ is cyclic if and only if *G* is Abelian.

Proof: Let us consider $G/Z(G)$ is cyclic. It means, if the element *a* is the generator of *G* then $Z(G)a$ will be generator of $G/Z(G)$.

Let $x, y \in G$ then $Z(G)x, Z(G)y \in G/Z(G) \Rightarrow \exists$ positive integers m, n such that

$Z(G)x = (Z(G)a)^m = Z(G)a^m$ & $Z(G)y = (Z(G)a)^n = Z(G)a^n$

$\Rightarrow$ we have $x = x_1 a^m$ where $x_1 \in Z(G)$ and $y = y_1 a^n$ where $y_1 \in Z(G)$

Now, $xy = (x_1 a^m)(y_1 a^n) = x_1(a^m y_1)a^n) = x_1(y_1 a^m)a^n = (x_1 y_1)a^m a^n = (y_1 x_1)a^m a^n$

$= y_1 x_1 (a^m a^n) = y_1 x_1 a^n a^m = y_1 a^n x_1 a^m = xy$

$\Rightarrow G$ is abelian.

Conversely, assume that *G* is Abelian. If *G* is Abelian then $Z(G) = G$.

$\Rightarrow G/Z(G) = \{e\}$ *i.e.* trivial subgroup which is always cyclic.

Hence the theorem.

Example 4: If *G* be a non-Abelian group of order P^3 where *P* is prime then *Z*(*G*) has exactly *P* element.

Proof: We have given be a non-Abelian group of order P^3 where *P* is prime. Then According to Lagrange's theorem possibilities of order of *Z*(*G*) is $1, P, P^2, P^3$.

Case Ist: We know by previous theorem if $O(G) = P^n$, where *P* is a prime number, then $Z(G) \neq \{e\} \Rightarrow O[Z(G)] > 1$.

Case IInd: Let $O[Z(G)] = P^2 \Rightarrow O(G/Z(G)) = P^3 / P^2 = P$

$\Rightarrow G/Z(G)$ is cyclic and by theorem we can say that *G* is Abelian which is a contradiction. So our assumption is wrong.

Case IIIrd: Let $O[Z(G)] = P^3 \Rightarrow O(G/Z(G)) = P^3 / P^3 = 1$

$\Rightarrow G/Z(G) = \{e\}$ is cyclic and by theorem we can say that *G* is Abelian which is again a contradiction. So again our one of the assumption is wrong.

So, the only possibilities is left that $O[Z(G)] = P$ *i.e.*, *Z*(*G*) has exactly *P* element.

9.6 *CAYLEY'S THEOREM*

Theorem 11: Every group G is isomorphic to a permutation group.

Proof: $A(G)$ is the collection of all permutations of the set G, where G is the any group. Let us define a map $f_a : G \to G$ such that

$f_a(x) = ax$, where $a \in G$

First we will check the mapping is well defined as,

$x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$

One-One: $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$ [By cancellation rule in G]

$\Rightarrow$ mapping is one-one

Onto: For any $y \in G$, since $f_a(a^{-1}y) = a(a^{-1}y) = y$. Here we can easily see that $a^{-1}y$ is pre-image of y or that f_a is onto and hence permutation on G.

Thus, $f_a \in A(G)$

Assume that K be set of all such permutations. Now we will show that K is a subgroup of $A(G)$. Since K is non-empty set because $f_e \in K$.

Let $f_a, f_b \in K$

Then since $f_b o f_{b^{-1}}(x) = f_b\left(f_{b^{-1}}(x)\right) = f_b(b^{-1}x) = b(b^{-1}x)$

$= ex = f_e(x) \forall x$

We find $f_{b^{-1}} = (f_b)^{-1}$ [Note $f_e = I$, identity of $A(G)$]

Also as $(f_a o\, f_b)(x) = f_a(bx) = a(bx) = (ab)x = f_{ab}(x) \forall x$

We find $f_{ab} = f_a\, o\, f_b$

So, $f_a\, o\, (f_b)^{-1} = f_a\, o\, f_{b^{-1}} = f_{ab^{-1}} \in K$

$\Rightarrow K$ is subgroup of $A(G)$.

Define mapping $\phi : G \to K$, s.t.,

$\phi(a) = f_a$

then ϕ is well defined as well as one-one map as,

$a = b$

$\Leftrightarrow ax = bx$

$\Leftrightarrow f_a(x) = f_b(x)\ \forall x$

$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \phi_a = \phi_b$

Obviously, ϕ is onto and

$\phi(ab) = f_{ab} = f_a\, o\, f_b = \phi(a)\phi(b)$

Hence, ϕ is a homomorphism and also an isomorphism which proves the result that every group G is isomorphic to a permutation group.

Remarks: We can define other statement of Cayley's theorems like " If G is finite group of order n then G will be isomorphic to the subgroup of symmetric group S_n.

Example 5: Using Cayley's theorem find the permutation group which is isomorphic to the group $G = \{2,4,6,8\}$ under the operation multiplication modulo $(\times_{10})$.

Answer: Let A be any permutation group such as defined in the Cayley's theorem.

$A = \{f_a \mid a \in G\}$, where f_a is defined as $f_a = ax\ s.t.\ \ a, x \in G$

So, $f_2(2) = 4,\ f_2(4) = 8,\ f_2(8) = 6,\ f_2(6) = 2$

$f_4(2) = 8,\ f_4(4) = 6,\ f_4(8) = 2,\ f_4(6) = 4$

$f_8(2) = 6,\ f_8(4) = 2,\ f_8(8) = 4,\ f_8(6) = 8$

$f_6(2) = 2,\ f_6(4) = 4,\ f_6(8) = 8,\ f_6(6) = 6$

Thus, $f_6 = I$ and $K = \{f_2, f_4, f_8, f_6 = I\}$

If we identify f_2 with the permutation (1234), other permutations are $(13)(24), (1432)$. Hence $A = \{(123), (13)(24), (1432), I\}$ is required permutation group isomorphic to G.

Example 6: Using Cayley's theorem find the permutation group which is isomorphic to the D_4.

Answer: As we know that the dihedral group (D_4) of order 8 is

$D_4 = \left\{a, a^2, a^3, a^4, ab, a^2b, a^3b, a^4b \mid a^4 = e = b^2, ab = ba^{-1}\right\}$

Let the set defined in the Cayley's theorem is given by $K = \{f_x \mid x \in G\}$ where function defined by, $f_x(y) = xy$ and $D_4 \cong K$ by the theorem. Now we determine K, the required permutation group as

$f_a(a) = a^2,\ f_a(a^2) = a^3,\ f_a(a^3) = a^4 = e,\ f_a(ab) = a^2b$

$f_{a^2}(a^2b) = b,\ f_a(a^3b) = b,\ f_a(b) = ab,\ f_a(e) = a$

Thus f_a can be identified with the permutation $(1234)(5678)$

Again, $f_{a^2}(a) = a^3$, $f_{a^2}(a^2) = e$, $f_{a^2}(a^3) = a$, $f_{a^2}(ab) = a^3b$

$f_{a^2}(a^2b) = b$, $f_{a^2}(a^2b) = ab$, $f_{a^2}(b) = a^2b$, $f_{a^2}(e) = a^2$

Thus, f_{a^2} can be identified with $(13)(24)(57)(68)$.

In the continuation, we can say, $f_{a^3} = (1432)(5876)$

Again, $f_{ab}(a) = aba = b$, $f_{ab}(a^2) = aba^2 = a^3b$ etc., we get

$f_{ab} = (18)(27)(36)(45)$

Similarly, $f_{a^2b} = (15)(28)(37)(46)$

$f_{a^3b} = (16)(25)(38)(47)$

$f_b = (17)(26)(35)(48)$

Therefore, $K = \begin{Bmatrix} (1234)(5678), (13)(24)(57)(68), (1432)(5876), I, (18)(27)(36)(45), \\ (15)(28)(37)(46), (16)(25)(38)(47), (17)(26)(35)(48) \end{Bmatrix}$

Hence, $K \cong D_4$

9.7 *CLASS EQUATION*

In the unit 2 we have already learned about some important theorems of class equations and their proof which are as follows:

Theorem 12: If G be the finite group and $Z(G)$ be the centre of the group G. Then class equation of G can be written as

$$O(G) = O[Z(G)] + \sum_{a \notin Z(G)} \frac{O(G)}{O[N(a)]}$$

In this section we will learn applications part of class equation in different type of examples.

Example 7: If n is the index of $Z(G)$ in a group G then the conjugate class has at most n elements.

Answer: We have $n = \frac{O(G)}{O(Z(G))}$ and $O(cl(a)) = \frac{O(G)}{O(N(a))}$

Since, $Z(G) \subseteq N(a)$ always

$O(Z(G)) \subseteq O(N(a)) \Rightarrow O(N(a)) = k.O(Z(G))$

i.e., $O(C(a)) = \frac{O(G)}{O(N(a))} = \frac{n.O(Z(G))}{k.O(Z(G))} = \frac{n}{k}$

Hence, maximum value of $O(C(a))$ is when $k = 1$.

Example 8: If P^3 be order of a non-abelian group then determine $O(Z(G))$ and also number of conjugate classes of *G*.

Solution: We have given group (G) is non-abelian, $\exists a \in G$, s.t., $Z(G) \subset_{\neq} N(a) \subset_{\neq} G$

Since we know that $O(Z(G)) \mid O(G) = P^3$

So, the possibilities that $O(Z(G))$ will be $1, P, P^2, P^3$

Similarly $O(N(a)) = 1, P, P^2, P^3$

But by the previous theorems we know that $O(Z(G)) \neq 1$. Since group is non-abelian then $O(Z(G)) \neq P^3$. So, the only possibilities will be $O(Z(G)) = P \, or \, P^2$.

Similarly, $O(N(a)) = P \, or \, P^2$ and as $Z(G) \subset_{\neq} N(a)$

So, we find $O(Z(G)) = P,\ O(N(a)) = P^2$

Let we assume *k* be the total number of conjugate classes. Since

$G = \underset{a \in G}{\cup} C(a)$

$$O(G) = \sum_{a \in G} O(C(a)) = \sum_{a \in Z(G)} O(C(a)) + \sum_{a \notin Z(G)} O(C(a))$$

$$p^3 = O(Z(G)) + \sum_{a \notin Z(G)} O(C(a))$$

When $a \in Z(G)$ then number of conjugate classes is $O(Z(G)) = p$

[Since $a \in Z(G) \Leftrightarrow C(a) = \{a\} \, or \, O(C(a)) = 1$]

So, $k - p$ are remaining classes and each have order given by

$$O(C(a)) = \frac{O(G)}{O(N(a))} = \frac{p^3}{p^2} = p$$

Hence, $p^3 = p + (k - p)p \Rightarrow k = p^2 + p - 1$

Example 9: Write the class equation of quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Solution: We have the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

First we determine the conjugate class of i. Since we know that in any group $< a > \subseteq N(a)$

[$x \in < a > \Rightarrow x = a^m$ and as $a.a^m = a^m.a$, we find $a^m \subseteq N(a)$]

Thus, $< i > \subseteq N(i)$ or $\{i, i^2, i^3, i^4 = 1\} \subseteq N(i)$

Therefore, $< i > \subseteq N(i) \leq Q_8$ gives $4 \mid O(N(i)) \mid 8$

Since $j \notin N(i)$ because $ji \neq ij$

And $j \in Q_8 \Rightarrow N(i) \underset{\neq}{\subset} Q_8$

Hence $O(N(i)) = 4$ or $N(i) =< i >$

As we know that $O(C(a)) = \dfrac{O(G)}{O(N(a))}$

$\Rightarrow O(C(i)) = \dfrac{O(Q_8)}{O(N(i))} = \dfrac{8}{4} = 2$

$\Rightarrow C(i) = \{i, -i\}$ [as $i \in C(i)$ and $-i = kik^{-1}, -i \in C(i)$]

Similarly other conjugate classes are $C(j) = \{j, -j\}, C(k) = \{k, -k\}, \{1\}, \{-1\}$

Since we know that $O(C(a)) = 1 \Leftrightarrow a \in Z(G)$ then as $O(C(1)) = 1, O(C(-1)) = -1$

$\Rightarrow Z(Q_8) = \{1, -1\}$

Now, we verify the class equation as

$$O(G) = O(Z(G)) + \sum_{a \notin Z(G)} O(C(a))$$

$8 = 1 + 1 + (2 + 2 + 2)$, which is the class equation of the group Q_8.

Example 10: For a finite group G let number of conjugate class is 3. Then prove that either group is cyclic or isomorphic to S_3.

Solution: Since we have given that group G has number of conjugate classes are 3. If these conjugate classes are of order 1, then $O(G) = 3$, which is of order prime that means group will be cyclic. If G has a class of order >1 then G is non-abelian because if G will abelian then there does not exist any class of order >1.

Let three classes of G are C_1, C_2, C_3.

Assume that $O(C_3) > 1$.

If $O(C_1) = O(C_2) = 1 \Rightarrow O(C_3) = n - 2$ [If we have assume that $O(G) = n$]

$\because O(C_3) = n - 2 \mid O(G)$ and also we have $n - 2 \mid n - 2$

$\Rightarrow (n-2) \mid n - (n-2) = 2$

$\Rightarrow n - 2 = 1 or 2$

$\Rightarrow n = 3 or 4$

$\Rightarrow G$ is abelian. [Because we know every group of order p or p^2 is abelian]

Now there is only one possibility left that in G one class is of length 1. Let $O(C_1)=1, O(C_2)>1, O(C_3)>1$. It means $O(Z(G))=1$.

By class equation, $n=O(G)=O(C_1)+O(C_2)+O(C_3)=1+O(C_2)+O(C_3)$

But $O(C_3)\,|\,O(G)=n, O(C_3)\,|\,O(C_3)$

$\Rightarrow O(C_3)\,|\,n-O(C_3)=1+O(C_2)$

$\Rightarrow O(C_3)\le 1+O(C_2)$

Similarly, $O(C_2)\le 1+O(C_3)$

If $O(C_3)<1+O(C_2)$ and $O(C_2)<1+O(C_3)$

Then $O(C_3)\le O(C_2)$, $O(C_2)\le O(C_3)$

$\therefore O(C_3)=O(C_2)$

$\therefore O(C_3)\,|\,1+O(C_3)\Rightarrow O(C_3)\,|\,1\Rightarrow O(C_3)=1$

This is a contradiction

Thus either $O(C_3)=1+O(C_2)$

Or $O(C_2)=1+O(C_3)$

If $O(C_3)=1+O(C_2)$

Then $O(G)=1+O(C_2)+1+O(C_2)$

$\Rightarrow O(G)-2O(C_2)=2$

But $O(C_2)\,|\,O(G), O(C_2)\,|\,O(C_2)\Rightarrow O(C_2)\,|\,2O(C_2)$

$\therefore\ O(C_2)\,|\,O(G)-2O(C_2)=2$

$\therefore\ O(C_2)=2$ and $O(C_3)=3$

Or that $O(G)=6$

Similarly, if $O(C_2)=1+O(C_3)$, then $O(G)=6$

$\therefore G$ is non-abelian group of 6 which is isomorphic to S_3 i.e., $G\cong S_3$.

Example 11: Let G be a group such that $e\neq a\in G, O(a)=$ finite. If G has only two conjugate classes then prove that G is a group of order 2.

Answer: Let $e\neq b\in G$. Since G has only 2 conjugate classes, namely $\{e\}$ and $C(a)$.

$b\in C(a)\therefore b=g^{-1}ag$ for some $g\in G$.

$\therefore\ O(b) = O(a)$ for all $b \neq e$ in G.

Suppose $O(a) = mn, m > 1, n > 1$

Then $O(a^m) = m$

Since order of all non identify elements in G is same, $O(a^m) = mn$

$\therefore n = mn \Rightarrow m = 1$; a contradiction

$\therefore O(a) = p = prime$

$\therefore O(b) = p =$ for all $e \neq b \in G$

Suppose $p \neq 2$

then $a^2 \neq e \Rightarrow a^2 \in C(a)$

$\therefore a^2 = g^{-1}ag$ for some $g \in G$

$\therefore (a^2)^2 = (g^{-1}ag)^2 = g^{-1}a^2g$

$\therefore (a^2)^2 = (g^{-1}ag)^2 = g^{-1}(g^{-1}ag)g = g^{-2}ag^2$

In this way, we get $a^{2^p} = g^{-p}ag^p$

Since $O(g) = O(a) = p$

$a^{2^p} = eae = a$

$\Rightarrow a^{2^p-1} = e \Rightarrow O(a) = p \mid 2^p - 1$

By Fermat's theorem, $p \mid 2^p - 2$

$\therefore\ p \mid (2^p - 1) - (2^p - 2) = 1$, a contradiction

$\therefore\ p = 2$

$\Rightarrow O(a) = 2$. So, $O(b) = 2$ for all $e \neq b \in G$

$\Rightarrow G$ is abelian.

So, each conjugate class in G is of length one. Since G has only two classes, which means G is of order 2.

Note: There are infinite group having non-trivial element has finite order and group has only 2 conjugate classes. Therefore, it is necessary to assume that $\exists e \neq a \in G$ s.t. $O(a) =$ finite.

9.8 *PARTITION OF AN INTEGER*

Let n be a positive integer. A sequence of positive integers $n_1, n_2, ..., n_k$ where $n_1 \le n_2 \le ... \le n_k$ such that $n = n_1 + n_2 + ... + n_k$ is called a partition of n and $n_1, n_2, ..., n_k$ are called parts of partition.

For example, let $n = 3$, then number of partition are 3 i.e.,

$$3 = \begin{cases} 1+1+1 \\ 1+2 \\ 3 \end{cases}$$

let $n = 4$, then number of partition are 5 i.e.,

$$4 = \begin{cases} 1+1+1+1 \\ 1+1+2 \\ 2+2 \\ 1+3 \\ 4 \end{cases}$$

The number of partition of any integer n is denoted by $P(n)$. For example, $P(1) = 1$, $P(2) = 1, P(3) = 4, P(4) = 5$ e.tc.

Theorem 13: The number of conjugate classes in S_n is $P(n)$.

Proof: Let $A =$ Collection of all conjugate classes in S_n.

$B =$ Collection of all partition of *n*.

Let $C(\sigma), \sigma \in S_n$.

Assume that σ as product of disjoint cycles as $(a_1 ... a_{n_1})(b_1 ... b_{n_k})$ where $n_1 + ... + n_k = n$.

the selection of cycles in a pattern such that $n_1 \le ... \le n_k$. This gives a partition

$\{n_1, n_2, ..., n_k\}$ of n.

Now we define $f : A \to B$ s.t.,

$f(C(\sigma)) = \{n_1, n_2, ..., n_k\}$

f is well defined as $C(\sigma) = C(\eta)$

$\Rightarrow \sigma, \eta \in C(\sigma)$

$\Rightarrow \sigma, \eta$ are conjugate in S_n

$\Rightarrow \sigma, \eta$ are similar in S_n

$\Rightarrow \sigma = (a_1, ..., a_{n_1})..(b_1, ..., b_{n_k})$

$\eta = (a_1', ..., a'_{n_1})..(b'_1, ..., b'_{n_k})$

$\Rightarrow f(C(\sigma)) = \{n_1, n_2, ..., n_k\} = f(C(\eta))$

Suppose $C(\sigma) \neq C(\eta)$

So, σ, η are not conjugate $\Rightarrow \sigma, \eta$ are not similar

$\Rightarrow \sigma, \eta$ have different cycle structure

$\Rightarrow$Corresponding partitions are different

i.e., $\{n_1, n_2, ..., n_k\} \neq \{n'_1, n'_2, ..., n'_r\}$ where, of course,

$n = n_1 + n_2 + ... + n_k = n'_1 + n'_2 + ... + n'_r$

$\Rightarrow f(C(\sigma)) \neq f(C(\eta))$

$\Rightarrow f$ is one-one

f is onto for, let $\{n_1, n_2, ..., n_k\} \in B$ be a partition of n. Then $n = n_1 + n_2 + ... + n_k$

Define $\sigma = (a_1, ..., a_{n_1})..(b_1, ..., b_{n_k}) \in S_n$

Then $C(\sigma) \in A$

And $f(C(\sigma)) = \{n_1, n_2, ..., n_k\}$

$\therefore f$ is both 1-1 and onto

So, $O(A) = O(B) = P(n)$

$\Rightarrow$number of conjugate classes in S_n is $P(n)$

Example 12: Verify the class equation in S_4 and also find its all conjugate classes.

Answer: By the theorem 4 we know that number of conjugate classes in S_4 are $P(4)$ which is 5. Also we know that two conjugate classes of any group are either disjoint or identical. In other word we can say that two permutations are conjugate if and only they are similar. In S_4 the base elements of conjugate classes are $I, (12), (123), (1234), (12)(34)$

As we know that in the permutation group S_n number of distinct *r*-cycle are $\frac{1}{r}\frac{n!}{(n-r)!}$. So,

in S_4 number of distinct cycle of length 2 are $\frac{1}{2}\frac{4!}{(4-2)!} = 6$

Similarly, in S_4 number of distinct cycle of length 3 are $\frac{1}{3}\frac{4!}{(4-3)!} = 8$

Similarly, in S_4 number of distinct cycle of length 4 are $\frac{1}{4}\frac{4!}{(4-4)!} = 6$

in S_4 number of permutation of type $(ab)(cd)$ are $(12)(34),(13)(24),(14)(23)$

so, $O(C((12)(34))=3$

Since centre of S_4 contains only identity element so, $O(Z(S_4))=1$ i.e., $O(C(I))=1$

Now the class equation of S_4 is,

$$O(S_4)=O(Z(S_4))+\sum_{a\notin Z(S_4)}\frac{O(S_4)}{O(N(a))}=O(Z(S_4))+\sum_{a\notin Z(S_4)}O(C(a))$$

i.e., $24=1+6+8+6+3$

Example 13: Find the class equation of a group of order 6.

Answer: Let G be a group of order 6. So, there are two cases arises that either group is abelian or not.

Case I: Let group is abelian then we know that G will be isomorphic to Z_6 i.e., $G\cong Z_6$ *or* $G\cong Z_2\times Z_3$

Since G is abelian then $O(Z(G))=6$

So, the class equation will be, $6=1+1+1+1+1+1$

Case II: If group is non-abelian then we know that G will be isomorphic to S_3 or D_3 i.e., $G\cong S_3\cong D_3$

As we know that the permutation on group on the 3 symbol $\{1,2,3\}$ is $S_3=\{I,(12),(13),(23),(123),(132)\}$.

Initially we examine the conjugacy classes of S_3 for it first we will find center element of S_3.

Since, $(12)(13)=(132)\neq(123)=(13)(12)$ and $(12)(23)=(123)\neq(132)=(23)(12)$ and so $(12),(23),(13)\notin Z(S_3)$

Further, $(123)(12)=(13)\neq(23)=(12)(123)$ and $(132)(12)=(23)\neq(13)=(12)(132)$.

So, $(123),(132)\notin Z(S_3)$. So the only trivial conjugacy class is [(1)]={1} i.e., $Z(S_3)=I$ or $O(Z(S_3))=1$.

