CHAPTER 4

ALGEBRAIC STRUCTURES

This chapter explores the hierarchy of fundamental algebraic structures: **groups**, **rings**, and **fields**. Beginning with internal composition laws, we develop group theory including subgroups, homomorphisms, and Lagrange's Theorem. The discussion extends to rings, examining ideals and special elements, culminating in the study of fields with emphasis on finite fields $\mathbb{F}_p$ and classical examples. The chapter demonstrates how these structures abstract and generalize properties of familiar number systems while providing powerful tools for diverse mathematical applications.

4.1 Internal Composition Laws

4.1.1 Definition and Basic Properties

Definition 4.1 *Let E be a set. An **internal composition law** (binary operation) on E is any mapping:*

$$\star : E \times E \longrightarrow E$$

that assigns to each ordered pair $(a, b) \in E \times E$ a unique element $a \star b \in E$.

Definition 4.2 *A subset F of E is called **stable** with respect to the law $\star$ if:*

$$\forall a, b \in F, \quad a \star b \in F$$

Example 33 *1. Let A be a set and $E = \mathcal{P}(A)$. Then intersection $\cap$ and union $\cup$ are internal composition laws on E, since for all $X, Y \in \mathcal{P}(A)$, we have $X \cap Y \subseteq A$ and $X \cup Y \subseteq A$.*

2. Consider $F = \{\{a, b\}, \{a, c\}, \{b, c\}\} \subset \mathcal{P}(\{a, b, c\})$. Then F is not stable under intersection or union because:

$$\{a, b\} \cap \{a, c\} = \{a\} \notin F \quad \text{and} \quad \{a, b\} \cup \{a, c\} = \{a, b, c\} \notin F$$

4.1.2 Properties of Composition Laws

Definition 4.3 *Let $\star$ and $\bullet$ be two internal composition laws on E. We say that:*
*$\star$ is **commutative** if: $\forall a, b \in E, a \star b = b \star a$*
*$\star$ is **associative** if: $\forall a, b, c \in E, (a \star b) \star c = a \star (b \star c)$*
*$\star$ is **distributive** over $\bullet$ if: $\forall a, b, c \in E,$*

$$a \star (b \bullet c) = (a \star b) \bullet (a \star c) \quad \text{and} \quad (b \bullet c) \star a = (b \star a) \bullet (c \star a)$$

*$e \in E$ is a **left identity** (respectively **right identity**) for $\star$ if:*

$$\forall a \in E, e \star a = a \quad (\text{respectively } a \star e = a)$$

Example 34 *Let F be a set and $E = \mathcal{P}(F)$. Then:*
$\cap$ and $\cup$ are associative and commutative
$\emptyset$ is the identity element for $\cup$
F is the identity element for $\cap$
$\cap$ is distributive over $\cup$ and $\cup$ is distributive over $\cap$

4.1.3 Identity Elements and Inverses

Proposition 4.1 *If a composition law $\star$ has a right identity e' and a left identity e'', then $e' = e''$ and it is the unique identity element of $\star$.*

Proof. Let e' be a right identity and e'' a left identity. Then:

$$e' = e'' \star e' \quad (\text{since } e'' \text{ is left identity}) \quad \text{and} \quad e'' = e'' \star e' \quad (\text{since } e' \text{ is right identity})$$

Therefore, $e' = e''$. □

Definition 4.4 *Let $\star$ be a composition law on E with identity element e. An element $a \in E$ is:*
***right invertible** if: $\exists a' \in E, a \star a' = e$*
***left invertible** if: $\exists a' \in E, a' \star a = e$*
***invertible** (or symmetric) if it is both right and left invertible*

Example 35 *Consider $E = \{\alpha, \beta, \gamma\}$ with the operation defined by the table:*

$\star$	α	β	γ
α	α	β	γ
β	β	γ	α
γ	γ	α	α

Here:
α is the identity element
α is its own inverse
γ is the inverse of β
Both β and γ are inverses of γ

4.1.4 Uniqueness of Inverses

Proposition 4.2 *Let $\star$ be an associative composition law on E with identity element e. If an element $x \in E$ has a right inverse x_1 and a left inverse x_2, then $x_1 = x_2$.*

Proof. Suppose $x \star x_1 = e$ and $x_2 \star x = e$. Then:

$$x_1 = e \star x_1 = (x_2 \star x) \star x_1 = x_2 \star (x \star x_1) = x_2 \star e = x_2$$

□

Corollary 6 *In an associative structure with identity, if an element is invertible, its inverse is unique.*

Proposition 4.3 *Let $\star$ be an associative composition law on E with identity element e. Then:*
1. *The identity element e is invertible and its only inverse is itself*
2. *If a is invertible with inverse a', then a' is also invertible and a is its inverse*
3. *If a and b are invertible, then $a \star b$ is invertible and $(a \star b)^{-1} = b^{-1} \star a^{-1}$*

Proof. Let $\star$ be an associative composition law on E with identity element e.

1. Since $e \star e = e$, the identity element is its own inverse. If e' were another inverse of e, then $e \star e' = e' \star e = e$. But since e is the identity, we also have $e \star e' = e'$ and $e' \star e = e'$, so $e' = e$.

2. By definition, $a \star a' = a' \star a = e$. This means that a' is invertible with inverse a, so $(a')^{-1} = a$.

3. We verify that $b^{-1} \star a^{-1}$ is indeed the inverse of $a \star b$:

$$\begin{aligned}(a \star b) \star (b^{-1} \star a^{-1}) &= a \star (b \star b^{-1}) \star a^{-1} \\ &= a \star e \star a^{-1} \\ &= a \star a^{-1} = e\end{aligned}$$

$$\begin{aligned}(b^{-1} \star a^{-1}) \star (a \star b) &= b^{-1} \star (a^{-1} \star a) \star b \\ &= b^{-1} \star e \star b \\ &= b^{-1} \star b = e\end{aligned}$$

Therefore, $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

□

4.1.5 Regular Elements

Definition 4.5 *Let $\star$ be a composition law on E. An element $r \in E$ is:*
right regular *if:* $\forall b, c \in E, b \star r = c \star r \Rightarrow b = c$
left regular *if:* $\forall b, c \in E, r \star b = r \star c \Rightarrow b = c$
regular *if it is both right and left regular*

Proposition 4.4 *Let $\star$ be an associative composition law on E with identity element e. Then every invertible element is regular.*

Proof. Let x be invertible with inverse x^{-1}. Suppose $a \star x = b \star x$. Then:

$$(a \star x) \star x^{-1} = (b \star x) \star x^{-1} \Rightarrow a \star (x \star x^{-1}) = b \star (x \star x^{-1}) \Rightarrow a \star e = b \star e \Rightarrow a = b$$

So x is right regular. Similarly, x is left regular. □

4.2 Groups

4.2.1 Definition and Examples

Definition 4.6 *A **group** is a set G equipped with an internal composition law $\star$ satisfying:*
1. ***Associativity:*** $\forall a, b, c \in G, (a \star b) \star c = a \star (b \star c)$
2. ***Identity element:*** $\exists e \in G, \forall a \in G, a \star e = e \star a = a$
3. ***Inverses:*** $\forall a \in G, \exists a^{-1} \in G, a \star a^{-1} = a^{-1} \star a = e$

*If additionally the law is commutative, the group is called **abelian**.*

Example 36 *1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups*
2. $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ are abelian groups (where * denotes nonzero elements)
3. The set of bijections from a set to itself forms a non-abelian group under composition

4.2.2 Subgroups

Definition 4.7 *Let $(G, \star)$ be a group. A subset $H \subseteq G$ is called a **subgroup** of G if:*
1. H is non-empty: $H \neq \emptyset$
2. H is closed under the group operation: $\forall a, b \in H, a \star b \in H$
3. H contains inverses: $\forall a \in H, a^{-1} \in H$
We denote this by $H \leq G$.

