Rings Introduction

Gudfit

Contents

0

Sets and Fundamentals

We begin by formalising the definitions and operations of set theory that serve as the foundation for ring theory.

0.1 *Sets and Subsets*

Definition 0.1. ***Set.***
A **set** is a collection of distinct objects, referred to as **elements**. We denote sets by uppercase letters $(A, B, \dots)$ and elements by lowercase letters $(a, b, \dots)$.

- If an element a belongs to a set A, we write $a \in A$.
- If a does not belong to A, we write $a \notin A$.

A set may be defined by listing its elements or by specifying a property $P(x)$ satisfied by all members: $A = \{x \mid P(x)\}$. For example, the set of even integers is written as $\{a \in \mathbb{Z} \mid a \equiv 0 \pmod{2}\}$.

定義

Definition 0.2. ***Subsets and Equality.***
Let A and B be sets.

1. A is a **subset** of B, denoted $A \subseteq B$ or $B \supseteq A$, if every element of A is also an element of B (see *figure 1*).
2. A and B are **equal**, denoted $A = B$, if $A \subseteq B$ and $B \subseteq A$.
3. If $A \subseteq B$ but $A \neq B$, then A is a **proper subset** of B, denoted $A \subset B$ or $A \subsetneq B$.

定義

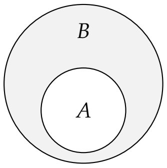

Figure 1: Visualisation of inclusion: $A \subseteq B$.

Two specific concepts regarding the size and emptiness of sets are essential.

Definition 0.3. ***Empty and Finite Sets.***

- The **empty set**, denoted $\varnothing$, is the set containing no elements. It is a subset of every set and a proper subset of every non-empty set.
- A set A is **finite** if it contains a finite number of elements. This number is called the **cardinality** or order of A, denoted $|A|$.
- If A is not finite, we define its order as $|A| = \infty$.

定義

Remark.

One may conceptualise these definitions through an analogy: a *Class* corresponds to a Set, the *Students* are the Elements, and a *Study Group* forms a Subset. The set of all classes constitutes a family of sets.

Definition 0.4. ***Power Set.***
The **power set** of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

定義

Operations on Sets

We define the standard algebraic operations on sets. Let A and B be sets, and let $\{A_i\}_{i\in I}$ be a family of sets indexed by I.

Definition 0.5. ***Intersection.***
The **intersection** of A and B, illustrated in *figure 2*, is the set of elements common to both:

$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}.$$

For an indexed family, the intersection is defined as:

$$\bigcap_{i\in I} A_i := \{x \mid x \in A_i \text{ for all } i \in I\}.$$

定義

Definition 0.6. ***Union.***
The **union** of A and B is the set of elements belonging to at least one of them:

$$A \cup B := \{x \mid x \in A \text{ or } x \in B\}.$$

For an indexed family:

$$\bigcup_{i\in I} A_i := \{x \mid x \in A_i \text{ for some } i \in I\}.$$

If the sets A_i are pairwise disjoint (i.e., $A_i \cap A_j = \varnothing$ for $i \neq j$), their union is called a **disjoint union**, denoted $\bigsqcup_{i\in I} A_i$.

定義

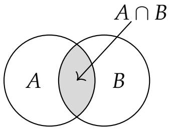

Figure 2: The intersection $A \cap B$.

Definition 0.7. ***Difference.***
Let A and B be subsets of a universal set U. The **difference** (or rela-

tive complement) of B in A is:

$$A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}.$$

The **complement** of A in U is:

$$A^c := \{x \in U \mid x \notin A\}.$$

定義

It follows directly from the definitions that a set can be partitioned by any subset:

$$A = (A \cap B) \sqcup (A \setminus B).$$

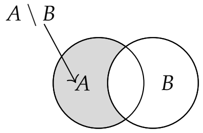

Figure 3: The set difference $A \setminus B$.

For finite sets, the sizes of unions and intersections are related by the Inclusion-Exclusion Principle. The base case for two sets is given by:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

This generalises to arbitrary finite collections.

Proposition 0.1. ***Inclusion-Exclusion Principle.***
Let $A_1, \ldots, A_n$ be finite subsets of a set U. Then:

$$|A_1 \cup \cdots \cup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{\{i_1,\ldots,i_j\} \subseteq \{1,\ldots,n\}} |A_{i_1} \cap \cdots \cap A_{i_j}|.$$

命題

Proof

We proceed by induction on n, the number of sets. The base case $n = 2$ is stated above. The inductive step involves applying the base case to the union of A_{n+1} and the set $S = \bigcup_{k=1}^{n} A_k$, then expanding using the inductive hypothesis.

■

The interaction between union, intersection, and complements is governed by De Morgan's laws.

Proposition 0.2. ***De Morgan's Laws.***
Let $\{A_i\}_{i \in I}$ be a family of subsets of U. Then:

$$\bigcap_{i \in I} A_i^c = \left(\bigcup_{i \in I} A_i \right)^c.$$

命題

Proof

> We track the logical equivalence of element membership:
>
> $$x \in \bigcap_{i \in I} A_i^c \iff \forall i \in I,\ x \in A_i^c \iff \forall i \in I,\ x \notin A_i \iff \neg(\exists i \in I,\ x \in A_i)$$
> $$\iff x \notin \bigcup_{i \in I} A_i \iff x \in \left(\bigcup_{i \in I} A_i\right)^c.$$
>
> ■

Algebraic structures often involve pairs or tuples of elements.

> **Definition 0.8.** ***Cartesian Product.***
> The **Cartesian product** of two sets A and B is the set of all ordered pairs:
>
> $$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$
>
> More generally, for a family $\{A_i\}_{i \in I}$, the product is the set of sequences (or functions $I \to \cup A_i$):
>
> $$\prod_{i \in I} A_i := \{(a_i)_{i \in I} \mid a_i \in A_i\}.$$
>
> 定義

Throughout these notes, we adhere to the following standard notation for numerical sets:

- $\mathbb{Z}_+$: The set of positive integers $\{1, 2, 3, \ldots\}$.
- $\mathbb{N} = \mathbb{Z} \cup \{0\}$: The set of natural numbers (including 0).
- $\mathbb{Z}$: The set of integers.
- $\mathbb{Q}$: The set of rational numbers.
- $\mathbb{R}$: The set of real numbers.
- $F[X]$: The set of polynomials in variable X with coefficients in a field (or ring) F.

0.2 *Mappings and Binary Operations*

The concept of a function, central to analysis, is generalised in algebra to the notion of a mapping between arbitrary sets.

> **Definition 0.9.** ***Mapping.***
> Let A and B be sets. A **mapping** (or map) $f : A \to B$ is a rule that assigns to every element $a \in A$ a unique element $b \in B$, denoted by $f(a) = b$.
>
> - A is the **domain** of f.
> - The set $f(A) = \{f(a) \mid a \in A\} \subseteq B$ is the **image** (or range) of f.
> - If $f(a) = b$, then b is the image of a, and a is a **preimage** of b.
>
> 定義

Two mappings $f, g : A \to B$ are **equal**, denoted $f = g$, if $f(a) = g(a)$

for all $a \in A$.

> **Definition 0.10.** ***Properties of Mappings.***
> A mapping $f : A \to B$ is:
>
> ***Injective*** (or one-to-one) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$ for all $a_1, a_2 \in A$.
>
> ***Surjective*** (or onto) if for every $b \in B$, there exists at least one $a \in A$ such that $f(a) = b$. Equivalently, $f(A) = B$.
>
> ***Bijective*** (or a one-to-one correspondence) if it is both injective and surjective.
>
> 定義

Mappings can be combined sequentially.

> **Definition 0.11.** ***Composition.***
> Let $f : A \to B$ and $g : B \to C$ be mappings. The **composite mapping** $g \circ f : A \to C$ is defined by:
>
> $$(g \circ f)(a) = g(f(a)) \quad \text{for all } a \in A.$$
>
> 定義

While composition is not commutative in general (i.e., $g \circ f \neq f \circ g$), it satisfies a fundamental stability property known as associativity.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

Figure 4: Composition of mappings.

> **Proposition 0.3.** ***Associativity of Composition.***
> Let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be mappings. Then:
>
> $$(h \circ g) \circ f = h \circ (g \circ f).$$
>
> 命題

> *Proof*
>
> For any $a \in A$, we evaluate both sides:
>
> $$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))).$$
>
> $$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))).$$
>
> Since the mappings agree on every element of the domain, they are equal.
>
> ■

Algebraic structures are essentially sets equipped with operations that combine elements.

> **Definition 0.12.** ***Binary Operation.***
> Let X be a set. An **algebraic binary operation** (or composition law) on X is a function $T : X \times X \to X$. For every ordered pair $(a, b) \in X \times$

X, this map assigns a unique element $T(a, b) \in X$.

定義

Rather than writing $T(a, b)$, we typically use infix notation such as $a * b$, $a \circ b$, $a + b$, or simply ab. In group theory, we most frequently use multiplicative notation (ab) or additive notation ($a + b$).
A set X equipped with a specific binary operation $*$ is called an **algebraic structure** or algebraic system, denoted $(X, *)$. It is important to note that a single set can support multiple distinct operations. For instance, the integers $\mathbb{Z}$ form different structures under addition $(\mathbb{Z}, +)$ and multiplication $(\mathbb{Z}, \cdot)$. One could even define exotic operations like $n * m = n + m - nm$, creating yet another structure.
While one can define endless arbitrary operations, algebra focuses on those satisfying specific, powerful axioms. One such fundamental property is the existence of a neutral element.

Definition 0.13. ***Unit Element.***
An element $e \in X$ is called a **unit element** (or neutral element) relative to the operation $*$ if $e * x = x * e = x$ for all $x \in X$.

定義

It follows immediately that such an element, if it exists, is unique.

Proposition 0.4. ***Uniqueness of Unit Element.***
An algebraic structure $(X, *)$ possesses at most one unit element.

命題

Proof

Suppose e and e' are unit elements. By the defining property of e, we have $e * e' = e'$. By the defining property of e', we have $e * e' = e$. Thus $e = e'$.

■

Example 0.1. Arithmetic Operations. The standard operations of addition (+), subtraction (−), and multiplication (×) are binary operations on $\mathbb{R}$. Division is not a binary operation on $\mathbb{R}$ because division by zero is undefined; however, it is a binary operation on the set of non-zero real numbers $\mathbb{R} \setminus \{0\}$.

範例

Example 0.2. Function Spaces. Let Σ_A be the set of all mappings from a set A to itself. The composition of mappings $\circ$ is a binary operation on Σ_A. Similarly, let S_A be the set of all bijections from A to itself. Since the composition of bijections is a bijection, $\circ$ is also a binary operation on S_A.

範例

Definition 0.14. ***Associativity and Commutativity.***
Let $*$ be a binary operation on S.

1. The operation is **associative** if for all $a, b, c \in S$:

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

2. The operation is **commutative** if for all $a, b \in S$:

$$a * b = b * a.$$

定義

0.3 *Equivalence Relations and Partitions*

In many contexts, we wish to treat distinct elements as "effectively equal" if they share a specific property (e.g., integers with the same parity). This leads to the concept of equivalence relations.

Definition 0.15. ***Equivalence Relation.***
A relation $\sim$ on a set A is an **equivalence relation** if it satisfies three axioms for all $a, b, c \in A$:
Reflexivity: $a \sim a$.
Symmetry: If $a \sim b$, then $b \sim a$.
Transitivity: If $a \sim b$ and $b \sim c$, then $a \sim c$.

定義

An equivalence relation allows us to group elements together.

Definition 0.16. ***Partition.***
A **partition** of a set A is a decomposition of A into a disjoint union of non-empty subsets. That is, $A = \bigsqcup_{i \in I} A_i$.

定義

These two concepts are mathematically dual. Given an equivalence relation $\sim$, we define the **equivalence class** of a as:

$$[a] = \{x \in A \mid x \sim a\}.$$

Lemma 0.1. ***Properties of Classes.***
For any $a, b \in A$, either $[a] = [b]$ (if $a \sim b$) or $[a] \cap [b] = \varnothing$ (if $a \nsim b$).

引理

Proof

If $x \in [a] \cap [b]$, then $x \sim a$ and $x \sim b$. By symmetry $a \sim x$, and by transitivity $a \sim b$. If $a \sim b$, let $y \in [a]$. Then $y \sim a$ and $a \sim b \implies y \sim b \implies y \in [b]$. Thus $[a] \subseteq [b]$. By symmetry, $[b] \subseteq [a]$, so $[a] =$

> $[b]$.
>
> ■

Consequently, the distinct equivalence classes form a partition of A:

$$A = \bigsqcup_{a \in A} [a].$$

> **Theorem 0.1.** ***Equivalence and Partitions.***
> There is a one-to-one correspondence between equivalence relations on a set A and partitions of A.
> - Every equivalence relation induces a partition into equivalence classes.
> - Conversely, given a partition $A = \bigsqcup_{i \in I} A_i$, the relation defined by "$a \sim b$ if a and b belong to the same subset A_i" is an equivalence relation.
>
> 定理

> **Example 0.3.** Parity. Let $A = \mathbb{Z}$. The relation $a \equiv b \pmod 2$ is an equivalence relation. It partitions $\mathbb{Z}$ into two classes:
> - $[0] = \{\dots, -2, 0, 2, \dots\}$ (the even integers).
> - $[1] = \{\dots, -1, 1, 3, \dots\}$ (the odd integers).
>
> 範例

Partitions Induced by Mappings

A natural source of equivalence relations is the "fiber" structure of a mapping. Let $f : A \to B$ be a mapping. For any $b \in f(A)$, the **preimage** or fiber of b is:

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}.$$

Since every element $a \in A$ maps to exactly one image, the fibers are pairwise disjoint and cover A. Thus, we have the partition:

$$A = \bigsqcup_{b \in f(A)} f^{-1}(b).$$

The corresponding equivalence relation is defined by $a \sim a' \iff f(a) = f(a')$.

> **Example 0.4.** Geometric Partition. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be defined by $f(x, y) = x - y$. For any real number $c \in \mathbb{R}$, the fiber $f^{-1}(c)$ is the set of points satisfying $x - y = c$, or $y = x - c$. Geometrically, this partitions the plane $\mathbb{R}^2$ into a family of parallel lines with slope 1 (see *figure 5*). Points are equivalent if they lie on the same line.
>
> 範例

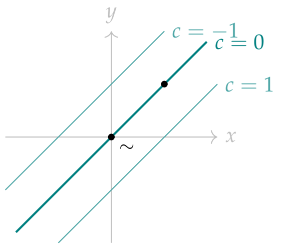

Figure 5: The equivalence classes of $f(x, y) = x - y$ form parallel lines.

