Group Theory

Assis. Prof. Dr Ali A Alabdali

2024-2025

Year 2

Lecture 1

Binary Operation

Definition

A **binary operation** $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, we will

denote the element $*\ (a, b)$ of S by $a * b$.

Examples

i. The addition + is a binary operation on the set $\mathbb{R}$**.** Our usual multiplication is a different binary

ii. operation on $\mathbb{R}$. In this example, we could replace $\mathbb{R}$ by any of the sets $\mathbb{C}$, $\mathbb{Z}$, $\mathbb{R}^+$ or $\mathbb{Z}^+$.

Groups

A pair $(G,*)$ where G is a non-empty set and '$*$` a binary operation in G is a group if and only if:

i. The binary operation $*$ closed, *i.e.*, $a * b = b * a, \forall a, b \in G$

ii. The binary operation $*$ is associative, i.e., $a * b * c = a * (b * c), \forall a, b, c \in G$

iii. There is an identity element $e \in G$ such that for all $a \in G, a * e = e * a = a$

iv. For each $a \in G$ there is an element $a' \in G$ such that $a * a' = a' * a = e$

- a' is called the inverse of a in G and is denoted by a^{-1}.

Properties of a Group:

Let G be a group, then following are the some important properties of G;

a) Cancelation law holds in G. That is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for all $a, b, c \in G$.

b) Identity element is unique.

c) Inverse of an element is unique.

d) $(a^{-1})^{-1} = a$, $\forall\ a \in G$.

- e) $(ab)^{-1} = b^{-1}a^{-1}$.

Semigroup And Monoid

A set with an associative binary operation is called a semigroup. A semigroup that has an identity element for the binary operation is called monoid.

Note that: every group is both a semigroup and a monoid.

Commutative Group

A group G is abelian if its binary operation is commutative. That is,let $(G, *)$ be a group. Let a, $b \in G$**,** then G is called an abelian group if and only if

$$a * b = b * a$$

Examples

a. The familiar additive properties of integers, rational, real and complex numbers show that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ under addition abelian groups.

b. The set $\mathbb{Z}^+$ under addition is not a group. There is no identity element for **+** in $\mathbb{Z}^+$.

c. The set $\mathbb{Z}^+$ under multiplication is not a group. There is an identity 1, but no inverse of 3.

Lecture 2

Example

Example Let $*$ be defined on $\mathbb{Q}^+$ by $a \ * \ b \ = \frac{ab}{2}$. Then $a * \ (b \ * \ c) = a * \frac{bc}{2} = \frac{abc}{4}$, and likewise $(a \ * \ b) * c \ = \frac{ab}{2} * c = \frac{abc}{4}$

SOLUTION Let $*$ defined on $\mathbb{Q}^+$ by $a * \ b \ = \frac{ab}{2}$

i. Closed property. For $a, b \in \mathbb{Q}^+$, we have $a * \ b \ = \frac{ab}{2}$. Thus, closed property holds.

ii. Associative property. For $a, b, c \in \mathbb{Q}^+$, $(a \ * \ b) * \ c \ = \frac{ab}{2} * c = \frac{abc}{2} \times \frac{1}{2} = \frac{abc}{4}$,

$a * \ (b \ * \ c) = a * \frac{bc}{2} = \frac{1}{2} \times \frac{abc}{2} = \frac{abc}{4}$.

Thus, associative law holds.

Following the solution

iii. Identity. Given that $a * b = \frac{ab}{2}$. Let $e \in \mathbb{Q}^{+}$, since $a * e = e * a = a$. Now $a * e = \frac{ae}{2}$

$\Rightarrow a * 2 = \frac{a \times 2}{2} = a$

Similarly, $\Rightarrow 2 * a = \frac{2 \times a}{2} = a$. Thus $e = 2$ is the identity element.

iv. Inverse. For $a \in \mathbb{Q}^{+}$, since $a * a' = a' * a = e$. By computing $a * a' = \frac{aa'}{2}, a * \frac{4}{a} = \frac{a \times 4}{2 \times a} = 2$

Similarly, $\frac{4}{a} * a = 2$

$a' = \frac{4}{a}$ is the inverse of a. Hence inverse of each element exists. Thus $(\mathbb{Q}^{+}, *)$ is a group.