Proposition 4.5 ***(Subgroup Test):*** *A non-empty subset $H \subseteq G$ is a subgroup if and only if:*

$$\forall a, b \in H, a \star b^{-1} \in H$$

Proof. ($\Rightarrow$) If H is a subgroup and $a, b \in H$, then $b^{-1} \in H$ and $a \star b^{-1} \in H$.
($\Leftarrow$) Suppose $H \neq \emptyset$ and $\forall a, b \in H, a \star b^{-1} \in H$.
Take any $a \in H$. Then $a \star a^{-1} = e \in H$.
For any $a \in H$, $e \star a^{-1} = a^{-1} \in H$.
For any $a, b \in H$, $a \star b = a \star (b^{-1})^{-1} \in H$.
Thus H is a subgroup. □

Example 37 *1. In $(\mathbb{Z}, +)$, the set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subgroup for any $n \in \mathbb{Z}$*
2. In $(\mathbb{R}^*, \times)$, the set $\mathbb{R}^+$ of positive real numbers is a subgroup
3. In any group G, $\{e\}$ and G itself are subgroups (trivial subgroups)
4. The set of even permutations forms a subgroup of the symmetric group S_n (the alternating group A_n)

Proposition 4.6 *Let H and K be subgroups of G. Then:*
1. $H \cap K$ is a subgroup of G
2. $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$

Proof. 1. Let $H \cap K \neq \emptyset$ (since $e \in H \cap K$). For any $a, b \in H \cap K$, we have $a, b \in H$ and $a, b \in K$. Since H and K are subgroups, $a \star b^{-1} \in H$ and $a \star b^{-1} \in K$, so $a \star b^{-1} \in H \cap K$.
2. ($\Rightarrow$) If $H \cup K$ is a subgroup and $H \not\subseteq K$, then $\exists h \in H \setminus K$. For any $k \in K$, since $h, k \in H \cup K$ and $H \cup K$ is a subgroup, $h \star k \in H \cup K$. If $h \star k \in K$, then $h = (h \star k) \star k^{-1} \in K$, contradiction. So $h \star k \in H$, hence $k = h^{-1} \star (h \star k) \in H$. Thus $K \subseteq H$.
($\Leftarrow$) If $H \subseteq K$, then $H \cup K = K$ is a subgroup. Similarly if $K \subseteq H$. □

4.2.3 Cosets and Lagrange's Theorem

Definition 4.8 *Let H be a subgroup of G and $a \in G$. The sets:*
$aH = \{a \star h \mid h \in H\}$ *(left coset)*
$Ha = \{h \star a \mid h \in H\}$ *(right coset)*
*are called the **cosets** of H in G.*

Proposition 4.7 *Let H be a subgroup of G. Then:*

1. *The cosets of H partition G*
2. *All cosets have the same cardinality as H*
3. *$aH = bH$ if and only if $a^{-1} \star b \in H$*

Proof. Let H be a subgroup of G and consider the left cosets of H in G.

1. We need to show that:

   - Every element of G belongs to some coset
   - Different cosets are either equal or disjoint

   For any $g \in G$, we have $g \in gH$ since $e \in H$ and $g = g \star e$. Thus every element belongs to at least one coset.

   Now suppose $aH \cap bH \neq \emptyset$. Then there exist $h_1, h_2 \in H$ such that $a \star h_1 = b \star h_2$. This implies:

   $$a = b \star h_2 \star h_1^{-1}$$

   Let $h = h_2 \star h_1^{-1} \in H$ (since H is a subgroup). Then for any $a \star h' \in aH$:

   $$a \star h' = b \star h \star h' = b \star (h \star h') \in bH$$

   since $h \star h' \in H$. Thus $aH \subseteq bH$. Similarly, $bH \subseteq aH$, so $aH = bH$.

   Therefore, the cosets form a partition of G.

2. Consider the map $\phi : H \to aH$ defined by $\phi(h) = a \star h$. This map is:

   - **Surjective:** By definition of aH, every element is of the form $a \star h$ for some $h \in H$.
   - **Injective:** If $a \star h_1 = a \star h_2$, then by left cancellation (valid in groups), $h_1 = h_2$.

   Thus ϕ is a bijection, so $|aH| = |H|$ for all $a \in G$.

3. ($\Rightarrow$) If $aH = bH$, then $b \in aH$ (since $b = b \star e \in bH$). So there exists $h \in H$ such that $b = a \star h$, which implies $a^{-1} \star b = h \in H$.

   ($\Leftarrow$) If $a^{-1} \star b \in H$, then for any $b \star h \in bH$:

   $$b \star h = a \star (a^{-1} \star b) \star h = a \star ((a^{-1} \star b) \star h) \in aH$$

   since $(a^{-1} \star b) \star h \in H$. Thus $bH \subseteq aH$.

   Conversely, for any $a \star h \in aH$:

   $$a \star h = b \star (b^{-1} \star a) \star h = b \star ((a^{-1} \star b)^{-1} \star h) \in bH$$

since $(a^{-1} \star b)^{-1} \star h \in H$. Thus $aH \subseteq bH$.

Therefore, $aH = bH$.

□

Theorem 7 ***(Lagrange's Theorem):*** *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G:*

$$|G| = [G : H] \cdot |H|$$

where $[G : H]$ is the number of distinct cosets of H in G (the index of H in G).

Proof. Since the cosets partition G and all have size $|H|$, we have $|G| = [G : H] \cdot |H|$. □

Corollary 8 *In a finite group G:*
1. The order of any element divides $|G|$
2.If $|G|$ is prime, then G is cyclic
3. For any $a \in G$, $a^{|G|} = e$

Proof. Let G be a finite group of order $n = |G|$.

1. Let $a \in G$ and consider the cyclic subgroup generated by a:

   $$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

   The order of a is defined as the smallest positive integer m such that $a^m = e$, and this equals the order of the subgroup $\langle a \rangle$, i.e., $|\langle a \rangle| = m$.

   By Lagrange's Theorem, since $\langle a \rangle$ is a subgroup of G, we have:

   $$|G| = [G : \langle a \rangle] \cdot |\langle a \rangle|$$

   Therefore, $m = |\langle a \rangle|$ divides $|G|$.