0.4 Exercises

1. **Distributive Laws.** Let B and $\{A_i\}_{i\in I}$ be subsets of a universal set Ω. Prove:

   (a) $B \cap (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(B \cap A_i)$.

   (b) $B \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(B \cup A_i)$.

2. **Power Set Cardinality.** Let A be a finite set with n elements. Let $\mathcal{P}(A)$ be the set of all subsets of A. Prove that $|\mathcal{P}(A)| = 2^n$.

   Consider the correspondence between subsets and binary strings of length n.

3. **One-Sided Inverses.** Let $f : A \to B$ be a map with $A \neq \varnothing$.

   (a) Prove that f is injective if and only if there exists a left inverse $g : B \to A$ such that $g \circ f = \mathrm{id}_A$.

   (b) Prove that f is surjective if and only if there exists a right inverse $h : B \to A$ such that $f \circ h = \mathrm{id}_B$. (Uses the Axiom of Choice to pick one preimage for each $b \in B$.)

4. **Inverse of Composition.** Let $f : A \to B$ and $g : B \to C$ be bijections. Prove that $g \circ f$ is a bijection and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

5. **Counting Functions.** Let A and B be finite sets with $|A| = m$ and $|B| = n$.

   (a) How many distinct maps $f : A \to B$ exist?

   (b) How many distinct binary operations can be defined on A?

6. **Kernel Equivalence.** Let $f : A \to B$ be a map. Define a relation $\sim$ on A by $a \sim a'$ if and only if $f(a) = f(a')$. Prove that this is an equivalence relation. What are the equivalence classes?

7. **Independence of Axioms.** Prove that the three axioms of an equivalence relation (reflexivity, symmetry, transitivity) are independent. Specifically, for each axiom, construct a relation that fails that axiom but satisfies the other two.

   For example, find a relation that is symmetric and transitive but not reflexive.

1
Rings and Fields

We now turn our attention to algebraic structures equipped with two binary operations. In the study of elementary number theory, the integers $\mathbb{Z}$ form the prototypical example of such a structure, possessing both addition and multiplication. Specifically, the set of polynomials $F[X]$ and the set of $n \times n$ matrices $M_n(F)$ share these arithmetic properties. We formalise this commonality through the definition of a ring.

Rings unify arguments across distinct contexts:

Number Theory. Extensions of $\mathbb{Z}$ facilitate the solution of Diophantine equations. For example, $n = x^2 + y^2$ factors as $(x+iy)(x-iy)$ in the Gaussian integers $\mathbb{Z}[i]$.

Algebraic Geometry. Geometric shapes defined by polynomial systems are analysed via their rings of functions.

Topology. Cohomology classes of topological spaces form rings, translating topological structure into algebra.

1.1 *Definitions and Examples*

Definition 1.1. ***Ring.***
A **ring** is a set R equipped with two binary operations, denoted by addition $(+)$ and multiplication $(\cdot)$, and two distinguished elements $0 \in R$ (the zero) and $1 \in R$ (the identity), satisfying the following axioms:

$(R, +)$ *is an Abelian group with identity* 0. That is:

- *(Associativity)* $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$.
- *(Commutativity)* $a+b = b+a$ for all $a, b \in R$.
- *(Identity)* $a+0 = a$ for all $a \in R$.
- *(Inverse)* For every $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.

$(R, \cdot)$ *is a monoid with identity* 1. That is:

(Associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

(Identity) $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Distributivity That is:

Multiplication distributes over addition $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

If the multiplication operation is commutative (i.e., $a \cdot b = b \cdot a$ for all $a, b \in R$), then R is called a **commutative ring**.

定義

Remark.

We adhere to the convention that a ring must possess a multiplicative identity 1. Some authors refer to structures without a multiplicative identity as *rngs*, but we shall not consider them here.

Proposition 1.1. ***Basic Properties of Rings.***
Let R be a ring. For any $a, b \in R$:

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. If $1 = 0$, then $R = \{0\}$.

命題

Proof

1. We observe that $0 + 0 = 0$. Distributivity implies:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Adding $-(a \cdot 0)$ to both sides (using the group property of addition) yields $0 = a \cdot 0$. The proof for $0 \cdot a$ is similar.

2. We compute $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$. Thus $a \cdot (-b)$ is the additive inverse of $a \cdot b$.
3. Apply (2) twice: $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.
4. If $1 = 0$, then for any $r \in R$, $r = r \cdot 1 = r \cdot 0 = 0$.

■

The simplest possible ring is the **zero ring**, $R = \{0\}$, where $1 = 0$. In all other cases, we assume $1 \neq 0$.

Example 1.1. Standard Numerical Rings. The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all commutative rings under the standard operations.

範例

Example 1.2. Matrix Rings. Let R be a commutative ring. The set $M_n(R)$ of $n \times n$ matrices with entries in R forms a ring under matrix addition and multiplication.

- The zero element is the zero matrix 0_n.

- The identity element is the identity matrix I_n.

If $n \geq 2$, matrix multiplication is generally not commutative, so $M_n(R)$ is a non-commutative ring. The group of units of this ring, $U(M_n(R))$, is called the **general linear group**, denoted $GL_n(R)$.

範例

Example 1.3. Quaternions. The quaternions are a subring of $M_2(\mathbb{C})$. We denote the ring of quaternions by $\mathbb{H}$. Let

$$\mathbb{H} = \left\{ \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}.$$

Then $\mathbb{H}$ forms a non-commutative ring under matrix addition and multiplication. Similarly, the subset

$$\mathbb{H}(\mathbb{Q}) = \left\{ \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \mid \alpha, \beta \in \mathbb{Q}(i) \right\}$$

is also a non-commutative ring, where $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

範例

Example 1.4. Ring of Functions. Let X be a non-empty set and R a ring. The set R^X of functions $f : X \to R$ is a ring under pointwise addition and multiplication:

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x).$$

The zero element is the constant function $x \mapsto 0$, and the identity is $x \mapsto 1$.

範例

A fundamental class of rings in number theory arises from the equivalence classes of integers.

Example 1.5. Integers Modulo n. Let n be a positive integer. Recall from the definition of an Equivalence Relation that the relation defined by $a \equiv b \pmod{n}$ (meaning $n \mid (a-b)$) partitions $\mathbb{Z}$ into n distinct equivalence classes. We denote the set of these classes by $\mathbb{Z}/n\mathbb{Z}$.

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

We define operations on these classes by:

$$[a] + [b] = [a+b], \quad [a] \cdot [b] = [ab].$$

One may verify that these operations are well-defined (independent of the choice of representatives). Under these operations, $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring.

範例

For commutative rings, the algebraic expansion of powers behaves as it does in elementary algebra.

Theorem 1.1. ***Newton's Binomial Theorem.***
Let R be a commutative ring. For any $x, y \in R$ and $n \in \mathbb{Z}_+$:

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

定理

Proof

The proof proceeds by induction on n, using the property $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$. We rely on the commutativity of R to rearrange terms such that $x^a y^b = y^b x^a$.

■

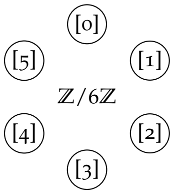

Figure 1.1: The elements of the ring $\mathbb{Z}/6\mathbb{Z}$.

Special Elements and Structures

In $\mathbb{Z}$, the product of two non-zero integers is always non-zero. This property does not hold for arbitrary rings.

Definition 1.2. ***Zero Divisors and Units.***
Let R be a ring.

1. A non-zero element $a \in R$ is a **zero divisor** if there exists a non-zero $b \in R$ such that $ab = 0$ or $ba = 0$.
2. An element $a \in R$ is a **unit** (or invertible) if there exists $b \in R$ such that $ab = ba = 1$. This inverse is unique and denoted a^{-1}.

定義

Remark.

Not to be confused with the 'unit element' (identity) of Chapter 0; here 'unit' means invertible.

Example 1.6. Zero Divisors in $\mathbb{Z}/6\mathbb{Z}$. In $\mathbb{Z}/6\mathbb{Z}$, we observe that $[2] \cdot [3] = [6] = [0]$. Thus, both $[2]$ and $[3]$ are zero divisors.

範例

Lemma 1.1. ***Group of Units.***
The set of units of a ring R, denoted $U(R)$ or $R^\times$, forms a group under multiplication.

引理

Proof

Identity 1 is clearly a unit ($1 \cdot 1 = 1$). If a is a unit with inverse a^{-1}, then a^{-1} is a unit with inverse a. If a, b are units, then

> $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(1)a^{-1} = 1$, so ab is a unit.
>
> ■

We classify commutative rings based on the behaviour of their zero divisors and inverses.

> **Definition 1.3.** ***Integral Domains and Fields.***
> Let R be a commutative ring with $1 \neq 0$.
> 1. R is an **integral domain** if it has no zero divisors. That is, $ab = 0 \implies a = 0$ or $b = 0$.
> 2. R is a **field** if every non-zero element is a unit.
>
> 定義

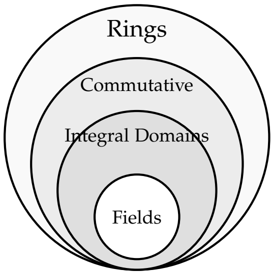

Figure 1.2: Hierarchy of ring structures.

The standard inclusions are visualised in *figure* 1.2. Note that every field is an integral domain (since units cannot be zero divisors), but the converse is not true (e.g., $\mathbb{Z}$ is a domain but not a field).

> **Proposition 1.2.** ***Cancellation Law.***
> Let R be a commutative ring. R is an integral domain if and only if the cancellation law holds: for all $a, b, c \in R$ with $a \neq 0$, if $ab = ac$, then $b = c$.
>
> 命題

> *Proof*
>
> Suppose R is a domain and $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$. Since a is not a zero divisor, $b - c = 0$, so $b = c$. Conversely, if the cancellation law holds and $ab = 0$ with $a \neq 0$, then $ab = a \cdot 0 \implies b = 0$. Thus R has no zero divisors.
>
> ■

Polynomial Rings

A very important class of rings that we will study are the polynomial rings. Given a ring R, we can construct a new ring consisting of polynomials with coefficients in R.

> **Definition 1.4.** ***Polynomial Ring.***
> The **polynomial ring** $R[X]$ consists of formal sums
>
> $$f(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \cdots + a_n X^n,$$
>
> where $a_i \in R$ and $n \geq 0$. Addition and multiplication are defined naturally:
> *Sum:* $\sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i$.
> *Product:* $\left(\sum a_i X^i\right)\left(\sum b_j X^j\right) = \sum c_k X^k$, where $c_k = \sum_{i+j=k} a_i b_j$.
>
> 定義

We may extend this construction to multiple variables. The ring $R[X, Y]$ can be viewed as $(R[X])[Y]$. If R is an integral domain, then $R[X]$ is also an integral domain.

Example 1.7. Gaussian Integers as a Quotient. Consider the polynomial ring $\mathbb{Z}[X]$. The set of numbers $a + bi$ with $a, b \in \mathbb{Z}$ (the Gaussian integers) has the same algebraic structure as the quotient structure $\mathbb{Z}[X]/(X^2 + 1)$, a concept we shall define in subsequent chapters.

範例

1.2 *Substructures and New Rings from Old*

Having established the definitions of rings and fields, we now examine how to locate these structures within larger ones (subrings) and how to construct new rings from existing ones (direct products and fractions).

Subrings and Subfields

Just as subgroups are central to group theory, we define subsets of rings that preserve the algebraic structure.

Definition 1.5. ***Subring.***
Let R be a ring. A subset $S \subseteq R$ is a **subring** of R if S is a ring under the induced operations of addition and multiplication from R, and S shares the same multiplicative identity as R. Specifically, S must satisfy:

1. $0_R \in S$ and $1_R \in S$.
2. For all $a, b \in S$, we have $a + b \in S$ and $a \cdot b \in S$.
3. For all $a \in S$, $-a \in S$.

Similarly, a subset K of a field F is a **subfield** if K is a field under the induced operations. This requires K to be a subring where every nonzero element has a multiplicative inverse in K.

定義

Remark.

Some definitions of subrings do not require the presence of the identity 1_R, but in these notes, all subrings are assumed to contain the identity element.

Example 1.8. Rational Quaternions. Recall the ring of quaternions $\mathbb{H}$ (example 1.3). The subset

$$\mathbb{H}(\mathbb{Q}) = \left\{ \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \mid \alpha, \beta \in \mathbb{Q}(i) \right\}$$

forms a subring of $\mathbb{H}$.

範例

It is a routine verification that the intersection of subrings is itself a subring.

Lemma 1.2. ***Intersections of Subrings.***
Let $\{S_i\}_{i\in I}$ be a family of subrings of a ring R. Then the intersection $\bigcap_{i\in I} S_i$ is a subring of R.

引理

Proof

Since $1 \in S_i$ for all i, $1 \in \bigcap S_i$. If $a, b \in \bigcap S_i$, then $a, b \in S_i$ for all i, implying $a - b \in S_i$ and $ab \in S_i$. Thus the intersection is closed under subtraction and multiplication.

■

This lemma allows us to define the smallest subring satisfying certain properties.

Definition 1.6. ***Generated Subring.***
Let S be a subring of R and let $\alpha \in R$. The **subring generated by** α **over** S, denoted $S[\alpha]$, is the intersection of all subrings of R containing both S and α. Explicitly, elements of $S[\alpha]$ are polynomials in α with coefficients in S:

$$S[\alpha] = \left\{ \sum_{k=0}^{n} s_k \alpha^k \;\middle|\; n \in \mathbb{N}, s_k \in S \right\}.$$

We say we obtain $S[\alpha]$ by **adjoining** α to S.

定義

Example 1.9. Gaussian Integers. Adjoining the imaginary unit $i = \sqrt{-1}$ to $\mathbb{Z}$ yields the ring of **Gaussian integers** $\mathbb{Z}[i]$. Elements are of the form $\sum_{k=0}^{n} a_k i^k$. Since $i^2 = -1$, powers of i cycle through $1, i, -1, -i$. Thus, any polynomial expression reduces to a linear form.

範例

Proposition 1.3. ***Structure of Gaussian Integers.***
Every element in $\mathbb{Z}[i]$ can be uniquely expressed as $a + bi$ where $a, b \in \mathbb{Z}$.

命題

Proof

Given a polynomial expression $\sum_{n=0}^{N} a_n i^n$, we separate terms by the parity of the exponent:

$$\sum_{n=0}^{N} a_n i^n = (a_0 - a_2 + a_4 - \dots) + i\,(a_1 - a_3 + a_5 - \dots)\,.$$

Let $A = \sum_k (-1)^k a_{2k}$ and $B = \sum_k (-1)^k a_{2k+1}$. Then the sum equals $A + Bi$ with $A, B \in \mathbb{Z}$. Uniqueness follows from the linear independence of 1 and i over $\mathbb{R}$. If $a + bi = c + di$, then $(a - c) = (d - b)i$. Squaring gives $(a-c)^2 = -(d-b)^2$. Since squares of real numbers are non-negative, this forces $a = c$ and $b = d$.

