Chapter 7
Algebraic Structures

In mathematics, a **group** is viewed as consisting of a set of elements together with an operation to combine any two of its elements to get new element that also belongs to the same set while satisfying four conditions, namely, group axioms, closure, associativity, identity and invertibility.

Main classes of groups : The groups are divided into five main classes, listed below.

1. **Permutation groups**
2. **Matrix groups**
3. **Transformation groups**
4. **Abstract groups**
5. **Topological and algebraic groups**

General Properties

Let S- be a non-empty set and * (star) be an operation on S. The operation on the set is a rule, which assigns to each ordered pair of elements of the set, a unique element of S.

Closure Property

Consider a binary operation, . The operation * is said to be closed, if for all $\forall a, b \in S, a * b \in S$.

The new element also belongs to S.

Example : A set of integers Z is closed with respect to the binary operations, namely, addition, multiplication and subtraction but not with respect to division.

$$\forall a, b \in Z, (a \pm b) \in S, (a \bullet b) \in Z, (a / b) \notin Z.$$

Example: The set of odd integers is not closed with respect to addition, since sum of two odd integers is an even, which is not the member of the set.

Associative Property

Consider a binary operation *.

For any $\forall a, b, c \in S : (a * b) * c = a * (b * c)$

Example The addition (+) and multiplication (.) are Associative in the following sets .

N = The set of natural numbers, I or Z = The set of Integers, Q = The set of Rational, R = The set of real, C = The set of Complex numbers.

(a+b) + c = a+ (b+c) , (a.b) . c = a. (b.c)

Existence of Identity Element

If there exists an element $e \in s$

Such that for all $x \in s$

$$x * e = e * x = x$$

Then the $e \in s$ *is said to be the identity element of X*

For example : 0 and 1 are the identity elements of Z with respect to the operations of addition and multiplication respectively.

Existence of Inverse:

Consider an element $a \in s$. The element a^{-1} , is called the inverse of a under the operation * .such that

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

Groups

Let G – be a non-empty set and $*$ be a binary operation on G. Then G- is called a group under the operation $*$ if the following properties hold good.

- Closure Property:
- Associative Property:
- Existence of Identity element:
- Existence of Inverse element:
- In addition to the foresaid four properties, if the group satisfies the commutative property, then the group $(G,*)$ is called commutative group or **abelian group**.

Example : Show that the four matrices $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

forms a group under matrix multiplication.

Now G = {I,A,B,C}

Proof: IA = AI= A, IB =BI= B, IC= CI = C. I is Identity matrix.

Closure Property holds good.

It can be shown that BA=C, AC=B, BC = A, AA=I, BB=I, CC=I by virtue of matrix multiplications.

The composition operation is given in the following group table.

Composition operation.

.	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

1. The entries in the table are the same as the elements of set G. The closure property is satisfied.
2. Associative axiom. $A(BC) = A(A) = I$, $(AB)C = C(C) = I$. Associative property is satisfied.
3. Identity axiom: I is the identity element.
4. Inverse axiom: Every element of G has an inverse. Inverses of I, A, B, C are respectively I, A, B, C.

Hence G – is a group under multiplication

Semi-groups

Let S- be a nonempty set and is a binary operation on S, then

the algebraic system (S,*) is called a semi-group , if the Following conditions are satisfied:

1) S is closed with respect to the binary operation *.
2) S is associative with respect to the binary operation *.

Example:-

The set of +ve integers under the operation '+' is a Semi-group

Monoid: If a semi- group (M,*) has an identity element with respect to the operation *, then (M,*) is called a monoid. The algebraic system is called a monoid.

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

$$\forall e \in M, a*e = e*a = a$$

The set of positive even numbers is a semi-group with respect to the binary operation addition and Multiplication.

Example: The set of negative integers is not a semi-group. Hence, the operation - is closed in Z. But the operation is not associative.

Consider a = -2 , b = -5, and c = -6

(-2-(-5)) –(- 6) = 3 + 6 = 9 which is not the element of Z

-2-(-5 –(- 6)) = -2 - (1) = -3,

Example : The set of natural numbers N ={ 1,2,3,---} is a semi-group under the operation addition, but not a monoid, since the identity element does not exists i.e., $0 \notin N$.

Homomorphisms

Homomorphism is derived from the Greek word “ homoiosorphe”, (meaning similar form), is defined as a special correspondence between
the members (elements) of two algebraic systems, such as two groups,
two rings, or two fields.
Two homomorphic systems have the same basic structure, and, while their elements and operations may appear entirely different.

Sub Group:
A non-empty subset *‘H’* of a group *‘G’* is said to be subgroup of *‘G’* if *‘H’* itself is a group under the binary composition of G.

Definition : Let (G,*) and(H,*) be the group and its subgroup then the function $f : G \longrightarrow H$ is a ***homomorphism*** and the following relation holds,

$$f(x \circ y) = f(x) * f(y) \; \forall x, y \in G$$

A homomorphism is an **isomorphism** if it is bijective equivalently.

If G and H are groups, G and H are **isomorphic** if there is an isomorphism.

$f : G \longrightarrow H$. Isomorphic groups are the same as groups.

Example: Consider logs and exponentials, $\exp : (R, +) \rightarrow (R^+, \bullet)$, is a homomorphism from the real set under addition to the positive real set under multiplication. The operation on the domain R is addition, while the operation on the range is multiplication. Therefore, we can show that exp is a homomorphism,

$$\exp(x + y) = \exp(x).\exp(y) \quad \forall x, y \in R$$

But $\exp(x + y) = e^{x+y}$ and $\exp(x).\exp(y) = e^x e^y$,

If f: G→G' is a homomorphism, then the following are satisfied:

a) f(e) = e', where e is the identity of G and e' is the identity of G'

b) $f(a^{-1}) = (f(a))^{-1}$ for all a belongs to G

c) $f(a^n) = (f(a))^n$ where n is an integer

hence from identity $e^{x+y} = e^x e^y$ exp is a homomorphism.

Applications of group theory

Application of group theory is widespread. Galois theory uses groups to describe the symmetries of the roots of a polynomial. The fundamental theorem of Galois theory provides a link between algebraic field extensions and group theory. It gives an effective criterion for the solvability of polynomial equations in terms of the corresponding Galois group. For example, S, the symmetric group in 5 elements, is not solvable, which implies that the general equation of degree (n>5) cannot be solved by radicals as done in case lower orders. The theory, being one of the historical roots of group theory, is still fruitfully applied to yield new results in areas such as class field theory.

The concept of the Lie group, named after mathematician Sophus Lie, is important in the study of differential equations and manifolds. These describe the symmetries of continuous geometric and analytical structures.

In physics, groups are important because they describe the symmetries which the laws of physics seem to obey. According to Noethers's theorem, every symmetry of a physical system corresponds to a conservation law of the system.

Summary

- Modern group theory is a research area in mathematics. Groups are algebraic systems that find applications in coding theory. Cryptography is an active research area in the Internet era, where secured transmission of information is a challenge.
- Haar measures, that is integrals invariant under the translation in a Lie group, are used for pattern recognition and other image processing techniques. In material science, groups are used to classify crystal structures, regular polyhedral, and the symmetry of molecules.