Group Theory Notes

Subgroup, Generator of a Group, Cyclic Group and Properties

1. Subgroup
Let (G, *) be a group. A non-empty subset H of G is called a **subgroup** of G if H itself forms a group under the operation * defined on G.

Subgroup Test (Necessary and Sufficient Condition):
A non-empty subset H of a group G is a subgroup if:
1. For all a, b in H, a * b is in H (closure).
2. For every a in H, a^{-1} is in H (existence of inverse).
Equivalently, H is a subgroup if for all a, b in H, a * b^{-1} is in H.

Examples of Subgroup:
1. Z is a group under addition. The set 2Z = {…, -4, -2, 0, 2, 4, …} is a subgroup of Z.
2. In the group (R, +), the set of integers Z is a subgroup.
3. In any group G, the trivial subgroup {e} and G itself are subgroups.

2. Generator of a Group

Let G be a group and a be an element of G. The **generator** of G is an element such that every element of G can be written as a power of a (or multiple in additive notation).

The set generated by a is denoted by **<a>** and is defined as:
<a> = { a■ | n ∈ Z } (multiplicative group)
or <a> = { na | n ∈ Z } (additive group).

Examples:
1. In the group (Z, +), the element 1 is a generator since every integer can be written as n×1.
2. In the group {1, -1} under multiplication, -1 is a generator.

3. Cyclic Group

A group G is called a **cyclic group** if there exists an element a in G such that G = <a>. Such an element a is called a generator of G.

Examples of Cyclic Groups:
1. (Z, +) is a cyclic group generated by 1 or -1.
2. The group {1, i, -1, -i} under multiplication is cyclic, generated by i.
3. Z■ = {0, 1, 2, …, n-1} under addition modulo n is a cyclic group.

4. Properties of Cyclic Groups

1. Every cyclic group is abelian (commutative).
2. Every subgroup of a cyclic group is cyclic.
3. A cyclic group of order n has exactly one subgroup of order d for every positive divisor d of n.
4. If G = <a> and |G| = n, then a■ = e, where e is the identity element.

Finite and Infinite Cyclic Groups:

1. (Z, +) is an infinite cyclic group.
2. Z■ under addition modulo n is a finite cyclic group of order n.

Important Note:

Cyclic groups play a fundamental role in group theory and are often used to understand the structure of more complex groups.