■

If the element α satisfies no polynomial equation with coefficients in S (i.e., α is transcendental), the structure of $S[\alpha]$ has the same algebraic structure as the polynomial ring $S[X]$.

Example 1.10. Adjoining π. Consider $\mathbb{Z}[\pi] \subset \mathbb{R}$. Since π is transcendental, no non-zero polynomial in $\mathbb{Z}[X]$ vanishes at π. Thus, the representation of elements is unique:

$$\sum_{n=0}^{k} a_n \pi^n = \sum_{n=0}^{m} b_n \pi^n \implies a_n = b_n \text{ for all } n.$$

範例

Direct Products

We can construct a new ring from two existing rings by defining operations component-wise.

Definition 1.7. ***Direct Product.***
Let R_1 and R_2 be rings. The **direct product** $R = R_1 \times R_2$ is the set of pairs (r_1, r_2) with operations:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2).$$

The additive identity is $(0_{R_1}, 0_{R_2})$ and the multiplicative identity is $(1_{R_1}, 1_{R_2})$.

定義

Remark.

The direct product of two non-zero rings is never an integral domain. Consider $a = (1, 0)$ and $b = (0, 1)$. Both a and b are non-zero, yet their product is $(0, 0)$.

Fields of Fractions and Localisation

For the integers $\mathbb{Z}$, division is not always possible. To resolve this, we construct the rationals $\mathbb{Q}$. We can generalise this process to any integral domain.

> **Definition 1.8.** *Field of Fractions.*
> Let R be an integral domain. The **field of fractions** of R, denoted $K(R)$ or $\operatorname{Frac}(R)$, is the set of equivalence classes of pairs $(a, b) \in R \times (R \setminus \{0\})$, typically written as fractions a/b. The equivalence relation is defined by:
>
> $$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc.$$
>
> Addition and multiplication are defined as in elementary arithmetic:
>
> $$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$
>
> We identify $r \in R$ with the fraction $r/1 \in K(R)$, making R a subring of $K(R)$.
>
> 定義

The field of fractions is the "smallest" field containing R. However, sometimes we do not wish to invert *every* non-zero element, but only a specific subset.

> **Definition 1.9.** *Multiplicative System.*
> A subset $S \subseteq R$ is a **multiplicative system** if:
> 1. $1 \in S$.
> 2. $0 \notin S$.
> 3. If $a, b \in S$, then $ab \in S$.
>
> 定義

> **Definition 1.10.** *Localisation.*
> Let R be an integral domain and S a multiplicative system. The **localisation** of R at S, denoted $S^{-1}R$, is the subring of $K(R)$ consisting of fractions with denominators in S:
>
> $$S^{-1}R = \left\{ \frac{a}{b} \in K(R) \;\middle|\; a \in R, b \in S \right\}.$$
>
> 定義

> **Example 1.11.** Dyadic Rationals. Let $R = \mathbb{Z}$ and let $S = \{2^n \mid n \in \mathbb{N}\}$ be the set of powers of 2. The localisation $S^{-1}\mathbb{Z} = \mathbb{Z}[\frac{1}{2}]$ consists of rational numbers whose denominators are powers of 2.
>
> 範例

$$\begin{tikzcd}
K(R) \\
S^{-1}R \arrow[u, hook] \\
R \arrow[u, hook]
\end{tikzcd}$$

Figure 1.3: Embeddings of a domain into its localisation and field of fractions, where $\hookrightarrow$ denotes inclusion.

> **Example 1.12.** Localisation at Odd Integers. Let S be the set of odd integers in $\mathbb{Z}$. Then $S^{-1}\mathbb{Z}$ is the ring of rational numbers a/b where b is odd. In this ring, 2 is not invertible, but $3, 5, 7, \ldots$ are units.
>
> 範例

1.3 *Exercises*

In the following exercises, R denotes a ring with identity $1 \neq 0$ unless otherwise specified.

1. **Invertibility in $\mathbb{Z}/n\mathbb{Z}$.** Let $n \geq 2$ be a positive integer.
   (a) The necessary and sufficient condition for element $[a]$ in the ring $\mathbb{Z}/n\mathbb{Z}$ to be invertible is $\gcd(a, n) = 1$.
   (b) If p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field. If $n \geq 2$ is not a prime number, then $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.
2. **Quaternions.** Prove that any non-zero element in $\mathbb{H}$ is multiplicatively invertible.
3. **Quadratic Integers.**
   (a) Let $d \geq 1$ be a positive integer. Use $R = \mathbb{Z}[\sqrt{-d}] \subseteq \mathbb{C}$ to explain that R is an integral domain and determine the unit group of R.
   (b) Now consider the real quadratic case. For $d = 2$, find a unit in $\mathbb{Z}[\sqrt{2}]$ of infinite order, contrasting with the finite unit groups found in (1).
4. **Endomorphism Ring.** Let A be an Abelian group, and let $\mathrm{End}(A)$ be the set of all functions $f : A \to A$ such that $f(a+b) = f(a) + f(b)$ for all $a, b \in A$. For $f, g \in \mathrm{End}(A)$, define

   $$(f+g)(a) = f(a) + g(a), \quad (f \cdot g)(a) = f(g(a)) \quad (a \in A).$$

   Prove that $\mathrm{End}(A)$ is a ring with identity under the above operations, and find its unit group.
5. **Group Rings.** Let G be a multiplicative group, and R be a ring with identity. Define the set

   $$R[G] = \left\{ \sum_{g \in G} r_g g \mid r_g \in R, \text{ and there are only finitely many } r_g \neq 0 \right\}.$$

   Define on the set $R[G]$:

   $$\sum_{g\in G} r_g g + \sum_{g\in G} t_g g = \sum_{g\in G} (r_g + t_g) g, \quad \left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} t_g g\right) = \sum_{g\in G}\left(\sum_{g'g''=g} r_{g'} t_{g''}\right) g.$$

(a) Prove: The addition and multiplication defined above are binary operations in $R[G]$, and $R[G]$ forms a ring, called the group ring of group G over ring R.

(b) $R[G]$ is commutative if and only if R is a commutative ring and G is an Abelian group.

(c) If the identity of ring R is 1_R and the identity of group G is e, then $1_R e$ is the identity element of the group ring $R[G]$.

(d) R can be naturally viewed as a subring of $R[G]$.

(e) Try to determine the unit groups of $\mathbb{Z}[C_2]$ (where $C_2 = \{1, \sigma\}$ is the cyclic group of order 2) and $R[\mathbb{Z}]$, where R is an integral domain.

6. ***p*-adic Integers.** Let $R = \{a = (a_1, a_2, \dots) \mid a_n \in \mathbb{Z}, 0 \leq a_n \leq p^n - 1, a_n \equiv a_{n+1} \pmod{p^n}\}$. Let $a, b \in R$. Define

$$a + b = c, \quad 0 \leq c_n \leq p^n - 1, c_n \equiv a_n + b_n \pmod{p^n},$$

$$a \cdot b = d, \quad 0 \leq d_n \leq p^n - 1, d_n \equiv a_n b_n \pmod{p^n}.$$

(a) R becomes a commutative ring with identity, called the p-adic integer ring, denoted as $\mathbb{Z}_p$.

(b) $\mathbb{Z}$ can be naturally viewed as a subring of $\mathbb{Z}_p$.

(c) Try to determine the unit group of $\mathbb{Z}_p$.

7. Quadratic Fields. Let $d \in \mathbb{Q}^\times \setminus (\mathbb{Q}^\times)^2$. Prove $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$, and determine all subfields of $\mathbb{Q}[\sqrt{d}]$.

8. Centralizer and Centre. Let R be a ring, $a \in R$.

(a) Prove $\{r \in R \mid ra = ar\}$ is a subring of R (called the centralizer of a).

(b) The *centre* of a ring R, denoted $Z(R)$, is the set of elements that commute with every element of R. Prove that $Z(R)$ is a subring of R.

(c) Let $R = M_2(\mathbb{R})$. Determine $Z(R)$.

(d) Let $R = \mathbb{H}$, the ring of real quaternions. Determine $Z(\mathbb{H})$.

9. Power Set Ring. Let U be a set. S is the family of all subsets of U, i.e., $S = \{V \mid V \subseteq U\}$. For $A, B \in S$, define

$$A \setminus B = \{c \in U \mid c \in A, c \notin B\},$$

$$A + B = (A \setminus B) \cup (B \setminus A), \quad A \cdot B = A \cap B.$$

Prove that $(S, +, \cdot)$ is a commutative ring with identity.

10. Boolean Rings. Let R be a ring. If every element $a \in R$ satisfies $a^2 = a$, R is called a Boolean ring. Prove:

(a) A Boolean ring R must be commutative, and $a + a = 0_R$ (for every $a \in R$);

For (1): Consider $(x + y)^2$.

(b) The ring S in item 9. is a Boolean ring.

11. **Finite Fields.** A non-zero finite integral domain must be a field.

12. **Nilpotent Elements.** An element a in ring R is called nilpotent if there exists a positive integer m such that $a^m = 0$.

    (a) Prove that when R is a commutative ring, if a and b are both nilpotent elements, then $a+b$ is also a nilpotent element.
    (b) If R is not a commutative ring, does the conclusion in (1) still hold?
    (c) Prove that if x is nilpotent, then $1+x$ is a unit.

13. **Jacobson's Lemma.** Let a, b be elements in a ring R with identity. Then $1 - ab$ is invertible is equivalent to $1 - ba$ being invertible.

14. **Right Inverses.** If an element in a ring with identity has more than one right inverse, then it must have infinitely many right inverses.

15. **Ring of Continuous Functions.** Let $C(\mathbb{R})$ denote the set of all continuous real functions $f : \mathbb{R} \to \mathbb{R}$. Define

$$(f+g)(a) = f(a)+g(a), \quad (fg)(a) = f(a)g(a), \forall f, g \in C(\mathbb{R}), a \in \mathbb{R}.$$

    Prove that $C(\mathbb{R})$ thereby becomes a commutative ring with identity. Is $C(\mathbb{R})$ an integral domain? Does it contain nilpotent elements? What is the group of units?

16. **Frobenius Map.** Let R be a commutative ring where $p \cdot 1_R = 0$ for a prime number p. Define the map $\phi : R \to R$ by $\phi(x) = x^p$.

    (a) Prove that ϕ satisfies $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$.
    (b) If R is a finite field, prove that ϕ is a bijection.
    (c) Conclude that for any finite field D and any $a \in D$, $a^{|D|} = a$.

17. **Intersections of Localisations.**

    (a) Let $\mathbb{Z}[\frac{1}{2}]$ denote the localisation of $\mathbb{Z}$ at the set of powers of 2. Characterise the elements of $\mathbb{Z}[\frac{1}{2}]$.
    (b) Let α be an **algebraic number** (a root of a polynomial with integer coefficients). Specifically, let $\alpha = \frac{1+\sqrt{5}}{2}$ (the golden ratio). Determine the intersection $\mathbb{Z}[\frac{1}{2}] \cap \mathbb{Z}[\alpha]$.
    (c) $\star$ Generalise the above: For which pairs $a, b \in \mathbb{Z}[\frac{1}{2}]$ does the element $a + b\alpha$ belong to the ring $\mathbb{Z}[\alpha]$?

2 Homomorphisms and Isomorphisms

In the previous chapter, we established the structural definitions of rings and fields. We now turn to the relationships between these structures. Just as linear transformations relate vector spaces and group homomorphisms relate groups, ring homomorphisms allow us to compare rings, transport properties between them, and construct new rings from old ones.

2.1 Ring Homomorphisms

A ring homomorphism is a map that preserves the algebraic structure — addition, multiplication, and the identity elements.

> **Definition 2.1.** ***Ring Homomorphism.***
> Let R and S be rings. A map $\phi : R \to S$ is a **ring homomorphism** if it satisfies the following axioms for all $a, b \in R$:
> ***Preservation of Identity:*** $\phi(1_R) = 1_S$.
> ***Preservation of Addition:*** $\phi(a + b) = \phi(a) + \phi(b)$.
> ***Preservation of Multiplication:*** $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.
>
> 定義

> *Remark.*
>
> While the preservation of the additive identity ($\phi(0_R) = 0_S$) follows from the additivity property (since $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0)$), the preservation of the multiplicative identity does not follow from the multiplicative property alone.
>
> Consider the map $f : \mathbb{R} \to M_2(\mathbb{R})$ defined by $x \mapsto \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$. This map preserves addition and multiplication, but $f(1) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq I_2$. Thus, f is not a ring homomorphism under our definition.

We classify homomorphisms based on their behaviour as set maps.

Definition 2.2. ***Types of Homomorphisms.***
Let $\phi : R \to S$ be a ring homomorphism.

- If ϕ is injective, it is a **monomorphism** (or embedding).
- If ϕ is surjective, it is an **epimorphism**.
- If ϕ is bijective, it is an **isomorphism**. We write $\phi : R \xrightarrow{\sim} S$ for the map and $R \cong S$ to indicate that R and S are isomorphic.
- An isomorphism from a ring to itself is an **automorphism**.

定義

The structural properties of elements are preserved under homomorphisms.

Proposition 2.1. ***Properties of Homomorphisms.***
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. If $u \in R^\times$ is a unit, then $\phi(u) \in S^\times$ is a unit and $\phi(u^{-1}) = \phi(u)^{-1}$.

Consequently, ϕ restricts to a group homomorphism $\phi|_{R^\times} : R^\times \to S^\times$.

命題

Proof

1. As noted in the remark, $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$, implying $\phi(0) = 0$ by cancellation in the additive group $(S, +)$.
2. $\phi(a) + \phi(-a) = \phi(a + (-a)) = \phi(0) = 0$. Thus $\phi(-a) = -\phi(a)$.
3. Since $uu^{-1} = 1$, we have $\phi(u)\phi(u^{-1}) = \phi(1) = 1$. Similarly $\phi(u^{-1})\phi(u) = 1$.

■

Example 2.1. Embeddings of Subrings. If R is a subring of S, the inclusion map $\iota : R \to S$ defined by $\iota(r) = r$ is essentially a monomorphism. The standard chain of number systems gives a sequence of inclusions:

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}.$$

範例

Example 2.2. Modular Arithmetic. The projection map $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\pi(a) = [a]_n$ is a surjective homomorphism (epimorphism). The conditions $\pi(a+b) = \pi(a) + \pi(b)$ and $\pi(ab) = \pi(a)\pi(b)$ correspond to the definition of modular arithmetic operations.

