III SEM

amittyagiiitkgp

April 2024

1 Introduction

Group Definition:

A *group* G is a set together with a binary operation $*$ (often denoted as $(G, *)$) that satisfies the following properties:

1. **Closure:** For all $a, b \in G$, $a * b \in G$.
2. **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
3. **Identity Element:** There exists an element $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.
4. **Inverse Element:** For every $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$, where e is the identity element.

Example:
Consider the set of integers modulo 4, denoted as $Z_4 = \{0, 1, 2, 3\}$, with addition modulo 4 as the binary operation. We can verify that $(Z_4, +)$ forms a group:

1. **Closure:** For any $a, b \in Z_4$, $a + b \in Z_4$.
2. **Associativity:** Addition modulo 4 is associative.
3. **Identity Element:** The identity element is 0, as $a + 0 = 0 + a = a$ for all $a \in Z_4$.
4. **Inverse Element:** For each $a \in Z_4$, the inverse element a^{-1} such that $a + a^{-1} = 0$ is simply the negative of a modulo 4. For example, $1 + 3 = 0$, $2 + 2 = 0$, and $3 + 1 = 0$.

Therefore, $(Z_4, +)$ forms a group.
Example: Symmetric Group S_3
Consider the set S_3 of permutations of three elements, denoted $\{1, 2, 3\}$. Let's denote these permutations as:
The set $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ is a group under composition of permutations.
Properties of S_3:

1. **Closure:** The composition of any two permutations in S_3 results in another permutation in S_3.
2. **Associativity:** Composition of permutations is associative.
3. **Identity Element:** The identity permutation, σ_1, leaves all elements unchanged when composed with any other permutation.
4. **Inverse Element:** Each permutation in S_3 has an inverse within S_3. For example, σ_2 is its own inverse, σ_3 is its own inverse, σ_4 is its own inverse, σ_5 is its own inverse, and σ_6 is its own inverse.

Therefore, S_3 forms a group under composition of permutations.
Abelian Group Definition:
An Abelian group is a set G equipped with an operation $\cdot$ satisfying the following properties:

1. **Closure:** For all a, b in G, $a \cdot b$ is also in G.
2. **Associativity:** For all a, b, c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

3. **Identity Element:** There exists an element e in G such that for all a in G, $a \cdot e = e \cdot a = a$.

4. **Inverse Element:** For every element a in G, there exists an element b in G such that $a \cdot b = b \cdot a = e$, where e is the identity element.

5. **Commutativity:** For all a, b in G, $a \cdot b = b \cdot a$.

Example:
Consider the set of integers Z under addition. This set forms an Abelian group. Here's why:

1. **Closure:** For any integers a and b, $a + b$ is also an integer.

2. **Associativity:** For any integers a, b, and c, $(a + b) + c = a + (b + c)$.

3. **Identity Element:** The identity element for addition is 0, since $a + 0 = 0 + a = a$ for any integer a.

4. **Inverse Element:** For any integer a, its inverse under addition is $-a$, since $a + (-a) = (-a) + a = 0$.

5. **Commutativity:** For any integers a and b, $a + b = b + a$.

Therefore, the set of integers under addition forms an Abelian group.
General Properties of a Group:
A group is a set G equipped with a binary operation ($\cdot$ or simply juxtaposition) that satisfies the following properties:

1. **Closure:** For all a, b in G, $a \cdot b$ is also in G.

2. **Associativity:** For all a, b, c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

3. **Identity Element:** There exists an element e in G such that for all a in G, $e \cdot a = a \cdot e = a$.

4. **Inverse Element:** For every element a in G, there exists an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = e$, where e is the identity element.

If the group operation is commutative, i.e., $ab = ba$ for all a, b in G, the group is called an **Abelian group**.
Composition Table of a Group:
Consider a group G with elements e, a, b, and c, where e is the identity element. Here's the composition table for the group:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Each row and column represents an element of the group, and the entry at the intersection of row x and column y represents the result of combining x and y under the group operation.
Example:
Suppose this group represents the symmetries of a square. Here's what each element represents:

- e: Identity transformation (doing nothing).
- a: 90-degree clockwise rotation.
- b: Reflection about a vertical axis.
- c: Reflection about a horizontal axis.

For example, applying a followed by b results in c, which represents a reflection about a diagonal axis.
Similarly, applying b followed by c results in a, which represents a 90-degree clockwise rotation.