2. Suppose $|G| = p$ where p is prime. Let $a \in G$ with $a \neq e$. Consider the cyclic subgroup $\langle a \rangle$. By part (1), the order of a divides p. Since $a \neq e$, the order of a cannot be 1, so it must be p. Therefore:

   $$|\langle a \rangle| = p = |G|$$

   which implies $\langle a \rangle = G$. Thus G is cyclic, generated by a.

3. Let m be the order of a. By part (1), m divides $|G|$, so we can write $|G| = m \cdot k$ for some $k \in \mathbb{Z}^+$. Then:

   $$a^{|G|} = a^{m \cdot k} = (a^m)^k = e^k = e$$

   This completes the proof.

□

4.2.4 Basic Properties of Groups

Proposition 4.8 *In any group $(G, \star)$:*

1. *The identity element is unique*
2. *Every element has a unique inverse*
3. $\forall a, b \in G, (a \star b)^{-1} = b^{-1} \star a^{-1}$
4. $\forall a \in G, (a^{-1})^{-1} = a$
5. *Cancellation laws hold:* $a \star b = a \star c \Rightarrow b = c$ *and* $b \star a = c \star a \Rightarrow b = c$

Proof. Let $(G, \star)$ be a group. We prove each property:

1. **Uniqueness of the identity element:**

   Suppose e and e' are both identity elements in G. Then:

   $$e = e \star e' \quad \text{(since } e' \text{ is an identity)}$$

   $$e \star e' = e' \quad \text{(since } e \text{ is an identity)}$$

   Therefore, $e = e'$. The identity element is unique.

2. **Uniqueness of inverses:**

   Let $a \in G$ and suppose b and c are both inverses of a. Then:

   $$b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c$$

   Therefore, the inverse of each element is unique.

3. **Inverse of a product:** $\forall a, b \in G, (a \star b)^{-1} = b^{-1} \star a^{-1}$

   We verify that $b^{-1} \star a^{-1}$ is indeed the inverse of $a \star b$:

   $$(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} = a \star a^{-1} = e$$

   $$(b^{-1} \star a^{-1}) \star (a \star b) = b^{-1} \star (a^{-1} \star a) \star b = b^{-1} \star e \star b = b^{-1} \star b = e$$

   Therefore, $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

4. **Inverse of an inverse:** $\forall a \in G, (a^{-1})^{-1} = a$

   By definition, a^{-1} is the inverse of a, so:

   $$a \star a^{-1} = a^{-1} \star a = e$$

   This also means that a is the inverse of a^{-1}, so $(a^{-1})^{-1} = a$.

5. **Cancellation laws:**
   Left cancellation: $a \star b = a \star c \Rightarrow b = c$
   Multiply both sides on the left by a^{-1}:

$$a^{-1} \star (a \star b) = a^{-1} \star (a \star c)$$

$$(a^{-1} \star a) \star b = (a^{-1} \star a) \star c$$

$$e \star b = e \star c \Rightarrow b = c$$

   Right cancellation: $b \star a = c \star a \Rightarrow b = c$
   Multiply both sides on the right by a^{-1}:

$$(b \star a) \star a^{-1} = (c \star a) \star a^{-1},$$

$$b \star (a \star a^{-1}) = c \star (a \star a^{-1}),$$

$$b \star e = c \star e \Rightarrow b = c.$$

□

4.2.5 Homomorphisms

Definition 4.9 *Let $(G, \star)$ and $(H, \bullet)$ be groups. A function $\phi : G \to H$ is called a **group homomorphism** if:*

$$\forall a, b \in G, \quad \phi(a \star b) = \phi(a) \bullet \phi(b)$$

Proposition 4.9 *Let $\phi : G \to H$ be a group homomorphism. Then:*

1. *$\phi(e_G) = e_H$ (preserves identity)*
2. *$\forall a \in G, \phi(a^{-1}) = (\phi(a))^{-1}$ (preserves inverses)*
3. *If $K \leq G$, then $\phi(K) \leq H$ (image of subgroup is subgroup)*
4. *If $L \leq H$, then $\phi^{-1}(L) \leq G$ (preimage of subgroup is subgroup)*

Proof. 1. $\phi(e_G) = \phi(e_G \star e_G) = \phi(e_G) \bullet \phi(e_G)$, so by cancellation, $\phi(e_G) = e_H$
2. $\phi(a) \bullet \phi(a^{-1}) = \phi(a \star a^{-1}) = \phi(e_G) = e_H$, so $\phi(a^{-1}) = (\phi(a))^{-1}$
3. Let $K \leq G$ and take $\phi(a), \phi(b) \in \phi(K)$. Then:

$$\phi(a) \bullet (\phi(b))^{-1} = \phi(a) \bullet \phi(b^{-1}) = \phi(a \star b^{-1}) \in \phi(K)$$

So $\phi(K)$ is a subgroup.
4. Let $L \leq H$ and take $a, b \in \phi^{-1}(L)$. Then:

$$\phi(a \star b^{-1}) = \phi(a) \bullet \phi(b^{-1}) = \phi(a) \bullet (\phi(b))^{-1} \in L$$

So $a \star b^{-1} \in \phi^{-1}(L)$, hence $\phi^{-1}(L)$ is a subgroup. □

Definition 4.10 *Let $\phi : G \to H$ be a group homomorphism. The **kernel** of ϕ is:*

$$\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$$

*The **image** of ϕ is:*

$$Im(\phi) = \{\phi(g) \mid g \in G\}$$

Proposition 4.10 *For any group homomorphism $\phi : G \to H$:*
1. $\ker(\phi)$ *is a normal subgroup of* G
2. $Im(\phi)$ *is a subgroup of* H
3. ϕ *is injective if and only if* $\ker(\phi) = \{e_G\}$

Proof. 1. From Proposition 2.11(4), $\ker(\phi) = \phi^{-1}(\{e_H\})$ is a subgroup. To show normality: for any $g \in G$ and $k \in \ker(\phi)$,

$$\phi(g \star k \star g^{-1}) = \phi(g) \bullet \phi(k) \bullet \phi(g^{-1}) = \phi(g) \bullet e_H \bullet (\phi(g))^{-1} = e_H$$

So $g \star k \star g^{-1} \in \ker(\phi)$.
2. From Proposition 2.11(3), $\text{Im}(\phi) = \phi(G)$ is a subgroup.
3. ($\Rightarrow$) If ϕ is injective and $\phi(g) = e_H$, then $\phi(g) = \phi(e_G)$, so $g = e_G$.
($\Leftarrow$) Suppose $\ker(\phi) = \{e_G\}$ and $\phi(a) = \phi(b)$. Then:

$$\phi(a \star b^{-1}) = \phi(a) \bullet (\phi(b))^{-1} = e_H$$

So $a \star b^{-1} \in \ker(\phi) = \{e_G\}$, hence $a = b$. □

4.2.6 Isomorphisms

Definition 4.11 *A group homomorphism $\phi : G \to H$ is called a **group isomorphism** if it is bijective. In this case, we say G and H are **isomorphic** and write $G \cong H$.*

