Group Theory

Contents

Order of a Group

- The number of elements in a finite group G is called the order of the group G.
- It is denoted as $o(G)$.
- An infinite group is a group of infinite order.

$\boxed{|G| = n}$

Examples

- The set Z of integers is an infinite group with respect to the addition operation.
- Let $G = \{1, -1\}$, then G is an abelian group of order 2 with respect to multiplication.

Order of an element of a group

- Let G be a group under multiplication. Let e be the identity element in G.
- Suppose, a is any element in G, then the smallest positive integer m if exist, such that $a^m = e$, is said to be order of the element a.
- It is represented as $o(a) = m$.
- In case, where, such a positive integer does not exist, then order of the element a is infinite.

Example

- Consider a multiplicative group $G = \{1, \ i, -1, -i\}$. Find order of its elements.

Subgroup

- A non empty subset H of group $(G,*)$ is said to be subgroup of G, if $(H,*)$ is itself a group.

Example

- $(\{1,-1\},\times)$ is a subgroup of $(\{1,I,-1,-i\},\ \times)$.

Lagrange's Theorem

- If G is a finite group and H is a subgroup of G, then order of H, $i.e.$ $|H|$ divides the order of group , i.e. $|G|$.

- Converse of the Lagrange's Theorem is not true.

Cyclic Group

- A group G is cyclic if it is generated by a single element, which is denoted by G = $< a >$. A cyclic group of n elements may be denoted by C_n.

- A finite cyclic group generated by a can be written (multiplicatively) as:

$$\{e, a, a^2, \ldots, a^{n-1}\} \; with \;\; a^n = e$$

- A finite cyclic group generated by a can be written (additively) as:

$$\{e, a, 2a, \ldots, (n-1)a\} \; with \;\; na = e.$$


Thank you !!! ...