Definitions

Order of a Group

The number of elements in a group $(G,*)$ is called the order of a group and is denoted by $|G|$.

Order of an element

Let a be any element of a group G. A non-zero positive integer n is called the order of a if $a^n = e$ and n is the least such integer, and e is the identity element of G.

Finite and Infinite Group

A group G is said to be finite if G consists of the finite number of elements. A group G is said to be an infinite group if G consists of the infinite number of elements.

Examples

i. Let $\mathbb{Z} \ = \{\ldots\ , -3, -2, -1, 0, +1, +2, +3, \ldots\ \}$ is a group under addition, then

$|Z| = \ \infty$ and for $2\ \in\ \mathbb{Z}$, $|2|\ =\ \infty$.

ii. Let $G\ \ = \{\ 1, -1, i, -i\}$, then $|G|\ =\ 4.$

Lecture 3

Subgroup

If a subset H of a group G is closed under the binary operation defined on G and if H with the induced operation of G is itself a group, then H is called a **subgroup** of G and is denoted by $H \preccurlyeq G$ or $G \succcurlyeq H$.

OR

A subset H of a group G is called a **subgroup** of G if and only if H is itself a group under the same binary operation defined on G.

Remark Every group G has a subgroup G itself and the identity $\{e\}$, where e is the identity element. The subgroups G and $\{e\}$ are called **trivial subgroups** of G. All other subgroups of G are called the **non-trivial (proper) subgroups** of G.

Examples

i. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}\ , +)$ and $(\mathbb{Q}\ , +)$ is a subgroup of $(\mathbb{R}\ , +)$.

ii. The set $\mathbb{Q}^{+}$ under multiplication is a subgroup of $\mathbb{R}\ ^{+}$under the algebraic operation multiplication.

Theorem

Theorem: A non-empty subset H of a group G is a subgroup of G if and only if for any pair of $a, b \in H$, $ab^{-1} \in H$; $a \neq b \neq e$.

Proof: Suppose that H is a subgroup of a group G, then $(H,*)$ is a group.

Therefore, if $b \in H$, $b^{-1} \in H \Rightarrow ab^{-1} \in H$ and $ab^{-1} \in H$ (closed property)

Conversely, suppose that for $a, b \in H$, $ab^{-1} \in H$.

To prove H is a subgroup, put $b = a \Rightarrow a, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$.

$\Rightarrow$ identity element exists.

Following the proof

Now , let $e, b \in H \Rightarrow e, b^{-1} \in H \Rightarrow eb^{-1} \in H \Rightarrow b^{-1} \in H$.

$\Rightarrow$ inverse of each element exists in H.

Again, let $a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow a(b^{-1})^{-1} \in H$

$\Rightarrow ab \in H$

Thus, H is closed under the induced algebraic operation. The associative law holds in H as it holds in G.

Therefore, H is a subgroup.

Theorem

Theorem: Prove that the intersection of family of subgroups of a group G is a subgroup of G.

Proof Let $\{H_\alpha\}_{\alpha \in I}$ be a family of subgroups of G. we have to show that $H = \bigcap_{\alpha \in I} H_\alpha$ is a subgroup of G.

Let $a, b \in H$, then $a, b \in H_\alpha$ for each $\alpha \in I$.

Since H_α is a subgroup of G, so $ab^{-1} \in H_\alpha$ for each $\alpha \in I$.

Therefore, $ab^{-1} \in \bigcap_{\alpha \in I} H_\alpha = H$

$\Rightarrow$ H is a subgroup of G. Hence the intersection of family of subgroups of G is a subgroup of G.

Lecture 4

Theorem

Theorem: The union $H \cup K$ of two subgroups H, K of a group G is a subgroup of G if and only if either $H \subseteq K \; or \; K \subseteq H$.