Proposition 4.11 *Let $\phi : G \to H$ be a group isomorphism. Then:*
1. $\phi^{-1} : H \to G$ *is also a group isomorphism*
2. $|G| = |H|$ *(isomorphic groups have the same order)*
3. G *is abelian if and only if* H *is abelian*
4. G *is cyclic if and only if* H *is cyclic*

Proof. 1. For any $x, y \in H$, let $a = \phi^{-1}(x)$, $b = \phi^{-1}(y)$. Then:

$$\phi^{-1}(x \bullet y) = \phi^{-1}(\phi(a) \bullet \phi(b)) = \phi^{-1}(\phi(a \star b)) = a \star b = \phi^{-1}(x) \star \phi^{-1}(y).$$

2. Since ϕ is bijective, $|G| = |H|$
3. If G is abelian, then for any $x, y \in H$:

$$x \bullet y = \phi(\phi^{-1}(x)) \bullet \phi(\phi^{-1}(y)) = \phi(\phi^{-1}(x) \star \phi^{-1}(y)) = \phi(\phi^{-1}(y) \star \phi^{-1}(x)) = y \bullet x.$$

4. If $G = \langle g \rangle$, then $H = \langle \phi(g) \rangle$. □

Example 38 *1.* $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$ *via the isomorphism* $\phi(x) = e^x$
2. For any cyclic group G *of order* n, $G \cong \mathbb{Z}/n\mathbb{Z}$
3. The Klein four-group $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
4. S_3 *(symmetric group on 3 elements) is not isomorphic to* $\mathbb{Z}/6\mathbb{Z}$ *because* S_3 *is non-abelian while* $\mathbb{Z}/6\mathbb{Z}$ *is abelian*

4.2.7 First Isomorphism Theorem

Theorem 9 ***(First Isomorphism Theorem):*** *Let* $\phi : G \to H$ *be a group homomorphism. Then:*

$$G/\ker(\phi) \cong Im(\phi)$$

Specifically, the map $\psi : G/\ker(\phi) \to Im(\phi)$ *defined by* $\psi(g\ker(\phi)) = \phi(g)$ *is a well-defined group isomorphism.*

Proof. 1. **Well-defined:** If $g\ker(\phi) = h\ker(\phi)$, then $h^{-1} \star g \in \ker(\phi)$, so:

$$\phi(h^{-1} \star g) = e_H \Rightarrow (\phi(h))^{-1} \bullet \phi(g) = e_H \Rightarrow \phi(g) = \phi(h)$$

2. **Homomorphism:**

$$\psi((g\ker(\phi)) \star (h\ker(\phi))) = \psi((g \star h)\ker(\phi)) = \phi(g \star h) = \phi(g) \bullet \phi(h) = \psi(g\ker(\phi)) \bullet \psi(h\ker(\phi))$$

3. **Injective:** If $\psi(g\ker(\phi)) = e_H$, then $\phi(g) = e_H$, so $g \in \ker(\phi)$, hence $g\ker(\phi) = \ker(\phi)$
4. **Surjective:** For any $\phi(g) \in \mathrm{Im}(\phi)$, we have $\psi(g\ker(\phi)) = \phi(g)$ □

Example 39 *1. The determinant map* $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ *has kernel* $SL_n(\mathbb{R})$ *and image* $\mathbb{R}^*$*, so:*

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*.$$

2. The sign homomorphism $sgn : S_n \to \{\pm 1\}$ *has kernel* A_n *and image* $\{\pm 1\}$*, so:*

$$S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}.$$

3. The exponential map $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ *has kernel* $\{0\}$ *and image* $\mathbb{R}^+$*, confirming* $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$.

4.3 Rings

4.3.1 Definition and Basic Properties

Definition 4.12 *A **ring** is a set R equipped with two internal composition laws $+$ (addition) and $\times$ (multiplication) satisfying:*

1. *$(R, +)$ is an abelian group*
2. *Multiplication is associative: $\forall a, b, c \in R, (a \times b) \times c = a \times (b \times c)$*
3. *Multiplication is distributive over addition:*

$$a \times (b + c) = (a \times b) + (a \times c) \quad \text{and} \quad (a + b) \times c = (a \times c) + (b \times c)$$

*The ring is called **commutative** if multiplication is commutative, and **unital** if it has a multiplicative identity.*

Example 40 1. *$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ are commutative unital rings*
2. *The set of $n \times n$ matrices with real entries forms a non-commutative unital ring*
3. *The set of even integers forms a commutative ring without unity*

4.3.2 Subrings

Definition 4.13 *Let $(R, +, \times)$ be a ring. A subset $S \subseteq R$ is called a **subring** of R if:*

1. *S is non-empty: $S \neq \emptyset$*
2. *S is closed under subtraction: $\forall a, b \in S, a - b \in S$*
3. *S is closed under multiplication: $\forall a, b \in S, a \times b \in S$*

Proposition 4.12 ***(Subring Test):** A non-empty subset $S \subseteq R$ is a subring if and only if:*

$$\forall a, b \in S, a - b \in S \quad \text{and} \quad a \times b \in S$$

Proof. The conditions ensure that:
$(S, +)$ is a subgroup of $(R, +)$ (since $0 = a - a \in S$ and $-b = 0 - b \in S$).
S is closed under multiplication.
The ring axioms are inherited from R. □

Example 41 1. *In $(\mathbb{Z}, +, \times)$, the set $n\mathbb{Z}$ is a subring for any $n \in \mathbb{Z}$*
2. *In $(\mathbb{R}, +, \times)$, $\mathbb{Z}$ and $\mathbb{Q}$ are subrings*
3. *The set of diagonal matrices is a subring of the ring of $n \times n$ matrices*
4. *The set of continuous functions is a subring of the ring of all real-valued functions*

4.3.3 Special Elements in Rings

Definition 4.14 *Let R be a ring with multiplicative identity $1 \neq 0$. An element $a \in R$ is:*
*A **unit** if it has a multiplicative inverse*
*A **zero divisor** if $a \neq 0$ and $\exists b \neq 0$ such that $a \times b = 0$ or $b \times a = 0$*
***Nilpotent** if $\exists n \in \mathbb{N}^*$ such that $a^n = 0$*

4.4 Rules of Calculation in Rings

Proposition 4.13 (Calculation Rules in Rings) *Let R be a ring. For all $a, b, c \in R$:*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$
5. $(a - b) \cdot c = a \cdot c - b \cdot c$

Proof.

1. $a \cdot 0 = 0 \cdot a = 0$**:** Using the distributive property and the fact that 0 is the additive identity:
$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$
Adding $-(a \cdot 0)$ to both sides:
$$a \cdot 0 + [-(a \cdot 0)] = [a \cdot 0 + a \cdot 0] + [-(a \cdot 0)]$$
$$0 = a \cdot 0 + [a \cdot 0 + (-(a \cdot 0))] = a \cdot 0 + 0 = a \cdot 0$$
Similarly, $0 \cdot a = 0$ by the same argument.

2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$**:** First, show $a \cdot (-b) = -(a \cdot b)$:
$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$$
Therefore, $a \cdot (-b)$ is the additive inverse of $a \cdot b$, so:
$$a \cdot (-b) = -(a \cdot b)$$
Similarly, $(-a) \cdot b = -(a \cdot b)$:
$$a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$$
So $(-a) \cdot b = -(a \cdot b)$.