Now observe that for the element (12) we have that:

$(12)(12)(12)^{-1}=(12)(12)(21)=(12)$

$(13)(12)(13)^{-1}=(13)(12)(31)=(23)$

$(23)(12)(23)^{-1}=(23)(12)(32)=(13)$

$(123)(12)(123)^{-1}=(123)(12)(321)=(23)$

$(132)(12)(132)^{-1} = (132)(12)(231) = (13)$

So, the conjugacy class of (12) is $C((12)) = \{(12),(13),(23)\}$ and the conjugacy classes of remaining elements are $C((123)) = C((132)) = \{(123),(132)\}$

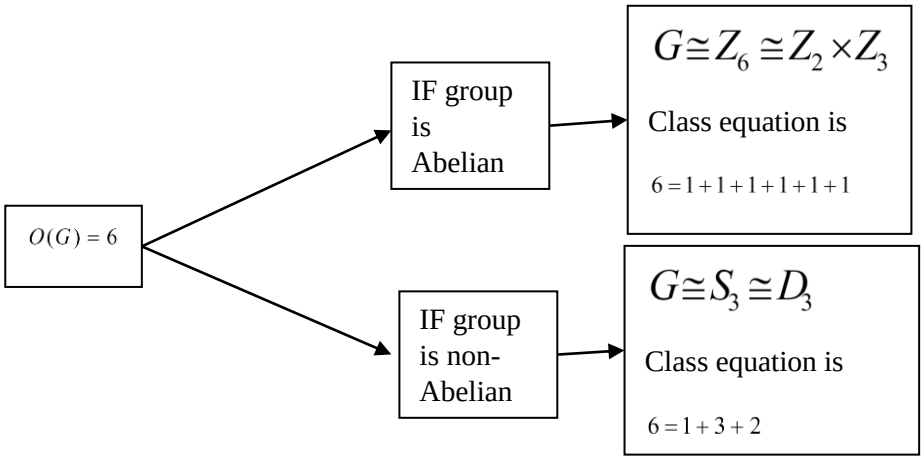
So, the conjugacy classes of S_3 is,

$S_3 = C(I) \cup C((12)) \cup C((123))$

And the class equation is,

$6 = 1 + 3 + 2$

Hence,



Note: Two permutations in S_n are conjugates iff they have the same cycle type. Let $\sigma \in S_n$ and also let $m_1, m_2, ..., m_r$ are the distinct integers which appear in $a_1, a_2, ..., a_r$ times respectively in the cycle type of σ (including 1 cycles). Let a_i be the number of cycles of length $m_i, i = 1 to r$, so that $\sum_{i=1}^{r} a_i m_i = n$

then, number of conjugate of $\sigma = \dfrac{n!}{(m_1^{a_1} a_1!)(m_2^{a_2} a_2!)...(m_r^{a_r} a_r!)}$

OR

Number of element commutes with $\sigma = \dfrac{n!}{(m_1^{a_1} a_1!)(m_2^{a_2} a_2!)...(m_r^{a_r} a_r!)}$

Example 14: Find the number of cycle which commute with $\alpha = (543)(26)(78910) \in S_{10}$

Solution: We first rewrite the given permutation as $\alpha = (1)(543)(26)(78910) \in S_{10}$. Since all cycles of permutations are disjoint so they are commutes i.e., $\alpha = (1)(26)(543)(78910) \in S_{10}$. So, cycle type of α is,

Cycle of length $1 = (1)$

Cycle of length $2 = (26)$

Cycle of length $3 = (543)$

Cycle of length $4 = (78910)$

i.e., cycle type of $\alpha = (1,2,3,4)$, where $1+2+3+4=10$

So, number of conjugate of $\alpha = \dfrac{10!}{(1^1 1!)(2^1 1!)(3^1 1!)(4^1 1!)} = \dfrac{10!}{2.3.4}$

Example 15: Find the number of cycle which commute with $\alpha = (596)(874)(12) \in S_{11}$

Solution: We first re-write the given permutation as $\alpha = (12)(596)(874) \in S_{11}$. Since all cycles of permutations are disjoint so they are commutes i.e., $\alpha = (3)(4)(10)(11)(1\ 2)(596)(874) \in S_{11}$. So, cycle type of α is,

Cycle of length $1 = (3)(4)(10)(11)$

Cycle of length $2 = (1\ 2)$

Cycle of length $3 = (596)$

Cycle of length $4 = (874)$

i.e., cycle type of $\alpha = (1,1,1,1,2,3,3)$, where $1+1+1+1+2+2+3=11$

So, number of conjugate of $\alpha = \dfrac{11!}{(1^4 4!)(2^1 1!)(3^2 2!)} = \dfrac{11!}{4!.2.9.2}$

Example 16: Evaluate all permutations in A_5 which commutes with

(***i***) $\alpha = (12345)$ (***ii***) $\beta = (123)$ (***iii***) $\gamma = (12)(34)$

Solutions (***i***)**:** As we know that $O(A_5) = \dfrac{O(S_5)}{2} = \dfrac{120}{2} = 60$. Since $\alpha = (12345) \in A_5$ and $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 = I$ are distinct permutation in A_5.

$\therefore O(N(\alpha)) = 5 \text{ in } A_5$

$\therefore O(C(\alpha)) = \dfrac{O(A_5)}{O(N(\alpha))} = \dfrac{60}{5} = 12 \text{ in } A_5$

As we know (12345) and (13245) break up into two conjugate classes each conjugate classes are of length 12 in A_5.

(***ii***)**:** Let $\theta \in S_5$ s.t. θ fixes 1, 2, 3. Then either $\theta = (45)$ or $\theta = I$. Since $\beta\theta, \beta^2\theta, \theta$ are all permutation in S_5 commuting with β. Thus β, β^2, I are only permutation in A_5 commuting with β.

$\therefore O(N(\beta)) = 3 \text{ in } A_5$

$\therefore O(C(\beta)) = \dfrac{O(A_5)}{O(N(\beta))} = \dfrac{60}{3} = 20 \text{ in } A_5$

$\therefore C(\beta)$ has all cycles of length 3 in S_5

(***iii***)**:** As we know that there are 8 permutations in S_5 commuting with γ which are:

$\{I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$. From this set only even permutation $\{I, (12)(34), (13)(24), (14)(23)\} \in A_5$. All these permutations of A_5 commuting with $\gamma = (12)(34)$

$\therefore O(N(\gamma)) = 4 \text{ in } A_5$

$\therefore O(C(\gamma)) = \dfrac{O(A_5)}{O(N(\gamma))} = \dfrac{60}{8} = 15$ in A_5 which is same like $\therefore O(C(\gamma))$ in S_5.

Hence conjugate class of γ in A_5 and S_5 remains same.

Example 17: Find all the conjugate classes of A_5 and also show that A_5 is simple.

Answer: By using the previous examples we can verify that A_5 has 5 conjugate classes and these are:

$C(I) = \{I\}$

$C((123)) = \{\text{All 20 permutation commute with cycle } (123) \text{ of length 3 in } S_5.\}$

$C((12)(34)) = \{\text{All 15 permutation commute with cycle } (12)(34) \text{ in } S_5.\}$

$C((12345)) = \{12 \text{ cycles of length 5}\}$

$C((13245)) = \{12 \text{ cycles of length 5}\}$

These are the total 60 elements in A_5.

Let H be any subgroup of A_5 which is normal s.t $H \neq \{I\}$, $H \neq \{A_5\}$. As H is the union of some conjugate classes in A_5. Since $I \in H, O(H)$ cannot divide $O(A_5) = 60$.

Hence, A_5 is simple

Check your progress

Problem 1: What will be the class equation of any group of order 3?

Problem 2: What will be the class equation of Klein group (**Klein group:** Any group of order 4 such that each of its non-identity elements are self inverse, generally this group is denoted by K_4 -group)?

Problem 3: Which of the following isomorphism relation is correct and why?

(***i***) $D_2 \cong Z_4$ (***ii***) $D_2 \cong Z_2 \times Z_2$

Problem 4: Find the finite number of distinct classes in $Q_4 = \{1,-1,i,-i\}$?

Problem 5: Find the number of element in the centre of $Q_4 = \{1,-1,i,-i\}$?

Problem 6: Find the class equation of $Q_4 = \{1,-1,i,-i\}$?

9.9 *SUMMARY*

In this unit, we have studied the definition and theorems related to conjugate of an element, normalizer of an element and centre of the group and also learn their implementation on various examples. We have also learn in this unit how these subgroup are essentials in the formation of class equation which will further discussed briefly in the upcoming units. The overall summarization of this units are as follows:

- Conjugacy relation is an equivalence relation on *G*.
- $O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$ is known as class equation of any group.
- Every group of order p^2 is abelian group.

Also in this unit, we have studied about the Cayley's theorem, various examples related to the class equations and partition of an integer. After completions of this unit learners will be able to characterized to any group into distinguish conjugacy classes and also by the class equation of any group learners will be able to find the number of element in the centre, number of different conjugate classes, number of element in the different conjugate class and order of the group. In a simple way we can say that with the help of conjugate classes we can get most of the information about the group without any prior knowledge.

9.10 *GLOSSARY*

- $b \sim a$ denotes two elements a, b of a group *G* are conjugate to each other.

- $C(a)$ denotes collection of elements of group which are conjugate to a.
- c_a denotes number of elements in group which are conjugate to a.
- $Z(G)$ denotes centre of the group.
- $N(a)$ denotes the normalizer of a.
- $P(n)$ denotes the partition of any positive integer

9.11 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- https://en.wikipedia.org/wiki/Center_(group_theory)#:~:text=By%20definition%2C%20the%20center%20is,of%20each%20element%20of%20G.

9.12 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.

9.13 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that any two conjugate classes of a group are either disjoint or identical.

2. If the order of a group G is prime (p), then prove of G has exactly p elements.

3. If H is normal subgroup of G, having prime index p then prove that G/N is cyclic.

4. If G be a non-Abelian group of order $O(G)=1331$ then prove that number of elements in centre of group $Z(G)$ are 11.

5. If G be a group of order $O(G)=121$ then find the number of elements in its centre.

6. State and prove the class equation.

7. Prove that cojugacy is an equivalence relation.

8. State and prove the Cayley's theorem.

9. Prove that dihedral group D_3 is isomorphic to the symmetric group S_3.

10. Find number of conjugate classes in S_5.

11. Find the class equation of a non-abelian group of order 8.

12. Find the number of cycle which commute with $\alpha=(596)(874)\in S_{11}$.

13. Prove that A_5 is simple.

14. Let G be a group such that $e\neq a\in G$, $O(a)=$ finite. If G has only two conjugate classes then prove that G is a group of order 2.

15. Prove that the number of conjugate classes in S_n is $P(n)$.

16. Find the conjugate class of i and -1 in Q_8 and also find the class equation of Q_8.

Short Answer Type Question:

1. Find the number of elements of the in the centre of the group having order $O(G)=5,7,25,31,49$.

2. Prove that centre of the group is an abelian group

3. If G is a non-abelian of order 8 then prove that $Z(G)$ has exactly 2 element.

4. Find number of element which are conjugate to $(12)\in S_3$.

5. Prove that if G is finite, $a\in Z(G)$ *iff* $O(N(a))=O(G)$.

6. Write the class equation of non-abelian group of order 2^3.

7. Write all the partition of 5 i.e., $P(5)$.

8. Find the number of elements in the centre of the group having class equation $8=1+1+(2+2+2)$.

9. Write the class equation of $U(7)=\{1,2,3,4,5,6\}$ under the operation multiplication modulo 7.

Fill in the blanks:

1. Two elements *a* and *b* in a group *G* are such that $b=x^{-1}ax$ then *b* will called …… to *a*.

2. Every group of order p^2 (p = *prime*) is …….

3. Centre of the group *G* is the …… subgroup of *G*.

4. If *G* is non-abelian group of order 125 then *Z*(*G*) has …….. elements.

5. Every group *G* is isomorphic to a …….

6. A_5 is ……. group.

7. Number of conjugate classes in S_n are …….

8. The class of non-abelian group of order 6 is ……

9. If the class equation of any group is $4=1+1+1+1$ then group is ……

9.14 *ANSWERS*

Answer of self cheque question:

1. 1+1+1 **2.** 1+1+1+1

3. $D_2 \cong Z_2 \times Z_2$ is correct because D_2 is abelian group not cyclic.

4. 4 **5.** 4 **6.** $Q_4 = 1+1+1+1$

Answer of long question:

5. 121 **10.** 6 **12.** $\frac{11!}{(1^5 5!)(3^2.2!)}$

16. $C(i)=\{i,-i\}, C(-1)=\{-1\}$ and class equation is $8=1+1+(2+2+2)$

Answer of short question:

1. $5, 7, 25, 31, 49$ **4.** 3

Answer of fill in the blanks:

1.	Conjugate	**2.**	Abelian	**3.**	Normal	**4.**	**5**
5.	Permutation group	**6.**	Simple	**7.**	$P(n)$	**8.**	6 = 1+2+3
9.	Abelian						

BLOCK- III

RING, IDEAL, INTEGRAL DOMAIN AND FIELD

Unit-10: INTRODUCTION TO RING

CONTENTS:

10.1 *INTRODUCTION*

In algebra, the study of rings is known as ring theory. In rings, addition and multiplication are defined and have characteristics in common with those of the operations

specified for integers. Ring theory explores the structure of rings, their representations, or in other words, modules, special classes of rings (such as group rings, division rings), as well as a variety of properties that have proven useful both for the theory's own purposes and for its practical applications, such as homological properties and polynomial identities. Rings that are commutative are significantly easier to understand than those that are not.

Commutative ring theory, often known as commutative algebra, is a significant branch of modern mathematics that has its roots in algebraic geometry and algebraic number theory, which offer several natural instances of commutative rings. The relationship between these three disciplines algebraic geometry, algebraic number theory, and commutative algebra is so close that it is sometimes impossible to determine which discipline a given result belongs to. A basic theorem for algebraic geometry is, for instance, Hilbert's Nullstellensatz, which is formulated and proven in terms of commutative algebra.

Noncommutative rings have a very distinct character since they have a greater potential for strange behaviour. Although the theory has grown on its own, a relatively recent tendency has attempted to mirror the commutative growth by geometrically modelling the theory of some classes of noncommutative rings as if they were rings of functions on (inexistent) "noncommutative spaces." With the advancement of noncommutative geometry and the discovery of quantum groups, this movement began in the 1980s. Noncommutative rings, particularly noncommutative Noetherian rings, have been better understood as a result.

10.2 *OBJECTIVES*

The study of rings is a deep and multifaceted field with applications in various areas of mathematics and beyond, the importance of ideals in the study of rings and algebraic structures. The Ring Theory unit aims to:

1. Introduce the Concept of Rings:

- Define rings, subrings, and different types of rings (commutative, non-commutative, rings with unity, etc.).
- Provide examples like Z, Q, R and $M_n(R)$ (matrix rings).

2. Understand Basic Properties and Operations in Rings:

- Explain addition and multiplication in rings.
- Discuss distributive, associative, and commutative properties.
- Introduce zero divisors, units, boolean ring and polynomial ring.

10.3 *RING*

Let R be a non-empty set then the algebraic structure $(R,+,.)$ equipped with two binary operations addition and multiplication is called a ring if the following conditions are satisfied:

i. $(R,+)$ is an abelian group.

ii. $(R,.)$ is semi group.

iii. Distributive laws holds, i.e.,

$$a.(b+c) = a.b + a.c \quad \forall\, a,b,c \in R \qquad \text{[Right distributive law]}$$

$$(b+c).a = b.a + c.a \quad \forall\, a,b,c \in R \qquad \text{[Left distributive law]}$$

Example 1: Show that the set $R = \{a + b\sqrt{3} \mid a,b \in Q)$ is a ring under the usual addition and multiplication as binary compositions.

Solution: First we can easily prove that $(R,+)$ is an abelian group and $(R,.)$ is a semi group.

Let $x = a + b\sqrt{3}$, $y = c + d\sqrt{3}$ and $z = e + f\sqrt{3} \in R$

Then $xy = (a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3} \in R$

Since $ac + 3bd \in Q$ and $ad + bc \in Q$

Now, $(xy)z = \{(ac + 3bd) + (ad + bc)\sqrt{3}\}(e + f\sqrt{3})$

$= (ace + 3bde + 3adf + 3bcf) + (acf + 3bdf + ade + bce)\sqrt{3}$

$\therefore (xy)z = x(yz)$

Finally, $x(y+z) = (a + b\sqrt{3})\{(c+e) + (d+f)\sqrt{3}\}$

$= (ac + ae + 3bd + 3bf) + (ad + af + bc + be)\sqrt{3}$

$= \{(ac + 3bd) + (ad + bc)\sqrt{3}\} + \{(ae + 3bf) + (af + be)\sqrt{3}\}$

$\therefore x(y+z) = xy + xz$

Similarly, $(x+y)z = xy + yz$.

Hence R is a ring.

Example 2: A **Gaussian integer** $Z[i]$ is a complex number defined as $Z[i] = \{a + ib \mid a,b \in Z\}$. Show that $Z[i]$ forms a ring under ordinary addition and multiplication of complex numbers.

Solution: Let $a + ib$ and $c + id$ be any Gaussian integer then,

$(a + ib) + (c + id) = (a + c) + i(b + d)$

And $(a + ib) + (c + id) = (ac - bd) + i(ad + bc)$

These are again Gaussian integer because $(a+c),(b+d),(ac-bd),(ad+bc)$ all are again belongs to Z. Hence we can say that $Z[i]$ is closed with respect to ordinary addition and multiplication of complex numbers.

As we know that set is complex number is form abelian group with respect to addition and hence $Z[i]$ will be also associative and as well as commutative with respect to addition.

Since $0+i\,0 \in Z[i]$ is the additive identity of the Gaussian integer. The additive inverse of $a+i\,b$ is $(-a)+i\,(-b)$.

Now, $1+i\,0 \in Z[i]$ is the multiplicative inverse of the Gaussian integer because $\forall\, a,b \in Z$

$(1+i\,0)(a+i\,b) = a+ib = (a+i\,b)(1+i\,0)$.

Also $Z[i]$ satisfies the left and right distributive law. Hence we can say that the Gaussian integer $Z[i]$ form ring *i.e.*, $(Z[i],+,.)$ is form ring.

10.4 *RING WITH UNITY*

In a ring R, if there exist an element $1 \in R$ (multiplicative identity) such that $1.a = a = a.1 \forall\, a \in R$, then R is called a ring with unit element. Here, the element $1 \in R$, is called the unit element of the ring. Thus if a ring possesses multiplicative identity, then it is a ring with unity.

10.5 *COMMUTATIVE RING*

If a ring R is commutative with respect to the operation multiplication then the ring $(R,+,.)$ is called commutative ring i.e., if we have $a.b = b.a \;\forall\, a,b \in R$, then R is called a commutative ring.

Note: In future we shall denote the multiplication composition in a ring R not by the symbol '.' but by multiplicative notation. Thus we shall write ab in place of $a.b$.

Example:

1. $(Z,+,.)$ is a ring. This ring is called ring of integers.
2. $(mZ,+,.)$ is a ring, m being fixed integer. This ring is Commutative ring.
3. $(R,+,.)$ is a ring. This ring is called ring of real numbers. This ring is a commutative ring with unity element.
4. $(Q,+,.)$ is a commutative ring. This ring is called ring of rational numbers.

10.6 *BOOLEAN RING*

A ring $(R, +, .)$ is called Boolean ring if all elements are indempotent *i.e.*,

$$a.a = a, i.e., a^2 = a \; \forall a \in R.$$

e.g., $Z_2 = \{0,1\}$ is the Boolean ring because $0^2 = 0.0 = 0$ and $1^2 = 1.1 = 1$

10.7 *p- RING*

A ring $(R, +, .)$ is called p-ring if

$$a^p = a \;\; and \; pa = 0 \forall a \in R.$$

Similarly we define 2-ring.

10.8 *ZERO DIVISOR*

The non zero elements a,b of a ring R are knows as proper divisors of zero or zero divisors if $ab = 0$ or $ba = 0$.

Example:

1. The ring has matrices has zero divisors, for example if

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0, & 0 \\ 1 & 1 \end{bmatrix}$$

   Then

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

   Hence the ring $R = \{0,1,2,3,4,5,6,7\}$ of matrices has zero divisors.
2. The rings of a number do not have zero divisors. For∃ no two non-zero numbers such that their product is zero.

10.9 *RING WITHOUT ZERO DIVISORS*

A ring is called without zero divisors if product of two non-zero elements of R is not zero if $ab = 0$ where $a, b \in R$, $a = 0 \; or \; b = 0$ both $a = 0$ and $b = 0$.

If we say that R is aring with zero divisors $\{a \neq 0 \; b \neq 0 \; then \; ab = 0\}$

Some common examples on ring

As we have already discussed, in abstract algebra, a ring is a set equipped with two binary operations (usually addition and multiplication) that generalize arithmetic properties. Here are some common examples:

1. Standard Number Rings

I. Integers (Z) – The set of all integers with usual addition and multiplication. This is a commutative ring with identity 1.
II. Integers modulo n (Z_n) – The set $\{0, 1, ..., n-1\}$ under modular arithmetic. This is a finite ring.
III. Rational, Real, and Complex Numbers (Q, R, C) – These form fields, which are also rings.
IV. Gaussian Integers ($Z[i]$) – The set of complex numbers of the form $a+ib$, where $a,b \in Z$.

2. Polynomial Rings

I. Polynomial Ring ($Z[x]$, $R[x]$, $C[x]$) – The set of polynomials with coefficients in a given ring (e.g., integers or real numbers).
II. Modular Polynomial Ring ($Z_n[x]$) – Polynomials with coefficients in Z_n.

3. Matrix Rings

I. Ring of $n \times n$ Matrices ($M_n(R)$) – The set of all $n \times n$ matrices over a ring R, with usual matrix addition and multiplication.
II. Upper Triangular Matrix Ring – Matrices where all entries below the diagonal are zero.

4. Function Rings

I. Ring of Continuous Functions $C(X,R)$ – The set of all continuous real-valued functions on a space X, with pointwise addition and multiplication.
II. Laurent Series Ring ($C((x))$– The ring of formal power series that allow negative exponents.

5. Special Rings

I. Boolean Ring – A ring where $x^2 = x$ for all x (e.g., Z_2).
II. Quaternions (H) – A non-commutative ring that extends complex numbers.
III. Group Rings (Z[G]) – Rings constructed from a group G and a ring R.

Later in higher classes you will learn with deeper explanation of these.

Some proof of useful rings

1. The Ring of Integers Z: The set of integers Z with standard addition and multiplication forms a ring.

Proof: Closure: Sum and product of any two integers is an integer.

- **Associativity**: Addition and multiplication are associative.
- **Additive Identity**: 0 is in Z and $a+0=a$
- **Additive Inverse**: For every $a \in Z$, there exists –a such that $a+(-a)=0$
- **Distributivity**: $a(b+c)=ab+ac$
- **Commutativity of Addition**: $a+b=b+a$

Since *Z* satisfies all the ring axioms, it is a commutative ring with identity 1.

2. The Ring of Integers Modulo *n*, Z_n: The set $\{0,1,...,n-1\}$ with addition and multiplication modulo *n* forms a ring.

Proof: Closure: If $a,b \in Z_n$, then $(a+b) \bmod n$ and $(a.b) \bmod n$ are in Z_n.

- **Associativity**: Follows from associativity of integer addition and multiplication.
- **Additive Identity**: $0 \bmod n$ is the identity.
- **Additive Inverse**: Every $a \in Z_n$ has an inverse $-a \bmod n$.
- **Distributivity**: $a(b+c) \equiv ab+ac \pmod n$.

Thus, Z_n is a finite commutative ring with identity 1.

3. The Ring of Polynomials *R*[*x*]:

For any commutative ring *R*, the set of polynomials with coefficients in *R* forms a ring under usual addition and multiplication.

Proof: Closure: The sum/product of two polynomials is still a polynomial.

- **Associativity**: Follows from associativity of polynomial addition and multiplication.
- **Additive Identity**: The zero polynomial 0 exists.
- **Additive Inverse**: Given $P[x]=a_n x^n+...+a_0$, the inverse is
  $-P[x]=-(a_n x^n+...+a_0)=-a_n x^n-...-a_0$
- **Distributivity**: Polynomial multiplication distributes over addition.

Thus, *R*[*x*] is a commutative ring with identity 1 if *R* has identity.

4. The Ring of $n \times n$ Matrices $M_n(R)$

The set of all $n \times n$ matrices with entries in a ring *R*, with matrix addition and multiplication, forms a ring.

Proof: Closure: Sum and product of two $n \times n$ matrices remain in $M_n(R)$.

- **Associativity**: Follows from associativity of matrix addition and multiplication.
- **Additive Identity**: The zero matrix 0 satisfies $A + 0 = A = 0 + A$
- **Additive Inverse**: Each A has an inverse $-A$ such that $A + (-A) = 0 = (-A) + A$
- **Distributivity**: $A(B + C) = AB + AC$ and $(A + B)C = AC + BC$.

This is a non-commutative ring if $n > 1$.

5. The Boolean Ring

A Boolean ring consists of elements {0, 1} with addition and multiplication defined as:

- Addition: $a + b$ is XOR: $0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0$
- Multiplication: $a.b$ is AND: $0.0 = 0, 0.1 = 0, 1.0 = 0, 1.1 = 1$

Proof: Closure: XOR and AND are well-defined for {0, 1}.

- **Associativity**: XOR and AND are associative.
- **Additive Identity**: 0 is the identity for addition.
- **Additive Inverse**: Each element is its own inverse since $a + a = 0$
- **Distributivity**: $a.(b + c) = ab + ac$.
- **Idempotence**: $a^2 = a$, which is a special property of Boolean rings.

This is a commutative ring without an identity.

6. The Ring of Continuous Functions *C*(*X*, *R*)

Let *C*(*X*, *R*) be the set of all real-valued continuous functions on a topological space *X*. Addition and multiplication are defined pointwise:

- $(f + g)(x) = f(x) + g(x)$
- $(f.g)(x) = f(x)g(x)$

Proof: Closure: Sum and product of continuous functions remain continuous.