範例

Example 2.3. Block Matrices. Let R be a ring and $m, n \in \mathbb{Z}_+$. We

> construct a map into the larger matrix ring:
>
> $$f : M_m(R) \times M_n(R) \to M_{m+n}(R), \quad (A, B) \mapsto \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$
>
> This map is a monomorphism. If R is commutative, restricting f to the groups of units yields an embedding of general linear groups:
>
> $$GL_m(R) \times GL_n(R) \hookrightarrow GL_{m+n}(R).$$
>
> 範例

The Characteristic of a Ring

The ring of integers $\mathbb{Z}$ plays a universal role in ring theory. There is a canonical way to map $\mathbb{Z}$ into any arbitrary ring R.

> **Proposition 2.2.** ***The Unique Homomorphism from $\mathbb{Z}$.***
> Let R be a ring. There exists a unique ring homomorphism $\phi : \mathbb{Z} \to R$.
>
> 命題

> *Proof*
>
> If ϕ is a homomorphism, it must satisfy $\phi(1) = 1_R$. By additivity, for any positive integer n:
>
> $$\phi(n) = \phi(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\phi(1) + \cdots + \phi(1)}_{n \text{ times}} = n \cdot 1_R.$$
>
> Since $\phi(0) = 0_R$ and $\phi(-n) = -\phi(n)$, the value of ϕ is determined for all $z \in \mathbb{Z}$ by the additive structure of R. Explicitly,
>
> $$\phi(n) = \begin{cases} n \cdot 1_R & n > 0, \\ 0_R & n = 0, \\ -(|n| \cdot 1_R) & n < 0. \end{cases}$$
>
> It is routine to verify that this map preserves multiplication (i.e., $(nm) \cdot 1_R = (n \cdot 1_R)(m \cdot 1_R)$) and is thus a homomorphism.
>
> ■

This proposition allows us to classify rings by the kernel of this unique map. Since every ideal of $\mathbb{Z}$ is generated by a single integer, the kernel is of the form $n\mathbb{Z}$ for a unique non-negative integer $n \geq 0$.

> **Definition 2.3.** ***Characteristic.***
> The **characteristic** of a ring R, denoted $\text{char}(R)$, is the non-negative integer n such that $\ker(\phi) = n\mathbb{Z}$, where $\phi : \mathbb{Z} \to R$ is the unique ho-

momorphism.

- If ϕ is injective (i.e., $n = 0$), R has characteristic 0. This implies $\mathbb{Z}$ embeds into R.
- If $n > 0$, then n is the smallest positive integer such that

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

定義

Evaluation Homomorphisms

Polynomial rings satisfy a universal property that characterises them: to define a map from $R[X]$, it suffices to define it on R and specify where the variable X is sent.

Definition 2.4. ***Evaluation Homomorphism.***
Let $\phi : R \to S$ be a ring homomorphism and let $s \in S$. The **evaluation homomorphism** at s (extending ϕ) is the map $\Phi_s : R[X] \to S$ defined by:

$$\Phi_s\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} \phi(a_i) s^i.$$

定義

This construction effectively "substitutes" s for X.

$$\begin{tikzcd}
R \arrow[r, "\iota"] \arrow[dr, "\phi"'] & R[X] \arrow[d, dashed, "\Phi_s"] \\
 & S
\end{tikzcd}$$

Figure 2.1: The universal property of polynomial rings: $\Phi_s \circ \iota = \phi$ and $\Phi_s(X) = s$.

Proposition 2.3. ***Universal Property of Polynomial Rings.***
The map Φ_s is the unique ring homomorphism from $R[X]$ to S such that $\Phi_s|_R = \phi$ and $\Phi_s(X) = s$.

命題

Proof

That Φ_s is a homomorphism follows from the properties of ϕ and the commutativity of s with elements in the image of ϕ (if R is commutative, or if s is central). Uniqueness is guaranteed because any homomorphism is determined by its values on the generators R and X.

■

A specific case of immense utility is when R is a subring of S and ϕ is the inclusion. Then $\Phi_s : R[X] \to S$ maps $f(X) \mapsto f(s)$. The image of this map is the subring $R[s]$ generated by s.

Automorphisms of $\mathbb{R}$

While many rings possess rich automorphism groups (for instance, $\mathrm{Aut}(\mathbb{C})$ is infinite and non-trivial, containing the conjugation map $z \mapsto \bar{z}$), the real numbers are algebraically rigid.

> **Theorem 2.1.** ***Rigidity of Real Numbers.***
> The only automorphism of the field of real numbers $\mathbb{R}$ is the identity map. That is, $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$.
>
> 定理

> *Proof*
>
> Let $\sigma \in \mathrm{Aut}(\mathbb{R})$.
>
> ***σ fixes $\mathbb{Q}$:*** Since $\sigma(1) = 1$, by the uniqueness of the map from $\mathbb{Z}$, $\sigma(n) = n$ for all $n \in \mathbb{Z}$. For any rational $q = m/n$,
>
> $$\sigma(m/n) = \sigma(m)\sigma(n^{-1}) = m\sigma(n)^{-1} = m/n.$$
>
> Thus $\sigma|_{\mathbb{Q}} = \mathrm{id}$.
>
> ***σ preserves order:*** Let $x > 0$. Then $x = y^2$ for some $y \in \mathbb{R}$.
>
> $$\sigma(x) = \sigma(y^2) = (\sigma(y))^2 \geq 0.$$
>
> Since σ is injective and $\sigma(0) = 0$, if $x > 0$ then $\sigma(x) > 0$. Consequently, if $a > b$, then $a - b > 0$, so $\sigma(a-b) > 0$, implying $\sigma(a) > \sigma(b)$.
>
> ***σ is the identity:*** Suppose, for contradiction, that $\sigma(x) \neq x$ for some $x \in \mathbb{R}$. Assume $\sigma(x) < x$ (the case $\sigma(x) > x$ is similar). By the density of rationals, there exists $q \in \mathbb{Q}$ such that $\sigma(x) < q < x$. Applying the order-preserving σ to the inequality $q < x$, we get $\sigma(q) < \sigma(x)$. Since σ fixes rationals, $\sigma(q) = q$. Thus $q < \sigma(x)$, which contradicts $\sigma(x) < q$.
>
> Therefore, $\sigma(x) = x$ for all $x \in \mathbb{R}$.
>
> ■

2.2 *Kernels and Ideals*

A homomorphism $\phi : R \to S$ identifies a substructure of R that collapses to the zero element in S. This substructure, known as the kernel, plays a role analogous to normal subgroups in group theory, allowing us to construct quotient rings.

> **Definition 2.5.** ***Image and Kernel.***
> Let $\phi : R \to S$ be a ring homomorphism.
>
> 1. The **image** of ϕ is the set of values taken by ϕ in S:
>
> $$\mathrm{im}\,\phi = \{\phi(r) \mid r \in R\} \subseteq S.$$
>
> 2. The **kernel** of ϕ is the set of elements in R mapped to zero:
>
> $$\ker\phi = \{r \in R \mid \phi(r) = 0_S\} \subseteq R.$$

定義

Note

The image of a homomorphism is easily seen to be a subring of S.

Example 2.4. Evaluation Image. If R is a subring of S, $\iota : R \to S$ is the inclusion, and $s \in S$, then the image of the evaluation homomorphism $\Phi_s : R[X] \to S$ is precisely the subring $R[s]$ of S generated by s.

範例

Since $\phi(0_R) = 0_S$, the kernel is non-empty. Moreover, the kernel satisfies strong closure properties.

Proposition 2.4. ***Structure of the Kernel.***
Let $\phi : R \to S$ be a ring homomorphism. The set $K = \ker \phi$ satisfies:

1. **Additive Subgroup:** For any $x, y \in K$, the difference $x - y \in K$.
2. **Absorption:** For any $k \in K$ and any $r \in R$, both $rk \in K$ and $kr \in K$.

命題

Additive Subgroup.

Linearity implies $\phi(x - y) = \phi(x) - \phi(y) = 0 - 0 = 0$.

証明終

Absorption.

The multiplicative property implies $\phi(rk) = \phi(r)\phi(k) = \phi(r) \cdot 0 = 0$. Similarly, $\phi(kr) = 0$.

証明終

This leads to the general definition of an ideal. While subrings are closed under multiplication *within* the subset, ideals are closed under multiplication by *any* element of the ambient ring.

Definition 2.6. ***Ideal.***
A subset I of a ring R is an **ideal** if it is a subgroup of the additive group $(R, +)$ and absorbs multiplication from R. That is:

- $I \neq \varnothing$ (usually ensured by $0 \in I$).
- For all $x, y \in I$, $x - y \in I$.
- For all $a \in I$ and $r \in R$, both $ra \in I$ and $ar \in I$.

If $I \neq R$, it is called a **proper ideal**. The ideals $\{0\}$ and R are called **trivial ideals**.

定義

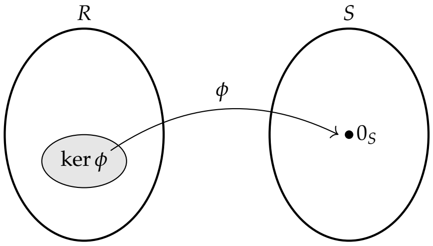

Figure 2.2: The kernel collapses to the zero element.

Proposition 2.5. ***Injectivity and Kernels.***
A ring homomorphism $\phi : R \to S$ is a monomorphism (injective) if and only if $\ker \phi = \{0\}$.

命題

Proof

If $\ker \phi = \{0\}$, suppose $\phi(x) = \phi(y)$. Then $\phi(x - y) = 0$, so $x - y \in \ker \phi$, implying $x - y = 0$ and $x = y$. Conversely, if ϕ is injective and $x \in \ker \phi$, then $\phi(x) = 0 = \phi(0)$, so $x = 0$.

■

Example 2.5. Ideals in Fields. Let F be a field. The only ideals of F are $\{0\}$ and F itself.

範例

Proof

Let I be a non-zero ideal of F. Take any non-zero element $x \in I$. Since F is a field, x has an inverse $x^{-1} \in F$. By the absorption property, $1 = x^{-1} \cdot x \in I$. For any $a \in F$, $a = a \cdot 1 \in I$, so $I = F$.

■

Consequently, any homomorphism from a field to a non-zero ring is injective.

Example 2.6. Ideals in $\mathbb{Z}$. The ideals of $\mathbb{Z}$ are exactly the sets $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ for $n \geq 0$. Since ideals are additive subgroups, this follows immediately from the classification of subgroups of cyclic groups.

範例

2.3 *Principal Ideals and Domains*

The simplest ideals are those generated by a single element.

Definition 2.7. ***Generated Ideals.***
Let S be a subset of a ring R. The **ideal generated by** S, denoted (S), is the smallest ideal of R containing S. It is the intersection of all ideals containing S. If $S = \{a_1, \ldots, a_n\}$ is finite, we write $(a_1, \ldots, a_n)$ and say the ideal is **finitely generated**.

定義

Definition 2.8. ***Principal Ideal.***
An ideal generated by a single element $x \in R$, denoted (x), is called a **principal ideal**.

- If R is commutative, this is the set of multiples of x:

$$(x) = Rx = \{rx \mid r \in R\}.$$

- If R is non-commutative, the generated ideal is the set of all finite sums $\sum r_i x s_i$.

定義

We focus primarily on commutative domains where ideal theory behaves most like arithmetic.

> **Definition 2.9.** ***Principal Ideal Domain (PID).***
> An integral domain R is called a **Principal Ideal Domain** (PID) if every ideal in R is a principal ideal.
>
> 定義

> **Example 2.7.** Non-PID Example. Consider the ring $\mathbb{Z}[X]$. The ideal generated by 2 and X, denoted $I = (2, X) = \{2p(X) + Xq(X) \mid p, q \in \mathbb{Z}[X]\}$, consists of polynomials with an even constant term. Suppose $I = (f)$ for some $f \in \mathbb{Z}[X]$. Then f must divide 2, so $f \in \{\pm 1, \pm 2\}$.
> - If $f = \pm 1$, then $1 \in I$. But constant terms of elements in I are even, a contradiction.
> - If $f = \pm 2$, then f must divide X, which is impossible in $\mathbb{Z}[X]$.
>
> Thus I is not principal.
>
> 範例

2.4 *Applications and Further Examples*

We can use the concepts of kernel and ideals to deduce structural properties of rings.

Characteristic of Integral Domains

Recall from *proposition* 2.2 that for any ring R, there is a unique homomorphism $\phi : \mathbb{Z} \to R$. The kernel of this map, $\ker \phi$, is an ideal of $\mathbb{Z}$, hence of the form $n\mathbb{Z}$. The non-negative integer n is the characteristic of R.

> **Proposition 2.6.** ***Characteristic of a Domain.***
> If R is an integral domain, then $\operatorname{char}(R)$ is either 0 or a prime number p.
>
> 命題

> *Proof*
>
> Let $n = \operatorname{char}(R)$. Thus $n \cdot 1_R = 0_R$. Suppose n is composite, say $n = ab$ with $1 < a, b < n$. Then:
>
> $$(a \cdot 1_R)(b \cdot 1_R) = (ab) \cdot 1_R = n \cdot 1_R = 0_R.$$
>
> Since R is an integral domain, it has no zero divisors, so either $a \cdot 1_R = 0$ or $b \cdot 1_R = 0$. This implies n divides a or n divides b (by the definition of characteristic as the generator of the kernel), which contradicts $a, b < n$. Thus n must be prime or zero.
>
> ■

Example 2.8. Finite Fields. Every finite field $\mathbb{F}$ must have prime characteristic p, and it contains $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ as a subfield.

範例

Isomorphisms of Polynomial Rings

Using the universal property of polynomial rings (*proposition* 2.3), we can derive isomorphisms between different polynomial constructions.

Corollary 2.1. *Multivariate Isomorphism.* Let R be a ring. There is a canonical isomorphism

$$R[X, Y] \cong (R[X])[Y].$$

推論

Proof

Let $S = (R[X])[Y]$.

(i) There is a homomorphism $\phi : R \to S$ (inclusion).

(ii) By the universal property of $R[X]$, identifying X with the constant polynomial $X \in S$ gives a map $R[X] \to S$.

(iii) By the universal property of $(R[X])[Y]$, identifying Y with $Y \in S$ extends this to $\Phi : R[X, Y] \to S$.

Conversely, we construct the inverse by mapping coefficients in $R[X]$ to the corresponding terms in $R[X, Y]$. The bijection implies the rings are isomorphic.

■

Example 2.9. Adjoining Elements. Let $\alpha \in \mathbb{C}$. The evaluation homomorphism $\Phi_\alpha : \mathbb{Z}[X] \to \mathbb{C}$ defined by $f(X) \mapsto f(\alpha)$ has image $\mathbb{Z}[\alpha]$.