Composition Table of a Group:

Consider a group G with elements e, a, b, and c, where e is the identity element. Here's the composition table for the group:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Each row and column represents an element of the group, and the entry at the intersection of row x and column y represents the result of combining x and y under the group operation.

Example:

Suppose this group represents the symmetries of a square. Here's what each element represents:

- e: Identity transformation (doing nothing).
- a: 90-degree clockwise rotation.
- b: Reflection about a vertical axis.
- c: Reflection about a horizontal axis.

For example, applying a followed by b results in c, which represents a reflection about a diagonal axis.
Similarly, applying b followed by c results in a, which represents a 90-degree clockwise rotation.

Ring Definition:

A ring is a set R equipped with two binary operations, usually denoted as addition $(+)$ and multiplication $(\cdot)$, satisfying the following properties:

1. **Additive Closure:** For all a, b in R, $a + b$ is also in R.
2. **Additive Associativity:** For all a, b, c in R, $(a + b) + c = a + (b + c)$.
3. **Additive Identity:** There exists an element 0 in R such that for all a in R, $a + 0 = 0 + a = a$.
4. **Additive Inverse:** For every element a in R, there exists an element $-a$ in R such that $a+(-a) = (-a)+a = 0$.
5. **Multiplicative Closure:** For all a, b in R, $a \cdot b$ is also in R.
6. **Multiplicative Associativity:** For all a, b, c in R, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
7. **Distributivity:** Multiplication distributes over addition, i.e., for all a, b, c in R, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

A ring may or may not have a multiplicative identity element.

Examples:

1. **Integers** (Z): The set of integers with the usual addition and multiplication forms a ring.
2. **Polynomial Ring**: The set of all polynomials with coefficients in a ring R, denoted as $R[x]$, forms a ring.
3. **Matrix Ring**: The set of all $n \times n$ matrices with entries from a ring R, denoted as $M_n(R)$, forms a ring.

Examples of Rings with Solutions:

1. **Integers** (Z)**:**
   - **Addition:** $3 + 4 = 7$, $(-2) + 5 = 3$, etc.
   - **Multiplication:** $3 \times 4 = 12$, $(-2) \times 5 = -10$, etc.
2. **Polynomial Ring** $(R[x])$**:**

- Let $f(x) = x^2 - 2x + 1$ and $g(x) = 3x^2 + 2x - 5$.
- **Addition:** $f(x) + g(x) = (x^2 - 2x + 1) + (3x^2 + 2x - 5) = 4x^2 + 1$.
- **Multiplication:** $f(x) \cdot g(x) = (x^2 - 2x + 1)(3x^2 + 2x - 5) = 3x^4 - 4x^3 - 7x^2 + 8x - 5$.

3. **Matrix Ring ($M_2(R)$):**
   - Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & 0 \\ 2 & 5 \end{pmatrix}$.
   - **Addition:** $A + B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 5 & 9 \end{pmatrix}$.
   - **Multiplication:** This operation can be performed similarly.

Field Definition:

A field is a set F equipped with two binary operations, usually denoted as addition (+) and multiplication (·), satisfying the following properties:

1. **Additive Closure:** For all a, b in F, $a + b$ is also in F.
2. **Additive Associativity:** For all a, b, c in F, $(a + b) + c = a + (b + c)$.
3. **Additive Identity:** There exists an element 0 in F such that for all a in F, $a + 0 = 0 + a = a$.
4. **Additive Inverse:** For every element a in F, there exists an element $-a$ in F such that $a+(-a) = (-a)+a = 0$.
5. **Multiplicative Closure:** For all a, b in F, $a \cdot b$ is also in F.
6. **Multiplicative Associativity:** For all a, b, c in F, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
7. **Distributivity:** Multiplication distributes over addition, i.e., for all a, b, c in F, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.
8. **Multiplicative Identity:** There exists an element 1 in F such that for all a in F, $a \cdot 1 = 1 \cdot a = a$.
9. **Multiplicative Inverse:** For every nonzero element a in F, there exists an element a^{-1} in F such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Example:

The set of real numbers (R) with the usual addition and multiplication operations forms a field.