- **Associativity**: Follows from real number operations.
- **Additive Identity**: The zero function $f(x) = 0$

- **Additive Inverse**: $-f(x)$ is still continuous.
- **Distributivity**: $f.(g+h) = fg + fh$

This is a commutative ring with identity (the constant function 1).

7. The Quaternions *H*

The set of quaternions consists of numbers of the form:

$$a + bi + cj + dk, a, b, c, d \in R$$

where $i^2 = j^2 = k^2 = i\,j\,k = -1$

Proof: Closure: Sum and product of quaternions remain quaternions.

- **Associativity**: Holds for quaternion addition and multiplication.
- **Additive Identity**: $0 + 0i + 0\,j + 0k$
- **Additive Inverse**: The inverse of $a + bi + c\,j + d\,k$ is $-a - bi - c\,j - d\,k$
- **Distributivity**: $q(r+s) = qr + qs$

8. The Ring of *p*-adic Integers Z_p

The ***p*-adic integers** form a ring where numbers are represented using an infinite sequence of digits in base *p*. The set Z_p consists of limits of sequences of integers modulo increasing powers of *p*.

Proof: We have to prove that Z_p is a Ring

- **Closure**: Addition and multiplication are well-defined in Z_p
- **Associativity**: Inherited from integer operations.
- **Additive Identity**: The element 0 (represented as 0, 0, 0, …) is in Z_p.
- **Additive Inverse**: Every element has an inverse in Z_p
- **Distributivity**: Follows from modular arithmetic in powers of *p*.

Z_p is a commutative ring with identity**.**

9. The Ring of Continuous Functions *C*(*X*, *R*)

The set of all continuous functions $f : X \to R$ forms a ring under point-wise addition and multiplication.

Proof: We have to prove that $C(X, R)$ is a Ring

- **Closure**: Sum and product of continuous functions remain continuous.
- **Associativity**: Inherited from R.
- **Additive Identity**: The zero function $f(x) = 0$
- **Additive Inverse**: If $f(x)$ is continuous, so is $-f(x)$
- **Distributivity**: $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$

$C(X, R)$ is a commutative ring with identity.

10.10 *CHARACTERISTIC OF A RING*

The characteristic of a ring R is explained as the smallest positive in integer$n$. s.t. $na = 0 \forall a \in R$. If their exist no positive integer, then R is called characteristic zero. Therefore R is of characteristic zero if $na \neq 0 \forall a \in R$ and for any positive integer$n$.

Theorem 1: (Elementary properties of ring) If a, b, c are arbitrary elements of a ring R, then
Prove that.

i. $a0 = 0a = 0$

Solution: Let

$$0 + 0 = 0$$
$$a(0 + 0) = a0 \quad \text{by left distribution law}$$
$$a0 + a0 = a0$$
$$a0 + a0 = a0 + 0 \quad as\ x + 0 = x$$

Now we get

$$a0 = 0 \quad \ldots (1)$$

Again

$$0 + 0 = 0$$
$$(0 + 0)a = 0a \quad \text{by right distribution law}$$
$$0a + 0a = 0a$$
$$0a + 0a = 0a + 0$$

By cancellation law in (R,+), we obtain

$$0a = 0 \quad \ldots (2)$$

ii. $a(-b) = -(ab) = (-a)b$

Solution: From (1) and (2) ,we obtain the results

$$a(-b + b) = a(-b) + ab \quad \text{For } -b + b = 0$$
$$a(0) = a(-b) + ab$$
$$0 = a(-b) + ab$$
$$a(-b) = -(ab) \quad \ldots (3)$$

Since the additive inverse of ab is a$a(-b)$

Similarly

$$(-a + a)b = b(-a) + ba$$
$$(-a + a) = 0 \text{ and } 0b = 0$$
$$0 = (-a)b + ba$$

Since the additive inverse of ab is a$(-a)b$.

$$-(ab) = (-a)b \quad \ldots (4)$$

From (3) and (4), we obtain

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

iii. $(-a)(-b) = ab$

Solution: Let $(-a)(-b) = -[a(-b)]$, by (ii)

$= -[-(ab)]$ again by (ii)

$= ab$ For $-(-x) = x \ \forall x \in R$.

iv.

Solution: $a(b-c) = a[b+(-c)]$

$= ab + a(-c)$

$= ab + [-ac]$

$= ab - ac$

v.

Solution: $(b-c)a = [b+(-c)]a$

$= ba + (-c)a$

$= ba + [-ca]$

$= ba - ca$

Theorem 2: If R is a ring with unity element 1, then
$(-1)a = -a = a(-1)$ $\forall a \in R$ and $(-1)(-1) = 1$.

Proof: $(-1+1)a = (-1)a + 1.a$

$0.a = (-1)a + 1.a$

$0 = (-1)a + a$

Since $(-1)a = -a$, [For $a + x = 0, a = -x$]

Again $a(-1+1) = a(-1) + a.1$

$a.0 = a(-1) + a.1$

$0 = a(-1) + a$

This implies $a(-1) = -a$ Also $(-1)a = -a$

$(-1)a = -a = a(-1)$

Now taking $a = -1$in above equation

$(-1)(-1) = (-1)(-1) = -(-1)$

$(-1)(-1) = -(-1) = 1$

For $-(-x) = x$ in additive group or $(-1)(-1) = 1$.

Theorem 3: A ring without zero divisors iff the cancellation laws hold in R.

Proof: Suppose R be a ring without zero divisors.

To prove that cancellation laws hold in R.

Since let $a, b, c \in R \ s.t. ab = ac \ and \ a \neq 0$.

Then $ab = ac \Rightarrow a(b-c) = 0$

Also $a \neq 0$ and R has no zero divisors.

Hence $b - c = 0 \Rightarrow b = c$

Thus $ab = ca, a \neq 0 \Rightarrow b = c$

Similarly we can show that $ba = ca, a \neq 0 \Rightarrow b = c$

Conversely, Let R be a ring s.t. cancellation laws hold in R.

To prove that R has no zero divisors.

Suppose the contrary. Then R has zero divisors, then

$\exists a, b \in R \; s.t. \; ab = 0$ and $a, b \neq 0$

$ab = 0, a \neq 0 \Rightarrow ab = a.0$ for a.0=0 $\Rightarrow b = 0$. By left cancellation law

A Contradiction, for $b \neq 0$

Similarly$ab = 0, b \neq 0 \Rightarrow a = 0$. A Contradiction, for $a \neq 0$.

Theorem 4: If R is a Boolean ring then

(i) $2a = 0 \; \forall \; a \in R$

(ii) $ab = ba \;\; i.e. R$ is commutative.

Proof:

(i) Suppose $2a = a + a$

$= (a + a)^2$ $\because R$ is Boolean ring, $x^2 = x \; \forall \; x \in R$

$= (a + a)(a + a)$

$= a^2 + a^2 + a^2 + a^2$

5

$= 4a^2$

$2a = 4a$ $a^2 = a$ (R is Boolean)

$4a - 2a = 0$

$2a = 0$ or $a + a = 0$.

(ii) Now

$(a + b)^2 = a + b$ $\because R$ is Boolean

$(a + b)(a + b) = a + b$

$a(a + b) + a(a + b) = a + b$

$(a^2 + ab) + (ba + b^2) = a + b$ By distributive law

$(a + ab) + (ba + b) = a + b$ $\because \; a^2 = a, b^2 = b$

Finally, $(a + b) + (ab + ba) = a + b$

$(a + b) + (ab + ba) = a + b + 0$.

Left cancellation law of addition in R gives$ab + ba = 0$.

Taking$ab = a'$, $ba = b'$, we get

$a' + b' = 0$

$a' + b' = 0 \Longrightarrow a' + b' = 0 = a' + a'$

$\Longrightarrow a' + b' = a' + a'$

$\Longrightarrow b' = a'$, by left cancellation law

$\Longrightarrow ba = ab$.

Theorem 5: If R is any ring with identity 1, show that R has positive characteristic n iff n is the at least positive integer for which$n.1 = 0$, 0 being additive identity of R.

Proof: Let R be a ring with unity element e.

$o(e) = 0 \Longrightarrow$ characteristic of R is 0.

Suppose $o(e) = n = a$ finite number so that n is at least positive integer s.t. $ne = 0$. Let a be any element of R. Then

$na = n(ea)$. For $ea = a = ae$.

$(ne)a = 0a = 0$.

Thus n is the least positive integer s.t. $na = 0$.

This proves that the characteristic of R is n.

SOLVED EXAMPLE

Example 3: Let a and b be arbitrary elements of a ring R whose characteristic is two and $ab = ba$. Then prove that, $(a+b)^2 = a^2 + b^2 = (a-b)^2$

Solution: Suppose $ab = ba = x \in R$

The characteristic of R is two $\Rightarrow 2x = 0 \ \forall x \in R$

$$\Rightarrow x + x = 0$$

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

$$= a^2 + ab + ba + b^2 = a^2 + (x+x) + b^2 = a^2 + 0 + b^2$$

$$= a^2 + b^2$$

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

$$= a^2 - ab - ba + b^2 = a^2 - (x+x) + b^2 = a^2 - 0 + b^2$$

$$= a^2 + b^2$$

Hence, $(a+b)^2 = a^2 + b^2 = (a-b)^2$

Example 4: If any element a has the multiplicative inverse, then a cannot be a divisor of zero, where the underlying set of a ring.

Solution: Suppose let R be a ring and $a \in R$ s.t. a has the inverse $a^{-1} \in R$ so $a \neq 0$

To prove that a is not zero divisor of zero. Suppose not then

a is divisor of zero so ∃ the element $b \in R \quad s.t. \ b \neq 0$ and $ab = 0$.

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow (a^{-1}a)b = 0$$

$$\Rightarrow 1b = 0 \Rightarrow b = 0$$

Contrary$b \neq 0$. Hence required the solution.

10.11 *SUBRING*

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 under addition and multiplication in R and S itself is a ring for those operations.

iff S is closed for compositions in R

iff $\forall\ a, b \in S \Longrightarrow a + b \in S, ab \in S$.

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,b ∈ S ⟹ a-b∈S. (ii)) a,b ∈ S ⟹ ab∈ S.

Proof: Let S be a Subring of a ring R so that S itself is a ring.

To prove that

(i) a,b ϵ S ⟹ a-b ∈ S. (ii) a,b ϵS ⟹ ab ∈S.

S is ring ⟹ (S, +) is an abelian group.

Hence a,b ϵ S ⟹ a, -b ∈ S [Each elemant of S has additive inverse in S]

⟹ a+(-b)∈ S [S is closed w.r.t.(+)]

⟹ a-b ∈ S. Hence the condition (i)

Again S is ring ⟹(S, ·) is a semi group

⟹ S is closed w.r.t. multiplication

⟹ab∈S ∀ a,b∈S. Hence the condition (ii)

Conversely, let S is non empty subset of R s.t. the conditions (i) and (ii) hold.

To prove that S is a subring of R, it is enough to show that S is a ring.

The condition (i) says that

a,a ∈ S ⟹ a-a ∈S ⟹0 ∈S.

Again 0∈ S, a∈S ⟹ 0-a ∈S ⟹-a∈S.

i.e. a ∈ S ⟹-a ∈ S.

Consequently, a, b ∈S ⟹a, -b ∈S

⟹a-(-b) ∈S by condition (i)

⟹ a+b ∈S

a,b∈ S⟹ a,b∈ R

⟹a+b= b+a. Fot (R, +) is a abelian group.

Similarly, we can show that

a+ (b+c) = (a+b)+c ∀ a,b, c ∈S.

Hence the above facts prove that (S, +) is an abelian group. Associatively of multiplication over

addition holds in S. Since they hold in R. Finally we have show that (S, +, ·) is a ring.

Theorem 7: The intersection of two subring is again a subring.

Proof: Let S_1 and S_2 be two subring of ring R.

Since $0 \in S_1$ and $0 \in S_2$ at least $0 \in S_1 \cap S_2$. Therefore $S_1 \cap S_2$ is non-empty.

Let $a,b \in S_1 \cap S_2$, then

$$a \in S_1 \cap S_2 \Rightarrow a \in S_1 \text{ and } a \in S_2$$

and $$b \in S_1 \cap S_2 \Rightarrow b \in S_1 \text{ and } b \in S_2.$$

But S_1 and S_2 are subring of R, therefore

$$a, b \in S_1 \Rightarrow a-b \in S_1 \text{ and } ab \in S_1$$

and $$a, b \in S_2 \Rightarrow a-b \in S_2 \text{ and } ab \in S_2.$$

Consequently, $a,b \in S_1 \cap S_2 \Rightarrow a-b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$.

Hence $S_1 \cap S_2$ is a subring of R.

10.12 *PROPER AND IMPROPER SUBRING*

If R is any ring, then $\{0\}$ and R are always subring of R. These are said to be improper subrings. The subrings of R other than these two, if any, are said to be proper subrings of R.

Example:

- **(i)** The ring of Gaussian integers is a subring of ring of complex numbers.
- **(ii)** The ring of rational numbers is a subring of ring of real numbers.
- **(iii)** The ring of integers is a subring of a ring of rational numbers.

Check your progress

Problem 1: Check that the singleton set $\{0\}$ is ring or not?

Problem 2: Check that the singleton set contain the identity element form a ring?

Problem 3: Check that the set $\{0,1\}$ is ring with unity or not?

10.13 *SUMMARY*

In this unit, we have studied the basic terminology used in ring theory. We have also read about the basic idea of ring with some theorems and examples. We have defined commutative and non commutative.

Ring theory is a fundamental branch of abstract algebra that studies algebraic structures called **rings**, which consist of a set equipped with two binary operations: addition

and multiplication. Rings generalize number systems like integers and polynomials, allowing for diverse structures such as **commutative rings, integral domains, division rings, and fields**. Key concepts include **ideals, ring homomorphisms, quotient rings, and polynomial rings**, which play a crucial role in algebraic structures and applications in number theory, geometry, and cryptography. The study of **zero divisors, units, and prime/maximal ideals** helps in understanding factorization and divisibility in algebra. Ring theory provides a foundation for advanced topics like **module theory, field extensions, and algebraic geometry**. This unit is basic outlook of ring theory and concepts of this unit will be beneficial for the learners in the upcoming units.

10.14 *GLOSSARY*

- Ring
- Gaussian integer
- Subring
- Boolean Ring
- Characteristic of ring
- Ring with unity
- Ring with zero divisor
- Ring without zero divisor

10.15 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

10.16 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

10.17 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Prove that set of integers is a commutating ring 'or' $(Z,+,.)$ is a commutative ring.

2. Prove that set of rational numbers is a commutative ring.

3. Prove that ring without zero divisors *iff* the cancellation laws hold in *R*

4. State and prove the necessary and sufficient condition for any subset of ring to be a subring.

5. Prove that set of rational numbers is a subring of set of real number.

Short Answer Type Question:

1. If R is any ring with identity 1, then prove that R has positive characteristic n iff n is the at least positive integer for which $n.1 = 0$, 0 being additive identity of R.

2. In any ring (*R*) any element *a* has the multiplicative inverse, then prove that *a* cannot be a divisor of zero.

3. Prove that intersection of two subring of a ring is also a subring.

4. Define the ring and subring with example.

5. Let a and b be arbitrary elements of a ring R whose characteristic is two and $ab = ba$. Then prove that,

$$(a+b)^2 = a^2 + b^2 = (a-b)^2$$

Objective type questions

1. Which of the following is NOT necessarily true for a ring (R, +, ·)?

A) R is closed under addition and multiplication.
B) R has an additive identity.
C) R is commutative under multiplication.
D) R satisfies the distributive laws.

2. The ring Z_n is a field if and only if:

A) n is even.
B) n is prime.
C) n is a perfect square.
D) n is composite.

3. Which of the following is an example of a non-commutative ring?

A) Z
B) $M_2(R)$ (the set of 2×2 real matrices)
C) $Q[x]$
D) R

4. A ring *R* is called an integral domain if:

A) R is commutative and has no zero divisors.
B) Every nonzero element of R has a multiplicative inverse.
C) R contains no proper ideals.
D) R has characteristic 0.

5. Which of the following is NOT an ideal in *Z*?

A) $2Z$
B) $3Z$
C) Z
D) Q

6. The characteristic of the ring Z/6Z is:

A) 0
B) 6
C) 3
D) 2

7. The set of all *n*×*n* upper triangular matrices over a field forms a:

A) Commutative ring
B) Non-commutative ring
C) Integral domain
D) Field

8. In a Boolean ring, which property always holds?

A) $x^2 = x$ for all $x \in R$
B) $x^3 = x$ for all $x \in R$
C) R is a field
D) R is an integral domain

9. If *R* is a ring with unity, which of the following must be true?

A) Every element of *R* has a multiplicative inverse.
B) *R* must be commutative.
C) *R* contains a multiplicative identity.
D) *R* is a field.

10. The center of a ring *R* is defined as:

A) The set of units in *R*.
B) The set of all elements that commute with every element of *R*.
C) The set of all nilpotent elements.
D) The set of all zero divisors.

Fill in the blanks:

1. Intersection of two subring of any ring is also a …….

2. Intersection of two ideal of any ring is also an …….

3. Set of rational number is subring of set of ……..

4. A ring (*R*) without zero divisors *iff* the cancellation laws …….. in R.

5. Set of integers is a …….. ring with unity

True and False questions:

1. Every ring has a multiplicative identity.

2. Every field is an integral domain.

3. The set of all **2×2** real matrices forms a commutative ring under matrix addition and multiplication.

4. The set *Z* of integers forms a field.

5. The characteristic of any finite field is always a prime number.

6. Every integral domain is a field.

7. If a ring is commutative and has no zero divisors, then it must be a field.

8. In a Boolean ring, every element is idempotent.

9. Every finite integral domain is a field.

10. If *R* is a ring and $ab = 0$ for some $a, b \in R$, then either $a = 0$ or $b = 0$

10.18 *ANSWERS*

Answer of self cheque question:

1. Yes **2.** Yes **3.** Yes

Answer of objective type question

1.	C	2.	B	**3.**	B	**4.**	A
5.	D	**6.**	B	**7.**	B	**8.**	A
9.	C	**10.**	B				

Answer of fill in the blanks:

1. Subring **2.** Ideal **3.** Real **4.** R **5.** Commutative

Answer of true and false:

1.	False	2.	True	**3.**	False	**4.**	False
5.	True	**6.**	False	**7.**	False	**8.**	True
9.	True	**10.**	False				

Unit-11: INTEGRAL DOMAIN

CONTENTS:

11.1 *INTRODUCTION*

The concept of an **integral domain** originates from the study of number systems and algebraic structures, particularly in the development of **ring theory** in the late 19th and early 20th centuries. Mathematicians such as **Richard Dedekind** and **David Hilbert** contributed significantly to the formalization of rings and ideals, which laid the foundation for the study of integral domains. The term "integral domain" itself emerged as algebraists sought to generalize the properties of integers to more abstract settings, particularly in algebraic number theory and polynomial rings.

An integral domain is a commutative ring with unity ($1 \neq 0$) that has no zero divisors. This means that for any two elements a, b in the ring, if $ab = 0$, then either $a = 0$ or $b = 0$. This property ensures that multiplication behaves similarly to that in the integers, preventing the collapse of nonzero elements into zero. Integral domains generalize the arithmetic of integers and appear naturally in many mathematical structures, including polynomial rings, algebraic number fields, and function fields.

Historically, the study of integral domains led to further classifications, such as principal ideal domains (PIDs), unique factorization domains (UFDs), and fields. The concept is

fundamental in many areas of mathematics, including algebraic geometry, number theory, and commutative algebra.

11.2 *OBJECTIVES*

The objectives of studying the integral domain unit are:

1. **Understanding the Definition**:
   - Learn what an integral domain is and how it differs from other algebraic structures.
2. **Properties of Integral Domains**:
   - Identify key properties such as commutativity, unity, and absence of zero divisors.
   - Understand the cancellation law in an integral domain.
3. **Examples and Counterexamples**:
   - Study examples of integral domains like $\mathbb{Z}$ **(integers),** $\mathbb{Q}$ **(rationals),** $\mathbb{R}$ **(reals), and polynomial rings**.
   - Identify rings that are **not** integral domains due to the presence of zero divisors (e.g., $\mathbb{Z}/6\mathbb{Z}$).
4. **Difference Between Integral Domains and Other Rings**:
   - Compare integral domains with commutative rings, fields, and division rings.
   - Understand why every field is an integral domain, but not every integral domain is a field.
5. **Zero Divisors and Their Absence**:
   - Learn how the absence of zero divisors affects calculations in an integral domain.
6. **Applications in Algebra and Beyond**:
   - Explore the role of integral domains in abstract algebra, number theory, and cryptography.

11.3 *INTEGRAL DOMAIN*

Definition: Any ring (R) is called integral domain, if it satisfies the following conditions

(i) R should be commutative ring

(ii) R has unit element

(iii) R should be without zero divisors.

Some authors defining to integral domain in a different way that an integral domain is a commutative ring without zero divisors. They do not demand that an integral domain have the unit element without a doubt.

Set of integer (I) is a most common example of a ring to be an integral domain. We know that I is a commutative ring with unity and also I does not possess zero divisors. We know that if a, b are integers such that $ab = 0$, then either a or b must be zero.

The other rings which are examples of infinite integral domains are $(C,+,.),(Q,+,.),(R,+,.)$ and the example of finite integral domain is $(\{0,1,2,3,4\},+_5,\times_5)$.

Inversible elements in a ring with unity: In a ring (R) each element possess additive inverse. Therefore when we talking about inversible of an element, we only asking about invertiablity with respect to the operation multiplication. If R is a ring with unity, then an element $a \in R$ is called inversible, if there exist $b \in R$ such that $ab = 1 = ba$. Then we rewrite $b = a^{-1}$.

Examples 1: In the ring of integers 1 and -1 are the only two inversible elements.

2: In the set of $n \times n$ 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.

Example 3: Prove that the set of integers Z with standard addition and multiplication is an integral domain.

Solution: Z is a Commutative Ring with Unity

- Addition and multiplication are associative and commutative.
- The additive identity is 0 and the multiplicative identity is 1.
- The distributive property holds: $a(b + c) = ab + ac$ for all $a, b, c \in Z$
- Every integer has an additive inverse (e.g., $-a$ is the inverse of a).

No Zero Divisors

- Suppose $a, b \in Z$ such that $a.b = 0$
- This means $ab = 0$
- Since integers obey the fundamental property that the product of two nonzero integers is never zero, it follows that either $a = 0$ or $b = 0$
- Hence, Z has no zero divisors.

Example 4: The set of all polynomials with integer coefficients, denoted as Z[x], forms an integral domain**.**

Solution: Z[x] is a Commutative Ring with Unity

- Addition and multiplication of polynomials satisfy associativity and commutativity.
- The additive identity is 0 (the zero polynomial).
- The multiplicative identity is 1 (the constant polynomial 1).

- The distributive property holds.

No Zero Divisors

- Suppose $f(x), g(x) \in Z[x]$ such that $f(x).g(x) = 0$
- This means the product of the two polynomials is the zero polynomial.
- In polynomial rings over an integral domain (like *Z*), if the product is zero, then at least one of the polynomials must be the zero polynomial.
- Since Z is an integral domain, Z[x] inherits this property.

Thus, Z[x] is an **integral domain**.

Example 5: The set of rational numbers *Q* forms an **integral domain** under standard addition and multiplication.

Solution: Q is a Commutative Ring with Unity

- Rational numbers satisfy the properties of a ring (associativity, commutativity, distributivity).
- The additive identity is 0.
- The multiplicative identity is 1.
- Every element has an additive inverse.

No Zero Divisors

- Suppose $a, b \in Q$ such that $a.b = 0$.
- Since Q consists of fractions $\frac{p}{q}$ (where $p, q \in Z$, $q \neq 0$), the product $\frac{p_1}{q_1}.\frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2}$
- If $\frac{p_1 p_2}{q_1 q_2} = 0$, then $p_1 p_2 = 0$
- Since integers have no zero divisors, either $p_1 = 0$ or $p_2 = 0$, meaning either $a = 0$ or $b = 0$

Thus, *Q* is an **integral domain**.

Example 6: Give an example of ring which is not an integral domain?

Solution: As we know that Z_n is a ring for all $n \in N$. But Z_n is not an integral domain for all $n \in N$. For e.g., $Z_8 = \{0,1,2,3,4,5,6,7\}$ is a ring but it is not an integral domain as Z_8 is not without zero divisor.