- If α is **transcendental** (e.g., π), then $\ker \Phi_\alpha = \{0\}$. Thus $\mathbb{Z}[X] \cong \mathbb{Z}[\pi]$.
- If α is **algebraic** (e.g., i), the kernel is non-zero. For $\alpha = i$, $\ker \Phi_i = (X^2 + 1)$, and $\mathbb{Z}[X]/(X^2 + 1) \cong \mathbb{Z}[i]$.

範例

2.5 *Exercises*

In the following exercises, R denotes a ring with identity $1 \neq 0$ unless otherwise specified.

1. **Ideals in Quadratic Integers.** Prove that any non-zero ideal of the integral domain $\mathbb{Z}[\sqrt{d}]$ contains a non-zero integer.

2. **Automorphism Groups.** Determine the automorphism groups $\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])$ for $d \in \mathbb{Q}^\times \setminus (\mathbb{Q}^\times)^2$, and $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$.

3. **Matrix Embedding of $\mathbb{C}$.** Prove that the complex field $\mathbb{C}$ can be embedded into the ring of 2×2 real matrices $M_2(\mathbb{R})$.

4. **Kernels of Evaluation Maps.** Find the generators of the kernel of the following homomorphisms:

   (a) $\mathbb{R}[X, Y] \to \mathbb{R} : f(X, Y) \mapsto f(0, 0)$;
   (b) $\mathbb{R}[X] \to \mathbb{C} : f(X) \mapsto f(2 + i)$;
   (c) $\mathbb{Z}[X] \to \mathbb{R} : f(X) \mapsto f(1 + \sqrt{2})$;
   (d) $\mathbb{C}[X, Y, Z] \to \mathbb{C}[T] : X \mapsto T, Y \mapsto T^2, Z \mapsto T^3$.

5. **Geometric Kernel.** Find the kernel K of the ring homomorphism $\varphi : \mathbb{C}[X, Y] \to \mathbb{C}[T]$ defined by $X \mapsto T + 1$ and $Y \mapsto T^3 - 1$. Prove that every ideal I of $\mathbb{C}[X, Y]$ containing K can be generated by 2 elements.

6. **Ideal Arithmetic.** Let I, J be ideals of a ring R. Prove:

   (a) The product $IJ = \{\sum_{k=1}^{n} a_k b_k \mid a_k \in I, b_k \in J\}$ is an ideal of R, and $IJ \subseteq I \cap J$.
   (b) The sum $I + J$ is an ideal of R, and it is the smallest ideal containing both I and J.
   (c) Let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ (with $n, m \geq 1$) be ideals of $\mathbb{Z}$. Determine IJ, $I + J$, and $I \cap J$ in terms of n and m.

7. **The Radical Ideal.** Let I be an ideal in a commutative ring R. The *radical* of I is defined as:

$$\sqrt{I} = \{r \in R \mid \exists n \geq 1 \text{ such that } r^n \in I\}.$$

   Prove the following:

   (a) $\sqrt{I}$ is an ideal of R.
   (b) $\sqrt{I} = R$ if and only if $I = R$.
   (c) $\sqrt{\sqrt{I}} = \sqrt{I}$.
   (d) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$ and $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{IJ}$.

8. **Homomorphisms from Skew Fields.** Let $f : R \to S$ be a ring homomorphism. If R is a skew field (a ring where every non-zero element is a unit, also known as a division ring), prove that f is either the zero homomorphism or an embedding.

9. **Ascending Chains.** Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots$ be an ascending chain of ideals in a ring R. Prove that the union $\bigcup_{i=1}^{\infty} I_i$ is also an ideal of R.

10. **Ideals in Matrix Rings.**

    (a) Let R be a commutative ring with identity. Prove that every ideal in the ring $M_n(R)$ is of the form $M_n(I)$, where I is an ideal of R.
    (b) Deduce that if F is a field, then $M_n(F)$ is a *simple ring* (i.e., it

possesses no non-trivial ideals).

11. **Triangular Matrices.** Prove that the set $T = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}$ is a subring of $M_2(\mathbb{Z})$. Determine all ideals of the ring T.

12. **Ring of Germs.** Let z be a point in the complex plane $\mathbb{C}$. Two functions f and g that are analytic at z (expressible as a convergent power series in a neighbourhood of z) are said to be *equivalent* if they agree on some open neighbourhood of z. Let $\mathcal{O}_z$ denote the set of equivalence classes (germs) of functions analytic at z.

    (a) Verify that $\mathcal{O}_z$ forms a ring under pointwise addition and multiplication.

    (b) Determine the group of units $\mathcal{O}_z^\times$.

    (c) Determine all ideals of $\mathcal{O}_z$.

3
Quotient Rings and Homomorphism Theorems

We have previously established that ideals are the kernels of ring homomorphisms. In group theory, normal subgroups allow us to construct quotient groups. Similarly, ideals allow us to construct quotient rings. This construction provides a framework for modular arithmetic and enables the simplification of algebraic structures by "modding out" specific properties.

3.1 The Quotient Ring Construction

Let R be a ring and let I be an ideal of R. Since I is an additive subgroup of $(R, +)$, the quotient group R/I is well-defined as an abelian group. We denote the coset of an element $a \in R$ by $\bar{a} = a + I$. Recall that congruence modulo I is defined by $a \equiv b \pmod{I} \iff a - b \in I$.

To endow the additive group R/I with a ring structure, we define multiplication of cosets using representatives.

> **Theorem 3.1.** ***Existence of Quotient Ring.***
> Let I be an ideal of a ring R.
> 1. There exists a unique ring structure on the set of cosets R/I such that the canonical projection $\pi : R \to R/I$, defined by $a \mapsto a + I$, is a surjective ring homomorphism.
> 2. The kernel of this homomorphism is exactly I.
>
> 定理

> *Proof*
>
> The additive structure of R/I follows immediately from the fact that I is a subgroup of the abelian group R. We define multiplication on R/I by:
> $$(a + I)(b + I) = ab + I.$$
> We must prove this operation is well-defined; that is, it is independent of the choice of representatives. Suppose $a_1 \equiv a \pmod{I}$ and $b_1 \equiv b \pmod{I}$. Then $a - a_1 \in I$ and $b - b_1 \in I$. Consider the

difference of the products:

$$ab - a_1b_1 = ab - a_1b + a_1b - a_1b_1 = (a - a_1)b + a_1(b - b_1).$$

Since I is an ideal, $(a - a_1)b \in I$ and $a_1(b - b_1) \in I$. Because I is closed under addition, the sum lies in I. Thus $ab \equiv a_1b_1 \pmod{I}$, and the multiplication is well-defined. The ring axioms (associativity, distributivity, identity) for R/I are inherited directly from R via the map π. For instance:

$$\pi(a)\pi(b) = (a + I)(b + I) = ab + I = \pi(ab).$$

Finally, $\ker \pi = \{a \in R \mid a + I = 0 + I\} = \{a \in R \mid a \in I\} = I$.

■

Remark.

It is crucial to distinguish between the product of cosets in a quotient ring and the set-theoretic product of subsets. In group theory, if H is a subgroup, $aH \cdot bH = abH$ holds as an equality of sets. In rings, for the ideal I, the set product is:

$$(a+I)(b+I) = \{(a+i)(b+j) \mid i, j \in I\} = \{ab+aj+ib+ij \mid i, j \in I\}.$$

This set is a subset of the coset $ab + I$, but they are not necessarily equal. The definition of the quotient ring operation selects the *coset* containing the set product.

Note

The requirement that I be an ideal is necessary. If S is merely a subring (or additive subgroup) and we attempt to define $(a + S)(b + S) = ab + S$, well-definedness fails unless S absorbs multiplication. Specifically, taking $a_1 \in S$ (so $a_1 \equiv 0$) and $b \in R$, we would require $0 \cdot b \equiv a_1b \in S$, enforcing the ideal condition.

Example 3.1. Finite Fields Construction. Consider the polynomial ring $\mathbb{R}[X]$ and the ideal generated by $X^2 + 1$, denoted $I = (X^2 + 1)$. The quotient ring $K = \mathbb{R}[X]/I$ consists of cosets represented by polynomials $a + bX$.

The multiplication is defined by $(X + I)^2 = X^2 + I = -1 + I$. Identifying $X + I$ with i, we see that K is isomorphic to the field of complex numbers $\mathbb{C}$.

範例

The relationship between homomorphisms, ideals, and quotient rings is encapsulated in the Fundamental Homomorphism Theorem (or First Isomorphism Theorem). It states that the image of a homomorphism is structurally identical to the quotient of the domain by the kernel.

Theorem 3.2. ***First Isomorphism Theorem.***
Let $\phi : R \to S$ be a ring homomorphism.

1. The kernel $\ker\phi$ is an ideal of R, and the image $\operatorname{im}\phi$ is a subring of S.
2. There is a unique isomorphism $\bar{\phi} : R/\ker\phi \xrightarrow{\sim} \operatorname{im}\phi$ such that $\phi = \iota \circ \bar{\phi} \circ \pi$, where $\pi : R \to R/\ker\phi$ is the canonical projection and $\iota : \operatorname{im}\phi \hookrightarrow S$ is the inclusion.

定理

Proof

Let $K = \ker\phi$. We define the map $\bar{\phi} : R/K \to \operatorname{im}\phi$ by $\bar{\phi}(a + K) = \phi(a)$. From the group-theoretic First Isomorphism Theorem, we know that $\bar{\phi}$ is a well-defined isomorphism of additive groups. We need only verify the multiplicative property and identity preservation.

Identity: $\bar{\phi}(1_R + K) = \phi(1_R) = 1_S$.

Multiplication: For any cosets $\bar{a}, \bar{b} \in R/K$:

$$\bar{\phi}(\bar{a}\bar{b}) = \bar{\phi}(ab + K) = \phi(ab) = \phi(a)\phi(b) = \bar{\phi}(\bar{a})\bar{\phi}(\bar{b}).$$

Thus $\bar{\phi}$ is a ring isomorphism.

■

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d, "\pi"'] & S \\
R/\ker\phi \arrow[r, "\sim", "\bar{\phi}"'] & \operatorname{im}\phi \arrow[u, hook, "\iota"']
\end{tikzcd}$$

Figure 3.1: Commutative diagram for the First Isomorphism Theorem.

This theorem allows us to define standard rings as quotients. For example, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the image of $\mathbb{Z}$ under the modulo n map.

When we form a quotient ring R/J, the ideal structure of the quotient is directly linked to the ideal structure of R. This relationship is often called the Lattice Isomorphism Theorem or the Correspondence Theorem.

Theorem 3.3. ***Correspondence Theorem.***
Let R be a ring and J an ideal of R. Let $\pi : R \to R/J$ be the canonical projection.

1. There is a one-to-one correspondence between the set of ideals of R containing J and the set of ideals of R/J, given by:
$$I \longleftrightarrow \pi(I) = I/J, \quad \text{where } J \subseteq I \subseteq R \text{ and } I/J = \{a + J \mid a \in I\}.$$
The inverse map is $\bar{I} \mapsto \pi^{-1}(\bar{I})$.
2. If an ideal $I \supseteq J$ corresponds to $\bar{I} \subseteq R/J$, then there is an isomorphism:
$$R/I \cong (R/J)/(I/J).$$

定理

The Bijection.

We must show that the maps are well-defined inverses.

(i) If I is an ideal of R, then $\pi(I)$ is an ideal of R/J because π is a surjective homomorphism.

(ii) Conversely, let $\bar{I}$ be an ideal of R/J. Consider the preimage $K = \pi^{-1}(\bar{I})$. Since $\bar{I}$ is the kernel of the map $R/J \to (R/J)/\bar{I}$, the composition $R \xrightarrow{\pi} R/J \to (R/J)/\bar{I}$ is a homomorphism with kernel K. Thus K is an ideal of R. Clearly $J = \pi^{-1}(\{0\}) \subseteq K$.

(iii) We verify the bijection. First, $\pi(\pi^{-1}(\bar{I})) = \bar{I}$ follows from the surjectivity of π. Second, we show $\pi^{-1}(\pi(I)) = I$ for $I \supseteq J$. The inclusion $I \subseteq \pi^{-1}(\pi(I))$ is clear. Let $x \in \pi^{-1}(\pi(I))$. Then $\pi(x) \in \pi(I)$, so there exists $y \in I$ such that $\pi(x) = \pi(y)$. This implies $\pi(x-y) = 0$, so $x - y \in \ker \pi = J$. Since $J \subseteq I$, we have $x - y \in I$, and thus $x = y + (x-y) \in I$.

証明終

The Third Isomorphism Theorem.

Let $\phi : R/J \to R/I$ be defined by mapping $r + J$ to $r + I$. This is well-defined because $J \subseteq I$. The kernel of this map is $\{r + J \mid r \in I\} = I/J$. By the First Isomorphism Theorem,

$$(R/J)/\ker\phi \cong \operatorname{im}\phi \implies (R/J)/(I/J) \cong R/I.$$

証明終

Example 3.2. Ideals in Quotients. Consider $R = \mathbb{Z}$ and $J = 12\mathbb{Z}$. The ideals of $\mathbb{Z}$ containing $12\mathbb{Z}$ are $n\mathbb{Z}$ where n divides 12 (i.e., $n \in \{1, 2, 3, 4, 6, 12\}$). The quotient ring is $\bar{R} = \mathbb{Z}/12\mathbb{Z}$. The ideals of $\bar{R}$ correspond exactly to these divisors. For instance, the ideal $I = 4\mathbb{Z}$ corresponds to $\bar{I} = \{[0], [4], [8]\} \subset \mathbb{Z}/12\mathbb{Z}$. The quotient $(\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

範例

$$\begin{tikzcd}
R \arrow[r, dashed, "\pi"] \arrow[d, dash] & R/J \arrow[d, dash] \\
I \arrow[r, dashed] \arrow[d, dash] & I/J \arrow[d, dash] \\
J \arrow[r, dashed] & \{0\}
\end{tikzcd}$$

Figure 3.2: Lattice correspondence of ideals.

3.2 Applications of the Homomorphism Theorems

We now illustrate the power of the Fundamental Homomorphism Theorem through several concrete examples. These applications range from determining the structure of specific quotient rings to defining universal maps in characteristic p.

A common problem in ring theory is to identify the structure of a quotient ring R/I by finding a simpler, isomorphic ring S. The strategy is to construct a surjective homomorphism $\phi : R \to S$ whose kernel is exactly I. By the First Isomorphism Theorem, $R/I \cong S$.

Example 3.3. Gaussian Integers Modulo $1 + 3i$. We assert that the quotient ring $\mathbb{Z}[i]/(1+3i)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.

