# Chapter 1

# Groups

## 1.1 Introduction to Groups

**Definition 1.1.1.** A *group* is a set $G$ equipped with a binary operation $\cdot : G \times G \to G$ satisfying the following properties:

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

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

(iii) *Inverses*: For each $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$.

If the operation is commutative (i.e., $a \cdot b = b \cdot a$ for all $a, b \in G$), the group is called *abelian*.

**Example 1.1.2.** The set of integers $\mathbb{Z}$ under addition forms an abelian group, with identity element 0 and inverse $-a$ for each $a \in \mathbb{Z}$.

**Theorem 1.1.3.** *Let $G$ be a group. The identity element $e \in G$ is unique.*

*Proof.* Suppose $e$ and $e'$ are both identity elements. Then, for any $a \in G$, we have $a \cdot e = a$ and $e' \cdot a = a$. Consider $e \cdot e'$. Since $e$ is an identity, $e \cdot e' = e'$. Since $e'$ is an identity, $e \cdot e' = e$. Thus, $e = e'$. □

## 1.2 Rings

**Definition 1.2.1.** A *ring* is a set $R$ equipped with two binary operations, addition $(+)$ and multiplication $(\cdot)$, satisfying:

(i) $(R, +)$ is an abelian group with identity 0.

(ii) Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

(iii) Distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

A ring is *commutative* if multiplication is commutative. A ring has a *multiplicative identity* if there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

**Example 1.2.2.** The set of integers $\mathbb{Z}$ with standard addition and multiplication is a commutative ring with multiplicative identity 1.

## 1.3 Fields

**Definition 1.3.1.** A *field* is a commutative ring with a multiplicative identity $1 \neq 0$ in which every non-zero element $a \in F$ has a multiplicative inverse, i.e., there exists $b \in F$ such that $a \cdot b = 1$.

**Example 1.3.2.** The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields under standard addition and multiplication. The set $\mathbb{Z}$ is not a field, as elements like 2 have no multiplicative inverse in $\mathbb{Z}$.

**Proposition 1.3.3.** *Every field is an integral domain, i.e., a commutative ring with* $1 \neq 0$ *and no zero divisors (if* $a \cdot b = 0$*, then* $a = 0$ *or* $b = 0$*).*

*Proof.* Let $F$ be a field, and suppose $a \cdot b = 0$ with $a \neq 0$. Since $F$ is a field, $a$ has a multiplicative inverse $a^{-1}$. Multiply both sides of $a \cdot b = 0$ by $a^{-1}$: $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$. This gives $(a^{-1} \cdot a) \cdot b = 0$, so $1 \cdot b = 0$, hence $b = 0$. Thus, $F$ is an integral domain. □