Because $2 \neq 0, 4 \neq 0 \in Z_8$ and $2.4 = 0 \in Z_8$.

Hence Z_8 is a ring but not an integral domain.

Theorem 1: A commutative ring R is an integral domain *iff* $\forall a,b,c \in R(a \neq 0)$

$$ab = ac \Rightarrow b = c$$

Proof: Let R is an integral domain.

Also let $ab = ac \ (a \neq 0)$

Then $ab - ac = 0$

$\Rightarrow a(b-c) = 0$

$\Rightarrow a = 0 \, or \, b - c = 0$

Since $a \neq 0$, we get $b = c$

Conversely, let the given condition holds good.

Let $a,b \in R$ be a arbitrary elements with $a \neq 0$.

Suppose $ab = 0$

Then $ab = a.0$

$\Rightarrow b = 0$ using given condition

Hence $ab = 0 \Rightarrow b = 0$ whenever $a \neq 0$ or that R is an integral domain.

Remark: Any ring (R) is said to satisfy left cancellation law if $\forall a,b,c \in R(a \neq 0)$

$ab = ac \Rightarrow b = c$

1. Similarly we can talk of right cancellation law. It is to notify that cancellation is of only non zero elements.

Theorem 2: The characteristic of an integral domain is 0 or $n > 0$ according as the order of any non-zero element regarded as a member of the additive group of the integral domain is either 0 or *n*.

Proof: Let *D* be an integral domain.

If a non-zero element of D is of order zero, then the characteristic of *D* is zero.

Let the order of the non-zero element *a* be finite and equal to n. Then $na = 0$. Suppose *b* is any other non-zero element of *D*.

We have $na = 0$

$\Rightarrow (na)b = 0$

$\Rightarrow (a + a + a + ... \text{ upto n terms})b = 0$

$\Rightarrow (ab + ab + ab + ... \text{ upto n terms}) = 0$

$\Rightarrow a(b + b + b + ... \text{ upto n terms}) = 0$

$\Rightarrow a(nb) = 0$

But D is without zero divisors. Therefore $a \neq 0$ and $a(nb) = 0$

$\Rightarrow a(nb) = 0$

But the order of a is $n \Rightarrow n$ is the least positive integer such that $na = 0$. Also we have $n0 = 0$. Thus n is the least positive integer such that $nx = 0 \forall x \in D$. Hence D is of characteristic n.

Theorem 3: Each non-zero element of an integral domain *D*, regarded as a member of the additive group of *D*, is of the same order.

Proof: Let *D* be an integral domain. Suppose *a* is a non-zero element of *D* and $O(a)$ is finite and say, equal to n.

Suppose b is any other non-zero element of D and $O(b) = m$.

We have $O(b) = n \Rightarrow na = 0$

$\Rightarrow nb = 0$

$\Rightarrow O(b) \leq n \Rightarrow m \leq n$.

Similarly, $O(b) = m \Rightarrow mb = 0 \Rightarrow a(mb) = 0$

$\Rightarrow a(b + b + ... \text{upto } m \text{ times}) = 0$

$\Rightarrow (ab + ab + ... \text{upto } m \text{ times}) = 0$

$\Rightarrow (ab + ab + ... \text{upto } m \text{ times}) = 0$

$\Rightarrow (a + a + ... \text{upto } m \text{ times})b = 0$

$\Rightarrow (ma)b = 0$

$\Rightarrow ma = 0$ [$\because b \neq 0$ and D is without zero divisors]

$\Rightarrow O(a) \leq m \Rightarrow n \leq m$

Now, $m \leq n$, $n \leq m \Rightarrow m = n$. Hence $O(a) = O(b)$.

Theorem 4: The characteristic of an integral domain is either 0 or a prime number.

Proof: Suppose D is an integral domain. Let $0 \neq a \in D$. If $O(a)$ is zero, then the characteristic of D is 0. If $O(a)$ is finite, let $O(a) = p$. Then the characteristic of D will be p. We have to now prove that p must be prime.

Suppose p is not prime. Let $p = p_1 p_2$ where $p_1 \neq 1, p_2 \neq 1$ and $p_1 < p$ also $p_2 < p$.

Since D is an integral domain, therefore the product of two non-zero element of D cannot be equal to 0.

$\therefore aa \neq 0$ i.e., $\therefore a^2 \neq 0$

Now in an integral domain two non-zero elements are of the same order.

$\therefore O(a) = p \Rightarrow O(a^2) = p \Rightarrow pa^2 = 0$

$\Rightarrow (p_1 p_2)a^2 = 0$ $[\because p = p_1 p_2]$

$\Rightarrow (a^2 + a^2 + \ldots \text{ upto } p_1 p_2 \text{ terms}) = 0$

$\Rightarrow (p_1 a)(p_2 a) = 0 \text{ terms}) = 0$

$\Rightarrow$ either $p_1 a = 0$ *or* $p_2 a = 0$ $[\because D$ is without zero divisors]

But $p_1 < p$ and $p_2 < p$. Also p is the least positive integer such that $pa = 0$. Hence p must be prime.

11.4 *ORDERED INTEGRAL DOMAINS*

Definition: An integral domain $(D, +, .)$ is said to be ordered if D contains a subset D_+ such that

(*i*) D_+ is closed with respect to addition and multiplication as defined on D.

(*ii*) $\forall a \in D$, one and only one of $a = 0, a \in D_+, -a \in D_+$, holds (principle of trichotomy).

The elements of D_+ are called the positive elements D, all other non-zero elements of *D* are called negative elements of *D*.

Theorem 5: Let D be an integral domain with unity element 1. If D is an ordered integral domain show that 1 is a positive element of D.

Proof: Let D be an ordered integral domain with unity element 1. Let D_+ denote the set of positive element of *D*. Suppose $1 \notin D_+$.

Now, $1 \neq 0$. Since $1 \notin D_+$ therefore by the definition of an ordered integral domain,

$-1 \notin D_+$ $[\because D_+$ is closed with respect to multiplication]

$\Rightarrow 1 \in D_+$, which is a contradiction.

Hence $1 \in D_+$ i.e., 1 is a positive element of *D*.

Definition: Let D be an ordered integral domain and D_+ be the set of positive elements of D. Then we defines 'less than' (<) 'greater than' (>) relations in *D* as follows:

For all $a, b \in D$, we have

(i) $a > b$ when $a - b \in D_+$

(ii) $a < b$ when $b - a \in D_+$

Obviously $a > b$ iff $b < a$

Theorem 6: The order relation in an ordered integral domain is transitive *i.e.*, $a > b, b > c \Rightarrow a > c$.

Proof: Let D be an ordered integral domain and let D_+ be the set of positive element of *D*.

We have $a > b \Rightarrow a - b \in D_+$

and $b > c \Rightarrow b - c \in D_+$

Now D_+ is closed with respect to addition.

$\therefore a - b \in D_+, b - c \in D_+ \Rightarrow (a - b) + (b - c) \in D_+$

$\Rightarrow a - b \in D_+ \Rightarrow a > c$

Check your progress

Problem 1: Check that the set Z_5 is integral domain or not?

Problem 2: Check that the set Z_{12} is integral domain or not?

Problem 3: Check that the set Z_{5^2} is integral domain or not?

11.5 *SUMMARY*

This unit**,** Integral Domain explores a special class of rings that are commutative, have a multiplicative identity ($1 \neq 0$), and contain no zero divisors**.** This ensures that the cancellation law holds, making integral domains fundamental in algebra. Key examples include $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers), and polynomial rings $\mathbb{Z}$[x]**.** The chapter also distinguishes integral domains from general rings and fields**,** noting that every field is an integral domain, but not every integral domain is a field**.** It also covers important results like every finite integral domain is a field and explores applications in number theory, cryptography, and algebraic structures**.**

11.6 *GLOSSARY*

- Integral Domain
- Ordered integral domain
- Without zero divisor

11.7 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

11.8 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

11.9 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Define an integral domain. Explain its properties with examples.
2. Give an example of a commutative ring that is not an integral domain. Explain why it fails to be an integral domain.
3. Explain the cancellation law in an integral domain and prove that it holds.
4. Discuss the difference between an integral domain and a field, providing examples of each.
5. Explain why the ring of integers modulo n ($\mathbb{Z}/n\mathbb{Z}$) is an integral domain if and only if n is a prime number.
6. Show that the set of 2×2 matrices over $\mathbb{Z}$ is not an integral domain.
7. Prove that the polynomial ring $\mathbb{Z}[x]$ is an integral domain.
8. Explain why $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, using the concept of zero divisors.
9. If R is an integral domain, prove that its polynomial ring R[x] is also an integral domain.

Short Answer Type Question:

1. Define an integral domain.
2. Give an example of an integral domain that is not a field.
3. What is the main difference between an integral domain and a field?
4. State the cancellation law in an integral domain.
5. Why is $\mathbb{Z}/6\mathbb{Z}$ not an integral domain?

6. Does every integral domain have a multiplicative inverse for every element? Why or why not?

7. Is the set of all 2×2 matrices over $\mathbb{Z}$ an integral domain? Why?

8. What is a zero divisor? Does an integral domain have zero divisors?

9. Give an example of a commutative ring that is not an integral domain.

10. Why is $\mathbb{Z}[x]$ (polynomials with integer coefficients) an integral domain?

Objective type questions

1. Which of the following is an essential property of an integral domain?

a) It has zero divisors
b) It is not commutative under multiplication
c) It is a commutative ring with unity and no zero divisors
d) Every element has a multiplicative inverse

2. Which of the following is an example of an integral domain?

a) The set of all integers ($\mathbb{Z}$)
b) The set of all $n \times n$ matrices under matrix multiplication
c) The set of integers modulo 6 ($\mathbb{Z}_6$)
d) The set of rational numbers modulo 4 ($\mathbb{Q}_4$)

3. If D is an integral domain, which of the following statements is always true?

a) D is a field
b) D is a commutative ring with identity
c) Every element in D has an inverse
d) D contains zero divisors

4. Which of the following rings is NOT an integral domain?

a) $\mathbb{Z}$ (Integers)
b) $\mathbb{Q}$ (Rational Numbers)
c) $\mathbb{Z}_6$ (Integers modulo 6)
d) $\mathbb{R}$ (Real Numbers)

5. If R is an integral domain, and a, b are elements of R such that ab = 0, what can be concluded?

a) Either a = 0 or b = 0
b) Both a and b are nonzero
c) R contains zero divisors
d) R is not commutative

6. Which of the following is true for every integral domain D?

a) Every nonzero element has a multiplicative inverse
b) Every nonzero element is a unit
c) If a, b, c ∈ D and a ≠ 0, then ab = ac implies b = c
d) Every element has an additive inverse and a multiplicative inverse

7. Which of the following rings is an integral domain?

a) The set of all n × n matrices under addition and multiplication
b) The ring $\mathbb{Z}$**/8**$\mathbb{Z}$ (integers modulo 8)
c) The ring $\mathbb{Z}$**[x]** (polynomials with integer coefficients)
d) The ring of even integers under normal addition and multiplication

8. Let R be an integral domain. Which of the following statements is false?

a) R contains no zero divisors
b) The product of two nonzero elements in **R** is always nonzero
c) Every nonzero element in **R** has a multiplicative inverse
d) The ring of integers $\mathbb{Z}$ is an integral domain

9. Which of the following is not an integral domain?

a) $\mathbb{Z}$ (Integers)
b) $\mathbb{Q}$ (Rational numbers)
c) $\mathbb{Z}$/4$\mathbb{Z}$ (Integers modulo 4)
d) $\mathbb{Z}$[x] (Polynomials with integer coefficients)

10. The field of real numbers $\mathbb{R}$ is an integral domain. Which additional property makes it a field?

a) It has no zero divisors
b) It has an identity element for multiplication
c) Every nonzero element has a multiplicative inverse
d) It satisfies the associative property of multiplication

Fill in the blanks:

1. An integral domain is a _____ ring with identity and no zero divisors.
2. The ring of integers $\mathbb{Z}$ is an example of an _____ domain.
3. If a ring contains zero divisors, then it is _____ an integral domain.
4. In an integral domain, the _____ law holds: If a ≠ 0 and ab = ac, then b = c.
5. Every field is an _____, but not every integral domain is a _____.
6. The set of polynomials $\mathbb{Z}$**[x]** with integer coefficients is an example of an _____.
7. The ring $\mathbb{Z}$**/6**$\mathbb{Z}$ is _____ an integral domain because it has zero divisors.
8. A ring R is an integral domain if it has no _____ divisors.

9. Every finite integral domain is a _____.
10. The ring of real numbers $\mathbb{R}$ is an example of both a _____ and a field.

True and False questions:

1. Every integral domain is a commutative ring with unity.
2. Every integral domain is a field.
3. The set of all **n × n** matrices over $\mathbb{Z}$ forms an integral domain.
4. If **R** is an integral domain and a, b ∈ R such that ab = 0, then either a = 0 or b = 0.
5. The set of all even integers forms an integral domain under normal addition and multiplication.
6. The set $\mathbb{Z}/6\mathbb{Z}$ (integers modulo 6) is an integral domain.
7. The ring of polynomials $\mathbb{Z}$**[x]** (polynomials with integer coefficients) is an integral domain.
8. Every finite integral domain is a field.
9. The real numbers $\mathbb{R}$ form an integral domain.
10. If **R** is an integral domain, then it must have a unique multiplicative inverse for every element.
11. The ring of integers $\mathbb{Z}$ is an integral domain.
12. The ring $\mathbb{Z}/8\mathbb{Z}$ (integers modulo 8) is an integral domain.
13. If **R** is an integral domain, then **R[x]** (the ring of polynomials over **R**) is also an integral domain.
14. In an integral domain, the cancellation law holds: if $\mathbf{a \neq 0}$ and **ab = ac**, then **b = c**.
15. A commutative ring with identity is always an integral domain.
16. If **R** is an integral domain, then every nonzero element of **R** must be invertible.
17. The set of rational numbers $\mathbb{Q}$ forms an integral domain.
18. The set of complex numbers $\mathbb{C}$ is an integral domain.
19. Every subring of an integral domain is also an integral domain.
20. The ring of **2 × 2** matrices over $\mathbb{Z}$ forms an integral domain.

11.10 *ANSWERS*

Answer of self cheque question:

1. Yes **2.** No **3.** No

Answer of objective type question

1.	c	2.	a	**3.**	b	**4.**	c
5.	a	**6.**	c	**7.**	c	**8.**	c
9.	c	**10.**	c				

Answer of fill in the blanks:

1.	commutative	**2.**	integral	**3.**	not	**4.**	cancellation
5.	integral domain, field			**6.**	Integral domain		
7.	not			**8.**	Zero		
9.	field			**10.**	Integral domain		

Answer of true and false:

1.	True	2.	False	**3.**	False	**4.**	True
5.	False	**6.**	False	**7.**	True	**8.**	True
9.	True	**10.**	False	**11.**	True	**12.**	False
13.	True	**14.**	True	**15.**	False	**16.**	False
17.	True	**18.**	True	**19.**	False	**20.**	False

Unit-12: IDEALS AND FACTOR RING

CONTENTS:

12.1 *INTRODUCTION*

An ideal of a ring in mathematics, and more specifically in ring theory, is a unique subset of its constituent parts. Certain subsets of the integers, such as the even numbers or the multiples of 3, are generalized by ideals. The defining characteristics of an ideal are closure and absorption: adding and subtracting even numbers maintains evenness, and multiplication an even number by any integer (even or odd) yields an even number. Similar to how a normal subgroup may be used to create a quotient group in group theory, an ideal can be used to create a quotient ring.

The ideals are the non-negative integers that correspond one-to-one with the integers; each ideal in this ring is a main ideal made up of multiples of a single non-negative number.

However, in other rings, the ideals might not exactly match the ring components, and when certain integer qualities are generalized to rings, they tend to attach to the ideals rather than the ring components more naturally. For instance, the Chinese remainder theorem may be used to ideals and the prime ideals of a ring are comparable to prime integers. The ideals of a Dedekind domain, a significant type of ring in number theory, have a variant of unique prime factorization.

In ring theory, **ideals** and **factor rings** play a fundamental role in understanding the structure of rings and their algebraic properties. An **ideal** is a special subset of a ring that is closed under addition and multiplication by any element of the ring, allowing the construction of quotient structures. Given a ring R and an ideal I, the **factor ring** (or quotient ring) R/I is formed by partitioning R into cosets of I, where elements are grouped based on their equivalence modulo I. This new ring inherits properties from R but may have a simpler or more useful structure. Factor rings help in studying homomorphisms, constructing new rings, and understanding fundamental concepts like ring isomorphisms and kernel characterization in algebra.

12.2 *OBJECTIVES*

The main objectives of this unit are as follows:

- **Understand the Concept of Ideals:**

1. Define left, right, and two-sided ideals in a ring.
2. Identify and differentiate between principal, prime, and maximal ideals.
3. Understand the role of ideals in ring theory and their relationship with subrings.

- **Learn Properties of Ideals:**

1. Determine whether a given subset of a ring is an ideal.
2. Understand how ideals behave under addition and multiplication.
3. Explore the role of the zero ideal and the entire ring as trivial ideals.

- **Explore Factor (Quotient) Rings:**

1. Define the quotient ring R/I and understand its construction.
2. Understand the fundamental homomorphism theorem for rings.
3. Analyze how the properties of R/I depend on the nature of I (e.g., when R/I is a field or an integral domain).

12.3 *IDEALS*

A non-empty Subset S of a ring R is called a **left ideal** of R if:

(i) S is additive Subgroup of R.

(ii) $rs \in S \; \forall \, r \in R$ and $\forall \, s \in S$

A non-empty subset S of a ring R is called a **right ideal** of R if:

(i) S is additive subgroup of R.

(ii) $sr \in S \; \forall \, r \in R$ and $\forall \, s \in S$.

A non-empty subset of a ring R is called an **ideal** or two sides ideal if it is both **left ideal** and **right ideal**, *i.e.* if:

(i) S is additive Subgroup of R.

(ii) $sr \in S$ and $rs \in S \; \forall \, r \in R \;\; \forall \, s \in S$.

Example:

(i) The subring of even integers is an ideal of ring integers.

(ii) The set $\{mx : x \in Z\}$ is an ideal of the ring of integers. M being any fixed integer.

(iii) If R is a ring, then the set $\{x \in R : ax = 0\}$ is a **right ideal** of R. a being any fixed element of R.

(iv) If R is a ring, then the set $\{x \in R : xa = 0\}$ is a **left ideal** of R. a being any fixed element of R.

Note 1: If we have to prove that a non-empty subset S of a ring R is an ideal of R, then it is sufficient to prove

(i) $a \in S$, $b \in S \Rightarrow a - b \in S$

(ii) $sr \in S$ and $rs \in S \; \forall \, r \in R$ and $\forall \, s \in S$.

2: Every ring R always possesses two important ideal: One R itself and the other consisting of 0 only. These are respectively known as **unit ideal** and the **null ideal**.

Theorem 1: The intersection of any two left ideals/ right ideals of a ring is again a left ideal/right ideal of the ring.

Proof: We will consider I_1 and I_2 are two left ideals of a ring R. Then we have to prove that $I_1 \cap I_2$ is also an left ideal of the ring R.

As I_1 and I_2 are two left ideals of a ring R then obviously I_1 and I_2 are also the additive subgroup of R. Since we know that intersection of two subgroups is again a subgroup. Thus, we can say that $I_1 \cap I_2$ is also a subgroup of R with respect to the operation addition.

Now, we have only to prove that $I_1 \cap I_2$ is left ideal of *R*. For it, we have to show $\forall r \in R, s \in I_1 \cap I_2 \Rightarrow rs \in I_1 \cap I_2$.

Let $s \in I_1 \cap I_2 \Rightarrow s \in I_1$ and $s \in I_2$

Since I_1 is ideal of *R* then $\forall s \in I_1, r \in R \Rightarrow rs \in I_1$

Similarly, I_2 is ideal of *R* then $\forall s \in I_2, r \in R \Rightarrow rs \in I_2$

Now, $rs \in I_1$ and $rs \in I_2 \Rightarrow rs \in I_1 \cap I_2$

Hence, $I_1 \cap I_2$ is left ideal of *R*.

Similarly we can prove that if I_1 and I_2 are two right ideals of a ring *R* then $I_1 \cap I_2$ is also an right an ideal of *R*.

Theorem 2: The arbitrary intersection of any two left ideals/ right ideals of a ring is again a left ideals/ right ideals of the ring.

Proof: Let *R* be a ring and let $\{S_t : t \in T\}$ 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 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 any elements of *S*. Then

$a, b \in S \Rightarrow a, b \in S_t \ \forall t \in T$

$\Rightarrow a - b \in S_t \ \forall t \in T$

$\Rightarrow a - b \in \bigcap_{t \in T} S_t \Rightarrow a - b \in S$

Now let a be any element of *S* and *r* be any element of *R*.

We have $a \in S \Rightarrow a \in \bigcap_{t \in T} S_t \Rightarrow a \in S_t \ \forall t \in T$

$\Rightarrow ra \in S_t \ \forall t \in T$

$\Rightarrow ra \in \bigcap_{t \in T} S_t \Rightarrow ra \in S$

Thus, $a, b \in S \Rightarrow a - b \in S$ and $r \in R, a \in S \Rightarrow ra \in S$

$\therefore S$ is left ideal of *R*.

Similarly we can prove that arbitrary intersection of right ideals of a ring *R* is also an right an ideal of *R*.

Smallest left ideal containing a given subset

Definition: Let *M* be a non-empty subset of a ring *R*. Then a left ideal *I* of *R* is called the smallest left ideal of *R* containing *M*, if *I* contains *M* and if *I* is contained is every left ideal of *R* containing *M*.

The smallest left ideal of *R* containing *M* is called **left ideal generated by** *M* and will be denoted by (*M*).

It can be easily seen that the intersection of the family of left ideals containing *M* is the left ideal generated by *M*.

Note: A similar definition can be given for the right ideal generated by *M* as well as for the ideal generated by *M*. For this purpose simply replace the word 'left ideal' by 'right ideal'or by 'ideal'.

Theorem 3: The left ideal generated by the union $I_1 \cup I_2$ of two left ideals is the set $I_1 + I_2$ consisting of the elements of *R* obtained by adding any elements of I_1 to any elements of I_2.

Proof: Let $a_1 + a_2,\ b_1 + b_2 \in I_1 + I_2$.

Then $a_1, b_1 \in I_1$ and $a_2, b_2 \in I_2$.

Since I_1, I_2 are left ideals of *R*, therefore they are subgroups of the additive group of *R*. Therefore

$a_1, b_1 \in I_1 \Rightarrow a_1 - b_1 \in I_1$ and $a_2, b_2 \in I_2 \Rightarrow a_2 - b_2 \in I_2$.

Consequently, $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in I_1 + I_2$

Therefore, $I_1 + I_2$ is a subgroup of the additive group of *R*.

Now let $r \in R$ and $(a_1 + a_2) \in I_1 + I_2$. Then $a_1 \in I_1, a_2 \in I_2$. We have,

$r(a_1 + a_2) = ra_1 + ra_2 \in I_1 + I_2$

[$\because I_1$ is left ideal implies $ra_1 \in I_1$ and similarly $ra_2 \in I_2$]

$\because I_1 + I_2$ is a left ideal of *R*.

Since $0 \in I_2$, therefore $a_1 \in I_1$ can be written as $a_1 + 0$. Thus, $a_1 \in I_1 \Rightarrow a_1 \in I_1 + I_2$

$I_1 \subseteq I_1 + I_2$.

Similarly, $I_2 \subseteq I_1 + I_2$.

$\therefore I_1 \cup I_2 \subseteq I_1 + I_2$

Thus $I_1 + I_2$ is a left ideal containing $I_1 \cup I_2$. Also if any left ideal contains $I_1 \cup I_2$, then it must contain $I_1 + I_2$.

$\therefore I_1 + I_2$ is the smallest left ideal containing $I_1 \cup I_2$.

$\therefore I_1 + I_2 =$ The left ideal generated by containing $I_1 \cup I_2 = (I_1 \cup I_2)$.

Note: A similar result can be proved for right ideals as well as for ideals.

Example 1: The set *N* of all 2×2 matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ for a, b integers is a left ideal but not a right ideal in the ring *R* of all 2×2 matrices with the elements as integer. Here *N* is the subset of *R* consisting of those elements whose second column contains only zeros.

Solution: Let $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$, $B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$ be any two elements of N. Then,

$$A - B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in N$$

$\therefore N$ is a subgroup of *R* under addition.

Now let $U = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ be any element of *R* and $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ be any element of *N*.

