Group Theory : Some Fundamentals

Sumit Kumar Adhya

Summer of Science
MnP Club
IIT Bombay

July 2024

Overview

Groups

Definition

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

1. Associativity: a * (b * c) = (a * b) * c, for all a, b, c.
2. Existence of Identity: ∃ an element e ∈ G, s.t., a * e = e * a = a for all a (e is then called identity).
3. Existence of Inverse: For every a ∈ G, ∃ a' ∈ G s.t., a * a' = a' * a = e (a' is then called inverse of a)

Definition

Order of a group G: no. of elements in G, denoted by o(G) or $|G|$. It can be either finite or infinite.

Abelian Groups

Example

The group of real numbers under addition as $a+(b+c)=(a+b)+c$, $a+0=0+a=a$ and $a+(-a)=(-a)+a=0$ where $a,b,c\in\mathbb{R}$ and 0 is the identity and inverse of a being (-a)

Definition

If a*b = b*a ∀ a,b ∈ G. Then G is said to be an abelian group.

Example

The previous example is an abelian group as $a+b=b+a$ for $a,b\in\mathbb{R}$

Theorem

In a group G, the properties hold true:

1. *Identity element e is unique.*
2. *Inverse of each a is unique.*
3. $(a^{-1})^{-1}=a \ \forall \ a \in G$
4. $(ab)^{-1} = b^{-1}a^{-1}$
5. *Cancellation laws:* $ab=ac \implies b=c$ *and* $ba=ca \implies b=c \ \forall \ a,b,c \in G$.

Proof

Proof.

1. Let there be two identities e and e' in a group G. Then since e is an identity, $ee' = e'e = e'$ and since e' is an identity, $e'e = ee' = e$. So, $e = e'$
2. Let there be two inverses a' and a'' of a. Then $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$
3. Since, a^{-1} is inverse of a, $aa^{-1} = a^{-1}a = e$ which also implies a is inverse of a^{-1}. So, $(a^{-1})^{-1} = a$
4. $ab(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1} = [a(bb^{-1})]a^{-1} = (ae)a^{-1} = e$. Similarly, $(b^{-1}a^{-1})ab = e$ and the result follows
5. Let $ab = ac$, then $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = ec = c$

□

Subgroups

Definition

Let H be a non-empty subset of a group G, then it's a subgroup of G if it forms a group under the binary composition of G.

Theorem

A non-empty subset H of a group G is a subgroup of G iff:

1. $a, b \in H \implies ab \in H.$
2. $a \in H \implies a^{-1} \in H$

Proof.

From (i), closure property is satisfied and as $H \subseteq G$, associative property would be satisfied in H as well. From (ii), the inverse exists and from (i) and (ii), $aa^{-1} \in H$ and so $e \in H$ □

Subgroups

Theorem

A non-empty subset H of a group G is a subgroup of G iff $a,b \in H \implies ab^{-1} \in H$.

Proof.

$aa^{-1} \in H \implies e \in H$. Now as $e, a \in H$, $ea^{-1} = a^{-1} \in H$. So the inverse exists. Finally for $a, b \in H \implies a, b^{-1} \in H \implies a(b^{-1})^{-1} \in H \implies ab \in H$. Now by the previous theorem, H is a subgroup of G. $\square$

Some more definitions

Definition

Centre of a group G: $Z(G) = \{x \in G \mid xg=gx \ \forall \ g \in G.\}$

Theorem (without proof)

Centre of a group G is a subgroup of G.

If $Z(G)=G \longleftrightarrow G$ is abelian.

Definition

Normalizer/Centralizer of a: $N(a) = \{x \in G \mid xa=ax\}$ for some $a \in G$.

Theorem (without proof)

Normalizer/Centralizer of a in G is a subgroup of G.

Some more definitions

Definition

Let H be a subgroup of G. For a,b $\in$ G, if $ab^{-1} \in H$, we say a is congruent to b mod H or a $\equiv$ b mod H

This relation is an equivalence relation. Corresponding to this, we therefore get equivalence classes. For any a $\in$ G, the equivalence class of a is cl(a)=$\{x \in G \mid x \equiv a \text{ mod } H\}$

Right and Left Cosets

Definition

Right or Left coset of H in G is Ha=$\{$ha | h $\in$ H $\}$ or aH=$\{$ah | h $\in$ H $\}$ respectively.

Theorem

Ha=cl(a) for any a $\in$ G. Therefore, Right cosets are equivalence classes.

Proof.

Let $x \in Ha$, then $x = ha$ for some $h \in H$. So, $xa^{-1} \in H \implies x \in cl(a) \implies Ha \subseteq cl(a)$. Again let $x \in cl(a) \implies x \equiv a \, mod \, H \implies xa^{-1} \in H \implies x = ha \in Ha$ for some $h \in H$. Thus $cl(a) \subseteq Ha$ and hence $Ha = cl(a)$ □

Right and Left Cosets

Two important properties of equivalence classes:

- Two equivalence classes are either identical or disjoint
- Union of all equivalence classes is the original set

From these two properties and the previous theorem we can conclude the following:

Theorem

Two right cosets in G are either equal or have no element in common and the union of all right cosets in G is equal to G.

Right and Left Cosets

Definition

The index of a subgroup H in G is the no. of distinct right(left) cosets of H in G, denoted by $i_G(H)$ or [G:H]

It is, of course possible for an infinite group G to have a subgroup H with finite index.

Example

G= $\langle Z, +\rangle$, H = {3n | n ∈ Z}. H has only 3 right cosets in G → H, H+1, H+2. So $i_G(H) = 3$

Cyclic Groups

Definition

Order of an element: o(a) or $|a|$ is the least positive integer n s.t $a^n = e$

Definition

Cyclic group:- A group G is defined to be a cyclic group if $\exists$ an element $a \in G$ s.t every element of G can be expressed as a power of a. In that case a is called the generator of G, denoted by $G = \langle a \rangle$ or (a).

Example

The group of integers under addition is a cyclic group, 1 and -1 being it's generators.

Example

The group $G = \{1, -1, i, -i\}$ under multiplication is cyclic as we can express it's members as i, i^2, i^3, i^4, so, i is it's generator.