範例

Proof

Consider the natural homomorphism from the integers:

$$\varphi : \mathbb{Z} \to \mathbb{Z}[i]/(1+3i), \quad n \mapsto n + (1+3i).$$

We must determine the kernel and verify surjectivity.

Kernel: Let $n \in \ker\varphi$. Then $n \in (1+3i)$, meaning $n = (1+3i)(x+yi)$ for some $x, y \in \mathbb{Z}$. Expanding the product:

$$n = (x - 3y) + i(3x + y).$$

For the imaginary part to vanish, we require $3x + y = 0$, or $y = -3x$. Substituting this into the real part:

$$n = x - 3(-3x) = 10x.$$

Thus, n must be a multiple of 10. Conversely, $10 = (1+3i)(1-3i) \in \ker\varphi$. Hence, $\ker\varphi = 10\mathbb{Z}$.

Surjectivity: The image of φ is the subring generated by 1. In the quotient ring, we have the relation $1 + 3i = 0$, or $3i = -1$. Note that in $\mathbb{Z}/10\mathbb{Z}$, 3 is invertible (since $3 \cdot 7 = 21 \equiv 1$). Multiplying $3i = -1$ by 7 gives:

$$21i = -7 \implies i = -7 = 3.$$

Thus, the element i is effectively the integer 3 in the quotient. Any element $a + bi$ maps to $a + 3b \pmod{10}$. Therefore, the map is surjective.

By the First Isomorphism Theorem, $\mathbb{Z}[i]/(1+3i) \cong \mathbb{Z}/10\mathbb{Z}$.

■

Example 3.4. The Union of Axes. Let $R = \mathbb{C}[X, Y]$ and let $I = (XY)$ be the ideal generated by the product of the variables. Geometrically, the condition $XY = 0$ corresponds to the union of the X-axis ($Y = 0$) and the Y-axis ($X = 0$) in $\mathbb{C}^2$.

We claim that R/I is isomorphic to the subring of the product $\mathbb{C}[X] \times \mathbb{C}[Y]$ consisting of pairs of polynomials that agree at the origin:

$$S = \{(p(X), q(Y)) \in \mathbb{C}[X] \times \mathbb{C}[Y] \mid p(0) = q(0)\}.$$

範例

Proof

Consider the homomorphism $\Phi : \mathbb{C}[X,Y] \to \mathbb{C}[X] \times \mathbb{C}[Y]$ defined by:

$$f(X,Y) \mapsto (f(X,0), f(0,Y)).$$

The kernel consists of polynomials vanishing on both axes, i.e., $f(X,0) = 0$ and $f(0,Y) = 0$. This implies every term in f must contain both X and Y, so $f \in (XY)$. The image is clearly contained in S because evaluating $f(X,0)$ at $X = 0$ and $f(0,Y)$ at $Y = 0$ both yield the constant term $f(0,0)$. Conversely, any pair $(p,q) \in S$ with common constant term c can be written as $p(X) = c + XP(X)$ and $q(Y) = c + YQ(Y)$. The polynomial $f(X,Y) = c + XP(X) + YQ(Y)$ maps to (p,q).

■

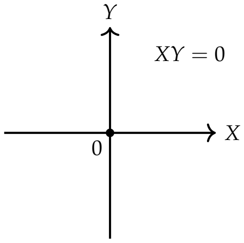

Figure 3.3: The ideal (XY) corresponds to the union of the axes. Functions on this variety are pairs $(p(X), q(Y))$ that agree at the intersection point.

The Frobenius Homomorphism

In rings of prime characteristic, the algebraic expansion of powers simplifies dramatically.

Proposition 3.1. ***Freshman's Dream.***
Let R be an integral domain of characteristic p, where p is a prime. Then for any $x, y \in R$:

$$(x+y)^p = x^p + y^p.$$

命題

Proof

By the Binomial Theorem $(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}$. Recall that the binomial coefficient is $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. For $1 \leq k \leq p-1$, the prime p divides the numerator but not the denominator. Thus $p \mid \binom{p}{k}$, which means $\binom{p}{k} = 0$ in R. The sum collapses to $x^p + y^p$.

■

Corollary 3.1. *The Frobenius Endomorphism.* Let R be an integral domain of characteristic p. The map $\sigma : R \to R$ defined by $\sigma(x) = x^p$ is a ring monomorphism, called the **Frobenius map**.

推論

Proof

By proposition 3.1, $\sigma(x+y) = \sigma(x) + \sigma(y)$. Clearly $\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$ and $\sigma(1) = 1$. To show injectivity, let $x \in \ker \sigma$. Then $x^p = 0$. Since R is an integral domain, $x^p = 0 \implies x = 0$. Thus $\ker \sigma = \{0\}$.

■

3.3 *The Chinese Remainder Theorem*

The Chinese Remainder Theorem (CRT) allows us to decompose a ring R modulo an intersection of ideals into a direct product of quotient rings, provided the ideals are "coprime". This generalizes the classical number-theoretic result for integers.

Definition 3.1. ***Comaximal Ideals.***
Two ideals I, J of a ring R are **comaximal** (or coprime) if $I + J = R$. That is, there exist $a \in I$ and $b \in J$ such that $a + b = 1$.

定義

Theorem 3.4. ***Chinese Remainder Theorem.***
Let R be a ring and let $I_1, \ldots, I_n$ be pairwise comaximal ideals (i.e., $I_i + I_j = R$ for all $i \neq j$). Then:

$$R / \bigcap_{i=1}^{n} I_i \cong \prod_{i=1}^{n} R/I_i.$$

定理

We proceed in three steps: establishing the comaximality of products, constructing the map, and verifying the kernel.

Claim 3.1. . For any i, $I_i + \prod_{j \neq i} I_j = R$.

主張

Proof

Without loss of generality, let $i = 1$. We prove $I_1 + I_2 \cdots I_n = R$ by induction. The base case $n = 2$ is given. Assume $I_1 + J = R$ where $J = I_2 \cdots I_k$. We know $I_1 + I_{k+1} = R$. Then

$$R = (I_1 + J)(I_1 + I_{k+1}) = I_1^2 + I_1 I_{k+1} + J I_1 + J I_{k+1}.$$

Since the first three terms lie in I_1, and $J I_{k+1} = I_2 \cdots I_{k+1}$, we have $R = I_1 + \prod_{j=2}^{k+1} I_j$.

■

Surjectivity.

By the claim, for each k, we can find $y_k \in I_k$ and $z_k \in \prod_{j \neq k} I_j$ such that $y_k + z_k = 1$. Observing congruences:

$$z_k \equiv 1 \pmod{I_k}, \quad z_k \equiv 0 \pmod{I_j} \text{ for } j \neq k.$$

Define the map $\phi : R \to \prod R/I_i$ by $x \mapsto (x + I_1, \ldots, x + I_n)$. Given any element $(a_1 + I_1, \ldots, a_n + I_n)$ in the product, construct $x = \sum_{k=1}^{n} a_k z_k$. Modulo I_k, the term $a_k z_k \equiv a_k \cdot 1 = a_k$, and all other terms vanish. Thus $\phi(x) = (a_k + I_k)_k$, proving surjectivity.

証明終

> *Kernel.*
>
> The kernel is simply the set of elements mapping to zero in every component:
>
> $$x \in \ker \phi \iff x \in I_1, \ldots, I_n \iff x \in \bigcap_{i=1}^{n} I_i.$$
>
> 証明終

The result follows from the First Isomorphism Theorem.

> *Remark.*
>
> If R is commutative, the intersection of pairwise comaximal ideals is equal to their product: $\bigcap I_i = \prod I_i$. This recovers the familiar form $R/(I_1 \cdots I_n) \cong \prod R/I_i$.

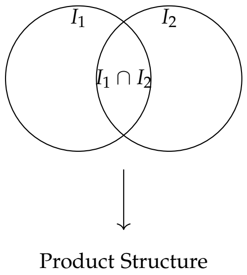

Figure 3.4: If $I_1 + I_2 = R$, the intersection decomposes the ring.

3.4 *Exercises*

In the following exercises, R denotes a ring with identity $1 \neq 0$ unless otherwise specified.

1. **The Nilradical.** Let R be a commutative ring. The set of nilpotent elements is called the **nilradical**, denoted $\mathrm{Nil}(R) = \{r \in R \mid r^n = 0 \text{ for some } n \geq 1\}$. Recall from Chapter 2, Exercise 7 that $\mathrm{Nil}(R) = \sqrt{(0)}$ is an ideal. Prove that the quotient ring $R/\mathrm{Nil}(R)$ has no non-zero nilpotent elements (i.e., its nilradical is zero).

2. **Matrix Rings over Quotients.** Let R be a commutative ring with identity and I be an ideal of R. Let $M_n(I)$ denote the set of matrices with entries in I. Prove the ring isomorphism $M_n(R)/M_n(I) \cong M_n(R/I)$.

3. **Induced Homomorphisms.** Let $f : R \to S$ be a ring homomorphism. Let I and J be ideals of R and S respectively, such that $f(I) \subseteq J$. Define the map between quotient rings:

   $$\bar{f} : R/I \to S/J, \quad a + I \mapsto f(a) + J.$$

   (a) Prove that $\bar{f}$ is well-defined and is a ring homomorphism.
   (b) Prove that $\bar{f}$ is an isomorphism if and only if $f(R) + J = S$ (surjectivity condition) and $I = f^{-1}(J)$ (kernel condition).

4. **Affine Ring Structure.** Let $(R, +, \cdot)$ be a ring with identity. For $a, b \in R$, define new operations:

   $$a \oplus b = a + b + 1, \quad a \odot b = ab + a + b.$$

   Prove that $(R, \oplus, \odot)$ forms a ring with identity, and construct an explicit isomorphism to $(R, +, \cdot)$.

5. **Principal Ideal Rings.** A ring is a principal ideal ring if every ideal is principal.

   (a) Prove that every homomorphic image of a principal ideal ring is also a principal ideal ring.

   (b) Deduce that $\mathbb{Z}/m\mathbb{Z}$ is a principal ideal ring for any $m \geq 1$.

6. **Universal Property of Product Rings.** Let $\{R_i\}_{i\in I}$ be a family of rings, and let $R = \prod_{i\in I} R_i$ be their Cartesian product.

   (a) Let $\pi_i : R \to R_i$ be the projection map $(a_j)_{j\in I} \mapsto a_i$. Prove that π_i is a ring homomorphism (the canonical projection).

   (b) Let S be any ring. Suppose that for every $i \in I$, there exists a homomorphism $\varphi_i : S \to R_i$. Prove that there exists a unique ring homomorphism $\varphi : S \to R$ such that $\pi_i \circ \varphi = \varphi_i, \forall i \in I$.

7. **Roots in Domains.** Let D be an integral domain. Let m, n be coprime positive integers. Prove that if $a, b \in D$ satisfy $a^m = b^m$ and $a^n = b^n$, then $a = b$.

   Use Bézout's identity for the exponents.

8. **Internal Direct Products.** Let $I_1, \ldots, I_n$ be ideals of a ring R satisfying two conditions: (a) The sum is the whole ring: $I_1 + \cdots + I_n = R$, (b) For each k, $I_k \cap (I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n) = \{0\}$. Prove that R is isomorphic to the product ring $\prod_{i=1}^{n} I_i$.

9. **Central Idempotents.** An element $e \in R$ is *idempotent* if $e^2 = e$. It is *central* if it commutes with all elements of R. Let R be a ring with identity and e a central idempotent.

   (a) Prove that $1 - e$ is also a central idempotent.

   (b) Prove that the principal ideals eR and $(1 - e)R$ are themselves rings (with identity elements e and $1 - e$ respectively), and establish the isomorphism $R \cong eR \times (1 - e)R$.

10. **Decomposition via Ideals.** Let I, J be ideals of a commutative ring R such that $I + J = R$ (comaximal) and $IJ = \{0\}$.

    (a) Prove that $R \cong R/I \times R/J$.

    (b) Identify the idempotent element in R corresponding to the component $(1_{R/I}, 0_{R/J})$ in the product.

11. **Orthogonal Idempotents.** A set of idempotents $\{e_1, \ldots, e_n\}$ is called *orthogonal* if $e_i e_j = 0$ for $i \neq j$. Let $R, R_1, \ldots, R_n$ be rings with identity. Prove that the following are equivalent:

    (a) $R \cong R_1 \times \cdots \times R_n$.

    (b) R contains a set of orthogonal central idempotents $\{e_1, \ldots, e_n\}$ summing to 1_R, such that the ideal $e_i R$ is isomorphic to R_i for each i.

4
Prime and Maximal Ideals

In the preceding chapter, we explored how the quotient construction R/I allows us to define new rings. A central motivation in ring theory — and indeed, in algebraic geometry and number theory — is the construction of fields, which facilitate the use of linear algebra. Since a field is a specific type of integral domain, we investigate the conditions on an ideal I such that the quotient R/I becomes an integral domain or a field.

4.1 Prime Ideals and the Spectrum

We begin by identifying ideals that yield integral domains upon taking quotients. In the ring of integers $\mathbb{Z}$, the quotient $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is a prime number (or zero). This observation motivates the general definition.

> **Definition 4.1.** ***Prime Ideal.***
> Let R be a commutative ring. A proper ideal $\mathfrak{p} \subsetneq R$ is called a **prime ideal** if for any $a, b \in R$,
>
> $$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$
>
> The set of all prime ideals of R is denoted by $\operatorname{Spec}(R)$ and is referred to as the **spectrum** of R.
>
> 定義

The definition of a prime ideal generalises Euclid's Lemma for integers. We now establish the fundamental relationship between prime ideals and integral domains, along with an equivalent condition involving ideal multiplication.

> **Proposition 4.1.** ***Characterisation of Prime Ideals.***
> Let R be a commutative ring and $\mathfrak{p}$ a proper ideal. The following conditions are equivalent:
> 1. $\mathfrak{p}$ is a prime ideal.
> 2. For any ideals I, J of R, if $IJ \subseteq \mathfrak{p}$, then $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.

3. The quotient ring $R/\mathfrak{p}$ is an integral domain.

命題

Proof

(1) $\implies$ (2): Suppose $I \not\subseteq \mathfrak{p}$ and $J \not\subseteq \mathfrak{p}$. Then there exist elements $a \in I \setminus \mathfrak{p}$ and $b \in J \setminus \mathfrak{p}$. The product ab lies in IJ. If $IJ \subseteq \mathfrak{p}$, then $ab \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this forces $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, a contradiction.

