7 The Group, Ring, and Field

7.1 Groups

Definition 7.1. Let G be a non-empty set. A function from $G \times G$ into G. That is, $* : G \times G \to G$ is a binary operation if and only if

$$a * b \in G, \quad \forall a, b \in G.$$

Example 7.1. The ordinary addition is a binary operation on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. This is because:

$$a + b \in \mathbb{Z}, \quad \forall a, b \in \mathbb{Z},$$

$$a + b \in \mathbb{Q}, \quad \forall a, b \in \mathbb{Q},$$

$$a + b \in \mathbb{R}, \quad \forall a, b \in \mathbb{R}.$$

The ordinary multiplication is also a binary operation on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.

Definition 7.2. A *semigroup* is a pair $(G, *)$ in which G is a non-empty set and $*$ is a binary operation on G that satisfies the associative law. i.e.
$(G, *)$ is a semigroup if and only if the following conditions hold:

- $G \neq \emptyset$,
- $*$ is a binary operation on G,
- For all $a, b, c \in G$, the operation satisfies the associative law:

$$(a * b) * c = a * (b * c).$$

Example 7.2. $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, +)$,$(\mathbb{R}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$ are semigroup.

Definition of Group

Definition 7.3. A pair $(G, *)$ is called a *group* if the following conditions are satisfied:

1. **Closure**: G is closed under the operation $*$, i.e., for all $a, b \in G$, we have $a * b \in G$.
2. **Associativity**: The operation $*$ is associative on G, i.e., for all $a, b, c \in G$, we have
$$(a * b) * c = a * (b * c).$$
3. **Identity element**: There exists an element $e \in G$ such that for all $a \in G$, we have
$$a * e = e * a = a.$$
4. **Inverse element**: For every element $a \in G$, there exists an element $a^{-1} \in G$ such that
$$a * a^{-1} = a^{-1} * a = e.$$

Remark 7.1.

1. The pair $(G, *)$ is a group if and only if $(G, *)$ is a semigroup with an identity element in which each element of G has an inverse.
2. Every group is a semigroup, but the converse is not true. For example, $(\mathbb{N}, +)$ is a semigroup but not a group because there does not exist an inverse element for every $a \in \mathbb{N}$, i.e., for some $a \in \mathbb{N}$, there is no element $a^{-1} \in \mathbb{N}$.

Definition 7.4. A group $(G, *)$ is called a *commutative group* (or *abelian group*) if and only if
$$a * b = b * a \quad \text{for all} \quad a, b \in G.$$

Example 7.3. The pairs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are commutative groups.

Example 7.4. Given: Let $G = \mathbb{Z}$ and define the operation $*$ on G by:

$$a * b = a + b + 2, \quad \forall a, b \in \mathbb{Z}.$$

We will show that $(G, *)$ satisfies the group axioms.

Step 1: Closure

By definition of $*$, for any $a, b \in \mathbb{Z}$,

$$a * b = a + b + 2 \in \mathbb{Z}.$$

Thus, G is closed under $*$.

Step 2: Associativity

To check associativity, we need to verify:

$$(a * b) * c = a * (b * c), \quad \forall a, b, c \in \mathbb{Z}.$$

Computing both sides:

Left-hand side:

$$(a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4.$$

Right-hand side:

$$a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4.$$

Since both sides are equal, $*$ is associative.

Step 3: Identity Element

Let e be the identity element, meaning:

$$a * e = a, \quad \forall a \in \mathbb{Z}.$$

Using the operation definition:

$$a * e = a + e + 2 = a.$$

Solving for e,

$$a + e + 2 = a \Rightarrow e + 2 = 0 \Rightarrow e = -2.$$

Thus, the identity element is $e = -2$.

Step 4: Inverse Element

For each $a \in \mathbb{Z}$, we need an element $a' \in \mathbb{Z}$ such that:

$$a * a' = e.$$

That is,

$$a + a' + 2 = -2.$$

Solving for a',

$$a' = -a - 4.$$

Since $a' \in \mathbb{Z}$ for all $a \in \mathbb{Z}$, every element has an inverse.

Since closure, associativity, identity, and inverses are satisfied, $(G, *)$ is a group.

Theorem 7.1. *The identity element of a group* $(G, *)$ *is unique.*

Proof. Let has two identity elements, say e and e'.

By the definition of the identity element, we have:

$$a * e = e * a = a, \quad \forall a \in G.$$

$$a * e' = e' * a = a, \quad \forall a \in G.$$

Since e' is identity, then

$$e' * e = e * e' = e. \tag{6}$$

Also, e ,

$$e * e' = e' * e = e'. \tag{7}$$

From (1) and (2), we have

$$e' = e.$$

Thus, the identity element in G is unique. □

7.2 Rings

Definition Ring

Definition 7.5. A ring $(R, +, \cdot)$ is a non-empty set R with two operations $(+)$ and $(\cdot)$, such that:

1. $(R, +)$ is an Abelian Group.
2. $(R, \cdot)$ is a semigroup.
3. Left and Right Distributive Laws Hold
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Example 7.5. The pairs $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, and $(\mathbb{R}, +, \cdot)$ are rings.

Commutative Ring

Definition 7.6. A ring $(R, \cdot)$ is said to be commutative ring if

$$a \cdot b = b \cdot a, \quad \forall a, b \in R.$$

Unity of Ring

Definition 7.7. A ring $(R, \cdot)$ is said to be ring with identity if there exists an element $e \in R$, such that

$$a \cdot e = e \cdot a = a, \forall a \in R.$$

e is called identity of R or unity of R

Example 7.6. The pairs $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, and $(\mathbb{R}, +, \cdot)$ are commutative rings with identity.

7.3 Field

Definition Field

Definition 7.8. A ring $(F, +, \cdot)$ is a non-empty set F with two operations $(+)$ and $(\cdot)$, such that:

1. $(F, +)$ is an Abelian Group.
2. $(F, \cdot)$ is an Abelian Group.
3. Left and Right Distributive Laws Hold
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in F$.

Example 7.7. The pair $(\mathbb{R}, +, \cdot)$ is Field.

7.4 Exercises of The Group, Ring, and Field

Exercises

1. Prove that in a group $(G, *)$, each element has exactly one inverse.

2. If $(G, *)$ is a group, then for all $a, b \in G$,

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

3. If $(G, *)$ is a commutative group, then for all $a, b \in G$,

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

4. Consider the set G of all diagonal matrices of the form

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R}, a, b \neq 0 \right\}$$

   Prove that $(G, \cdot)$ is abelian group.

5. Consider the set R of all diagonal matrices of the form

$$R = \left\{ \begin{pmatrix} 2^n & 0 \\ 0 & 2^m \end{pmatrix} : 2^n, 2^m \in \mathbb{R}, n, m \in \mathbb{Z} \right\}$$

   Is $(R, +\cdot)$ a commutative ring.

6. If $\forall a, b \in G$, $a * b = a + b + ab$. Is $(G, *)$ a group?

7. If $\forall a, b \in G$, $a * b = a^2 + b^2$. Is $(G, *)$ a ring?

8. If $\forall a, b \in G$, $a \oplus b = a + b - 1$ and $a \otimes b = a + b - ab$. Is $(G, *, \circ)$ a ring?