3. $(-a) \cdot (-b) = a \cdot b$**:** Using part 2 twice:

$$(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b$$

The last equality holds because the additive inverse of $-(a \cdot b)$ is $a \cdot b$.

4. $a \cdot (b - c) = a \cdot b - a \cdot c$**:**

Using the distributive property and part 2:

$$a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c$$

5. $(a - b) \cdot c = a \cdot c - b \cdot c$**:** Similarly:

$$(a - b) \cdot c = (a + (-b)) \cdot c = a \cdot c + (-b) \cdot c = a \cdot c + (-(b \cdot c)) = a \cdot c - b \cdot c$$

□

Remark 5 *These calculation rules are fundamental and are used constantly when working with rings. They show that despite the more abstract nature of rings compared to familiar number systems, many familiar algebraic manipulations remain valid.*

Example 42 *In the ring $\mathbb{Z}/6\mathbb{Z}$, we can verify these properties:*

- $\bar{2} \cdot \bar{0} = \bar{0}$ *(property 1)*
- $\bar{2} \cdot (-\bar{3}) = \bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ *and* $-(\bar{2} \cdot \bar{3}) = -\bar{0} = \bar{0}$ *(property 2)*
- $(-\bar{2}) \cdot (-\bar{3}) = \bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ *(property 3)*

4.4.1 Invertible Elements

Definition 4.15 *Let R be a ring with unity $1 \neq 0$. An element $a \in R$ is called* ***invertible*** *(or a* ***unit****) if there exists $b \in R$ such that:*

$$a \cdot b = b \cdot a = 1$$

The element b is called the ***inverse*** *of a and is denoted a^{-1}.*

Definition 4.16 *The set of all invertible elements in a ring R is denoted by $R^\times$ and forms a group under multiplication, called the* ***group of units****.*

Example 43 *1. In $\mathbb{Z}$, the only invertible elements are 1 and -1, so $\mathbb{Z}^\times = \{\pm 1\}$*

2. In $\mathbb{R}$, every nonzero element is invertible, so $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

3. In $\mathbb{Z}/n\mathbb{Z}$, an element $\bar{a}$ is invertible if and only if $\gcd(a, n) = 1$

4.4.2 Zero Divisors

Definition 4.17 *Let R be a ring. A nonzero element $a \in R$ is called a* ***zero divisor*** *if there exists a nonzero element $b \in R$ such that:*

$$a \cdot b = 0 \quad or \quad b \cdot a = 0$$

Definition 4.18 *A commutative ring with unity $1 \neq 0$ that has no zero divisors is called an* ***integral domain***.

Example 44 *1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are integral domains (no zero divisors)*

2. In $\mathbb{Z}/6\mathbb{Z}$, we have $\bar{2} \cdot \bar{3} = \bar{0}$, so $\bar{2}$ and $\bar{3}$ are zero divisors

3. The ring of $n \times n$ matrices over a field has zero divisors when $n > 1$

Proposition 4.14 *In an integral domain, the cancellation law holds: if $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$.*

Proof. Let R be an integral domain, and suppose $a \neq 0$ and $a \cdot b = a \cdot c$ for some $b, c \in R$.
Since $a \cdot b = a \cdot c$, we can rewrite this as:

$$a \cdot b - a \cdot c = 0$$

Using the distributive property:

$$a \cdot (b - c) = 0$$

Now, since R is an integral domain, it has no zero divisors. We have $a \neq 0$ and $a \cdot (b-c) = 0$. Therefore, by the definition of an integral domain (no zero divisors), we must have:

$$b - c = 0$$

which implies:

$$b = c$$

This proves the cancellation law: if $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$.
The same reasoning applies for right cancellation: if $b \cdot a = c \cdot a$ with $a \neq 0$, then:

$$(b - c) \cdot a = 0 \Rightarrow b - c = 0 \Rightarrow b = c$$

This completes the proof. □

4.4.3 Ring Homomorphisms

Definition 4.19 *Let R and S be rings. A function $\phi : R \to S$ is called a* ***ring homomorphism*** *if for all $a, b \in R$:*

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
3. *If R and S are rings with unity, we also require $\phi(1_R) = 1_S$*

Definition 4.20 *Let $\phi : R \to S$ be a ring homomorphism. The* ***kernel*** *of ϕ is:*

$$\ker(\phi) = \{a \in R : \phi(a) = 0_S\}$$

The ***image*** *of ϕ is:*

$$\mathrm{Im}(\phi) = \{\phi(a) \in S : a \in R\}$$

Proposition 4.15 *Let $\phi : R \to S$ be a ring homomorphism. Then:*

1. $\phi(0_R) = 0_S$
2. $\phi(-a) = -\phi(a)$ *for all* $a \in R$
3. $\ker(\phi)$ *is a subring of R (in fact, an ideal)*
4. $\mathrm{Im}(\phi)$ *is a subring of S*

Proof. Let $\phi : R \to S$ be a ring homomorphism.

1. For any $a \in R$, we have:

$$\phi(a) = \phi(a + 0_R) = \phi(a) + \phi(0_R)$$

Adding $-\phi(a)$ to both sides:

$$\phi(a) + (-\phi(a)) = \phi(a) + \phi(0_R) + (-\phi(a))$$

$$0_S = \phi(0_R)$$

Therefore, $\phi(0_R) = 0_S$.

2. For any $a \in R$, we have:

$$\phi(a + (-a)) = \phi(0_R) = 0_S$$

But also:

$$\phi(a + (-a)) = \phi(a) + \phi(-a)$$

So:

$$\phi(a) + \phi(-a) = 0_S$$

This means $\phi(-a)$ is the additive inverse of $\phi(a)$, so:

$$\phi(-a) = -\phi(a)$$

3. First, note that $\ker(\phi) = \{a \in R : \phi(a) = 0_S\}$.

- **Non-empty:** $\phi(0_R) = 0_S$, so $0_R \in \ker(\phi)$.
- **Closed under subtraction:** Let $a, b \in \ker(\phi)$. Then:

$$\phi(a - b) = \phi(a) - \phi(b) = 0_S - 0_S = 0_S$$

So $a - b \in \ker(\phi)$.

- **Closed under multiplication:** Let $a, b \in \ker(\phi)$. Then:

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) = 0_S \cdot 0_S = 0_S$$

So $a \cdot b \in \ker(\phi)$.

Thus $\ker(\phi)$ is a subring. In fact, it's an ideal because for any $a \in \ker(\phi)$ and $r \in R$:

$$\phi(a \cdot r) = \phi(a) \cdot \phi(r) = 0_S \cdot \phi(r) = 0_S$$

So $a \cdot r \in \ker(\phi)$, and similarly $r \cdot a \in \ker(\phi)$.

4. $\mathrm{Im}(\phi)$ **is a subring of** S

Let $\mathrm{Im}(\phi) = \{\phi(a) \in S : a \in R\}$.