Then $UA = \begin{bmatrix} w & x \\ y & z \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} wa + xb & 0 \\ ya + zb & 0 \end{bmatrix} \in N$

Therefore N is a left ideal of R. It is not a right ideal, since

$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in N$, $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \in R$

And the product $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$, which is not an element of *N*.

Example 2: If *U* is an ideal of a ring *R* with unity $1 \in U$ prove that $U = R$.

Solution: We have $U \subseteq R$ since *U* is an ideal of *R*. Let x be any element of R. Since U is an ideal of *R*, therefore

$1 \in U, x \in R \Rightarrow 1x \in U \Rightarrow x \in U$

$\therefore R \subseteq U$

$\therefore U = R$

Example 3: Prove that the subset *S* of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ with *a* and *b* integers, forms a subring of the ring R of all 2×2 matrices having elements as integers. Prove that further S is neither a right ideal nor a left 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 elements of *S*. Then

$A-B=\begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S$

Also, $AB=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}=\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S$

$\therefore S$ 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, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}=\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \notin S$. Therefore *S* is not a right ideal.

12.4 *IMPROPER AND PROPER IDEALS*

Let $(R, +, \cdot)$ be a ring. The ideal R and $\{0\}$ are called improper or trivial ideals of R. Any ideal other than these two ideals is called a proper (or non trivial) ideal of R.

12.5 *PRINCIPAL IDEAL*

A **left ideal** generated by single element a ∈R is also called **principal left ideal** of R. The set

$$\{ra + ma : r \in R, m \in Z\}$$

is a **principal left ideal** of R. a being fixed element of R.

If R is a ring with unity element e, and a ∈R, then Ra is **principal left ideal** of R.

A **right ideal** generated by single element a ∈R is also called **right principal ideal** of R. The set

$$\{ar + ma : r \in R, m \in Z\}$$

is a **principal right ideal** of R. a being fixed element of R.

If R is a ring with unity element e, then aR is defined as right ideal generated by an element a ∈R. aR is also defined as **principal right ideal** of R.

An ideal of a ring R is called **principal ideal** of R, if it is generated by single element of R. That is to say, the set

$$\{ra + as + ma : r, s \in R, m \in Z\}$$

is a principal ideal of R, generated by single element a∈ R. This set is also called **ideal** generated by an element a∈ R. The expression for principal ideal can be simplified if R is a ring with unity element e.

In this case

$$ra + as + ma = ra + as + m(ea). \quad \text{For } a = ea$$
$$= ra + as + r'a, \text{ where } r' = me \in R$$
$$= (r + r')a + as$$
$$= s'a + as, \text{ where } s' = r + r' \in R.$$

Hence a principal ideal of R is the set $\{s'a + as : s, s' \in R\}$ if R is a ring with unity element e.

More about principal ideal:

Definition: Any ideal S of a ring R will be called principal ideal if there exist an element $a \in S$ s.t. any ideal T of R that contain a also contains S *i.e.*, $S = (a)$.

Therefore, the principal ideal is an ideal generated by a single element in itself.

In a ring (R) if $1 \in R$, then the ideal generated by 1 is whole ring i.e., $(1) = R$, since each element of R can be expressed as $r1$. Ring itself is referred to be the unit ideal for this reason. The null ideal is the ideal produced by the zero element of R, or (0), which only contains the zero element. Every ring R has (0) as at least one of its primary ideals. Every ring with unity has two primary ideals at a minimum, namely (0) and (1).

Theorem 4: 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 have to prove that $a \in S$. Since R is ring with unit element 1, therefore $1a = a \in S$.

We must now demonstrate that S is an ideal of R. Therefore, we must first demonstrate that S is a subgroup of R under addition. Let the two element of S are u, v. 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 $r_1 - r_2 \in R$.

Since S is a subgroup of R under addition.

Now we have to prove that $x \in R, u \in S \Rightarrow xu \in S$ and $ux \in S$. But R is a commutating ring then,

$xu = ux$ and thus we have only to prove that $xu \in S$.

We have $xu = x(r_1 a) = (xr_1)a \in S$.

As we know $xr_1 \in R$

$\therefore S$ is an ideal of R and $a \in S$.

Now to prove that S is an ideal which is generated by the element a, We have only to show that if T is an ideal of R and $a \in T$, then $S \subseteq T$.

Let $ra \in S$ then $r \in R$. If T is an ideal of R s.t. $a \in T$ then $r \in R, a \in T \Rightarrow ra \in T$. Thus $S \subseteq T$.

Hence S is principal ideal of R s.t. $S = (a)$.

Example 4: To find the principal ideal in the ring (R) of integer generated by 5.

Solution: Since we know ring of integer (I) is a commutative ring with unity.

Since $(5) = \{5r \mid r \in I\}$

Thus, principal ideal of R generated by 5 is

$(5) = \{..., -10, -5, 0, 5, 10, ...\}$

and obviously, $(-5) = (5)$

12.6 *PRINCIPAL IDEAL RING*

A commutative ring with unity for which every ideal is a principal ideal is said to be a principal ideal ring.

12.7 *PRIME IDEAL*

Let R be a commutative ring. An ideal S of ring R is said to be a prime ideal of R if

$$ab \in S \Longrightarrow a \in \text{S or } b \in S.$$

If an ideal S of a ring R is generated by an element $a \in R$, then we write

$$S = (a).$$

Similarly if an ideal S of a ring R is generated by elements $a, b \in R$, then we write

$$S = (\{a, b\}).$$

Example 5: The ideal $S = \{3r : r \in Z\}$ is prime.

Solution: Let $S = \{3r : r \in Z\}$ is prime ideal of R generated by 3 and we also write $S = (3)$.

Here $ab \in S \Longrightarrow 3|ab$. Also 3 is prime

$\Longrightarrow 3|a$ and $3|b$

$\Longrightarrow a \in S$ or $b \in S$

$\Longrightarrow S$ is prime

12.8 *QUOTIENT RING/ FACTOR RING*

Let R be a ring and S be an ideal of R. Let R/S denote the family of cosets of S in R, i.e.,

$$\frac{R}{S} = \{S + a : a \in R\}.$$

Let $S + a, S + b$ be arbitrary elements of R/S. Define the operations of addition and multiplication on R/S as follows:

$$(S + a) + (S + b) = S + (a + b)$$
$$(S + a)(S + b) = S + ab.$$

Then R/S is a ring w.r.t. these operations. This ring $(R/S, +, \cdot)$ is called **quotient ring or factor ring**.

Theorem 5: If S is an ideal of a ring *R*, then the set

$R/S = \{S + a : a \in R\}$, i.e., the collection of all residue classes of *S* in *R*.

The composition in R/S is defined as follows:

Addition: $(S + a) + (S + b) = S + (a + b)$

Multiplication: $(S + a)(S + b) = S + ab.$

Prove that R/S forms a ring.

Proof: Since $S + (a + b)$ and $S + ab$ are also the residue classes of S in R, therefore we can say that R/S is closed with respect to addition and multiplication of residue classes. Initially, we have to prove that both addition and multiplication in R/S are well defined. For this we have 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 $a' + b' = (\alpha + a) + (\beta + b) = (a + b) + (\alpha + \beta)$.

$\therefore (a' + b') - (a + b) = \alpha + \beta \in S$

$\therefore S + (a' + b') = S + (a + b)$

$\Rightarrow (S + a') + (S + b') = (S + a) + (S + b)$

Thus addition in R/S is well defined.

Again $a' b' = (\alpha + a)(\beta + b) = \alpha\beta + \alpha b + a\beta + ab$

$= \alpha\beta + \alpha b + a\beta + ab$

$a'b' - ab = \alpha\beta + \alpha b + a\beta + ab \in S$ [Since S is an ideal therefore $\alpha, \beta \in S$ and $a, b \in R \Rightarrow a\beta \in S, \alpha\beta \in S, \alpha b \in S$ and finally $a\beta + \alpha\beta + \alpha b \in S$]

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: We have,

$(S + a) + [(S + b) + (S + c)] = (S + a) + [S + (b + c)]$

$S + [a + (b + c)] = S + [(a + b) + c] = [S + (a + b)] + (S + c)$

$= [(S + a) + (S + b)] + (S + c)$

Commutativity: We have,

$(S + a) + (S + b) = S + (a + b) = S + (b + a) = (S + b) + (S + a)$

Existence of 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 a additive identity.

Existence of inverse: Let $S + a \in R/S$, then

$S + (-a) \in R/S$, also we have

$[S + (-a)] + [S + a] = S[(-a) + a] = S + 0 = S$

$\therefore S + (-a)$ *OR* $S - a$ is the additive inverse of $S + a$.

Associativity of multiplication: We have

$[(S + a)(S + b)](S + c) = (S + ab)(S + c) = S + (ab)c$

$= S + a(bc) = (S + a)(S + bc) = (S + a)[(S + b)(S + c)]$.

Distributive of multiplication with respect to addition: We have

$(S + a)[(S + b) + (S + c)] = (S + a)[S + (b + c)] = S + a(b + c)$

$= S + (ab + ac) = (S + ab) + (S + ac)$

$= (S + a)(S + b) + (S + a)(S + c)$

In a similar way, we can prove that

$[(S + b) + (S + c)](S + a) = (S + b)(S + a) + (S + c)(S + a)$.

Hence we can say that R/S is a ring with respect to the composition addition and multiplication and the residue class $S+0$ or S is the zero element of this ring.

Example 6: If R/S is a ring of residue classes of *S* in *R*. Prove that

(i) If *R* is coomutative so also is R/S

(ii) If *R* has a unity element 1 so also has R/S, namely $S+1$

Solution (i): Suppose *R* is a commutative ring. Let $S+a, S+b$ be two elements in R/S. Then $a,b \in R$ and $ab=ba$

We have $(S+a)(S+b)=S+ab=S+ba=(S+b)(S+a)$

(ii): Suppose *R* is a ring with unit element 1. Then $S+1 \in R/S$. If $S+a$ is any element of R/S, then we have

$(S+1)(S+a)=S+(1a)=S+a$

And $(S+a)(S+1)=S+(a1)=S+a$

$\therefore S+1$ is the unit element of R/S.

Check your progress

Problem 1: Check that the $4Z$ is ideal of the ring of integers?

Problem 2: Check that the $7Z$ is prime ideal of the ring of integers?

Problem 3: Is $4Z$ is prime ideal of the ring of integers?

12.9 *SUMMARY*

This unit on **ideals and factor rings** explores the concept of **ideals**, which are special subsets of rings that are closed under addition and multiplication by ring elements. Ideals play a crucial role in constructing **quotient rings (factor rings)**, denoted as *R*/*I*, where *I* is an ideal of *R*. The chapter classifies ideals into **principal, prime, and maximal ideals**, with prime ideals ensuring that *R*/*I* is an **integral domain** and maximal ideals ensuring that *R*/*I* is a **field**. We will further discusses in next units the **First Isomorphism Theorem**, showing how ideals correspond to kernels of ring homomorphisms. Quotient rings simplify ring structures, leading to applications in **modular arithmetic, algebraic number theory, and cryptography**. This unit helps to understanding ideals and factor rings helps in analyzing ring properties and constructing new algebraic systems.

12.10 *GLOSSARY*

- Ideal.
- Improper and Proper ideal
- Principal ideal
- Principal ideal ring
- Prime ideal
- Quotient ring/ Factor ring

12.11 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

12.12 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

12.13 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. The set of all multiples of a fixed integer n forms an ideal in the ring of integers Z, and it is denoted by nZ.

2. Prove that an ideal I of a commutative ring R is called a maximal ideal if the only ideals containing I are I and R.

3. Prove that the quotient ring R/I is a field if and only if I is a maximal ideal of R.

4. Prove that an ideal I of R is called a prime ideal if whenever $ab \in I$ then either $a \in I$ or $b \in I$.

5. Prove that the factor ring R/I is an integral domain if and only if I is a prime ideal of R.

6. Prove that the sum of two ideals I and J in a ring R is also an ideal of R.

Short Answer Type Question:

1. Prove that intersection of two ideal of a ring is also an ideal of ring.

2. Define the ring and subring with example.

3. Define the ideal, prime ideal and principal ideal with example.

4. Define proper and improper ideal with example.

5. Let a and b be arbitrary elements of a ring R whose characteristic is two and $ab = ba$. Then prove that,

$$(a+b)^2 = a^2 + b^2 = (a-b)^2$$

Objective type question:

1. Which of the following is always an ideal in a ring R?

a) The set of all even integers in Z
b) The set of all prime numbers in Z
c) The set of all units in R
d) The set of all zero divisors in R

2. If I is an ideal of a ring R, what is the structure of the factor ring R/I?

a) Always a field
b) Always an integral domain
c) Always a ring
d) Always a group

3. For an ideal I of R, the factor ring R/I is a field if and only if:

a) I is a maximal ideal
b) I is a prime ideal
c) I contains all nilpotent elements
d) I is the zero ideal

4. Which of the following is a necessary and sufficient condition for a subset I of R to be an ideal?

a) I is closed under addition
b) I is closed under multiplication
c) I is closed under both addition and multiplication by elements of R
d) I contains the multiplicative identity of R

5. If R is a commutative ring with identity and P is a prime ideal of R, then R/P is always:

a) A ring with unity
b) An integral domain

c) A field
d) A division ring

6. Which of the following is NOT necessarily an ideal of a ring *R*?
a) The zero ideal {0}
b) The set of all nilpotent elements in *R*
c) The whole ring *R*
d) The set of all elements divisible by a fixed element in *R*

7. If I is a proper ideal of a commutative ring *R*, then *R*/*I* is a field if and only if *I* is:
a) A prime ideal
b) A maximal ideal
c) A principal ideal
d) A nil ideal

8. Which of the following is true for every ideal *I* of a ring *R*?
a) *I* is always a subring of *R*
b) *I* is always a subgroup of (*R*, +)
c) *I* always contains the multiplicative identity if *R* has one
d) *I* is always a field if *R* is a field

9. Let *R* be a commutative ring with unity. The quotient ring *R*/*I* is an integral domain if and only if *I* is:
a) A maximal ideal
b) A prime ideal
c) A principal ideal
d) A radical ideal

10. In the ring *Z*, the ideal 5*Z* is:
a) A prime ideal
b) A maximal ideal
c) Both prime and maximal
d) Neither prime nor maximal

11. If *R* is a commutative ring and *P* is a prime ideal, then which of the following is true for *R*/*P*?
a) It is always a field
b) It is always an integral domain
c) It is always a division ring
d) It is always a local ring

12. An ideal *I* in a ring *R* is said to be a maximal ideal if and only if:
a) *I* is the largest ideal in *R*
b) *I* is not contained in any other ideal
c) The only ideals containing *I* are *I* and *R*
d) *R*/*I* is an integral domain

13. If *R* is a commutative ring and *I* is a nil ideal, then every element in *I* is:
a) A unit
b) Nilpotent

c) Idempotent
d) Invertible

14. If *I* and *J* are ideals of a commutative ring *R*, then *I*+*J* is:
a) An ideal of *R*
b) A subring but not necessarily an ideal
c) A prime ideal
d) A maximal ideal

True and False questions:

1. Every ideal of a ring is a subring. **(T/F)**
2. Every subring of a ring is an ideal. **(T/F)**
3. The zero ideal **{0}** and the whole ring ***R*** are always ideals of ***R***. **(T/F)**
4. A maximal ideal is always a prime ideal. **(T/F)**
5. A prime ideal is always a maximal ideal. **(T/F)**
6. If ***I*** is an ideal of a ring ***R***, then the factor ring ***R/I*** is always a commutative ring. **(T/F)**
7. Every field has exactly two ideals: the zero ideal and the whole field. **(T/F)**
8. If ***I*** is an ideal of a ring ***R***, then ***R/I*** is always an integral domain. **(T/F)**
9. The set of all even integers forms an ideal in ***Z***. **(T/F)**
10. The sum of two ideals in a ring is always an ideal. **(T/F)**
11. If ***I*** is a maximal ideal of ***R***, then ***R/I*** is a field. **(T/F)**
12. If ***I*** is a prime ideal of ***R***, then ***R/I*** is a field. **(T/F)**
13. An ideal that contains a unit of the ring must be the entire ring. **(T/F)**
14. In a commutative ring ***R***, every prime ideal is also a maximal ideal. **(T/F)**

Fill in the blanks:

1. The set of all multiples of a fixed integer *n* forms an ideal in *Z*, denoted by …….
2. An ideal *I* of a commutative ring *R* is called a _____ if the only ideals containing *I* are *I* and *R*.
3. The factor ring *R*/*I* is a _____ if and only if *I* is a maximal ideal.
4. The ideal *I* of *R* is called a _____ ideal if whenever ab∈I, then either a∈I or b∈I.
5. The factor ring *R*/*I* is an _____ if and only if *I* is a prime ideal.
6. The sum of two ideals *I* and *J* in a ring *R* is always an _____ of *R*.
7. A ring *R* is a _____ if and only if it has exactly two ideals: {0} and *R*.
8. If *R* is a commutative ring with unity, then the quotient ring *R*/*I* is a field if and only if *I* is a _____ ideal.
9. The quotient ring Z/6Z has exactly _____ elements.
10. In any ring *R*, the set {0} is always an _____ of *R*.
11. If an ideal *I* contains a unit of the ring *R*, then *I* must be _____.
12. The set of all even integers forms an ideal in *Z*, and it is denoted by _____.
13. A two-sided ideal in a ring *R* is a subset that is closed under addition and closed under multiplication by _____.

14. If R is a commutative ring with identity and P is a prime ideal of R, then R/P is always an _____.

12.14 *ANSWERS*

Answer of self cheque question:

1. Yes **2.** Yes **3.** No

Answer of objective type question:

1:	a	**2:**	c	**3:**	a	**4:**	c
5:	b	**6:**	b	**7:**	b	**8:**	b
9:	b	**10:**	a	**11:**	b	**12:**	c
13:	b	**14:**	a				

Answer on True and False:

1.	False	**2:**	False	**3:**	True	**4:**	True
5:	False	**6:**	False	**7:**	True	**8:**	False
9:	True	**10:**	True	**11:**	True	**12:**	False
13:	True	**14:**	False				

Answer of fill in the blanks:

1.	nZ	**2.**	Maximal ideal	**3.**	Field
4.	prime	**5.**	Integral Domain	**6.**	Ideal
7.	Field	**8.**	Maximal	**9.**	6
10.	Ideal	**11.**	The whole ring of R	**12.**	$2Z$
13.	any element of R			**14.**	Integral domain

Unit-13: RING HOMOMORPHISM

CONTENT:

13.1 *INTRODUCTION*

A **ring homomorphism** is a fundamental concept in abstract algebra that describes a structure-preserving function between two rings. A function $f : R \to S$ is called a ring homomorphism if it satisfies two key properties: $f(a+b) = f(a) + f(b)$ and $f(a.b) = f(a).f(b)$ for all elements a, b in R. If the rings have a multiplicative identity, the homomorphism may also preserve unity, meaning $f(1_R) = 1_S$. The kernel of a ring homomorphism, defined as $\ker f = \{r \in R \mid f(r) = 0\}$, is always an ideal of R, which plays a crucial role in constructing quotient rings. Ring homomorphisms help in understanding the relationships between different algebraic structures, leading to key results like the First Isomorphism Theorem. They are essential in various areas of mathematics, including number theory, algebraic geometry, and functional analysis.

13.2 *OBJECTIVES*

After reading this unit learners will be able to

1. **Understand the Concept** – To define and explain what a **ring homomorphism** is and how it preserves ring operations (addition and multiplication).
2. **Explore Properties** – To study the key properties of ring homomorphisms, including the preservation of the additive identity (0) and, in some cases, the multiplicative identity (1).
3. **Kernel and Image** – To understand the **kernel** and **image** of a ring homomorphism and their roles in the structure of rings.
4. **Ideal and Subring Relations** – To learn that the kernel of a ring homomorphism is always an **ideal**, and the image is always a **subring** of the codomain.
5. **Types of Homomorphisms** – To differentiate between **injective, surjective, and bijective** ring homomorphisms and their significance in algebraic structures.
6. **Isomorphisms and Quotient Rings** – To explore the **First Isomorphism Theorem**, which connects homomorphisms to quotient rings and helps in classifying ring structures.
7. **Applications** – To apply ring homomorphism concepts in **abstract algebra, number theory, linear algebra**, and other mathematical disciplines.

13.3 *HOMOMORPHISM OF RINGS*

Definitions: (Homomorphism into) A mapping f from a ring R into a ring R' is said to be homomorphism of R into R' if,

(i) $f(a+b) = f(a) + f(b) \forall a, b \in R$

(ii) $f(ab) = f(a) f(b) \forall a, b \in R$

Homomorphism onto: A mapping f from a ring R onto a ring R' is said to be homomorphism of R onto R' if,

(i) $f(a+b) = f(a) + f(b) \forall a, b \in R$

(ii) $f(ab) = f(a) f(b) \forall a, b \in R$

Note: R' is said to be a homomorphic image of R.

Examples 1: Trivial Homomorphism: The function $f : S \to R$ given by $f(a) = 0$ for all $a \in R$ is always a ring homomorphism.

2. **Natural Inclusion**: If R is a subring of S, the inclusion map $f : R \to S$ defined by $f(a) = a$, is a ring homomorphism.
3. **Mod *n* Map**: The function $f : Z \to Z_n$ given by $f(a) = a \bmod n$ is a ring homomorphism.

Example 4: Consider the determinant function $f : M_2(R) \to R$ given by:

$$f(A) = \det(A)$$

Where, $M_2(R)$ is the ring of 2×2 real matrices.

This is a **multiplicative** ring homomorphism since:

$\det(AB) = \det(A).\det(B)$

but **not an additive** homomorphism because:

$\det(A + B) \neq \det(A) + \det(B)$

Therefore, this is not a full ring homomorphism, only a semigroup homomorphism.

Theorem 1: If f is a homomorphism of a ring R into a ring R', then

(i) $f(0) = 0'$, where 0 is the zero element of a ring R and $0'$ is the zero element of R'.

(ii) $f(-a) = -f(a) \forall\, a \in R$

Proof: (i) Let $a \in R$ then $f(a) \in R'$. We have

$f(a) + 0' = f(a) = f(a + 0) = f(a) + f(0)$ [$\because 0'$ is the additive identity of R']

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 $0' = f(0) = f[a + (-a)] = f(a) + f(-a)$

$\therefore f(-a)$ is the additive inverse of $f(a)$ in the ring R'. Thus $f(-a) = -f(a)$.

Theorem 2: Let ϕ be a homomrphic mapping of a ring R into a ring R'. Let S' be the homomorphic image of R into R'. Then S' is a subring of R'.

Proof: Since under the mapping ϕ, S' is the image of R in R' therefore,

$\phi(R) = S' \subseteq R'$.

Let a', b' be any two element of S'. Since $S' = \phi(R)$, therefore there exist element $a, b \in R$ such that $\phi(a) = a', \phi(b) = b'$.

We have $a' - b' = \phi(a) - \phi(b) = \phi(a - b)$ [Since ϕ is a homomorphism]

Now $a - b \in R$ is such that $a' - b' = \phi(a - b)$. Therefore,

$\Rightarrow a' - b' \in S'$

Further, $a'b' = \phi(a)\phi(b) = \phi(ab) \in S'$, Since $ab \in R$

Thus, $a', b' \in S' \Rightarrow a' - b' \in S'$ and $a'b' \in S'$

Hence by subring test, S' is subring of R'.

13.4 *KERNEL OF RINGS HOMOMORPHISM*

The **kernel** of a ring homomorphism is the set of elements in the domain that are mapped to the zero element in the codomain.

Definition: If f is a homomorphism of a ring R into a ring S, The **kernel** of *f*, denoted as *ker*(*f*), is defined as: $\ker(f) = \{a \in R \mid f(a) = 0_S\}$

Where 0_S is the additive identity (zero element) in *S*.

Example 5: Consider the ring homomorphism $f : Z \to Z_6$ given by:
$f(n) = n \bmod 6$

The kernel consists of all integers $n \in Z$ such that $f(n) = n \bmod 6$, meaning:

$Ker(f) = \{n \in Z \mid n \equiv 0 \bmod 6\} = 6Z$

which is the ideal generated by 6, written as (6).

Example 6: Consider the ring homomorphism from the ring of 2×2 matrices over *R*:

$f : M_2(R) \to R$ such that $f(A) = \det(A)$

The **kernel** consists of all 2×2 matrices with determinant zero:

$Ker(f) = \{A \in M_2(R) \mid \det(A) = 0\}$

This is the set of **singular matrices**, which **is not an ideal** (since it is not closed under matrix addition).

