BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India

Programme : M. Sc. Mathematics

Course Title : ALGEBRA - I

Course Code : 24S2M05CC

UNIT - I

BASIC GROUP THEORY

Dr. C. Durairajan

Professor

Department of Mathematics

Definition of Group

- A binary operation $\star$ on a set G is a function $\star : G \times G \to G$.
- A nonempty set G together with a binary operation $\star$ is said to be a **Group** if
  - $\star$ is associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
  - there is an identity element $e \in G$ such that $e * g = g = g * e$ for all $g \in G$.
  - for every element $a \in G$, there is an element $b \in G$ such that $a * b = e = b * a$.

Examples of Groups

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition but $\mathbb{N}$ is not a group under addition and multiplication because inverse element does not exist for all elements for addition but multiplication except 1.
2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ under multiplication.
3. $\frac{\mathbb{Z}}{n\mathbb{Z}}$ under addition.
4. $\frac{\mathbb{Z}}{n\mathbb{Z}}^* = \{a \in \frac{\mathbb{Z}}{n\mathbb{Z}} \mid a \,\text{is relatively prime to}\, n\}$ under multiplication.
5. The set $\mathbb{Z}_n$ of all integers modulo n form a group under addition modulo n.
6. The set $M_n(\mathbb{F})$ of all $n \times n$ matrices over a field $\mathbb{F}$ under matrix addition.
7. General linear groups $GL_n(\mathbb{F})$
8. Dihedral groups D_{2n}.
9. Symmetric groups S_n.

Abelian Group and Some Properties of Groups

A group G is said to an **abelian group** if it satisfies the commutative property.

In the above Examples, 1 to 6 are abelian groups and others are nonabelian groups.

Properties Let G be a group. Then

- the identity element in G is unique. We denote this element by e.
- for every $g \in G$, its inverse g^{-1} is unique.
- for any $x, y \in G$, $(x^{-1})^{-1} = x$ and $(xy)^{-1} = y^{-1}x^{-1}$.
- the cancellation laws are true;

  For any $a, b, c \in G$, $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$.

Finite Groups; Subgroups

- The order of G, denoted $|G|$, is the number of elements in G.
- The least positive integer n such that $x^n = e$ is called the**order of x.** If such n does not exist, then the order of x is infinite order.
- For any positive integer n, there exists a group of order n. This group is $(\mathbb{Z}_n, \oplus_n)$.
- $|\mathbb{Z}_{10}| = 10$. In $\mathbb{Z}_{10}$, $|5| = 2$.
- A subset H of a group G is said to be a subgroup of G if H itself is a group under the operation of G.
- Let G be a group. If $H \subseteq G$, then $ab^{-1} \in H$ for all $a, b \in H$ iff H is a subgroup of G.

Examples

- Finite subgroup test: Let $H \subseteq G$ is finite. If H is closed under the operation of G, then H is a subgroup of G.
- Examples of Subgroups:
  - $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ for any integer n.
  - Let G be a group and let $a \in G$. Then $< a >= \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G. This subgroup is called cyclic subgroup generated by a.
  - Center of G: $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$ is a subgroup of G.
  - Centralizer of a in G: $C(a) = \{g \in G | ga = ag\}$ is a subgroup of G. This is also know as normalizer of a.

Normal Subgroups

- **Coset of H in G**

  Let H be a subgroup of a group G, then the set

  $aH = \{ah \mid h \in H\}$ is called a **left coset of H in G**.

- Properties of Cosets

  For $a, b \in G$,

  - $a \in aH$.
  - $aH = bH \Leftrightarrow a^{-1}b \in H$.
  - aH is a subgroup of $G \Leftrightarrow a \in H$.
  - $aH = bH$ or $aH \cap bH = \emptyset$.

- A subgroup H of G is said to be a **normal subgroup** if

  $aH = Ha$ for all $a \in G$.

Continue ...

- If H is a normal subgroup of a group G, then the collection $\frac{G}{H} = \{aH \mid a \in G\}$ of all cosets of H in G from a group under the operation defined by $aHbH = abH$ for all $aH, bH \in \frac{G}{H}$. This group is called a **factor group of G or quotient group of G.**
- If a subgroup H of a group G is a normal subgroup, then the following conditions are equivalent
    1. $ghg^{-1} \in H$ for all $g \in G, h \in H$.
    2. $gHg^{-1} = H$ for all $g \in G$.
    3. $gH = Hg$ for all $g \in G$. That is every right coset of H is a left coset.
    4. H is the kernel of a homomorphism of G to some other group

- **Lagrange's Theorem**

  If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

- Note that the converse of Lagrange's theorem need not be true. For example the group A_4 of order 12 has no subgroup of order 6. But the coverse of this theorem is true for any finite abelian group.

