GROUP THEORY
COURSE-BCA
Subject- Discrete Mathematics
Unit-I
RAI UNIVERSITY, AHMEDABAD

GROUP THEORY

❖ Binary Operations:

A binary operation $f(x, y)$is an operation that applies to two quantities or expressions $x$and y.

A binary operation on a nonempty set A is a map $f: A \times A \rightarrow A$ such that

1. f is defined for every pair of elements in A, and

2. f uniquely associates each pair of elements in A to some element of A.

Examples of binary operation on A from $A \times A$ to A include addition $(+)$, subtraction $(-)$, multiplication $(\times)$ and division $(\div)$.

❖ Group:

If G is a nonempty set, a *binary operation* μ on G is a function μ: G × G → G.

For example:

- + is a binary operation defined on the integers Z. Instead of writing +(3, 5) = 8 we instead write 3 + 5 = 8. Indeed the binary operation μ is usually thought of as *multiplication* and instead of μ (a, b).
- we use notation such as ab, a +b, a ∘ b and a ∗ b. If the set G is a finite set of n elements we can present the binary operation, say ∗ , by an n by n array called the *multiplication table*. If a, b ∈ G, then the (a, b)–entry of this table is a ∗ b.

Here is an example of a multiplication table for a binary operation ∗ on the set G = {a, b, c, d}.

∗	a	b	c	d
a	a	b	c	a
b	a	c	d	d
c	a	b	d	c
d	d	a	c	b

Note that $(a * b) * c = b * c = d$ but $a * (b * c) = a * d = a$.

<u>Example 1</u>: The set of complex numbers G = {1, i, −1, −i} under multiplication. Draw the multiplication table for this group.

<u>Solution</u>:

∗	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

<u>Note</u>:

1. A *binary operation* ∗ on set G is *associative* if $(a * b) * c = a * (b * c)$, for all a, b, c ∈ G.
2. *If* G *is a group and* a ∈ G*, then* $a * a = a$ *implies* $a = e$.
3. Let G be a group. The unique element e ∈ G satisfying $e * a = a$ for all a ∈ G is called the **identity** for the group G.
   If a ∈ G, the unique element b ∈ G such that $b * a = e$ is called the **inverse** of a and we denote it by $b = a^{-1}$

❖ **<u>Abelian Group</u>:**
A group G is abelian if $a * b = b * a$ for all elements a, b ∈ G.

❖ **<u>Subgroup</u>:**
A nonempty subset S of the group G is a *subgroup* of G if S a group under binary operation of G. We use the notation $S \leq G$ to indicate that S is a subgroup of G.

- If S is a subgroup then 1 is the identity for G and also for S.

❖ **<u>Statement of some important theorems</u>:**

<u>Theorem1</u>: A subset S of the group G is a subgroup of G if and only if

(i) $1 \in S$;
(ii) $a \in S \Rightarrow a^{-1} \in S$;
(iii) $a, b \in S \Rightarrow ab \in S$.

Theorem 2: If S is a subset of the group G, then S is a subgroup of G if and only if S is nonempty and whenever a, b $\in$S, then ab^{-1} $\in$S.
Theorem 3: If S is a subset of the finite group G, then S is a subgroup of G if and only if S is nonempty and whenever a, b $\in$S, then ab $\in$S.

For example:

1. If a is an element of the group G, then
   $$\langle a\rangle = \{. . . , a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, a^4, . . .\}$$
   are all the powers of a. This is a subgroup.

2. Both {1} and G are subgroups of the group G. Any other subgroup is said to be a proper subgroup.
   The subgroup {1} consisting of the identity alone is often called the trivial subgroup.

- **Order of a Group:**

The number of elements in the finite group G is called the order of G and is denoted by |G|.

Note:

1. If x ∈ G and G is finite, the order of x is |x| = $|\langle x\rangle|$.
2. If x ∈ G and G is finite, then |x| divides |G|.

- **Lagrange's Theorem: (without proof)**

If S is a subgroup of the finite group G, then
$$|G : S| = \frac{|G|}{|S|}$$
Thus the order of S divides the order of G.

- **Cyclic Group:**

Among the first mathematics algorithms we learn is the division algorithm for integers. It says given an integer m and an positive integer divisor d there exists a quotient q and a remainder r < d such that
$$\frac{m}{d} = q + \frac{r}{d}$$

- **Some important theorem:**

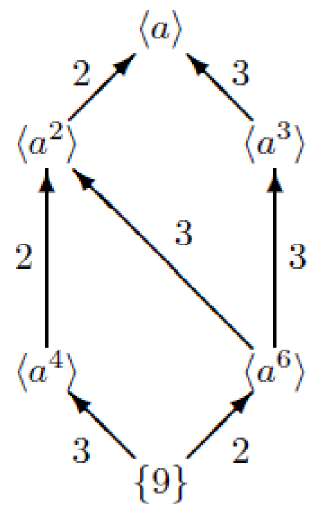
Theorem1: Given integers m and d > 0, there are uniquely determined integers d and r satisfying

$$m = dq + r \quad \text{and} \quad 0 \leq r < d$$

Theorem 2: Every subgroup of a cyclic group is cyclic.

❖ **For example:**

The subgroup lattice of the cyclic group G = $\langle a \rangle$ of order 12 is



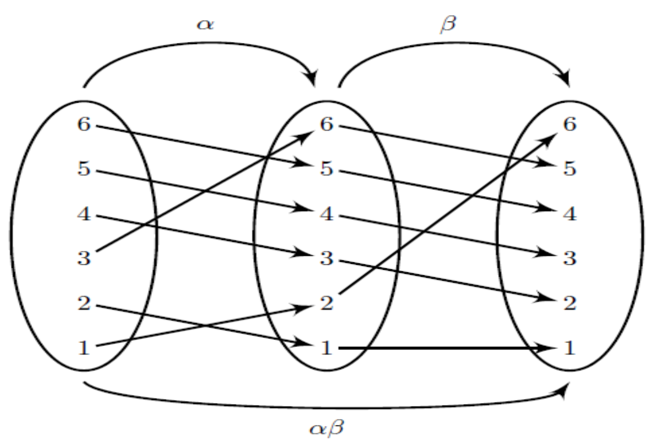
❖ **Permutation group:**

The product of two permutations α and β is function composition read from left to right. Thus

$$x^{\alpha\beta} = (x^{\alpha})^{\beta}$$

For example:

(1, 2, 3, 4)(5, 6) (1, 2, 3, 4, 5) = (1, 3, 5, 6)(2, 4)



The product of permutations α and β.

Note:

1. A permutation β of the form (a, b) is called a transposition.
2. Every permutation can be written as the product of transposition.

❖ **Exercise:**

1. The set of matrices
$$G = \left\{ e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$
under matrix multiplication. Draw multiplication table for this group.
2. Let G be a group in which the square of every element is the identity. Show that G is abelian.
3. Prove that a group G is abelian if and only if f : G → G defined by f(x) = X^{-1} is a homomorphism.
4. Write the permutation that results from the product

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 2 & 4 & 1 & 6 & 5 & 8 & 9 & 7 & 10 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 6 & 4 & 11 & 9 & 7 & 8 & 10 & 5 & 2 & 1 \end{pmatrix}$$

in cycle notation.

5. If S and T are subgroups of the group G, then S ∩ T is a subgroup of G.

6. Draw the subgroup lattice for a cyclic group of order 30.

7. If G/Z(G) is cyclic, then G is abelian.

❖ **Reference Book:**

1. **http://www.math.mtu.edu/~kreher/ABOUTME/syllabus/GTN.pdf**