- **Non-empty:** $\phi(0_R) = 0_S \in \mathrm{Im}(\phi)$.
- **Closed under subtraction:** Let $\phi(a), \phi(b) \in \mathrm{Im}(\phi)$. Then:

$$\phi(a) - \phi(b) = \phi(a - b) \in \mathrm{Im}(\phi)$$

- **Closed under multiplication:** Let $\phi(a), \phi(b) \in \mathrm{Im}(\phi)$. Then:

$$\phi(a) \cdot \phi(b) = \phi(a \cdot b) \in \mathrm{Im}(\phi)$$

Thus $\text{Im}(\phi)$ is a subring of S.

□

Example 45 *1. The map $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\phi(a) = \bar{a}$ is a ring homomorphism*

2. The evaluation map $\phi : \mathbb{R}[X] \to \mathbb{R}$ defined by $\phi(P) = P(\alpha)$ for fixed $\alpha \in \mathbb{R}$ is a ring homomorphism

3. The determinant map $\det : M_n(\mathbb{R}) \to \mathbb{R}$ is not a ring homomorphism (it doesn't preserve addition)

4.4.4 Ideals

Definition 4.21 *A subset I of a ring R is called an **ideal** if:*

1. *I is a subgroup of $(R, +)$*
2. *For all $a \in I$ and $r \in R$, we have $a \cdot r \in I$ and $r \cdot a \in I$ (absorption property)*

Definition 4.22 *An ideal I of a ring R is called:*

1. ***Proper** if $I \neq R$*
2. ***Maximal** if I is proper and there is no proper ideal J with $I \subsetneq J \subsetneq R$*
3. ***Prime** if for all $a, b \in R$, $a \cdot b \in I$ implies $a \in I$ or $b \in I$*

Example 46 *1. In $\mathbb{Z}$, the ideals are exactly the sets $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$*

2. The ideal $p\mathbb{Z}$ is prime (and maximal) if and only if p is prime

3. In any ring R, the sets $\{0\}$ and R are ideals (trivial ideals)

Definition 4.23 *A subring I of a ring R is called an **ideal** if:*

$$\forall a \in I, \forall r \in R, a \times r \in I \quad \text{and} \quad r \times a \in I$$

Proposition 4.16 *Let I and J be subrings of R. Then:*

1. *$I \cap J$ is a subring of R*
2. *If I and J are ideals, then $I + J = \{a + b \mid a \in I, b \in J\}$ is a subring of R*
3. *If I and J are ideals, then $I \cap J$ and $I + J$ are ideals*

Proof. Let I and J be subrings of R.

1. **$I \cap J$ is a subring of R**

   - **Non-empty:** Since I and J are subrings, $0_R \in I$ and $0_R \in J$, so $0_R \in I \cap J$.
   - **Closed under subtraction:** Let $a, b \in I \cap J$. Then $a, b \in I$ and $a, b \in J$. Since I and J are subrings:
   $$a - b \in I \quad \text{and} \quad a - b \in J$$
   Therefore, $a - b \in I \cap J$.
   - **Closed under multiplication:** Let $a, b \in I \cap J$. Then $a, b \in I$ and $a, b \in J$. Since I and J are subrings:
   $$a \cdot b \in I \quad \text{and} \quad a \cdot b \in J$$
   Therefore, $a \cdot b \in I \cap J$.

   Thus $I \cap J$ satisfies the subring criteria.

2. **If I and J are ideals, then $I + J = \{a + b \mid a \in I, b \in J\}$ is a subring of R**

   - **Non-empty:** $0_R = 0_R + 0_R \in I + J$ since $0_R \in I$ and $0_R \in J$.
   - **Closed under subtraction:** Let $x, y \in I + J$. Then there exist $a_1, a_2 \in I$ and $b_1, b_2 \in J$ such that:
   $$x = a_1 + b_1, \quad y = a_2 + b_2$$
   Then:
   $$x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$$
   Since I and J are subrings, $a_1 - a_2 \in I$ and $b_1 - b_2 \in J$. Therefore, $x - y \in I + J$.
   - **Closed under multiplication:** Let $x, y \in I + J$ with $x = a_1 + b_1$, $y = a_2 + b_2$ where $a_1, a_2 \in I$ and $b_1, b_2 \in J$. Then:
   $$x \cdot y = (a_1 + b_1) \cdot (a_2 + b_2) = a_1 \cdot a_2 + a_1 \cdot b_2 + b_1 \cdot a_2 + b_1 \cdot b_2$$
   Since I and J are ideals, then:
     - $a_1 \cdot b_2 \in I$ (since $b_2 \in J \subseteq R$ and I is an ideal)
     - $b_1 \cdot a_2 \in J$ (since $a_2 \in I \subseteq R$ and J is an ideal)

   So we have:
   $$x \cdot y = \underbrace{a_1 \cdot a_2}_{\in I} + \underbrace{a_1 \cdot b_2}_{\in I} + \underbrace{b_1 \cdot a_2}_{\in J} + \underbrace{b_1 \cdot b_2}_{\in J}$$

We can rewrite this as:

$$x \cdot y = \underbrace{(a_1 \cdot a_2 + a_1 \cdot b_2)}_{\in I} + \underbrace{(b_1 \cdot a_2 + b_1 \cdot b_2)}_{\in J} \in I + J$$

Therefore, $I + J$ is closed under multiplication.

Thus $I + J$ is a subring of R.

3. **If I and J are ideals, then $I \cap J$ and $I + J$ are ideals** We've already shown $I \cap J$ and $I + J$ are subrings. Now we show they are ideals.

   - **$I \cap J$ is an ideal:** Let $a \in I \cap J$ and $r \in R$. Since I and J are ideals:

     $$a \cdot r \in I \quad \text{and} \quad a \cdot r \in J$$

     So $a \cdot r \in I \cap J$. Similarly, $r \cdot a \in I \cap J$.

   - **$I + J$ is an ideal:** Let $x \in I + J$ and $r \in R$. Write $x = a + b$ with $a \in I$, $b \in J$. Then:

     $$x \cdot r = (a + b) \cdot r = a \cdot r + b \cdot r$$

     Since I and J are ideals, $a \cdot r \in I$ and $b \cdot r \in J$. Therefore, $x \cdot r \in I + J$. Similarly, $r \cdot x \in I + J$.

□

Example 47 *1. In $\mathbb{Z}$, the subring $n\mathbb{Z}$ is an ideal*

2. In any ring R, $\{0\}$ and R itself are ideals (trivial ideals)

3. In $\mathbb{Z}[x]$, the set of polynomials with even constant term is an ideal

Theorem 10 (First Isomorphism Theorem for Rings) *Let $\phi : R \to S$ be a ring homomorphism. Then:*

$$R/\ker(\phi) \cong \mathrm{Im}(\phi)$$

4.5 Fields

Definition 4.24 *A **field** is a commutative ring with unity $1 \neq 0$ in which every nonzero element is invertible. That is:*

1. $(K, +)$ is an abelian group

2. $(K^\times, \cdot)$ *is an abelian group, where* $K^\times = K \setminus \{0\}$

3. *Multiplication distributes over addition*

Proposition 4.17 *Every field is an integral domain.*

Proof. Suppose $a \cdot b = 0$ in a field K and $a \neq 0$. Then a^{-1} exists, so:

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$$

Thus K has no zero divisors. □

4.5.1 Finite Fields

Theorem 11 *For every prime number* p*, the ring* $\mathbb{Z}/p\mathbb{Z}$ *is a field, denoted* $\mathbb{F}_p$*.*

Proof. Let $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ be nonzero. Then $p \nmid a$, so $\gcd(a, p) = 1$. By BÃ©zout's identity, there exist integers x, y such that:

$$ax + py = 1$$

Reducing modulo p gives $\bar{a} \cdot \bar{x} = \bar{1}$, so $\bar{a}$ is invertible. □

Example 48 (The field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$)

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

This is the smallest field, with only 2 elements.