- If G is a finite group and H is a subgroup of G, then the number of cosets of H in G is $\frac{\#(G)}{\#(H)}$. That is, $\#(\frac{G}{H}) = \frac{\#(G)}{\#(H)}$.

- If G is a finite group, then $a^{\#(G)} = e$ for all $a \in G$ and hence the order of each element of the group divides the order of the group.

- **Orbit-Stabilizer Theorem**

  Let G be a finite group of Permutations of a set S. Then, for any $i \in S, \#(G) = \#(orb_G(i))\#(stab_G(i))$ where $orb_G(i) = \{\phi(i)|\phi \in G\}$ and $stab_G(i) = \{\phi \in G|\phi(i) = i\}$.

- In a group G, there is an element a in G such that $G = \{a^n|n \in \mathbb{Z}\}$. Then G is called a **cyclic group** and a **is called a generator of** G.

- If G is an infinite cyclic group, then there are exactly two generators.

- If G is a finite group of order n, then there are $\phi(n)$, the Euler ϕ-function, generators where $\phi(n) = \#\{i \mid (i, n) = 1\&1 \leq i < n\}$.

- Note that if a is a generator of a cyclic group, then its inverse is also a generator.
- $1, 3, 5, 7$ in $\mathbb{Z}_8$ are generators of $\mathbb{Z}_8$.
  That is, $\mathbb{Z}_8 =< 1 >=< 3 >=< 5 >=< 7 >$
- Let G be a cyclic group generated by a. Then
  1. every cyclic group is an abelian group.
  2. every subgroup of a cyclic group is cyclic
  3. if G is a cyclic group of order n generated by a, then for every positive divisor k of n, there is a unique subgroup of order k. In fact, the k order subgroup of G is $\langle a^m \rangle$ where $\frac{n}{k}$.

%subsectionPermutation Groups

- Permutation group of a set S

  A set of all bijective functions from S into S forms a group under composition of function. Its elements are called Permutations. This permutation group is denoted as $A(S)$.
- If $\#S = n$, then there are $n!$ bijections from S into S. The $A(S)$ is denoted as S_n.

Example

Let $S = \{x_1, x_2, x_3, x_4, x_5\}$, then a bijective function

$$x_1 \longmapsto x_3; x_2 \longmapsto x_4; x_3 \longmapsto x_1; x_4 \longmapsto x_5; x_5 \longmapsto x_2;$$

can be written as a product of cycles $(x_1, x_3)(x_2, x_4, x_5)$.

Continue ...

- Two cycles $(x_1, x_2, \cdots, x_r)$ and $(y_1, y_2, \cdots, y_s)$ are distinct if there is a map $a \longmapsto b$ in $(x_1, x_2, \cdots, x_r)$ but not in $(y_1, y_2, \cdots, y_s)$.
- Every permutation can be written as a cycle or a product of disjoint cycles.
- A cycle $(a_1, \ldots, a_m)$ is called a cycle of length m or m-cycle. For example, $(1, 2, 4)$ is a 3-cycle S_4.
- A cycle of length 2 is called a transposition.
- Every cycle can be written as a product of transpositions and hence every permutation can be written as a product of transpositions.

Continue ...

Example

$$(x_1, x_2, \cdots, x_r) = (x_1, x_2)(x_1, x_3)(x_1, x_4) \cdots (x_1, x_r)$$

- A permutation is said to be even(odd) if it can be written as a product of even(odd) number of transpositions.
- The order of a Permutation of a finite set is the least common multiple of the lengths of its disjoint cycle.

REFERENCES

- M. Artin, **Algebra**, Prentice Hall of India, New Delhi, 1994.
- David S. Dummit and Richard M. Foote,**Abstract Algebra**, 2nd Edition, Wiley Student Edition, 2008.
- I. N. Herstein, **Topics in Algebra**, John Wiley, 2nd Edition, 1975.
- Joseph Gallian, **Contemporary Abstract Algebra** , 9th Edition
- C. Lanski, **Concepts in Abstract Algebra**, AMS Indian edition, 2010.
- Serge Lang, **Algebra** - Revised third edition, Springer, Verlag - 2002.
- R. Solomon, **Abstract Algebra**, AMS Indian edition, 2010.
- John B. Fraleigh, **A First course in Abstract Algebra**, Narosa Publishing House, 2003.