(2) $\implies$ (3): Let $\bar{a}, \bar{b} \in R/\mathfrak{p}$ such that $\bar{a}\bar{b} = 0$. This implies $ab \in \mathfrak{p}$. Consider the principal ideals (a) and (b). We have $(a)(b) = (ab) \subseteq \mathfrak{p}$. By hypothesis, either $(a) \subseteq \mathfrak{p}$ or $(b) \subseteq \mathfrak{p}$, which implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Thus $\bar{a} = 0$ or $\bar{b} = 0$, so $R/\mathfrak{p}$ has no zero divisors.

(3) $\implies$ (1): Suppose $ab \in \mathfrak{p}$. Then in the quotient ring, $\bar{a}\bar{b} = \overline{ab} = 0$. Since $R/\mathfrak{p}$ is an integral domain, $\bar{a} = 0$ or $\bar{b} = 0$, which means $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

■

To obtain a field, we require a stronger condition on the ideal.

Definition 4.2. ***Maximal Ideal.***
A proper ideal $\mathfrak{m} \subsetneq R$ is called a **maximal ideal** if there exists no ideal J such that $\mathfrak{m} \subsetneq J \subsetneq R$. In other words, $\mathfrak{m}$ is a maximal element in the set of proper ideals partially ordered by inclusion. The set of all maximal ideals of R is denoted by $\mathrm{Max}(R)$.

定義

The maximality of an ideal is intrinsically linked to the field structure of its quotient.

Proposition 4.2. ***Maximal Ideals and Fields.***
Let R be a commutative ring and $\mathfrak{m}$ a proper ideal. Then $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.

命題

Proof

We rely on the Correspondence Theorem from the previous chapter. There is a one-to-one correspondence between ideals of $R/\mathfrak{m}$ and ideals of R containing $\mathfrak{m}$.

- $R/\mathfrak{m}$ is a field if and only if its only ideals are the zero ideal $\{\bar{0}\}$ and the ring itself.
- Under the correspondence, $\{\bar{0}\}$ corresponds to $\mathfrak{m}$, and the ring $R/\mathfrak{m}$ corresponds to R.
- Thus, $R/\mathfrak{m}$ is a field if and only if the only ideals of R contain-

ing $\mathfrak{m}$ are $\mathfrak{m}$ and R. This is precisely the definition of a maximal ideal.

■

Since every field is an integral domain, the relationship between these classes of ideals is immediate.

Corollary 4.1. *Maximal implies Prime.* Every maximal ideal is a prime ideal. Consequently, $\operatorname{Max}(R) \subseteq \operatorname{Spec}(R)$.

推論

Proof

If $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ is a field. Fields are integral domains, so by *proposition 4.1*, $\mathfrak{m}$ is a prime ideal.

■

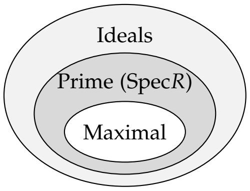

Figure 4.1: The hierarchy of ideals in a commutative ring.

We illustrate these concepts with the standard rings of number theory and polynomials.

Example 4.1. Spectrum of the Integers. In $\mathbb{Z}$, the quotient $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if n is prime or $n = 0$. It is a field if and only if n is prime.

- The ideal (0) is prime but not maximal (since $\mathbb{Z}$ is a domain but not a field).
- The ideals (p) for prime p are maximal.

Thus, $\operatorname{Spec}(\mathbb{Z}) = \{(0)\} \cup \{(p) \mid p \text{ is prime}\}$.

範例

Example 4.2. Polynomial Rings over Fields. Let F be a field and $R = F[X]$. In this ring, every ideal is generated by a single polynomial $f(X)$.

- The zero ideal (0) is prime (as $F[X]$ is a domain) but not maximal.
- A non-zero ideal $(f(X))$ is prime if and only if $f(X)$ is irreducible (i.e., $f(X)$ is a non-unit and $f(X) = g(X)h(X) \implies g(X) \in F^\times$ or $h(X) \in F^\times$).
- If $f(X)$ is irreducible, the quotient $F[X]/(f(X))$ is a field (see *proposition 4.2*). Thus, non-zero prime ideals are maximal.

Explicitly,

$$\operatorname{Spec}(F[X]) = \{(0)\} \cup \{(f(X)) \mid f(X) \text{ is monic irreducible}\}.$$

For the specific case $F = \mathbb{C}$, the Fundamental Theorem of Algebra (to be proved later) implies the only irreducibles are linear terms $X - \alpha$. Hence:

$$\operatorname{Spec}(\mathbb{C}[X]) = \{(0)\} \cup \{(X - \alpha) \mid \alpha \in \mathbb{C}\}.$$

範例

In rings with higher dimension, such as $\mathbb{Z}[x]$, strictly prime (non-maximal) ideals are more common.

> **Example 4.3.** Spectrum of $\mathbb{Z}[X]$. Consider the ring $R = \mathbb{Z}[X]$.
>
> - The ideal (2) is prime because $\mathbb{Z}[X]/(2) \cong (\mathbb{Z}/2\mathbb{Z})[X]$, which is an integral domain.
> - However, (2) is not maximal, as it is strictly contained in the ideal $(2, X)$.
> - The quotient $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$ is a field, so $(2, X)$ is maximal.
>
> This gives a chain of prime ideals $(0) \subsetneq (2) \subsetneq (2, X)$, illustrating that the spectrum can have a complex poset structure.
>
> 範例

A natural question arises: does every ring possess a maximal ideal? For Noetherian rings (where every ideal is finitely generated), this can be proven directly. For general rings, we require the Axiom of Choice, typically in the form of Zorn's Lemma.

> **Definition 4.3.** ***Partial Order and Chains.***
> A **partial order** on a set P is a relation $\leq$ that is reflexive ($a \leq a$), antisymmetric ($a \leq b$ and $b \leq a \implies a = b$), and transitive ($a \leq b$ and $b \leq c \implies a \leq c$). A set equipped with a partial order is a **partially ordered set** (or poset).
>
> - A subset $C \subseteq P$ is a **chain** (or totally ordered subset) if for any $a, b \in C$, either $a \leq b$ or $b \leq a$.
> - An element $u \in P$ is an **upper bound** for a subset $S \subseteq P$ if $s \leq u$ for all $s \in S$.
>
> 定義

> **Lemma 4.1.** Zorn's Lemma. Let P be a non-empty partially ordered set. If every totally ordered subset (chain) of P has an upper bound in P, then P contains at least one maximal element.
>
> 引理

> *Remark.*
>
> The proof of this lemma is a standard result in set theory (equivalent to the Axiom of Choice) and is omitted here.

We use this to prove Krull's Theorem, which asserts the ubiquity of maximal ideals.

> **Theorem 4.1.** ***Existence of Maximal Ideals (Krull's Theorem).***
> Let R be a commutative ring and $\mathfrak{a} \subsetneq R$ a proper ideal. Then there exists a maximal ideal $\mathfrak{m}$ of R such that $\mathfrak{a} \subseteq \mathfrak{m}$.
>
> 定理

Proof

Let $\mathcal{S}$ be the set of all proper ideals of R that contain $\mathfrak{a}$. The set is non-empty since $\mathfrak{a} \in \mathcal{S}$. We order $\mathcal{S}$ by set inclusion. Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a totally ordered subset of $\mathcal{S}$. Define $J = \bigcup_{\lambda\in\Lambda} I_\lambda$. We claim J is a proper ideal.

***J* is an ideal:** If $x, y \in J$, there exist indices α, β such that $x \in I_\alpha$ and $y \in I_\beta$. Since the set is totally ordered, assume $I_\alpha \subseteq I_\beta$. Then $x, y \in I_\beta$, so $x - y \in I_\beta \subseteq J$. Similarly, absorption holds.

***J* is proper:** Since each I_λ is proper, $1 \notin I_\lambda$ for all λ. Consequently, $1 \notin \bigcup I_\lambda = J$. Thus $J \neq R$.

Since $J \in \mathcal{S}$ and $I_\lambda \subseteq J$ for all λ, J is an upper bound for the chain. By Zorn's Lemma, $\mathcal{S}$ has a maximal element $\mathfrak{m}$. This $\mathfrak{m}$ is a maximal ideal of R, for if K were an ideal with $\mathfrak{m} \subsetneq K \subsetneq R$, then K would be in $\mathcal{S}$, contradicting the maximality of $\mathfrak{m}$ in $\mathcal{S}$.

■

4.2 *Universal Properties of Fractions*

In *definition* 1.8, we introduced the field of fractions K of an integral domain D. We now provide a analysis of this construction and characterise K via its universal property.

Construction and Well-Definedness

Recall that K consists of equivalence classes of pairs (r, s) with $s \neq 0$, denoted $\frac{r}{s}$, under the relation $(r, s) \sim (r', s') \iff rs' = r's$. The operations were defined as:

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

For these operations to define a field structure, they must be independent of the choice of representatives.

Lemma 4.2. ***Well-Definedness of Addition.***
The addition operation on K is well-defined.

引理

Proof

Suppose $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ and $\frac{r_1'}{s_1'} = \frac{r_2'}{s_2'}$. By definition, this implies:

$$r_1 s_2 = r_2 s_1 \quad \text{and} \quad r_1' s_2' = r_2' s_1'.$$

We must show that the sums are equivalent:

$$\frac{r_1 s_1' + r_1' s_1}{s_1 s_1'} = \frac{r_2 s_2' + r_2' s_2}{s_2 s_2'}.$$

This requires proving:

$$(r_1 s_1' + r_1' s_1)(s_2 s_2') = (s_1 s_1')(r_2 s_2' + r_2' s_2).$$

Expanding the left-hand side and applying the equivalence relations:

$$\begin{aligned}(r_1 s_1' + r_1' s_1) s_2 s_2' &= r_1 s_2 s_1' s_2' + r_1' s_2' s_1 s_2 \\ &= (r_2 s_1) s_1' s_2' + (r_2' s_1') s_1 s_2 \\ &= s_1 s_1' (r_2 s_2' + r_2' s_2).\end{aligned}$$

Thus, the operation is independent of the representatives.

■

The verification that multiplication is well-defined and that K satisfies the field axioms is similar and omitted.

The Universal Property

The field of fractions is not merely a field containing D; it is, in a precise sense, the smallest such field. Any embedding of D into a field F factors uniquely through K.

Theorem 4.2. ***Universal Property of the Field of Fractions.*** Let D be an integral domain and let K be its field of fractions.

1. The map $f : D \to K$ defined by $a \mapsto \frac{a}{1}$ is a ring monomorphism.
2. For any field F and any ring monomorphism $\varphi : D \to F$, there exists a unique field homomorphism $\psi : K \to F$ such that $\varphi = \psi \circ f$.

定理

Proof

Injectivity of f: Since f is a homomorphism, we examine its kernel:

$$\ker f = \left\{ r \in D \mid \frac{r}{1} = \frac{0}{1} \right\} = \{ r \in D \mid r \cdot 1 = 0 \cdot 1 \} = \{0\}.$$

Thus f is a monomorphism, identifying D as a subring of K.

Existence of ψ: We are given $\varphi : D \to F$. If ψ extends φ to fractions, it must satisfy $\psi(r/s) = \psi(r/1 \cdot (s/1)^{-1}) = \varphi(r)\varphi(s)^{-1}$. Accordingly, we define $\psi : K \to F$ by:

$$\psi\left(\frac{r}{s}\right) = \varphi(r)\varphi(s)^{-1}.$$

Note that $\varphi(s) \neq 0$ because φ is an embedding and $s \neq 0$. To show ψ is well-defined, suppose $r/s = r'/s'$. Then $rs' = r's$, so $\varphi(r)\varphi(s') = \varphi(r')\varphi(s)$, which implies $\varphi(r)\varphi(s)^{-1} = \varphi(r')\varphi(s')^{-1}$.

It is routine to verify that ψ is a homomorphism. Since the domain K is a field, $\ker \psi$ is either $\{0\}$ or K. Since $\psi(1) = 1 \neq 0$, the kernel is trivial, so ψ is an embedding.

Uniqueness: Any such map must satisfy $\psi(\frac{r}{1}) = \varphi(r)$ and $\psi(\frac{1}{s}) = \psi(\frac{s}{1})^{-1} = \varphi(s)^{-1}$. The structure of ψ is therefore forced. ■

$$\begin{tikzcd}
D \arrow[r, "f"] \arrow[dr, "\varphi"'] & K \arrow[d, dashed, "\psi"] \\
 & F
\end{tikzcd}$$

Figure 4.2: The universal property: every embedding into a field F factors through K.

Recall from Chapter 1 that this process of inverting elements can be generalised by inverting a specific multiplicative system S. This yields the localisation $S^{-1}D$, which forms an integral domain intermediate between the original domain D and its full field of fractions K.

$$D \subseteq S^{-1}D \subseteq K.$$

This technique, known as localisation, is fundamental in algebraic number theory and geometry, allowing us to focus on the properties of a ring "locally" at a prime ideal.

4.3 *Exercises*

1. **Prime Avoidance Lemma.** Let R be a commutative ring with identity. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be prime ideals of R and A an ideal of R. Prove that if $A \subseteq \bigcup_{i=1}^{m} \mathfrak{p}_i$, then $A \subseteq \mathfrak{p}_i$ for some $1 \leq i \leq m$.

2. **Primes in Finite Rings.** Prove that in a finite commutative ring with identity, every prime ideal is a maximal ideal.

3. **Nilradical Containment.** Recall the definition of the nilradical $\text{Nil}(R)$ from Chapter 3. Prove that every prime ideal in a commutative ring R must contain $\text{Nil}(R)$.

4. **Intersection Property.** Let $\mathfrak{p}$ be a prime ideal of a commutative ring R with identity, and let $I_1, \ldots, I_n$ be ideals of R. Prove that if $\mathfrak{p} = \bigcap_{i=1}^{n} I_i$, then $\mathfrak{p} = I_i$ for some i.

5. **Correspondence Under Homomorphisms.** Let $f : R \to S$ be a surjective ring homomorphism with kernel K. Prove:

   (a) If $\mathfrak{p}$ is a prime ideal of R containing K, then $f(\mathfrak{p})$ is a prime ideal of S.

   (b) If $\mathfrak{q}$ is a prime ideal of S, then $f^{-1}(\mathfrak{q})$ is a prime ideal of R containing K.

   (c) There is a bijection between $\text{Spec}(S)$ and the set $\{\mathfrak{p} \in \text{Spec}(R) \mid K \subseteq \mathfrak{p}\}$.

   (d) The same correspondence holds for maximal ideals.

6. **Spectrum of Quotients.** Let I be an ideal of R.

   (a) Prove that prime ideals in R/I are of the form $\mathfrak{p}/I$, where $\mathfrak{p} \in \text{Spec}(R)$ and $I \subseteq \mathfrak{p}$.