Example 49 (The field $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$)

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Note that $2^{-1} = 2$ *since* $2 \cdot 2 = 4 \equiv 1 \pmod 3$.

Theorem 12 *The number of elements in a finite field is always a prime power* p^n*. For each prime power, there exists essentially one field with that many elements, denoted* $\mathbb{F}_{p^n}$*.*

4.5.2 The Fields $\mathbb{R}$ and $\mathbb{C}$

Definition 4.25 *The field of **real numbers** $\mathbb{R}$ is a complete ordered field containing $\mathbb{Q}$ as a subfield.*

Definition 4.26 *The field of **complex numbers** $\mathbb{C}$ is defined as:*

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

with operations:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

Proposition 4.18 *$\mathbb{C}$ is a field with:*

1. *Additive identity:* $0 = 0 + 0i$
2. *Multiplicative identity:* $1 = 1 + 0i$
3. *Additive inverse:* $-(a + bi) = -a - bi$
4. *Multiplicative inverse:* $(a + bi)^{-1} = \dfrac{a - bi}{a^2 + b^2}$ *for* $a + bi \neq 0$

Theorem 13 (Fundamental Theorem of Algebra) *Every nonconstant polynomial with coefficients in $\mathbb{C}$ has at least one root in $\mathbb{C}$.*

Corollary 14 *Every polynomial of degree n with coefficients in $\mathbb{C}$ factors completely into n linear factors over $\mathbb{C}$.*

4.5.3 Field Characteristics

Definition 4.27 *The **characteristic** of a field K, denoted $\text{char}(K)$, is the smallest positive integer n such that:*

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

If no such n exists, we say the field has characteristic 0.

Example 50
1. $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$
2. $\text{char}(\mathbb{F}_p) = p$ *for any prime* p
3. $\text{char}(\mathbb{F}_{p^n}) = p$ *for any prime power* p^n

Theorem 15 *The characteristic of a field is either 0 or a prime number.*

4.6 Exercises

Exercise 1: Let R be a ring. Prove that for all $a, b \in R$:
a) $(-a) \cdot (-b) = a \cdot b$
b) $a \cdot (b - c) = a \cdot b - a \cdot c$

Solution.

1.

2. We prove $(-a) \cdot (-b) = a \cdot b$:

$$\begin{aligned}(-a) \cdot (-b) &= -[a \cdot (-b)] \quad \text{(by Proposition 4.13(2))} \\ &= -[-(a \cdot b)] \quad \text{(by Proposition 4.13(2))} \\ &= a \cdot b \quad \text{(since } -(-x) = x\text{)}\end{aligned}$$

3. We prove $a \cdot (b - c) = a \cdot b - a \cdot c$:

$$\begin{aligned}a \cdot (b - c) &= a \cdot [b + (-c)] \quad \text{(definition of subtraction)} \\ &= a \cdot b + a \cdot (-c) \quad \text{(distributivity)} \\ &= a \cdot b + [-(a \cdot c)] \quad \text{(by Proposition 4.13(2))} \\ &= a \cdot b - a \cdot c \quad \text{(definition of subtraction)}\end{aligned}$$

□

Exercise 2: Determine all invertible elements and zero divisors in $\mathbb{Z}/12\mathbb{Z}$.

Solution. The ring $\mathbb{Z}/12\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}$.
Invertible elements: An element $\bar{a}$ is invertible if and only if $\gcd(a, 12) = 1$.

$$\begin{aligned}\gcd(1, 12) = 1 &\Rightarrow \bar{1} \text{ is invertible} \\ \gcd(5, 12) = 1 &\Rightarrow \bar{5} \text{ is invertible} \\ \gcd(7, 12) = 1 &\Rightarrow \bar{7} \text{ is invertible} \\ \gcd(11, 12) = 1 &\Rightarrow \bar{11} \text{ is invertible}\end{aligned}$$

Also, $\bar{1}^{-1} = \bar{1}$, $\bar{5}^{-1} = \bar{5}$ (since $5 \times 5 = 25 \equiv 1 \pmod{12}$), $\bar{7}^{-1} = \bar{7}$ (since $7 \times 7 = 49 \equiv 1 \pmod{12}$), $\bar{11}^{-1} = \bar{11}$ (since $11 \times 11 = 121 \equiv 1 \pmod{12}$).

Zero divisors: An element $\bar{a} \neq \bar{0}$ is a zero divisor if there exists $\bar{b} \neq \bar{0}$ such that $\bar{a} \cdot \bar{b} = \bar{0}$.

$$\bar{2} \cdot \bar{6} = \bar{12} = \bar{0} \Rightarrow \bar{2}, \bar{6} \text{ are zero divisors}$$
$$\bar{3} \cdot \bar{4} = \bar{12} = \bar{0} \Rightarrow \bar{3}, \bar{4} \text{ are zero divisors}$$
$$\bar{4} \cdot \bar{3} = \bar{12} = \bar{0} \Rightarrow \bar{4}, \bar{3} \text{ are zero divisors}$$
$$\bar{6} \cdot \bar{2} = \bar{12} = \bar{0} \Rightarrow \bar{6}, \bar{2} \text{ are zero divisors}$$
$$\bar{8} \cdot \bar{3} = \bar{24} = \bar{0} \Rightarrow \bar{8}, \bar{3} \text{ are zero divisors}$$
$$\bar{9} \cdot \bar{4} = \bar{36} = \bar{0} \Rightarrow \bar{9}, \bar{4} \text{ are zero divisors}$$
$$\bar{10} \cdot \bar{6} = \bar{60} = \bar{0} \Rightarrow \bar{10}, \bar{6} \text{ are zero divisors}$$

So the zero divisors are: $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$. □

Exercise 3: Show that the set $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ forms a ring under usual addition and multiplication. Is it a field?

Solution. To show R is a ring, we verify the ring axioms:

1. **Closure under addition:** $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in R$
2. **Associativity of addition:** Follows from associativity in $\mathbb{R}$
3. **Additive identity:** $0 = 0 + 0\sqrt{2} \in R$
4. **Additive inverses:** $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in R$
5. **Commutativity of addition:** Follows from commutativity in $\mathbb{R}$
6. **Closure under multiplication:** $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in R$
7. **Associativity of multiplication:** Follows from associativity in $\mathbb{R}$
8. **Distributivity:** Follows from distributivity in $\mathbb{R}$

Thus R is a commutative ring with unity $1 = 1 + 0\sqrt{2}$.