However, it is a **nontrivial subring** of $M_2(R)$.

Theorem 3: If *f* is a homomorphism of a ring R into a ring R' with kernel S, then S is an ideal of R.

Proof: Let f be a homomorphism of a ring *R* into a ring R'. Let $0, 0'$ be the zero elements of R, R' respectively. Let *S* be the kernel of f. Then $S = \{x \in R \mid f(x) = 0'\}$.

Since $f(0) = 0'$, therefore at least $0 \in S$. Thus *S* is not empty.

Let $a, b \in S$. Then $f(a) = 0', f(b) = 0'$

We have $f(a-b) = f[a + (-b)] = f(a) + f(-b)'$

$= f(a) - f(b) = 0' - 0'$ $[\therefore a - b \in S]$

If r be any element of R, then

$f(ar) = f(a) f(r) = 0' f(r) = 0'$

And $f(ra) = f(r) f(a) = f(r) 0' = 0'$

$\therefore ar \in S, ra \in S$.

Thus $a, b \in S, r \in R \Rightarrow (a-b) \in S, ar \in S, ra \in S$

$\therefore$ *S* is an ideal of *R*.

Theorem 4: The homomorphism ϕ of a ring R into a ring R' is an isomorphism of R into a R' if and only if $I(\phi) = (0)$, where $I(\phi)$ denotes the kernel of ϕ.

Proof: Let ϕ be a homomorphism of a ring R into a ring R'. Let $0, 0'$ be the zero elements of R, R' respectively. Let $S = I(\phi)$ be the kernel of ϕ. Then S is an ideal of R and

$S = \{a \in R \mid \phi(a) = 0'\}$

Suppose ϕ is an isomorphism of R into a ring R'. Then ϕ is one-one. Let $a \in S$, then

$\phi(a) = 0'$ [By definition of kernel]

$\Rightarrow \phi(a) = \phi(0)$ [$\because \phi(0) = 0'$]

$\Rightarrow a = 0$ [$\because \phi$ is one-one]

Thus $a \in S \Rightarrow a = 0$. In other word 0 is the only element of R which belong to S. Therefore $S = (0)$.

Conversely, suppose that $S = (0)$. Then to prove that ϕ is an isomorphism of R into R' *i.e.*, to prove that ϕ is one-one.

If $a, b \in R, \phi(a) = \phi(b)$

$\Rightarrow \phi(a) - \phi(b) = 0'$ [$\because \phi(a), \phi(b)$ are in the ring R']

$\Rightarrow \phi(a - b) = 0'$ [$\because \phi$ is a homomorphism]

$\Rightarrow a - b \in S$ [By definition of kernel]

$\Rightarrow a - b = 0$ [$\because S = (0)$]

$\Rightarrow a = b$

$\because \phi$ is one-one. Hence ϕ is an isomorphism of R into R'.

Theorem 5: Suppose R is a ring, S an ideal of R. Let f be a mapping from R to R/S defined by $f(a) = S + a \; \forall \; a \in R$. Then f is a homomorphism of R onto R/S.

Proof: Consider the mapping $f : R \to R/S$ such that,

$f(a) = S + a \; \forall \; a \in R$.

Let $S + x$ be any element to R/S. Then $x \in R$.

We have $f(x) = S + x$. Therefore the mapping f is onto R/S. Let $a, b \in R$. Then

$f(a+b) = S + (a+b) = (S + a) + (S + b) = f(a) + f(b)$

Also, $f(ab) = S + ab = (S + a)(S + b) = f(a) f(b)$.

$\therefore f$ is a homomorphism of R onto R/S.

Hence, we can say that every quotient ring is a homomorphic image of the rings.

Example 7: Show that every homomorphic image of a commutative ring is commutative.

Solution: Let R be a commutative ring. Let f be a homomorphic mapping of R onto a ring R'. Then R' is a homomorphic image of R.

Let a', b' be any two elements of R'. Then $f(a) = a'$, $f(b) = b'$ for some $a, b \in R$ because f is onto R'. We have

$a'b' = f(a) f(b) = f(ab) = f(ba) = f(b) f(a) = b'a'$

$\therefore R'$ is a commutative ring.

Example 8: If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R' prove that $\phi(1)$ is the unit element of R'.

Solution: Since ϕ is a homomorphism of R onto R', therefore R' is a homomorphism image of R. If 1 is the unity element of R, then $\phi(1) \in R'$. Let a' be any element of R'. Then $a' = \phi(a)$ for some $a \in R$ since ϕ is onto R'. We have,

$\phi(1)a' = \phi(1)\phi(a) = \phi(1a) = \phi(a) = a'$

And $a'\phi(1) = \phi(a)\phi(1) = \phi(a1) = \phi(a) = a'$

$\therefore \phi(1)$ is the unity element of R'

Example 9: If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that kernel of ϕ *i.e.*, $I(\phi) \neq R$, then prove that $\phi(1)$ is the unit element of R'.

Solution: ϕ is a homomorphism of a ring R into an integral domain R'. Then kernel of ϕ,

$I(\phi) = \{x : x \in R \text{ and } \phi(x) = 0 \in R'\}$.

Since $I(\phi) \neq R$, therefore there exist an element $a \in R$ such that $\phi(a) \neq 0 \in R'$.

We have $\phi(1)\phi(a) = \phi(1a) = \phi(a)$

Now let b' be any element of R'. We have

$\phi(a)b' = \phi(a)b'$

$\Rightarrow \phi(1)\phi(a)b' = \phi(a)b'$ $[\because \phi(1)\phi(a) = \phi(a)]$

$\Rightarrow \phi(a)[\phi(1)b'] = \phi(a)b'$ $[\because \phi(1), \phi(a) \in R'$ which being an integral domain, is a commutative ring]

$\Rightarrow \phi(a)[\phi(1)b'] - \phi(a)b' = 0$

$\Rightarrow \phi(a)[\phi(1)b' - b'] = 0$

$\Rightarrow \phi(1)b' - b' = 0$ $[\because \phi(a) \neq 0$ and R' is without zero divisor]

$\Rightarrow \phi(1)b' = b' = b'\phi(1)$ $[\because R'$ is commutative ring]

Thus $\phi(1)b' = b' = b'\phi(1) \forall b' \in R'$.

Thus $\phi(1)$ is the unit element of R'.

13.5 *IMAGE OF RINGS HOMOMORPHISM*

The **image** of a ring homomorphism $f : R \to S$ is the set of all elements in S that have a preimage in R. Mathematically, it is defined as:

$\text{Im}(f) = \{f(r) \mid r \in R\}$

Example 10: Consider the ring homomorphism $f : Z \to Z/6Z$ given by:
$f(n) = n \bmod 6$

So, the image of *f* is {0, 1, 2, 3, 4, 5}, which also forms a subring of $Z/6Z$.

Theorem 6: Let $f : R \to S$ be a ring homomorphism. Then, the image $\text{Im}(f) = \{f(r) \mid r \in R\}$ is a **subring** of *S*.

Proof: To show $\text{Im}(f)$ is a subring, we need to verify closure under addition, multiplication, and the presence of 0_S.

Since *f* is a homomorphism, for any $a, b \in R$ then,

(i) $f(a) + f(b) = f(a+b) \in \text{Im}(f)$ [By the property of homomorphism]

(ii) $f(a).f(b) = f(ab) \in \text{Im}(f)$ [By the property of homomorphism]

(iii) $f(0_R) = f(0_S) \in \text{Im}(f)$
Thus, Im(*f*) is a subring of *S*.

Example 10: Let $f : R \to S$ be a ring homomorphism. The image $\text{Im}(f)$ is not necessarily an ideal of *S*, unless *S* satisfies additional conditions.

Solution: Consider the inclusion map $Z \to Q$, where $f(n) = n$. The image of *f* is *Z*, which is a subring of *Q*, but not an ideal since $\frac{1}{2}.1 \notin Z$.

Theorem 7: (Fundamental theorem on homomorphism of rings) Every homomorphic image of a ring *R* is isomorphic to some residue class ring (quotient ring) thereof.

Proof: Let R' be the homomorphic image of a ring R and f be the corresponding homomorphism. Then f is a homomorphism of R onto R'. Let *S* be the kernel of this homomorphism. Then *S* is an ideal of *R*. Therefore R/S is a ring residue classes of *R* relative to *S*. We shall prove that $R/S \cong R'$.

If $a \in R$, then $S + a \in R/S$ and $f(a) \in R'$. Consider the mapping $\phi : R/S \to R'$ such that

$\phi(S + a) = f(a) \forall a \in R$.

First we shall show that the mapping ϕ is well defined *i.e.*, if $a, b \in R$ and $S + a = S + b,$ then

$\phi(S + a) = \phi(S + b)$.

We have $S+a=S+b$

$\Rightarrow a-b\in S$

$\Rightarrow f(a-b)=0'$

$\Rightarrow f[a+(-b)=0' \Rightarrow f(a)+f(-b)=0' \Rightarrow f(a)-f(b)=0'$

$\Rightarrow f(a)=f(b)\Rightarrow \phi(S+a)=\phi(S+b)$

$\therefore \phi$ is well defined.

ϕ **is one-one:** We have $\phi(S+a)=\phi(S+b)$

$\Rightarrow f(a)=f(b)\Rightarrow f(a)-f(b)=0'$

$\Rightarrow f(a)+f(-b)=0' \Rightarrow f(a-b)=0'$

$\Rightarrow a-b\in S$ [$\because S$ is kernel of f]

$\Rightarrow S+a=S+b$

$\therefore \phi$ is one-one.

ϕ **is onto** R'**:** Let y be any element of R'. Then $y=f(a)$ for some $a\in R$ because *f* is onto R'. Now $S+a\in R/S$ and we have $\phi(S+a)=f(a)=y$. Therefore ϕ is onto R'.

Finally we have

$\phi[(S+a)+(S+b)]=\phi[S+(a+b)]=f(a+b)=f(a)+f(b)$

$=\phi(S+a)+\phi(S+b)$

Also, $\phi[(S+a)+\phi(S+b)]=\phi(S+ab)=f(ab)=f(a)f(b)=[\phi(S+a)][\phi(S+b)]$

$\therefore \phi$ is an isomorphism of R/S onto R'

Hence, we can say that $R/S\cong R'$.

Corollary 1: If $f:R\to S$ is a ring homomorphism. Then $R/\ker(f)\cong \mathrm{Im}(f)$

Where $\ker(f)=\{r\in R\mid f(r)=0_S\}$ is the kernel of *f*.

Proof: Define the map:
$\phi : R \to \text{Im}(f), \phi(r) = f(r)$

Step 1: ϕ is a Surjective Homomorphism

- Since every element of $\text{Im}(f)$ is of the form $f(r)$, it follows that ϕ is **surjective**.
- Since *f* is a ring homomorphism, ϕ\phiϕ is also a ring homomorphism.

Step 2: Kernel of ϕ is $\ker(f)$

By definition, $\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\} = \{r \in R \mid f(r) = 0_S\} = \ker(f)$

Thus, $\ker(\phi) = \ker(f)$

Step 3: Use the First Isomorphism Theorem

The First Isomorphism Theorem for rings states that:

$R / \ker(\phi) \cong \text{Im}(\phi)$

Since $\ker(\phi) = \ker(f)$ and $\text{Im}(\phi) = \text{Im}(f)$, we get:

$R / \ker(f) \cong \text{Im}(f)$

Corollary 2: If $f : R \to S$ is a surjective ring homomorphism, then $\text{Im}(f) = S$, and f is an isomorphism if and only if *f* is also injective**.**

Proof:

- Since *f* is surjective, every element of *S* is in the image of *f*, so $\text{Im}(f) = S$.
- If f is also injective, then $\ker(f) = \{0_R\}$, meaning $R / \ker(f) = R$
- By the First Isomorphism Theorem,

  $R / \ker(f) \cong \text{Im}(f) = S$

- Since $\ker(f)$ is trivial, we get $R \cong S$, meaning *f* is an **isomorphism**.

Thus, *f* is an isomorphism if and only if it is both surjective and injective.

13.6 *ISOMORPHISM OF RINGS*

Definition: Any ring R is said to be isomorphic to other ring R' if there exists a one-one and onto mapping f from R to R' such that

(*i*) $f(a+b) = f(a) + f(b)$

(*ii*) $f(ab) = f(a)f(b) \forall a, b \in R$.

Also such a mapping f is said to be an isomorphism of R onto R'. Symbolically it is denoted as $R \cong R'$, also R is said to be isomorphic image of R'.

Note: The compositions in the two rings have been represented by the identical symbols in the aforementioned definition of ring isomorphism. The constituent parts of any composition are revealed to us by the elements. For example, $a, b \in R$. When we write $a+b, ab$ then the respective compositions are addition and multiplication of R. Again $f(a), f(b) \in R'$. When we write $f(a) + f(b), f(a)f(b)$ then the respective compositions are addition and multiplication of R'

Relation of isomorphism in the set of all rings.

We can demonstrate that the relation of isomorphism in the set of all rings is an equivalence relation, as we have done in groups. In order to ensure that rings of the same class are all isomorphic to one another and rings of other classes are not, the set of all rings will be divided into disjoint equivalence classes. One can say that any two rings in the same equivalence class are abstractly similar.

Properties of isomorphism of rings:

Theorem 8: If f is an isomorphism of a ring R onto a ring R', then

(*i*) The image of $0 \in R$ is $0 \in R'$ *i.e.*, the additive identity element of ring R map into additive identity of the ring R'.

(*ii*) The negative of the image of an element of R is that element's image of its negative i.e., $f(-a) = -f(a) \forall a \in R$.

(*iii*) If R is the commutative ring, then R' is also a commutative a commutative ring.

(*iv*) If R is without zero divisors, then R' is also without zero divisors.

(*v*) If R is with unit element, then R' is also with unit element.

(*vi*) If R is field, then R' is also a field.

(*vii*) If R is skew field, then R' is also a skew field.

Proof (*i*): Let $a \in R$. Then $f(a) \in R'$. Let $0'$ denote the zero element of R'. To prove that $f(0) = 0'$.

We have $f(a)+0' = f(a) = f(a+0) = f(a)+f(0)$. By cancellation law for addition in R', we get from $f(a)+0' = f(a)+f(0)$, the result that $0' = f(0)$.

(*ii*) We have $f(a)+f(-a) = f[a+(-a)] = f(0) = 0'$

$\therefore f(-a)$ is the additive inverse inverse of $f(a)$ in R'. Thus $f(a) = -f(-a)$

(*iii*) Let $f(a)$ and $f(b)$ be any two elements of R'. Then $a, b \in R$

We have $f(a)f(b) = f(ab) = f(ba)$ [R is commutative $\Rightarrow ab = ba$]

$= f(b)f(a)$.

$\therefore R'$ is also commutative.

(*iv*) We have $f(0) = 0'$. Also f is one-one. Therefore 0 is the only element of R whose f-image is $0'$.

(*v*) Let 1 be the unit element of R. Then $f(1) \in R'$. If $f(a)$ is any element of R', we have

$f(1)f(a) = f(1a) = f(a)$ and $f(a)f(1) = f(a1) = f(a)$.

$\therefore f(1)$ is the unit element of R'.

(*vi*) R is commutative with unity if R is a field, and each non-zero element of R will have a multiplicative inverse. Now that this has been shown in (iii) and (v), R' will be commutative and possess the unit element *i.e.*, $f(1)$.

Let $f(a)$ be any non-zero element of R'. Then

$f(a) \neq 0' \Rightarrow a \neq 0 \Rightarrow a^{-1}$ exists.

Now $f(a^{-1}) \in R'$ and we have

$f(a^{-1})f(a) = f(a^{-1}a) = f(1)$ and $f(a)f(a^{-1}) = f(aa^{-1}) = f(1)$.

$\therefore f(a^{-1})$ is the multiplicative inverse of $f(a)$.

Hence R' is a field.

(*vii*) As shown in (v) R' will be with unit element i.e., $f(1)$ as shown in (vi) each non-zero element of R' will be inversible. Therefore R' is a skew-field.

Imbedding of a ring: A ring R is said to be imbedded in a ring R' if there is a subring S' of R' s.t. R is isomorphic to S'.

Any ring R is imbedded to other ring R' if there exists a one-one and onto mapping f from R to R' such that,

$f(a+b)=f(a)+f(b), f(ab)=f(a)f(b) \forall a,b \in R$.

Theorem 8: Any ring R without a unity element may be imbedded in a ring that contains a unity element.

Proof: Let R be any ring without unity element. Let Z is the ring of integers and $R' = R \times Z = \{(a,m) : a \in R, m \in Z\}$.

When appropriate binary operations have been specified in $R \times Z$, then it becomes a ring with a unity element containing a subring, isomorphic to R.

If (a,m) and (b,n) are any two elements of $R \times Z$, then we define addition in $R \times Z$ by the equation

$$(a,m)+(b,n)=(a+b,m+n) \quad \ldots(1)$$

And multiplication in $R \times Z$ by the equation

$$(a,m)(b,n)=(ab+na+mb,mn) \quad \ldots(2)$$

Since $a+b \in R$ and $m+n \in Z$, therefore $(a+b,m+n) \in R \times Z$. Thus $R \times Z$ is closed w. r. to addition. Further, $ab, na, mb \in R \Rightarrow ab+na+mb \in R$. Also $mn \in Z$. Therefore $(ab+na+mb,mn) \in R \times Z$ and $R \times Z$ is closed w. r. to. multiplication.

Now let $(a,m),(b,n),(c,p)$ be any element of $R \times Z$. Then we observe:

Associativity in addition: We have

$$[(a,m)+(b,n)]+(c,p)=(a+b,m+n)+(c,p)$$

$$=([a+b]+c,[m+n]+p)=(a+[b+c],m+[n+p])$$

$$=(a,m)+(b+c,n+p)=(a,m)+[(b,n)+(c,p)]$$

Commutativity in addition: We have

$$(a,m)+(b,n)=(a+b,m+n)$$

$$=(b+a,n+m) \quad [\because \text{Commutativity holds in addition}]$$

$$=(b,n)+(a,m).$$

Existence of identity: We have $(0,0) \in R \times Z$. Here the first 0 is the zero element of R and the second 0 is the zero integer.

Since, $(0,0)+(a,m)=(0+a,0+m)=(a,m)$

$\therefore (0,0)$ is the additive identity.

Existence of inverse: If $(a,m) \in R \times Z$, then

$(-a,-m) \in R \times Z$ and we have

$(-a,-m)+(a,m)=(-a+a,-m+m)=(0,0)$.

$\therefore (-a,-m)$ is additive inverse of (a,m)

Associativity of multiplication: We have

$[(a,m)(b,n)](c,p)=(ab+na+mb,mn)(c,p)$

$=((ab+na+mb)c+p(ab+na+mb)+(mn)c,(mn)p)$

$=(abc+n(ac)+m(bc)+p(ab)+(pn)a+(pm)b+(mr)c,(mn)p)$

Also $(a,m)[(b,n)(c,p)]=(a,m)(bc+pb+nc,np)$

$=(a(bc+pb+nc)+(np)a+m(bc+pb+nc),m(np))$

$=(abc+a(pb)+a(nc)+(np)a+m(bc)+m(pb)+m(nc),(mn)p)$

$=(abc+a(pb)+a(nc)+(np)a+m(bc)+m(pb)+m(nc),(mn)p)$

$=(abc+p(ab)+n(ac)+(np)a+m(bc)+(mp)b+(mn)c,(mn)p).$

We see that, $(a,m)[(b,n)](c,p)=(a,m)[(b,n)(c,p)]$

Distributive law: We have

$(a,m)[(b,n)+(c,p)]=(a,m)(b+c,n+p)$

$=(a(b+c)+(n+p)a+m(b+c),m(n+p))$

$=(ab+ac+na+pa+mb+mc,mn+mp)$

$=(a,m)(b,n)+(a,m)(c,p)$

In a similar manner, we may demonstrate that the other distributive law is equally valid.

In light of the operations described on it, $R \times Z$ is a ring.

Existence of identity: We have

$(0,1) \in R \times Z$. If $(a,m) \in R \times Z$, then

$(0,1)(a,m)=(0a+m0+1a,1m)=(0+0+a,m)=(a,m)$

Also $(a,m)(0,1)=(a0+1a+m0,m1)=(0+a+0,m)=(a,m)$.

$\therefore (0,1)$ is the multiplicative identity. So, $R \times Z$ is a ring with unity element (0, 1).

Now consider the subset $S' = R \times \{0\}$ of $R \times Z$ which consists of all pairs of the form $(a,0)$.

We shall show that $R \times \{0\}$ is a subring of $R \times Z$. Let $(a,0),(b,0)$ be any two elements of $R \times \{0\}$.

Then $(a,0)-(b,0)=(a,0)+(-b,-0)=(a-b,0) \in R \times \{0\}$.

Also, $(a,0)(b,0) = (ab + 0a + 0b, 00) = (ab + 0 + 0, 0) = (ab, 0) \in R \times \{0\}$.

$\therefore R \times \{0\}$ is a subring of $R \times Z$.

Finally we have to show that $R \cong R \times \{0\}$. Let ϕ be a mapping from R to $R \times \{0\}$ defined as $\phi(a) = (a, 0) \forall a \in R$.

ϕ **is one-one:** For it, let $\phi(a) = \phi(b) \Rightarrow (a,0) = (b,0) \Rightarrow a = b \Rightarrow \phi$ is one-one.

ϕ **is onto:** Let $(a,0) \in R \times \{0\}$. Then $a \in R$ and we have $\phi(a) = (a,0)$. Therefore ϕ is onto.

ϕ **preserves addition and multiplication:** If $a, b \in R$, then

$\phi(a+b) = (a+b, 0) = (a,0) + (b,0) = \phi(a)\phi(b)$.

Hence ϕ preserve the composition. *i.e.*, $R \cong R \times \{0\}$.

Check your progress

Problem 1: If $f : R \to S$ is a ring homomorphism, what can you say about $f(0)$?

Problem 2: Let $f : Z \to Z_6$ be defined by $f(n) = n \bmod 6$ then find $\ker f$?

Problem 3: Let $f : Z \to Z_6$ be defined by $f(n) = n \bmod 6$ then find $\text{Im } f$?

13.7 *SUMMARY*

The **Ring Homomorphism** chapter explores the structure-preserving functions between rings, ensuring that addition and multiplication operations remain intact. A function $f : R \to S$ is a ring homomorphism if it satisfies $f(a+b) = f(a) + f(b)$ and $f(a.b) = f(a).f(b)$ for all elements a, b in *R*. Key concepts include the **kernel** (an ideal of *R*) and the **image** (a subring of *S*), which help analyze ring structures. The chapter also covers different types of homomorphisms, such as **injective, surjective, and isomorphic maps**, and introduces the **First Isomorphism Theorem**, which connects homomorphisms to quotient rings. Understanding ring homomorphisms is essential in abstract algebra, as they aid in classifying rings, constructing new algebraic systems, and finding applications in number theory and algebraic geometry.

13.8 *GLOSSARY*

- Homomorphism of Ring.
- Kernel of ring homomorphism
- Image of ring homomorphism

- Isomorphism of rings

13.9 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

13.10 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra,* Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

13.11 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Define a ring homomorphism. State and prove that the kernel of a ring homomorphism is an ideal of the domain.

2. Explain the properties of a ring homomorphism. How does a ring homomorphism preserve the structure of a ring? Provide examples.

3. What is the First Isomorphism Theorem for rings? State and prove the theorem with a suitable example.

4. Differentiate between injective, surjective, and bijective ring homomorphisms. Give an example of each and explain their significance in algebra.

5. Let $f : R \to S$ be a ring homomorphism. Show that the image of f is always a subring of S. Explain why it may not necessarily be an ideal.

6. Discuss the role of ring homomorphisms in constructing quotient rings. How does the kernel of a ring homomorphism determine the quotient structure? Provide an example.

7. Prove that the composition of two ring homomorphisms is also a ring homomorphism. Give an example to illustrate your proof.

8. Consider the ring homomorphism $f : Z \to Z_n$ given by $f(x) = x \bmod n$. Determine the kernel and image of *f*, and discuss its implications in modular arithmetic.