Proof: Suppose that either $H \subseteq K \; or \; K \subseteq H$. We have to show that $H \cup K$ is a subgroup of G.

Now, $H \cup K = H \because K \subseteq H, H \cup K = K \because H \subseteq K$

Thus $H \cup K$ is a subgroup of G as H, K are subgroups of G.

Conversely, suppose that $H \cup K$ is a subgroup of G. To prove either $H \subseteq K \; or \; K \subseteq H$, suppose on contrary that $H \nsubseteq K$, $K \nsubseteq H$

Let $a \in H \backslash K, b \in K \backslash H$. Since, $b \in H \cup K$, therefore $ab \in H \cup K \because H \cup K$ is a subgroup.

Following the proof

$\Rightarrow$either $ab \in H$ or $ab \in K$. Suppose that $b \in H$, then

$b = a^{-1}(ab) \in H \because H$ is a subgroup

Similarly, suppose $b \in K$, then

$a = (ab)b^{-1} \in K \because K$ is a subgroup

This is contradiction to our supposition so either $H \subseteq K$ or $K \subseteq H$.

Theorem

Theorem: Show that $\mathbb{Z}_P$ has no proper subgroup if P is a prime number.

Proof: As number of subgroups of $\mathbb{Z}_P$ is the same as the number of distinct divisors of P which are 1 and P itself.

Hence the number of distinct subgroups of $\mathbb{Z}_P$ are two 1 and $\mathbb{Z}_P$itself.

Thus, the number of proper subgroups is zero (no proper subgroups), as we can say that $\mathbb{Z}_P$ has no proper subgroups.

Lecture 5

Cyclic Group

A group G is said to be cyclic if and only if it is generated by a single element. i.e., a group G is cyclic if there is some element $a \in G$ that generates G. If G is finite cyclic group of order n, then

$$G =< a : a^n = e >.$$

If an element of G is the generator of G then its inverse is also the generator of G.

Examples

i. A group $G = \{ 1, -1, i, -i\}$ is cyclic group as $< i >$ is its generator.

ii. A group $\mathbb{Z}_5 = \{0,1,2,3,4\}$ under modulo addition is cyclic group. Since every element of $\mathbb{Z}_5$ is in the power of a single element that is 1. Therefore 1 is the generator of $\mathbb{Z}_5$.

iii. A set $\{1, -1\}$ is a cyclic group under multiplication.

Theorem

Theorem: Every cyclic group is commutative.

Proof: Let G be a cyclic group and let a be a generator of G.

Let $x\,, y\ \in\ G$, then there exist integers m and n such that

$$x\ =\ a^m\,, y\ =\ a^n$$

Now, $xy\ =\ a^m\, a^n\ = a^{m+n}\ = a^{n+m}\ =\ a^n a^m\ =\ yx$

So G is commutative.

Following the proof

Theorem: Every subgroup of a cyclic group is cyclic.

Proof: Let G be cyclic group generated by a. Let H be a subgroup of G and k be the least positive integer such that $a^k \in H$. We have to prove that H is generated by a^k .

For this, let $a^m \in H, \forall\, m > k$, then there exist integers q and r such that

$$m = kq + r, 0 \leq r \leq k$$

$$\Rightarrow a^m = a^{kq} + a^r$$

$$= (a^k)^q \,.\, a^r$$

$$\Rightarrow a^m = (a^k)^{-q} = a^r$$

Following the proof

Since $a^m$and$(a^k)^{-q}$ are in H. Therefore,$a^r \in H$. But since k is the smallest integer for which $a^k \in H$ and $r < k$, so $a^k \in H$ is possible only if $r = 0$. But if $r = 0$, then $m = qk$

$$\Rightarrow a^m = a^{kq}$$

$$\Rightarrow a^m = a^{kq} \in H$$

$\Rightarrow a^k$ is the generator of H.

Hence H is cyclic subgroup of G.