Presentation

BASICS OF GROUP THEORY

by

Dr. Rajib Biswakarma

Silapathar- 787059
Assam, INDIA

22$^{\text{nd}}$ February, 2020

Content of Presentation

1. Set, Relation, Binary Operation, Algebraic Structure.
2. Groups and Subgroups.
3. Order of a Group Order of an element.
4. Some Important Properties and Examples of Group.
5. Related Theorems.

Set, Relation, Binary Operation, Algebraic Structure

Definition

A well defined collection of objects is called a set.

Well defined means no confusion occurres for inclusion and exclusion of an element.

Definition

Let A and B be two non-empty sets. Then any subset of $A \times B$ is called a relation. If $|A| = m$ and $|B| = n$ then $|A \times B| = m \times n$.

Definition

A relation $R \subseteq A \times A$ is called equivalence relation if R is reflexive, symmetric and transitive.

1. R is reflexive if $\forall a \in A$, $(a, a) \in R$.
2. R is called symmetric if $(a, b) \in R \Rightarrow (b, a) \in R$, $\forall a, b \in A$.
3. R is called transitive if $(a, b) \in R$ and $(b, c) \in R \Rightarrow (c, a) \in R$,

Set, Relation, Binary Operation, Algebraic Structure

Let A = Set of all lines in a plane.

1. R = {(l, m): l || m $\forall l, m \in A\}$ *is an equivalence relation.*
2. R = {(l, m): l $\perp m$ $\forall l, m \in A\}$ *is not an equivalence relation.*

Definition

If A is non-empty set and R be a relation defined on A and $a \in A$ then equivalence class of a i.e., $class(a) = [a] = \{x \in A : xRa\}$

Let $A = Z$, $aRb \Leftrightarrow 2|(a-b)$
$[0] = \{x \in A : 2|(x-0)\} = \{0, 2, -2, 4, -4, 6, -6, \ldots\}$
$[1] = \{x \in A : 2|(x-1)\} = \{1, -1, 3, -3, 5, -5, \ldots\}$
$[0] \cup [1] = A$

Set, Relation, Binary Operation, Algebraic Structure

Theorem

Let be an equivalence relation on non-empty set A, then for any $a, b \in A$

1. *cl(a)* $\neq \emptyset$.
2. *Either* $cl(a) \cap cl(b) = \emptyset$ *or* $cl(a) = cl(b)$.
3. *A* = $\cup_{a \in A} cl(a)$.

Definition

A binary operation on a non-empty set A is a function 'f' from $A \times A$ to A i.e., $f : A \times A \rightarrow A$. $\forall a, b \in A$, $f(a, b) = a * b = c \in A$

Definition

A non-empty set A with one or more binary operation is Algebraic structure. eg. $(N, +), (Z, +), (R, +, \times)$.

Groups and Subgroups

Definition

A system $(G, *)$, where G is a non-void set and $*$ is a binary composition in G, is called a Group if it satisfies the following postulates:

1. Associative Law: $a * (b * c) = (a * b) * c \; \forall \; a, b, c \in G$.

2. Existence of Identity: There exist an element $e \in G$ called an identity, such that $a * e = e * a = a \; \forall \; a \in G$.

3. Existence of Inverse: For each $a \in G$ there exist an element $a^{-1} \in G$, called an inverse, such that $a * a^{-1} = a^{-1} * a = e$.

If in addition to the above three postulates, the following postulate is also satisfied, the group is called a commutative or an *abelian group*.

1. Commutative Law: $a * b = b * a \; \forall \; a, b \in G$.

Groups and Subgroups

Example

$G = Q \setminus -1$ is a group under the composition defined by $a * b = a + b + ab, \forall a, b \in G$.

Definition

If H is a non-empty subset of a group G, then H is a subgroup of G if H is a group under the same operation as G.

Example

$H = (5Z, +)$ is a subgroup of a group $G = (Z, +)$.

Theorem

One step test for subgroup:

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

Order of a Group Order of an element

Definition

The number of elements in a group is called the order of the group. The order of a group G is denoted by $|G|$ or $o(G)$.

Definition

Let G be a group and let $a \in G$. Then a is said to be of finite order n if n is the least positive integer such that $a^n = e$, e is the identity of G. If $a^n \neq e$ for every $n \in N \Rightarrow O(a) = \infty$

Definition

A group G is said to be cyclic if $\exists$ an element $a \in G$ such that for every element of G is generated by a. and $G =< a >= \{a^n : n \in Z\}$. eg., $(Z_n, +_n)$ finite cyclic group, $(Z, +)$ infinite cyclic group.

Some Important Properties and Examples of Group

In a group G.

1. Identity element is unique.
2. Inverse of each $a \in G$ is unique.
3. $(a^{-1})^{-1} = a, \forall a \in G$.
4. $(ab)^{-1} = b^{-1}a^{-1}, \forall a, b \in G$.
5. $ab = ac \Rightarrow b = c, \forall a, b \in G$ (Left Cancellation Law).
6. $ba = ca \Rightarrow b = c, \forall a, b \in G$ (Right Cancellation Law).

Examples

Example

$K_4 = \{e, a, b, c\}$ is an abelian group under the composition defined by $a^2 = e, b^2 = e, c^2 = e$ and $ab = ba = c, ac = ca = b, bc = cb = a$ such that $o(K_4) = 4$. (K_4 is the smallest non-cyclic group).

Example

$D_n = \{< x, y >: x^2 = e, y^n = e, yx = xy^{-1}\}$ is known as dihedral group ($|D_n|$ is a non-abelian group for $n \geq 3$).
Group of Symmetries of a square is
$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

Example

Let $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is non-abelian, non-cyclic group under the composition defined by $i^2 = j^2 = k^2 = -1$ and $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$ such that $o(Q_8) = 8$. (Every proper subgroup of Q_8 is cyclic, abelian).

Related Theorems

Definition

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

Theorem

$Ha = \{x \in G : x \equiv a(\text{mod}H)\} = cl(a)$

Theorem

Lagrange's Theorem:
If G is a finite group and H is a subgroup of G then $o(H)|o(G)$.

Theorem

Converse of Lagrange's theorem for finite abelian group:
A finite abelian group G has a subgroup of order n for every divisor m of n.

Related Theorems

Definition

Let $(G, *)$ and (G', o) be any two group. A mapping $f : G \to G'$ is called Homomorphism if $f(a * b) = f(a) o f(b) \forall a, b \in G$. And if f is one-one and onto then f is called Isomorphism. $(G \cong G')$

Theorem

Any finite cyclic group G of order n is Isomorphic to Z_n i.e., $|G| = n \Rightarrow G \cong Z_n$

Theorem

Any infinite cyclic group G of order n is Isomorphic to $(Z, +)$.

Table of Contents

Surjit Singh, Qazi Zameeruddin, Modern Algebra, Vikas Publishing House Pvt Ltd.

$https://en.wikipedia.org/wiki/AbstractAlgebra$
(Accessed from Internet)