9. Explain how ring homomorphisms are used in field theory. Can a nonzero ring homomorphism from a field to a ring ever have a nontrivial kernel? Justify your answer

Short Answer Type Question:

1. Define a ring homomorphism.
2. What are the two main properties that a ring homomorphism must satisfy?
3. What is the kernel of a ring homomorphism?
4. What is the image of a ring homomorphism?
5. What is an injective ring homomorphism?
6. What is a surjective ring homomorphism?
7. When is a ring homomorphism called an isomorphism?
8. State the First Isomorphism Theorem for rings.
9. Give an example of a ring homomorphism.
10. If $f : R \to S$ is a ring homomorphism, what can you say about $f(0)$?
11. Is the kernel of a ring homomorphism always an ideal? Why?
12. Is the image of a ring homomorphism always an ideal? Explain.
13. What is the trivial ring homomorphism?
14. Give an example of a non-trivial ring homomorphism.

Objective type question:

1. Which of the following is true for a ring homomorphism $f : R \to S$?

a) $f(0_R) = 0_S$
b) $f(1_R) = 1_S$ always holds
c) f is always injective
d) f is always surjective

2. Let $f : R \to S$ be a ring homomorphism. What is the kernel of *f*?

a) $\{x \in R \mid f(x) = 0_S\}$
b) $\{x \in R \mid f(x) = 1_S\}$

c) $\{x \in R \mid f(x) = x\}$

d) $\{x \in R \mid f(x) = -x\}$

3. If $f : Z \to Z/6Z$ is the natural ring homomorphism given by $f(n) = n \bmod 6$, what is $\ker(f)$?

a) $6Z$

b) Z

c) $\{0,1,2,3,4,5\}$

d) $\{0\}$

4. A ring homomorphism $f : R \to S$ is called an isomorphism if:

a) It is injective

b) It is surjective

c) It is both injective and surjective

d) It is neither injective nor surjective

5. The image of a ring homomorphism $f : R \to S$ is always:

a) A subring of S

b) An ideal of S

c) A subfield of S

d) A subset but not necessarily a subring of S

6. A function $f : R \to S$ is called a ring homomorphism if for all $a, b \in R$, which of the following holds?

a) $f(a+b) = f(a) + f(b)$

b) $f(a.b) = f(a).f(b)$

c) $f(1_R) = 1_S$ (if R, S are rings with identity)

d) All of the above

7. If $f : R \to S$ is a ring homomorphism, then the kernel of f, $Ker\ f$, is:

a) A subring of R

b) An ideal of R

c) A subgroup of R^*

d) None of the above

8. The image of a ring homomorphism $f : R \to S$ is always:

a) A subring of S

b) An ideal of S

c) A normal subgroup of S^*
d) None of the above

9. The trivial ring homomorphism is defined as:
a) $f(x) = x$ for all $x \in R$
b) $f(x) = 0$ for all $x \in R$
c) $f(x) = 1$ for all $x \in R$
d) None of the above

10. A ring homomorphism is said to be injective if:
a) $\ker f = R$
b) $\ker f = \{0\}$
c) $f(0) = 0$
d) None of the above

11. If *R* and *S* are commutative rings with unity and $f : R \to S$ is a ring homomorphism, then $f(1)$ must be:
a) 0
b) 1
c) Either 0 or 1
d) None of the above

12. If $f : Z \to R$ is a ring homomorphism, then $f(n)$ is given by:
a) $f(n) = n.f(1)$
b) $f(n) = f(1)^n$
c) $f(n) = n^2.f(1)$
d) $f(n) = n + f(1)$

13. The fundamental theorem of ring homomorphism states that if $f : R \to S$ is a

surjective ring homomorphism with kernel *K*, then:
a) $S \cong R/K$
b) R/K is a subring of *S*
c) *K* is a maximal ideal
d) R/K is a prime ideal

14. A ring homomorphism between two integral domains is always:
a) Injective
b) Surjective
c) A monomorphism
d) None of the above

15. The identity map $id : R \to R$ defined by $id(x) = x$ is:

a) A ring homomorphism
b) An isomorphism
c) Both (a) and (b)
d) None of the above

True (T) and False (F) questions:

1. Every ring homomorphism preserves both addition and multiplication.
2. The kernel of a ring homomorphism is always a subring of the domain.
3. If a ring homomorphism is injective, then its kernel contains only the zero element.
4. A ring homomorphism always maps the identity of the domain to the identity of the codomain.
5. The composition of two ring homomorphisms is always a ring homomorphism.
6. A ring homomorphism from a field to a ring is always injective.
7. If $f : R \to S$ is a ring homomorphism, then the image of *f* is always an ideal of *S*.
8. The identity map on a ring *R* is always a ring homomorphism.
9. Every surjective ring homomorphism is also injective.
10. If *R* and *S* are rings, and $f : R \to S$ is a homomorphism, then $f(0)$ must be 0.

Fill in the blanks:

1. A function $f : R \to S$ is called a ring homomorphism if it preserves both _____ and _____ operations.
2. The kernel of a ring homomorphism $f : R \to S$, denoted as $\ker f$, is always an _____ of *R*.
3. A ring homomorphism is said to be injective if and only if its kernel contains only the element _____.
4. The image of a ring homomorphism is always a _____ of the codomain ring.
5. If R is a field and $f : R \to S$ is a ring homomorphism, then *f* is always _____.
6. The trivial ring homomorphism is the map $f(x) =$ _____ for all $x \in R$.
7. If $f : Z \to R$ is a ring homomorphism, then $f(n) =$ _____
8. The First Isomorphism Theorem states that if $f : R \to S$ is a surjective ring homomorphism, then $S \cong$ _____.
9. The identity function $id : R \to R$, given by $id(x) = x$, is always a _____ and _____ ring homomorphism.
10. If $f : R \to S$ is a ring homomorphism, then $f(0)$ must be _____.

13.12 *ANSWERS*

Answer of self cheque question:

1. A ring homomorphism always maps the **additive identity** (0) of *R* to the **additive identity** (0) of *S*, i.e., $f(0) = 0$

2. $6Z$? **3.** $\text{Im } f = \{0,1,2,3,4,5\}$

Answer of objective type question:

1.	a)	**2.**	a)	**3.**	a)	**4.**	c)
5.	a)	**6.**	d)	**7.**	b)	**8.**	a)
9.	b)	**10.**	b)	**11.**	c)	**12.**	a)
13.	a)	**14.**	a)	**15.**	c)		

Answer on True and False:

1.	T	**2.**	F	**3.**	T	**4.**	F
5.	T	**6.**	T	**7.**	F	**8.**	T
9.	F	**10.**	T				

Answer of fill in the blanks:

1.	Addition, Multiplication	**2.**	Ideal
3.	0 or the additive identity	**4.**	Subring
5.	Injective	**6.**	0
7.	*n.f*(1)	**8.**	(R / Ker f)
9.	Bijective, Isomorphic)	**10.**	0 or the additive identity of *S*

Unit-14: FIELD

CONTENT:

14.1 *INTRODUCTION*

Field theory is a fundamental area of abstract algebra that explores the properties and structures of **fields**, which are algebraic systems where addition, subtraction, multiplication, and division (except by zero) are well-defined and obey specific axioms. Fields provide a natural framework for studying polynomial equations, arithmetic in number systems, and algebraic extensions. Classical examples include the rational numbers (Q), real numbers (R), complex numbers (C), and finite fields used in cryptography and coding theory. One of the most significant developments in field theory is **Galois theory**, which establishes a deep connection between field extensions and group theory, helping to determine the solvability of polynomial equations by radicals. Field theory plays a crucial role in many areas of mathematics, including algebraic geometry, number theory, and theoretical physics.

The idea of a field extension expresses the relationship between two fields. The goal of the Galois theory, which Évariste Galois founded in the 1830s, is to comprehend the symmetries of field extensions. This theory demonstrates, among other things, that it is

impossible to square a circle and trisect an angle with a compass and straightedge. Additionally, it demonstrates that quintic equations are typically algebraically intractable.

In many areas of mathematics, fields are fundamental concepts. This comprises many mathematical analysis disciplines that are based on fields with extra structure. Analysis's fundamental theorems rely on the real numbers' structural characteristics. What's more, any field may be utilised as the scalars for a vector space, which is the usual generic setting for linear algebra. In-depth research is done on number fields, the siblings of the subject of rational numbers. Geometric object attributes may be described with the use of function fields.

14.2 *OBJECTIVES*

The main objectives of the **Field Theory** chapter at the entry level are:

1. **Understanding the Concept of Fields** – Introduce the definition of a field, its axioms, and fundamental properties.
2. **Recognizing Examples of Fields** – Explore common examples like *Q* (rational numbers), *R* (real numbers), *C* (complex numbers), and finite fields.
3. **Exploring Field Operations** – Study addition, multiplication, and the existence of inverses in fields.
4. **Introduction to Finite Fields** – Understand the construction and properties of fields with a finite number of elements

14.3 *FIELD*

Definition: A ring (R) with at least two elements is called a field (F) if it satisfies following conditions,

(*i*) It should be commutative

(*ii*) It has unity

(*iii*) Each non-zero element possess multiplicative inverse.

For example, ring of rational numbers $(Q,+,.)$ is a field because it satisfies aforementioned following conditions. Similarly, rings of real numbers $(R,+,.)$ and complex numbers $(C,+,.)$ are also common example of fields.

$(\{0,1,2,3,4\},+_5,\times_5)$ is an example of finite fields

If $a,0\neq b$ are elements of a finite field F, then we shall often write

$ab^{-1}=\frac{a}{b}=b^{-1}a$. In a field F, we have

$$\frac{a}{b}+\frac{c}{d}=(ab^{-1})+(cd^{-1})=(bd^{-1})(bd)[(ab^{-1})+(cd^{-1})]$$

$$=(bd^{-1})[(bd)(ab^{-1})+(bd^{-1})(bd)(cd^{-1})]=(bd^{-1})(ad+bc)=\frac{ad+bc}{bd}$$

[Because in the field (F) multiplication is commutative]

Also $\frac{a}{b}\frac{c}{d}=(ab^{-1})(cd^{-1})=(ac)(b^{-1}d^{-1})=(ac)(bd)^{-1}=\frac{ac}{bd}$.

14.3.1 *SUBFIELDS*

Definition: A non-empty subset K of a field F is said to be subfield if K is closed w.r.to. operation addition and multiplication in F and K itself is a field for these operation.

Conditions for a subfield: The necessary and sufficient condition for a non-empty subset K of field F to be subfield 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 condition: Let the subset K of field F is itself a field.

$\Rightarrow K$ is a group w.r.to. addition i.e. for each $a,b\in K\Rightarrow a-b\in K$

Now each non-zero element of K possesses multiplicative inverse. Therefore $a\in K, 0\neq b\in K\Rightarrow ab^{-1}\in K$

Hence condition is necessary.

Sufficient condition: Suppose K is non-empty subset of F and satisfying the condition **(*i*)** and **(*ii*)**. As similar we have proved in case of subring that $(K,+)$ is abelian group, in similar we will prove (i) that $(K,+)$ is abelian group.

Now let a be any non-zero element of K. Then from (ii) we have $a\in K, 0\neq a\in K\Rightarrow aa^{-1}\in K\Rightarrow 1\in K$

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

$a\in K, 0\neq b^{-1}\in K\Rightarrow a(b^{-1})^{-1}\in K\Rightarrow ab\in K$

Also if $b=0$, then $ab=0$ and $0\in K$

$\therefore ab \in K \forall a, b \in K$

Associativity of multiplication and distributivity of multiplication over addition must hold in K since they hold in F

14.4 *DIVISION RING AND SKEW FIELD*

Definition: A ring (R) with at least two elements is called a division ring or a skew field if is satisfies following conditions

(i) Has unity

(ii) Each non-zero element possesses its multiplicative inverse.

Thus a commutative division ring is a field.

A division ring is a field if it is also commutative but every field is also a division ring.

Theorem 1: Every field is an integral domain.

Proof: As we know that a field (F) is a commutative ring with unity, therefore to prove that every field is an integral domain we have only to prove 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

$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$

$\Rightarrow (a^{-1}a)b = 0$

$\Rightarrow 1b = 0$ $[\because a^{-1}a = 1]$

$\Rightarrow b = 0$ $[\because ab = b]$

Similarly, let $ab = 0$ and $b \neq 0$

Since $b \neq 0, b^{-1}$ exists and we have

$ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1}$

$\Rightarrow a(bb^{-1}) = 0 \Rightarrow a1 = 0 \Rightarrow a = 0$

Hence in a field $ab = 0 \Rightarrow a = 0$ or $b = 0$. Since field has no zero divisors therefore every field is an integral domain.

The converse of this theorem is not true i.e., every integral domain is not a field. For example, ring of integer is an integral domain while it is not a field because only inversible element in the ring of integer are 1 and -1.

Note: In the field unity and zero are different 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, $a^{-1} = 0 \Rightarrow aa^{-1} = a0 \Rightarrow 1 = 0 \Rightarrow a1 = a0 \Rightarrow a = 0$

This is a contradiction. Now, field has no zero divisors. Therefore, $1 = a^{-1}a \neq 0$.

Remarks: As we know field has no zero divisors. Therefore in the field product of two non-zero elements will again a non-zero element. Also each non-zero element and unit element possesses non-zero multiplicative inverse. Since multiplication is commutative as well as associative, therefore the non-zero elements of a field form abelian group w.r.to. multiplication.

Theorem 2: A skew field (D) has no zero divisors.

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 $a \neq 0$ s.t. $ab = 0$

Since $a \neq 0, a^{-1}$ exists and we have

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow (a^{-1}a)b = 0 \Rightarrow 1b = 0 \Rightarrow b = 0$$

Similarly, let $ab = 0$ with $b \neq 0$

Since $b \neq 0, b^{-1}$ exists and we have

$$ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1}$$

$$\Rightarrow a(bb^{-1}) = 0 \Rightarrow a1 = 0 \Rightarrow a = 0$$

Hence a skew field has no zero divisors.

Theorem 3: Every finite integral domain is a field '*OR*' A finite commutative ring without zero divisor is a field.

Proof: Let D be a finite commutative ring without zero divisor 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 should show that for every element $a \neq 0 \in D$ there exist an element $b \in D$ such that $ba = 1$.

Let $a \neq 0 \in D$. Consider the n products $aa_1, aa_2, aa_3, ..., aa_n$.

All these are element of D. Also they are all distinct. For suppose that $aa_i = aa_j$ for $i \neq j$.

Then $a(a_i - a_j) = 0$ … (1)

Since D is without zero divisors and $a \neq 0$, therefore (1) implies

$a_i - a_j = 0 \Rightarrow a_i = a_j$, contradicting $i \neq j$.

$\therefore aa_1, aa_2, aa_3, ..., aa_n$ are all 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 element of D. Then from the above discussion for some $x \in D$, we shall have $ax = y = xa$

Now, $1y = 1(ax)$ [$\because ax = y$]

$= (1a)x$

$= ax$ [$\because 1a = a$]

$= y$ [$\because ax = y$]

$= y1$ [$\because D$ is commutative]

Thus $1y = y = y1, \forall\, y \in D$. Therefore 1 is the unit element of the ring D.

Now $1 \in D$. Therefore from the above discussion one of the n products $aa_1, aa_2, aa_3, ..., aa_n$ 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.

$\Rightarrow D$ is a field.

Definition: In a ring R any element a is said to be idempotent if $a^2 = a$. Any ring R will be called Boolean Ring if and only if all of its elements are idempotent i.e., if $a^2 = a \,\forall\, a \in R$.

Example 1: In the ring of set M of 2×2 matrices over the field of real number with respect to matrix addition and multiplication evaluate the following:

(*i*) Is it a commutating ring with unity elements?

(*ii*) Find the zero elements.

(*iii*) Does this ring possess zero divisors?

Solution: Let $A, B \in M$. Then $A + B \in M$ and $AB \in M$. Therefore M is closed with respect addition and multiplication of matrices.

As we know that both addition and multiplication of matrices are associative composition.

$\therefore A + (B + C) = (A + B) + C \,\forall\, A, B, C \in M$

and $A(BC) = (AB)C \ \forall A, B, C \in M$

Commutative property holds in addition of matrices. Hence, $\forall A, B \in M$, 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 distributes w.r.to. addition.

$\therefore A(B + C) = AB + AC$

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

$A = \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$

Then, $AB = \begin{bmatrix} 2 & 8 \\ 3 & 11 \end{bmatrix}$ and $BA = \begin{bmatrix} 8 & 14 \\ 3 & 5 \end{bmatrix}$

Thus $AB \neq BA$ and so the ring is a non-commutative ring

If I be the unit matrix of the type 2×2 i.e., $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ then $I \in M$. Also we have

$AI = A = IA \forall A \in M$

$\therefore I$ is the multiplicative identity.

Thus the ring possesses the unit element and we have $I = 1$ (the unit element of the ring)

The 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 $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring.

Example 2: DO the following sets from integral domains w.r.to. ordinary addition and multiplication? If so state if they are fields.

(*i*) The set of numbers of the form $b\sqrt{2}$ with b rational.

(*ii*) The set of even integers.

(*iii*) The set of positive integers.

Solution (*i*): Let $A = \left\{ b\sqrt{2} : b \in Q \right\}$.

We have $3\sqrt{2} \in A$ and $5\sqrt{2} \in A$. Then $\left(3\sqrt{2}\right)\left(5\sqrt{2}\right) = 30$. Now 30 can not be put in the form $b\sqrt{2}$ where b is rational number. Therefore $30 \notin A$. Thus A is not closed with respect to multiplication. Therefore the question of A becoming a ring does not arises.

(*ii*): Let R be set of all even integers. Then R is a ring with respect to addition and multiplication of integers. Additionally, the composition of multiplication is commutative. Since the product of two non-zero even integers cannot equal zero, which is the zero element of this ring, R has no zero divisors. Since the integer $1 \notin R,$ therefore R is a ring without unity. If the presence of the unit clement is not a requirement for an integral domain, then R will be one. However, since the multiplicative identity does not exist, R is not a field.

(*iii*): N should be the collection of positive integers. The additive identity does not exist since the number $0 \notin N$. N won't be a ring, then.

Example 3: Show that collection of numbers of the form $a + b\sqrt{2}$, with a and b as rational numbers is a field.

Solution: Let $R = \left\{a + b\sqrt{2} : a, b \in Q\right\}$

Let $a_1 + b_1\sqrt{2} \in R$ and $a_2 + b_2\sqrt{2} \in R$ where $a_1, b_1, a_2, b_2 \in Q$

We have $\left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right) = \left(a_1 + a_2\right) + (b_1 + b_2)\sqrt{2} \in R$. Since $\left(a_1 + a_2\right), \left(b_1 + b_2\right) \in Q$

Also $\left(a_1 + b_1\sqrt{2}\right)\left(a_2 + b_2\sqrt{2}\right) = \left(a_1a_2 + 2b_1b_2\right) + \left(a_1b_2 + a_2b_1\right)\sqrt{2} \in R$.

Since $a_1a_2 + 2b_1b_2, a_1b_2 + a_2b_1 \in Q$

Thus R is closed w.r.to. addition and multiplication.

We know that addition and multiplication are both associative and commutative compositions in the set of real numbers since all the components of R are real numbers.

Further we have $0 + 0\sqrt{2} \in R$ since $0 \in Q$.

If $a + b\sqrt{2} \in R$, then

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

$\therefore\ 0 + 0\sqrt{2}$ is the additive identity.

Now again if $a + b\sqrt{2} \in R$, then $(-a) + (-b)\sqrt{2} \in R$ and we have

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

$\therefore$ each element of R posses its own additive inverse.

Since multiplication is distributive w.r.to. addition in the set of real number.

Again $1+0\sqrt{2} \in R$ and we have

$(1+0\sqrt{2})(a+b\sqrt{2}) = a+b\sqrt{2} = (a+b\sqrt{2})(1+0\sqrt{2}) \in R$

So, $(1+0\sqrt{2})$ is the multiplicative identity. Thus R is commutative ring with unity and the zero element of the ring is $0+0\sqrt{2}$ and $1+0\sqrt{2}$ is the unit element. If each non-zero element of R has a multiplicative inverse, then R will now be a field.

Let $a+b\sqrt{2} \neq 0+0\sqrt{2}$ be any element of this ring i.e., one of the element a and b is not zero.

Then $\dfrac{1}{a+b\sqrt{2}} = \dfrac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \dfrac{a-b\sqrt{2}}{a^2-2b^2}$

$= \left(\dfrac{a}{a^2-2b^2}\right) + \left(-\dfrac{b}{a^2-2b^2}\right)\sqrt{2}$

Now if a, b are rational numbers, then we can have $a^2 = 2b^2$ only if $a = 0, b = 0$. As we know that at least one of the rational numbers a and b is not 0. There we cannot have $a^2 = 2b^2$ i.e., $a^2 - 2b^2 = 0$.

$\therefore$ Both numbers $\dfrac{a}{a^2-2b^2}$ and $-\dfrac{b}{a^2-2b^2}$ are rational number and not both of them are zero.

$\therefore \left(\dfrac{a}{a^2-2b^2}\right) + \left(--\dfrac{b}{a^2-2b^2}\right)\sqrt{2}$ is non-zero multiplicative inverse of $a+b\sqrt{2}$. Hence the given system is a field.

Example 4: Give an example of an infinite commutative ring without zero divisors which is not a field.

Solution: Let Z be the set of integers. Then $(Z,+,.)$ is an infinite commutating ring without zero divisors and is not a field.

Example 5: If $(R,+,.)$ be a ring with n elements, $n > 2$ with no zero divisors, show that R is a division ring.

Solution: Let R be a finite consisting of n elements, where $n \geq 2$ s.t., R has no divisor of zero.

To prove that R is a division ring we have enough to prove that.

(i) R has a unit element 1.

(ii) Every non-zero element of R has multiplicative inverse in R.

(i) Prove of (i) is the part of Theorem 3.

(ii) $1 \in R \Rightarrow \exists\, a\, x_j \in R$ s.t. $a\, x_j = 1, 1 \le j \le n$

$\Rightarrow a$ is left inverse of x_j in R.

But left inverse = Right inverse.

$\Rightarrow a$ is the multiplicative inverse of x_j in R

Theorem 4: In the ordered integral domain D, the unity element is a positive element of D.

Proof: Let P be the collection of positive elements of integral domain D. We have to prove that $1 \in P$, for it we assume that $1 \notin P$.

Since $1 \notin P$, $1 \neq 0 \Rightarrow -1 \in P$ [By definition of P]

$\Rightarrow (-1)(-1) \in P$

$\Rightarrow 1 \in P$, which is a contradiction.

Hence the unity element is positive element of D.

Theorem 5: The field $(I_p, +_p, \times_p)$ is not ordered, where $I_p = \{0, 1, 2, ..., p-1\}$ and $p =$ prime.

Proof: To prove $(I_p, +_p, \times_p)$ is not ordered.

Suppose the contrary. Then $(I_p, +_p, \times_p)$ is ordered. Let P be the set of positive element of I_p. Since additive identity of I_p is '0'. By definition of P, $1 \in I_P$

$\Rightarrow$ only one of the following is true:

$1 = 0, 1 \in P$ or additive inverse of $1 \in P$.

Evidently $1 \neq 0$. Hence $1 \in P$ or additive inverse of $1 \in P$. Since P is closed w.r.to $+_p$.

$\therefore 1 \in P \Rightarrow 1 +_p 1 \in P \Rightarrow 2 \in P \Rightarrow 2 +_p 1 \in P \Rightarrow 3 \in P$

Repeating this process, we find that $1 \in P \Rightarrow p - 1 \in P$, i.e., $1 \in P$

$\Rightarrow$ additive inverse of 1 belongs to P. Which is a contradiction.

For both the possibilities $1 \in P$, $p - 1 \in P$ cannot holds simultaneously.

Here our initial assumption is wrong.

Therefore the required result follows.

Theorem 6: The set of complex number is not ordered integral domain.

Proof: Let C be the set of complex numbers. We know that $(C, +, .)$ is an integral domain. Let P be the set of positive element of C. Evidently $i \in C$ and $i \neq 0$.

Hence either $i \in P$ *or* $-i \in P$.

$i \in P \Rightarrow i.i \in P$, by definition of P

$\Rightarrow -1 \in P.$ For $i^2 = -1$.

A contradiction . For $-1 \in P$, by theorem 4.

$\therefore i \notin P$.

Again, $-i \in P \Rightarrow (-i)(-i) \in P \Rightarrow i^2 \in P \Rightarrow -1 \in P$.

Again we get a contradiction, $-i \notin P$.

Thus $i \neq 0, i \neq P, -i \notin P,$ i.e., any one of the following:

$i = 0, i \in P, -i \in P,$

does not hold. Hence C is not an ordered integral domain.

Theorem 7: The characteristic of a ring with unity is zero or $n > 0$ according as the unity element regarded as a member of additive group of R of order 0 or n.