Is it a field? No, R is not a field. For example, $2 = 2 + 0\sqrt{2} \in R$ but its multiplicative inverse is $\frac{1}{2} = \frac{1}{2} + 0\sqrt{2} \notin R$ since $\frac{1}{2} \notin \mathbb{Z}$. □

Exercise 4: Let $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the canonical homomorphism. Describe $\ker(\phi)$ and verify the First Isomorphism Theorem.

Solution. The canonical homomorphism is defined by $\phi(a) = \bar{a} = a + n\mathbb{Z}$.

Kernel:

$$\begin{aligned}\ker(\phi) &= \{a \in \mathbb{Z} : \phi(a) = \bar{0}\} \\ &= \{a \in \mathbb{Z} : \bar{a} = \bar{0}\} \\ &= \{a \in \mathbb{Z} : a \equiv 0 \pmod{n}\} \\ &= \{nk : k \in \mathbb{Z}\} = n\mathbb{Z}\end{aligned}$$

First Isomorphism Theorem verification: The theorem states that $\mathbb{Z}/\ker(\phi) \cong \text{Im}(\phi)$. We have:

- $\ker(\phi) = n\mathbb{Z}$
- $\text{Im}(\phi) = \mathbb{Z}/n\mathbb{Z}$ (since ϕ is surjective)
- $\mathbb{Z}/\ker(\phi) = \mathbb{Z}/n\mathbb{Z}$

Thus $\mathbb{Z}/\ker(\phi) = \mathbb{Z}/n\mathbb{Z} \cong \text{Im}(\phi) = \mathbb{Z}/n\mathbb{Z}$, verifying the theorem. □

Exercise 5: Prove that an ideal I in a commutative ring R is prime if and only if R/I is an integral domain.

Solution. Let I be an ideal in a commutative ring R.

($\Rightarrow$) Assume I is prime. We show R/I is an integral domain:

1. R/I is a commutative ring (since R is commutative)
2. R/I has unity $\bar{1} = 1 + I \neq \bar{0}$ (since I is proper)
3. Suppose $(\bar{a})(\bar{b}) = \bar{0}$ in R/I. This means $ab + I = I$, so $ab \in I$. Since I is prime, either $a \in I$ or $b \in I$, which means either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. Thus R/I has no zero divisors.

($\Leftarrow$) Assume R/I is an integral domain. We show I is prime: Suppose $ab \in I$. Then in R/I, we have $(\bar{a})(\bar{b}) = \overline{ab} = \bar{0}$. Since R/I is an integral domain (no zero divisors), either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, which means either $a \in I$ or $b \in I$. Thus I is prime. □

Exercise 6: Show that every finite integral domain is a field.

Solution. Let D be a finite integral domain with n elements: $D = \{0, a_1, a_2, \ldots, a_{n-1}\}$.

To show D is a field, we need to show that every nonzero element has a multiplicative inverse.

Take any nonzero element $a \in D$. Consider the map $f_a : D \to D$ defined by $f_a(x) = ax$.

We show f_a is injective: If $f_a(x) = f_a(y)$, then $ax = ay$, so $a(x - y) = 0$. Since D is an integral domain and $a \neq 0$, we must have $x - y = 0$, so $x = y$.

Since D is finite and f_a is injective, it must also be surjective. In particular, there exists some $x \in D$ such that $f_a(x) = ax = 1$. This x is the multiplicative inverse of a.

Since every nonzero element has an inverse, D is a field. □

Exercise 7: Verify that $\mathbb{Z}/5\mathbb{Z}$ is a field by constructing its multiplication table and showing every nonzero element has an inverse.

Solution. The multiplication table for $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ is:

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

From the table, we can identify the inverses:

- $\bar{1}^{-1} = \bar{1}$ (since $\bar{1} \times \bar{1} = \bar{1}$)
- $\bar{2}^{-1} = \bar{3}$ (since $\bar{2} \times \bar{3} = \bar{6} = \bar{1}$)
- $\bar{3}^{-1} = \bar{2}$ (since $\bar{3} \times \bar{2} = \bar{6} = \bar{1}$)
- $\bar{4}^{-1} = \bar{4}$ (since $\bar{4} \times \bar{4} = \bar{16} = \bar{1}$)

Every nonzero element has a multiplicative inverse, so $\mathbb{Z}/5\mathbb{Z}$ is a field. □

Exercise 8: Prove that there is no field with exactly 6 elements.

Solution. Suppose, for contradiction, that there exists a field F with exactly 6 elements.

By Theorem 4.10, the characteristic of a field is either 0 or a prime number. Since F is finite, its characteristic must be a prime p, and F contains $\mathbb{F}_p$ as a subfield.

By Theorem 4.7, the number of elements in a finite field is always a prime power p^n. Since $6 = 2 \times 3$ is not a prime power, there cannot be a field with exactly 6 elements.

More explicitly: If $\text{char}(F) = 2$, then $|F|$ would be 2^n for some n, but $2^n \neq 6$ for any integer n. If $\text{char}(F) = 3$, then $|F|$ would be 3^n for some n, but $3^n \neq 6$ for any integer n. If $\text{char}(F) = p > 3$, then $p^n \geq 5 > 6$ for $n \geq 1$.

Therefore, no field with exactly 6 elements can exist. □

Exercise 9: Let K be a field of characteristic $p > 0$. Show that the Frobenius map $\phi : K \to K$ defined by $\phi(x) = x^p$ is a field homomorphism.

Solution. We need to show that for all $x, y \in K$:

1. $\phi(x + y) = \phi(x) + \phi(y)$

2. $\phi(xy) = \phi(x)\phi(y)$

For (ii): $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$.
For (i): Using the binomial theorem:

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

For $0 < k < p$, the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p (since p is prime and doesn't divide $k!(p-k)!$ for $0 < k < p$). In a field of characteristic p, any multiple of p equals 0. Therefore:

$$(x+y)^p = x^p + y^p = \phi(x) + \phi(y)$$

Thus ϕ is a field homomorphism. □

Exercise 10: Show that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field.

Solution. We already know from Problem 3 that $\mathbb{Q}[\sqrt{2}]$ is a commutative ring with unity. To show it's a field, we need to show that every nonzero element has a multiplicative inverse.

Let $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ be nonzero. Then not both a and b are zero. Consider:

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

We claim $a^2 - 2b^2 \neq 0$. If $a^2 - 2b^2 = 0$, then either:

- If $b = 0$, then $a^2 = 0 \Rightarrow a = 0$, contradicting that $a + b\sqrt{2}$ is nonzero.
- If $b \neq 0$, then $\left(\frac{a}{b}\right)^2 = 2$, so $\frac{a}{b} = \pm\sqrt{2}$, but $\sqrt{2}$ is irrational, while $\frac{a}{b}$ is rational, contradiction.

Therefore, $a^2 - 2b^2 \neq 0$, and we can define the inverse:

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

Since every nonzero element has a multiplicative inverse in $\mathbb{Q}[\sqrt{2}]$, it is a field. □