Homomorphisms of Rings:

A homomorphism between two rings $(R, +, \cdot)$ and $(S, \oplus, \odot)$ is a function $\phi : R \to S$ that preserves the ring structure, i.e., for all a, b in R, the following properties hold:

1. **Preservation of Addition:** $\phi(a + b) = \phi(a) \oplus \phi(b)$
2. **Preservation of Multiplication:** $\phi(a \cdot b) = \phi(a) \odot \phi(b)$
3. **Preservation of Identity:** If R has a multiplicative identity 1_R and S has a multiplicative identity 1_S, then $\phi(1_R) = 1_S$

A homomorphism $\phi : R \to S$ is called an isomorphism if it is bijective.

Example:

Consider the rings Z and Z_6 under addition and multiplication modulo 6, i.e., $Z_6 = \{0, 1, 2, 3, 4, 5\}$ with operations modulo 6.

Define the function $\phi : Z \to Z_6$ by $\phi(x) = x \mod 6$.

This function is a homomorphism because it preserves addition and multiplication modulo 6. For example:

$$\phi(3 + 4) = \phi(7) = 1 \oplus 1 = 2$$

$$\phi(3) \odot \phi(4) = 3 \odot 4 = 2$$

Also, $\phi(1) = 1$ since 1 is the multiplicative identity in both Z and Z_6.

Thus, ϕ is a homomorphism from Z to Z_6.

Example of Homomorphism:

Consider the rings $(Z, +, \cdot)$ and $(Z_2, \oplus, \odot)$, where Z is the set of integers and Z_2 is the set of integers modulo 2. Define the function $\phi : Z \to Z_2$ as follows:

$$\phi(n) = n \mod 2$$

This function maps every integer n to its remainder when divided by 2.

Preservation of Addition: For any two integers a and b, we have:

$$\phi(a + b) = (a + b) \mod 2 = (a \mod 2 + b \mod 2) \mod 2 = \phi(a) \oplus \phi(b)$$

Preservation of Multiplication: Similarly, for any two integers a and b, we have:

$$\phi(a \cdot b) = (a \cdot b) \mod 2 = (a \mod 2 \cdot b \mod$$

Example of Isomorphism:

Consider the rings $(Z, +, \cdot)$ and $(Z_4, \oplus, \odot)$, where Z is the set of integers and Z_4 is the set of integers modulo 4. Define the function $\phi : Z \to Z_4$ as follows:

$$\phi(n) = n \mod 4$$

This function maps every integer n to its remainder when divided by 4.

Bijectivity: The function ϕ is bijective because it is both injective and surjective. For every element in Z_4, there exists a unique pre-image in Z.

Preservation of Addition: For any two integers a and b, we have:

$$\phi(a + b) = (a + b) \mod 4 = (a \mod 4 + b \mod 4) \mod 4 = \phi(a) \oplus \phi(b)$$

Preservation of Multiplication: Similarly, for any two integers a and b, we have:

$$\phi(a \cdot b) = (a \cdot b) \mod 4 = (a \mod 4 \cdot b \mod 4) \mod 4 = \phi(a) \odot \phi(b)$$

Preservation of Identity: Since 0 is the additive identity in both Z and Z_4, and 1 is the multiplicative identity in both rings, we have:

$$\phi(0) = 0 \mod 4 = 0$$

$$\phi(1) = 1 \mod 4 = 1$$

Thus, ϕ is an isomorphism from Z to Z_4.

Example of Isomorphism:

Consider the rings $(Z, +, \cdot)$ and $(Z_3, \oplus, \odot)$, where Z is the set of integers and Z_3 is the set of integers modulo 3. Define the function $\phi : Z \to Z_3$ as follows:

$$\phi(n) = n \mod 3$$

This function maps every integer n to its remainder when divided by 3.

Bijectivity: The function ϕ is bijective because it is both injective and surjective. For every element in Z_3, there exists a unique pre-image in Z.

Preservation of Addition: For any two integers a and b, we have:

$$\phi(a + b) = (a + b) \mod 3 = (a \mod 3 + b \mod 3) \mod 3 = \phi(a) \oplus \phi(b)$$

Preservation of Multiplication: Similarly, for any two integers a and b, we have:

$$\phi(a \cdot b) = (a \cdot b) \mod 3 = (a \mod 3 \cdot b \mod 3) \mod 3 = \phi(a) \odot \phi(b)$$

Preservation of Identity: Since 0 is the additive identity in both Z and Z_3, and 1 is the multiplicative identity in both rings, we have:

$$\phi(0) = 0 \mod 3 = 0$$

$$\phi(1) = 1 \mod 3 = 1$$

Thus, ϕ is an isomorphism from Z to Z_3.