OR

If R is any ring with identity 1, shows that R has positive characteristic n *iff* n is the least positive integer for which $n.1 = 0, 0$ being additive identity of R.

Proof: Let R be a ring with unity element e.

$O(e) = 0 \Rightarrow$ Characteristic of R is 0.

Suppose $O(e) = n = a$ finite number so that n is the least positive integer s.t. $ne = 0$. Let a be any element of R. Then

$na = n(ea).1$ For $ea = a = ae$

$= (ne)a = 0a = 0$

Thus n is the least positive integer s.t. $na = 0$. Hence the characteristics of R is n.

Theorem 8: Every finite integral domain D is of finite characteristics.

Proof: Let $(D, +, .)$ be a finite integral domain so that $(D, +, .)$ is a finite abelian group. We also known that characteristic of D is the order of unity element e of $(D, +, .)$.

$(D, +, .)$ is finite group $\Rightarrow O(e)$ finite.

$\Rightarrow$ Characteristic of D is finite.

Theorem 9(a): The characteristic of an integral domain is either 0 or a prime number according as the unity element *e* regarded as a member of the additive group of integral domain is of order 0 or a prime number.

Proof: (i) Let D be an integral domain. Then we prove that characteristic of D is either 0 or $p > 0$. [Proved in theorem 8]

(ii) If the characteristic is zero, the proof is complete.

Let the characteristic be $p > 0$. We have to show that p is a prime number.

Suppose p is not prime. Then p is composite integer. So we can write $p = p_1 p_2$: where $1 < p_1, p_2 < p$.

Characteristic of D is $p \Rightarrow$ order of e of the group $(D,+)$ is p. [e is unity element of D]

$\Rightarrow o(e) = p \Rightarrow pe = 0$

$\Rightarrow p_1 p_2 e = 0 \Rightarrow p_1(p_2 e) = 0$

$\Rightarrow (p_1 e)(p_2 e) = 0$

$\Rightarrow p_1 e = 0 \, or \, p_2 e = 0$ [For D has no zero divisor]

$\Rightarrow$ Characteristic of D is either p_1 or $p_2 < p$

$\Rightarrow Ch.D < p$. A contradiction.

Hence p is not composite.

Therefore p is prime.

Theorem 9(b): The characteristic of an integral domain is 0 or $n > 0$ according as the order of any non-zero element regarded as member of the additive group of the integral is either 0 or n.

Proof: Let $(D,+,.)$ be an integral domain and $a \in D$ and $a \neq 0$ and $O(a) = 0$ or n regarded as a member of $(D,+)$.

Then $na = 0, \; 0a = 0$ ...(1)

Aim: Characteristic of D is 0 or n.

For this have to show that $nx = 0 \; \forall \; x \in D$.

If $x \in D$, then (1) $\Rightarrow (na)x = 0 \Rightarrow (a + a + ... + a \, to \, n \, terms)\, x = 0$

$\Rightarrow (ax + ax + ... + a \, to \, n \, terms) = 0$

$\Rightarrow a(x + x + ... to \, n \, terms) = 0 \Rightarrow a(nx) = 0, a \neq 0$

$\Rightarrow nx = 0$ as D is free from zero divisors. Hence n is the least positive integer, according to (1).

Example 6: If there exist a positive integer m such that $ma = 0 \forall a \in F$, then show that m is a prime. What is this integer? F being a field.

Answer: Let F be a field and $a \in F$ be arbitrary. Also let

$$ma = 0 \quad \ldots(1)$$

where m is a positive integer. Let e be the multiple identity of F.

Then $ae = ea = 0$

(1) $\Rightarrow m(ea) = 0 \Rightarrow (me)(a) = 0 \Rightarrow me = 0 \, or \, a = 0$

$\Rightarrow$ in particular $me = 0$ …(2)

For F has no divisor of zero

F is field $\Rightarrow F$ is integral domain s.t. (2) holds.

It means that m is the characteristic of F. To prove that m is *prime*.

Now write proof of theorem 9a.

Theorem 10: Each non-zero element of an integral domain D, regarded as an element of the additive group D, is of the same order.

Proof: Let a, b be arbitrary non-zero elements of an integral domain D s.t. $a \neq b$.

Let $O(a) = n, O(b) = m$, where a, b are regarded as element of $(D, +)$ so that $na = 0, mb = 0$,

D is an integral domain $\Rightarrow D$ has no zero divisors.

$\Rightarrow$ cancellation law hold in D.

$na = 0 \Rightarrow a + a + \ldots upto\, n\, terms = 0$

$\Rightarrow b(a + a + \ldots upto\, n\, terms) = b.0 = 0$

$\Rightarrow ba + ba + \ldots upto\, n\, terms = 0$

$\Rightarrow n(ba) = 0 \Rightarrow (nb)a = 0 = 0a \Rightarrow (nb)a = 0a$

$\Rightarrow nb = 0$, by cancellation law

$\Rightarrow O(b) \leq n \Rightarrow m \leq n.$ For $O(b) = m$

$mb = 0 \Rightarrow b + b + \ldots upto\, n\, terms = 0$

$\Rightarrow a(b + b + \ldots upto\, n\, terms) = a.0 = 0$

$\Rightarrow ab + ab + \ldots upto\, n\, terms = 0$

$\Rightarrow m(ab) = 0 = 0b$

$\Rightarrow (ma)b = 0b$. Also $b \neq 0$

$\Rightarrow ma = 0$, By cancellation law

$\Rightarrow O(a) \leq m \Rightarrow n \leq m$. For $O(a) = n$

Thus we have shown that $n \leq m, m \geq n$.

$\therefore m = n,$ i.e., $O(a) = O(b)$.

When considered as members of an additive group, any two non-zero components of D have the same order.

Therefore, when considered a member of $(D, +)$, every non-zero element of D is of the same order.

Example 7: Give an example of skew-field which is not field.

Solution: Let R be a set of matrices of the form,

$$A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

Where a and b are complex numbers.

Let $$B = \begin{bmatrix} c & d \\ -\bar{d} & \bar{c} \end{bmatrix},$$

$$C = \begin{bmatrix} p & q \\ -\bar{q} & \bar{p} \end{bmatrix}$$ be any two member of R. Then

$$A + B = \begin{bmatrix} a+c & b+d \\ -(\bar{b}+\bar{d} & \bar{a}+\bar{c} \end{bmatrix}$$

$$AB = \begin{bmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -(\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \overline{ac} \end{bmatrix}$$

If we take $\alpha = a + c, \beta = b + d, \gamma = ac - b\bar{d}, \delta = ad + b\bar{c}$, then we have

$$A + B = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \in R$$

$$AB = \begin{bmatrix} \gamma & \delta \\ -\bar{\delta} & -\bar{\gamma} \end{bmatrix} \in R$$

(*i*) $(R, +)$ is an abelian group.

Closure axiom: $A+B \in R$ (already proved)

Commutativity: $A+B=B+A$.

This flows from the fact that $a+b=b+a$

Existence of identity: $O=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\in R$

is additive identity s.t. $A+O=O+A=A$

Associative law: $A+(B+C)=(A+B)+C$

It follows from the fact that

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

Existence of inverse: $-A=\begin{bmatrix}-a & -c\\ \bar{c} & -\bar{a}\end{bmatrix}\in R$

is inverse of A s.t. $A+(-A)=O$

(*ii*) $(R,.)$ is a group

Closure axioms: $AB \in R$ (already proved)

Existence of identity: $I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\in R$ is identity s.t. $AI=IA=A$.

Associative law: $(AB)C=A(BC)$

For $(ab)c=a(bc)$

Existence of inverse: If $A\neq O$, then

$$A^{-1}=\frac{adjA}{|A|}=\frac{1}{(a\bar{a}+b\bar{b})}\begin{bmatrix}\bar{a} & -b\\ \bar{b} & a\end{bmatrix}\in R$$

is inverse of A s.t. $AA^{-1}=A^{-1}A=I$

Commutative law: $AB=BA$ is not satisfied here.

For $BA=\begin{bmatrix}c & d\\ -\bar{d} & \bar{d}\end{bmatrix}\begin{bmatrix}a & b\\ -\bar{b} & \bar{a}\end{bmatrix}$

$$=\begin{bmatrix}ac-\bar{b}d & bc-\bar{a}d\\ -a\bar{d}-\bar{b}\bar{c} & -b\bar{d}+\bar{a}\bar{c}\end{bmatrix}\neq BA, \text{ by (1)}$$

Or $BA\neq AB$

(*iii*) Distributive law: $A(B+C)=AB+AC$

$$(B+C)A = BA+CA$$

It is true in general in case of matrices.

These fact show that $(R,+,.)$ is askew field but not field.

Example 8: Prove that the set $I_7 = \{0,1,2,...,6\}$ forms a field w.r.t. addition and multiplication modulo 7.

Solution: Let $I_7 = \{0,1,2,...,6\}$.

Let $a,b,c \in I_7$

We define $a +_7 b = \begin{cases} a+b \ if \ a+b<7 \\ r \quad\quad if \ a+b \geq 7 \end{cases}$

Where r is remainder when $a+b$ is divided by 7,

$\therefore \ 0 \leq r \leq 6$

Evidently, $a +_7 b \in I_7$

(*i*) First, we have to prove that $(I_7, +_7)$ is an abelian group.

Closure axioms: $a +_7 b \in I_7$ (already proved)

Existence of identity: $\exists 0 \in I_7$, called additive identity s.t.

$$a +_7 0 = 0 +_7 a = a$$

Commutative law: $a +_7 b = b +_7 a$.

This follow from the fact that, $a+b=b+a$

Associative law: $(a +_7 b) +_7 c = a +_7 (b +_7 c)$

Since $(a+b)+c = a+(b+c)$

Therefore each side leaves the same remainder when divided by 7.

$\therefore \ (a+b) +_7 c = a +_7 (b+c)$

Or $\therefore \ (a +_7 b) + c = a +_7 (b +_7 c)$

Existence of inverse: $\forall \ \ a \in I_7, \exists$ its inverse

$(7-a) \in I_7$ (if $a \neq 0$) s.t.

$(7-a) +_7 a = a +_7 (7-a) = 0$.

Inverse of 0 is 0 itself.

(*ii*) Write $I'_7 = \{1, 2, 3, ..., 6\} = I_7 - \{0\}$.

Let $a, b, c \in I'_7$. Define

$$a \times_7 b = \begin{cases} ab \ \text{if} \ ab \le 7 \\ s \ \ \text{if} \ ab \ge 7 \end{cases}$$

Where s is the remainder when ab is divisible by 7.

$$0 \le s \le 6$$

$s = 0 \Rightarrow ab$ is divisible by 7.

But 7 has divisor $\Rightarrow a$ or b is divisible by 7

$$\Rightarrow a \ge 7, b \ge 7.$$

A contradiction as $a, b < 7$.

$\therefore s \ne 0$. Consequently $0 < s \le 6$.

This $\Rightarrow s \in I'_7 \Rightarrow a \times_7 b \in I'_7$

Aim: Now we have to prove that $(I'_7, \times_7)$ is an abelian group.

Closure axioms: $a \times_7 b \in I'_7$ (already proved)

Commutative law: $a \times_7 b = b \times_7 a$

Associative law: $(a \times_7 b) \times_7 c = a \times_7 (b \times_7 c)$.

Since $(ab)c = a(bc)$

Existence of identity: $1 \in I'_7$ is identity element s.t.

$$1 \times_7 a = a \times_7 1 = a.$$

Existence of inverse: $\forall\, a \in I'_7$, we have its inverse $x \in I'_7$ s.t.

$$a \times_7 x = x \times_7 a = 1.$$

For the equation $ax \equiv 1 \pmod{p}$ has a solution x if p is prime.

[Inverse of 1, 2, 3, 4, 5, 6 are respectively 1, 4, 5, 2, 3, 6]

Thus $(I'_7, \times_7)$ is an abelian group.

(*iii*) **Distributive law:** $a \times_7 (b +_7 c) = (a \times_7 b) +_7 (a \times_7 c)$

$$(b +_7 c) \times_7 a = (b \times_7 a) +_7 (c \times_7 a)$$

This follows from the fact that

$a(b+c)=ab+ac$ and $(b+c)a=ba+ca$

Above arguments lead to the fact that $(I_7,+_7,\times_7)$ is a field.

Similar example 9: Let p be a positive prime number. Prove that the set $I_p=\{0,1,...,p-1\}$ forms a field w.r.t. addition and multiplication modulo p '*OR*'Ring of integers modulo a prime number p, is a field.

Example 10: If $I_5=\{0,1,2,3,4\}$ then prove that $(I_5,+_5,\times_5)$ is a field, where $+_5$ and $\times_5$ respectively denote addition and multiplication modulo 5.

Answer: The composition tables for two operations are given below:

(*i*) Closure axiom: From the two composition tables it is quite clear that all the entries in both composition tables belong to I_5. Hence I_5 is closed w.r.to. both operation

(*ii*) Commutative law: The entries in the 1st, 2nd, 3rd, 4th rows are coincident with the corresponding element of the 1st, 2nd, 3rd, 4th columns respectively relative to the both operations. Hence $+_5$ and $\times_5$ both are commutative in I_5.

(*iii*) Associative law: It is easy to verify that the associative law holds for $+_5$,

i.e., $a+_5(b+_5c)=(a+_5b)+_5c \ \ \forall a,b,c\in I_5$.

Similarly, $a\times_5(b\times_5c)=(a\times_5b)\times_5c \ \ \forall a,b,c\in I_5$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(*iv*) 0 is the additive identity and 1 is the multiplicative identity for I_5.

For $0+_5a=a\,\forall\,a\in I_5$

$1\times_5a=a\,\forall\,a\in I_5$ s.t. $a\neq0$

This follows from the composition tables.

(*v*) Existence of inverse: The additive inverse of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively. The multiplicative inverses of non-zero elements 1, 2, 3, 4 are 1, 3, 2, 4 respectively.

(*vi*) Distributive law: Multiplication is distributive over addition, i.e.,

$a \times_5 (b +_5 c) = a \times_5 b +_5 a \times_5 c \quad \forall a, b, c \in I_5$

$(b +_5 c) \times_5 a = b \times_5 a +_5 a +_5 c \times_5 a \quad \forall a, b, c \in I_5$

For $a \times_5 (b +_5 c) = a \times_5 (b + c)$. For $b +_5 c = b + c \pmod 5$

$=$ least positive remainder when $a \times (b + c)$ is divided by 5.

$=$ least positive remainder when $ab + ac$ is divided by 5.

$= ab +_5 ac$

$= a \times_5 b +_5 a \times_5 c$. For $a \times_5 b \equiv a \times b \pmod 5$

In similar way, we can prove other distributive law.

Hence $(I_5, +_5, \times_5)$ is a field.

Example 10: The set of all residue classes modulo a positive integer p is an integral domain *iff* p is prime.

Solution: Let R denote the set of all residue classes modulo a positive integer p so that

$R = \{[x] : x = 0, 1, 2, 3, ..., p-1\}$

Then we know that R is a commutative ring with unity element [1], [0] being the zero element of R. Let $[a], [b] \in R$ be arbitrary so that

$0 \le a, b \le p - 1$

R will be an integral domain iff it is free from zero divisors, i.e., iff

$[a][b] = [0] \Rightarrow [a] = [0]$ *or* $[b] = 0$

So we have to show that p is prime iff

$[a][b] = [0] \Rightarrow [a] = [0]$ *or* $[b] = 0$

(*i*) p is prime, $[a][b] = [0] \Rightarrow p$ is prime, $ab \equiv 0 \pmod p$

$\Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$

$\Rightarrow [a] = [0]$ *or* $[b] = [0]$ or $b \equiv 0 \pmod p$

(*ii*) Conversely supplies,

$[a][b] = [0] \Rightarrow [a] = [0]$ *or* $[b] = [0]$.

Now we have to prove that p is prime. For it let p is of composite order.

If p is of composite order $\Rightarrow p$ is expressible as, $p = p_1 p_2$, where $1 < p_1, p_2 < p$

$$\Rightarrow [p] = [p_1.p_2], [p_1] \neq [0], [p_2] \neq [0]$$

$$\Rightarrow [p_1.p_2] = [0]. \text{ For } [p] = [0]$$

$$\Rightarrow [p_1] = 0 \text{ or } [p_2] = [0], \text{ by assumption.}$$

Which is a contradiction.

For $[p_1] \neq 0$ and $[p_2] \neq [0]$.

Which shows our assumption is wrong. Therefore p is prime.

Similar problem 11: The set of all integers modulo a positive integer p is an integral domain *iff* p is prime.

Hint: $(I_p, +_p, \times_p)$ is integral domain, where $I_p = \{0, 1, 2, 3, ..., p-1\}$.

Check your progress

Problem 1: Check $I_4 = \{0, 1, 2, 3\}$ is field or not?

Problem 2: Check that the set $\{0, 1\}$ form a field?

Problem 2: Check that the singleton set $\{0\}$ form a field and why?

14.5 *SUMMARY*

In this unit, we have studied about the field, subfield and division ring or skew field in a ring. Throughout the all units we have learned about the basic definitions and their related theorems and examples on these major topics. In many areas of mathematics, fields are fundamental concepts. This comprises many mathematical analysis disciplines that are based on fields with extra structure. Analysis's fundamental theorems rely on the real numbers' structural characteristics. What's more, any field may be utilised as the scalars for a vector space, which is the usual generic setting for linear algebra. In-depth research is done on number fields, the siblings of the subject of rational numbers. Geometric object attributes may be described with the use of function fields. The overall summarization of this units are as follows:

- Every field is an integral domain.
- Every finite integral domain is field.
- The set of all integers modulo a positive integer p is an integral domain *iff* p is prime

14.6 *GLOSSARY*

- **Field:** A commutative ring with unity having each non-zero element possess its multiplicative inverse is called field.
- **Sub-field:** A subset of field which is itself a filed called subfield.
- **Division ring:** A ring with unity having each non-zero element possess its multiplicative inverse is called division ring.

14.7 *REFERENCES*

- Joseph A Gallian, (1999), *Contemporary Abstract Algebra* (4th Edition), Narosa, 1999.
- N. Herstein,(1975), *Topics in Algebra*, Wiley Eastern Ltd., New Delhi.
- V. K. Khanna and S. K. Bhambri (2021), *A Course in Abstract Algebra* (5th Edition), Vikas Publication House.
- Vasishtha, A. R., & Vasishtha, A. K. (2006). *Modern Algebra (Abstract Algebra)*. Krishna Prakashan Media.
- RamjiLal, Algebra 1: *Groups, Rings, Fields and Arithmetic*, Springer, 2017.

14.8 *SUGGESTED READING*

- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul: *Basic Abstract Algebra*, Cambridge Press, 1994.
- David S. Dummit and Richard M. Foote: *Abstract Algebra* (3rd Edition), Wiley, 2011.
- Michael Artin: *Algebra* (2nd edition), Pearson, 2014.

14.9 *TERMINAL QUESTIONS*

Long Answer Type Question:

1. Show that in an integral domain all non-zero elements generate additive cyclic groups of the same order which is equal to the characteristic of the integral domain.

2. Give without proof, an example of an integral domain which contains only five elements. Is this an ordered integral domain? Give reason?

3. Show that the matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, *a, b* real, forms a field.

4. Prove that a non-zero finite integral domain is a field.

5. Prove that $(I_7, +_7, \times_7)$ is a field, where $+_7$ and $\times_7$ respectively denote addition and multiplication modulo 5.

6. Give an example of skew-field which is not field.

7. Show that collection of numbers of the form $a + b\sqrt{2}$, with a and b as rational numbers is a field

Short Answer Type Question:

8. If D is a non-zero integral domain, then characteristic of D is either zero or a prime number.

9. The set of complex number is not ordered integral domain

10. Prove that a skew field has no zero divisor.

11. Write the definition of following with suitable example.

(*i*) Field

(*ii*) Integral domain

(*iii*) Skew-field

12. A commutative ring R is an integral domain *iff* $\forall\, a, b, c \in R (a \neq 0)$

$ab = ac \Rightarrow b = c$

Objective type questions

1. Which of the following is NOT a field?

a) Q (Rational Numbers)
b) Z (Integers)
c) R (Real Numbers)
d) C (Complex Numbers)

2. In a field, which of the following properties must hold for multiplication?

a) Commutativity
b) Associativity
c) Existence of Multiplicative Inverse (except for zero)
d) All of the above

3. Which of the following is a finite field?

a) Z_6
b) Z_5
c) Q
d) R

4. The smallest field containing only two elements is known as:
a) Q
b) F_2
c) R
d) Z_2

5. Which of the following is true for every field F?
a) F must have an infinite number of elements.
b) Every element in F has an additive and multiplicative inverse (except zero).
c) The set of natural numbers forms a field.
d) Fields always contain only real numbers.

6. Which of the following operations is NOT necessarily defined in a field?
a) Addition
b) Subtraction
c) Multiplication
d) Division by zero

7. A field must contain at least how many elements?
a) 1
b) 2
c) 3
d) 0

8. Which of the following is an example of a finite field?
a) Q (Rational Numbers)
b) Z_7
c) R (Real Numbers)
d) C (Complex Numbers)

9. If F is a field, which of the following must be true?
a) F has at least one element with no additive inverse.
b) Every element in F has a unique additive inverse.
c) Multiplication is not necessarily associative.
d) F contains at least one zero divisor.

10. The characteristic of a finite field F_p is always:
a) 0
b) 1
c) A prime number
d) Composite

11. Which of the following sets is a field under usual addition and multiplication?
a) The set of natural numbers N
b) The set of integers Z
c) The set of rational numbers Q
d) The set of even integers

12. If F is a field, then which of the following is true?
a) F must be an infinite set.
b) The sum of any two elements in F is always in F.
c) F contains at least one element without a multiplicative inverse.
d) The set of all positive integers is a field.

13. If p is a prime number, then the order of the field Z_p is:
a) $p-1$
b) p

c) $p+1$
d) $2p$

14. Which of the following is always true for a field F?
a) F is closed under addition and multiplication.
b) Every element in F has a multiplicative inverse, including zero.
c) F must have infinitely many elements.
d) The characteristic of F is always zero.

15. In which of the following fields does the equation $x^2+1=0$ have a solution?
a) R (Real numbers)
b) C (Complex numbers)
c) Q (Rational numbers)
d) Z_5

Fill in the blanks:

1. A commutative R is an integral domain iff …….

2. Every field is an ……..

3. A skew field has no …….

4. Every finite integral domain is ……

5. The set of all residue classes modulo a positive integer p is an integral domain *iff* p is ……..

True and False question:

1. Every field is a ring, but not every ring is a field. *(True / False)*
2. The set of integers Z is a field. *(True / False)*
3. In a finite field, the number of elements must always be a prime number. *(True / False)*
4. The set of all even integers forms a field under normal addition and multiplication. *(True / False)*
5. Every finite field has order p^n for some prime p and integer n. *(True / False)*
6. Every field is an integral domain. *(True / False)*
7. In a finite field, the sum of all elements is always zero. *(True / False)*
8. The order of a finite field must be a prime number. *(True / False)*
9. The characteristic of a field is always either 0 or a prime number. *(True / False)*
10. Every subring of a field is a field. *(True / False)*
11. The set of complex numbers C forms a field under usual addition and multiplication. *(True / False)*
12. In any field, the element 0 always has a multiplicative inverse. *(True / False)*
13. Every field is closed under addition, multiplication, and division (except by zero). *(True / False)*
14. If a field contains a finite number of elements, it is called a finite field. *(True / False)*
15. A finite field always has an even number of elements. *(True / False)*

14.10 *ANSWERS*

Answer of check your progress:

1. No 2. Yes **3.** No, because it does not contain unity element

Answer of objective type question:

1.	b	**2.**	d	**3.**	b	**4.**	b
5.	b	**6.**	d	**7.**	b	**8.**	b
9.	b	**10.**	c	**11.**	c	**12.**	b
13.	b	**14.**	a	**15.**	b		

Answer of true and false:

1.	True	**2.**	False	**3.**	False
4.	False	**5.**	True	**6.**	True
7.	True	**8.**	False	**9.**	True
10.	False	**11.**	True	**12.**	False
13.	True	**14.**	True	**15.**	False

Answer of fill in the blanks:

1.	Cancellation law holds	**2.**	Integral domain	**3.**	Zero divisor
4.	Field	**5.**	Prime		

Teen Pani Bypass Road, Transport Nagar
Uttarakhand Open University,
Haldwani, Nainital-263139
Phone No. 05946-261122, 261123
Toll free No. 18001804025
Fax No. 05946-264232,

E-mail:info@uou.ac.in
Website: https://www.uou.ac.in/