Group Theory

Subject: Discrete Structures

Subject Code: MCA-201

Dr. Hitesh Kumar Ranote
Assistant Professor
School of Basic and Applied Science

Introduction

- Group theory is the study of algebraic structures called groups, which play a fundamental role in mathematics and its applications.

Definition

A non empty set G, together with a binary composition * (star) is said to form a group, if it satisfies the following postulates:

- Closure: If a, b ∈ G, then a * b ∈ G
- Associativity: (a * b) * c = a * (b * c)
- Identity: There exists an e such that a * e = a
- Inverse: Every element has an inverse a^{-1} such that $a * a^{-1} = e$

Examples

1. Set of integers is a group under addition (Z, +) but under multiplication it is not a group.

2. Set if nonzero real numbers under multiplication (R*, ×) is a group.

3. Set of natural numbers under addition is not a group because it does not satisfy existance of identity.

Types of Groups

Abelian Groups: A group G is called abelian (Commutative) group if a * b= b * a. Otherwise it is called non-abelian groups (non-commutative).

- Examples: General Linear group is non-abelian group.

Finite Group: If the set G is finite (i.e., has finite number of elements) it is called a finite group otherwise, it is called an infinite group.

Subgroups

- A subset H of a group G is called a subgroup if H itself forms a group under the same operation.
- If G is a group with identity element e then the subsets {e} and G are trivially subgroups of G and we call them the trivial subgroups. All other subgroups will be called non-trivial (or proper subgroups).

Examples

1. Set of even integers form a subgroup of (Z, +), which is a subgroup of (Q, +) which is a subgroup of (R, +).
2. The subset {1, -1} will be a subgroup of G = {1, -1, i, -i} under multiplication.

Cyclic Groups

- A group G is cyclic if there exists an element a in G such that every element of G can be written as a^n for some integer n. It is denoted by G = <a>.
- a is called the generator of the group
- Every subgroup of a cyclic group is cyclic

Examples

1. Additive Group of Integers: (Z, +) is cyclic with generator 1.

2. Multiplicative Group of Integers Modulo n: (Z/nZ, +) is cyclic.

3. Unit Circle Group: Complex roots of unity form a cyclic group.

4. Permutation Groups: Certain groups of permutations are cyclic.

Normal Subgroups

- A subgroup N of a group G is called a normal subgroup if gN = Ng for all g in G.
- Alternatively, N is normal if for every g in G and n in N, $gng^{-1} \in N$.
- The normal subgroup is denoted by $N \lhd G$.

Properties of Normal Subgroups

1. Every subgroup of an abelian group is normal.

2. The kernel of a group homomorphism is always a normal subgroup.

3. The intersection of two normal subgroups is also normal.

4. If N and M are normal subgroups of G, then their product NM is also normal.

5. Normal subgroups are the building blocks for quotient groups.

Examples of Normal Subgroups

1. The center Z(G) of a group G is always normal.

2. The subgroup of scalar matrices in GL(n, R) is normal.

3. In the symmetric group S3, the alternating group A3 is a normal subgroup.

Applications of Group Theory

1. Cryptography
2. Quantum mechanics
3. Coding theory
4. Chemistry and physics

Conclusion

- Group theory is a fundamental area of mathematics with widespread applications in science, engineering, and technology.