(b) Use this to establish a bijection between $\operatorname{Spec}(R)$ and $\operatorname{Spec}(R/\operatorname{Nil}(R))$.

7. **Structure of $\mathbb{Z}/m\mathbb{Z}$.** Let $m \geq 2$. Explicitly determine the sets $\operatorname{Spec}(\mathbb{Z}/m\mathbb{Z})$ and $\operatorname{Max}(\mathbb{Z}/m\mathbb{Z})$.

8. **Finite Quotients.** Determine the structure of the ring $\mathbb{Z}[x]/(x^2 + 3, p)$ for the cases $p = 3$ and $p = 5$. Are these quotient rings fields?

9. **Maximal Ideals in Quotients.** Identify all maximal ideals in the following rings:

   (a) $\mathbb{R} \times \mathbb{R}$
   (b) $\mathbb{R}[x]/(x^2)$
   (c) $\mathbb{R}[x]/(x^2 - 3x + 2)$
   (d) $\mathbb{R}[x]/(x^2 + x + 1)$

10. **Specific Quotient Rings.** Describe the isomorphism class of the following rings:

    (a) $\mathbb{Z}[x]/(x^2 - 3, 2x + 4)$
    (b) $\mathbb{Z}[i]/(2 + i)$

11. ***p*-adic Integers.** Let $\mathbb{Z}_p$ denote the ring of p-adic integers (or consider the localization at p). Prove that $\mathbb{Z}_p$ is a Principal Ideal Domain with a unique maximal ideal $p\mathbb{Z}_p$.

12. **Local Rings.** A ring with a unique maximal ideal is called a *local ring*. Let R be a ring and $\mathfrak{m}$ a proper ideal. Prove that if every element in $R \setminus \mathfrak{m}$ is a unit, then R is a local ring with maximal ideal $\mathfrak{m}$.

13. **Localisation Properties.** Let D be an integral domain with field of fractions K, and let $S \subseteq D$ be a multiplicative system.

    (a) Prove that the construction $S^{-1}D$ satisfies the axioms of a subring of K containing D.
    (b) Prove that prime ideals in $S^{-1}D$ are of the form $S^{-1}\mathfrak{p} = \{m/n \mid m \in \mathfrak{p}, n \in S\}$, where $\mathfrak{p} \in \operatorname{Spec}(D)$ and $\mathfrak{p} \cap S = \varnothing$.
    (c) Establish a bijection between $\operatorname{Spec}(S^{-1}D)$ and $\{\mathfrak{p} \in \operatorname{Spec}(D) \mid \mathfrak{p} \cap S = \varnothing\}$.
    (d) For $D = \mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$, let $S = \mathbb{Z} \setminus \mathfrak{p}$. Show that $\mathbb{Z}/p\mathbb{Z} \cong S^{-1}\mathbb{Z}/S^{-1}\mathfrak{p}$.
    (e) Generally, determine when $D/\mathfrak{p} \cong S^{-1}D/S^{-1}\mathfrak{p}$.

14. **Localisation at a Prime.** Let R be an integral domain and $\mathfrak{p} \in \operatorname{Spec}(R)$. The localisation of R at $\mathfrak{p}$, denoted $R_{\mathfrak{p}}$, is the ring $(R \setminus \mathfrak{p})^{-1}R$. Determine all maximal ideals of $R_{\mathfrak{p}}$.

5 Factorisation

In this chapter, we extend the fundamental theorem of arithmetic to more general algebraic structures. Unless explicitly stated otherwise, we assume throughout this chapter that R is a commutative ring with identity.

5.1 *Unique Factorisation Domains*

The study of divisibility in general rings requires us to formalise the notions of factors, primes, and irreducibles, distinguishing between properties that coincide in $\mathbb{Z}$ but diverge in other settings.

Factors, Prime Elements, and Irreducible Elements

We begin by defining the divisibility relation in terms of the ring operations.

> **Definition 5.1.** ***Divisors and Associates.***
> Let $a, b \in R$.
> 1. We say a is a **divisor** (or factor) of b, denoted $a \mid b$, if there exists $x \in R$ such that $b = ax$. In this case, b is called a **multiple** of a.
> 2. If $a \mid b$ and $b \mid a$, we say a and b are **associates**, denoted $a \sim b$.
> 3. If $b = ax$ where x is not a unit, then a is called a **proper divisor** of b.
>
> 定義

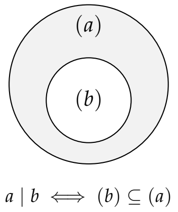

Figure 5.1: Divisibility corresponds to reverse inclusion of ideals.

The language of divisibility translates directly into the language of principal ideals established in the previous chapter.

> **Proposition 5.1.** ***Properties of Divisibility.***
> Let $a, b \in R$ and let $u \in R^\times$ be a unit.
> 1. $a \mid b$ if and only if the principal ideal generated by b is contained in that of a: $(b) \subseteq (a)$.
> 2. $a \sim b$ if and only if $(b) = (a)$.
> 3. The unit u is a factor of every element $r \in R$. If r is not a unit, then u is a proper divisor of r (often called a trivial divisor).

4. If $a = bu$, then $a \sim b$. If R is an integral domain, the converse holds: $a \sim b$ implies $a = bu$ for some unit u.
5. If R is an integral domain, then a is a proper divisor of b if and only if $(b) \subsetneq (a)$.

命題

Proof

1. This follows immediately from the definition of a principal ideal: $b \in (a) \iff b = ax \iff a \mid b$.
2. This follows from applying (1) in both directions.
3. Since $r = u(u^{-1}r)$, $u \mid r$. If r is not a unit, the factor $u^{-1}r$ cannot be a unit (otherwise r would be the product of units), so u is proper.
4. If $a = bu$, then $a \mid b$. Since $b = au^{-1}$, $b \mid a$. Thus $a \sim b$. Conversely, let R be an integral domain and assume $a \sim b$. Then $a = bx$ and $b = ay$ for some $x, y \in R$. Substituting, we get $a = axy$, or $a(1 - xy) = 0$. If $a = 0$, then $b = 0$, so $a = b \cdot 1$. If $a \neq 0$, the cancellation law implies $1 - xy = 0$, so $xy = 1$. Thus x is a unit.
5. Let $b = ax$. If x is not a unit, then $a \notin (b)$. Indeed, if $a \in (b)$, then $a = by$, implying $a = axy$. As in (4), this forces x to be a unit (assuming $a \neq 0$; if $a = 0$ then $b = 0$, and 0 is not a proper divisor of 0). Conversely, if $(b) \subsetneq (a)$, then $b = ax$ for some x. If x were a unit, we would have $a \sim b$ and $(a) = (b)$, a contradiction.

■

In the integers, primes are defined by their inability to be factored. In general rings, we must distinguish between elements that cannot be factored and elements that divide products in a specific way.

Definition 5.2. ***Prime and Irreducible Elements.***

1. A non-zero, non-unit element $p \in R$ is a **prime element** if $p \mid ab$ implies $p \mid a$ or $p \mid b$.
2. A non-zero, non-unit element $a \in R$ is an **irreducible element** (or maximal element) if it has no non-trivial factors. That is, if $a = xy$, then either x or y is a unit.

定義

Example 5.1. Primes in Integers. In the ring $\mathbb{Z}$, the set of prime elements coincides with the set of irreducible elements, which are exactly $\{\pm p \mid p \text{ is a prime number}\}$.

範例

The relationship between these elements and the ideal structure of R is central to ring theory.

Proposition 5.2. ***Primes, Irreducibles, and Ideals.***
Let R be an integral domain.

1. An element p is prime if and only if the principal ideal (p) is a prime ideal.
2. An element a is irreducible if and only if the ideal (a) is maximal amongst the set of proper principal ideals of R.
3. Every prime element is irreducible.
4. If R is a Principal Ideal Domain (PID), then every irreducible element is a prime element.

命題

Proof

1. Recall that an ideal P is prime if $ab \in P \implies a \in P$ or $b \in P$. If p is a prime element and $ab \in (p)$, then $p \mid ab$, which implies $p \mid a$ or $p \mid b$. In terms of ideals, $(a) \subseteq (p)$ or $(b) \subseteq (p)$, so $a \in (p)$ or $b \in (p)$. Conversely, if (p) is a prime ideal and $p \mid ab$, then $ab \in (p)$. By definition of prime ideals, $a \in (p)$ or $b \in (p)$, so $p \mid a$ or $p \mid b$.
2. Let a be irreducible. Suppose there exists a principal ideal (b) such that $(a) \subsetneq (b) \subsetneq R$. Then $b \mid a$, so $a = bx$. Since $(a) \neq (b)$, b is not an associate of a, so x is not a unit. Since $(b) \neq R$, b is not a unit. This contradicts the irreducibility of a. Conversely, assume (a) is maximal among principal ideals. Let $a = bx$. If b is a proper divisor, then $(a) \subsetneq (b)$. By maximality, $(b) = R$, implying b is a unit. Thus a has no proper divisors.
3. Let p be prime. Suppose $p = ab$. Then $p \mid ab$, so $p \mid a$ or $p \mid b$. Without loss of generality, assume $p \mid a$. Then $a = px$ for some x. Substituting back, $p = pxb$. Since R is a domain and $p \neq 0$, we cancel p to get $1 = xb$. Thus b is a unit. Hence p is irreducible.
4. Let R be a PID and let a be irreducible. By (2), (a) is maximal among principal ideals. Since every ideal in a PID is principal, (a) is a maximal ideal in R. Maximal ideals are prime ideals, so (a) is a prime ideal. By (1), a is a prime element.

■

5.2 *Unique Factorisation Domains*

Having defined the fundamental building blocks of divisibility we now formulate the definition of a domain where arithmetic behaves analogously to the integers.

Definition 5.3. ***Unique Factorisation Domain.***
An integral domain R is a **Unique Factorisation Domain** (UFD) if it satisfies two conditions:

1. **Existence of Factorisation:** Every non-zero non-unit $a \in R$ can be

written as a product of irreducible elements:

$$a = c_1 c_2 \dots c_n,$$

where each c_i is irreducible.

2. **Uniqueness of Factorisation:** If a has two factorisations into irreducibles

$$a = c_1 \dots c_n = d_1 \dots d_m,$$

then $n = m$, and there exists a permutation $\sigma \in S_n$ such that $c_i \sim d_{\sigma(i)}$ for all i.

定義

To appreciate the strength of this definition, it is instructive to examine rings where these properties fail.

Example 5.2. Failure of Existence. Let F be a field and consider the ring $R = F[x_1, x_2, \dots]$ modulo the relations $x_{n+1}^2 = x_n$ for all $n \geq 1$. In this ring, we have an infinite chain of roots:

$$x_1 = x_2^2 = x_3^4 = \dots$$

The element x_1 admits no finite factorisation into irreducibles, as any potential factor can be further decomposed.

範例

Example 5.3. Failure of Uniqueness in $\mathbb{Z}[\sqrt{-5}]$. Consider the ring $R = \mathbb{Z}[\sqrt{-5}]$. We examine the number 6:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

To determine if these factorisations are distinct, we introduce the **norm map** $N : R \to \mathbb{N}$ defined by $N(a + b\sqrt{-5}) = a^2 + 5b^2$.

- The norm is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.
- Units in R are elements with norm 1. Since $a^2 + 5b^2 = 1$ has integer solutions only for $a = \pm 1, b = 0$, the units are $U(R) = \{\pm 1\}$.

We claim that 2 is irreducible. If $2 = \alpha\beta$ with non-units α, β, then $N(2) = N(\alpha)N(\beta) = 4$. This implies $N(\alpha) = 2$. However, the equation $a^2 + 5b^2 = 2$ has no integer solutions. Thus, no proper splitting exists. Similarly, 3 and $1 \pm \sqrt{-5}$ are irreducible (having norms 9 and 6 respectively; no elements exist with norms 3 or 2). Since $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, 2 is not associate to $1 + \sqrt{-5}$. Thus, factorization is not unique.

範例

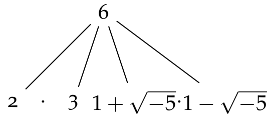

Figure 5.2: Two distinct decompositions of 6 into irreducibles in $\mathbb{Z}[\sqrt{-5}]$.

Remark.

example 5.3 also demonstrates that irreducible elements need not be prime.

Note that $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$. However, $2 \nmid (1+\sqrt{-5})$ because $N(2) = 4$ does not divide $N(1+\sqrt{-5}) = 6$ in $\mathbb{Z}$? No, $4 \nmid 6$ is false logic for divisibility. Rather,

$$\frac{1+\sqrt{-5}}{2} \notin R.$$

Thus 2 is irreducible but not prime.

Greatest Common Divisors

In a general ring, the greatest common divisor is defined via divisibility rather than magnitude.

Definition 5.4. ***Greatest Common Divisor.***
Let R be a ring and $a, b \in R$. An element $d \in R$ is a **Greatest Common Divisor** (GCD) of a and b, denoted (a, b), if:
1. $d \mid a$ and $d \mid b$ (it is a common divisor).
2. If d' is any element such that $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

If $(a, b) \sim 1$, we say a and b are **coprime**.

定義

If a GCD exists, it is unique only up to associates. We typically abuse notation and write $d = (a, b)$ to mean d is *a* GCD.

Definition 5.5. ***Least Common Multiple.***
Let R be a ring and $a, b \in R$. An element $m \in R$ is a **Least Common Multiple** (LCM) of a and b, denoted $[a, b]$, if:
1. $a \mid m$ and $b \mid m$ (it is a common multiple).
2. If n is any element such that $a \mid n$ and $b \mid n$, then $m \mid n$.

定義

Lemma 5.1. ***Properties of GCDs.***
Let R be an integral domain where GCDs exist. For any $a, b, c \in R$:
1. $c(a, b) \sim (ca, cb)$.
2. If $(a, b) \sim 1$ and $(a, c) \sim 1$, then $(a, bc) \sim 1$.

引理

Proof

1. Let $d = (a, b)$. Since d divides a and b, cd divides ca and cb. Thus cd is a common divisor. Let k be any common divisor of ca and cb. Then $ca = kx$ and $cb = ky$. Let $(ca, cb) = g$. Then $cd \mid g$. Conversely, since $c \mid ca$ and $c \mid cb$, we must have $c \mid g$. Write $g = cy$. Then $cy \mid ca \implies y \mid a$ and $cy \mid cb \implies y \mid b$. Thus y is a common divisor of a, b, so $y \mid d$. Hence $cy \mid cd$, or $g \mid cd$. Since $g \mid cd$ and $cd \mid g$, they are associates.
2. Since $(a, b) \sim 1$, using property (1) we have $(ac, bc) \sim c(a, b) \sim c$.

We compute (a, bc). Since $(a, ac) \sim a$:

$$(a, bc) \sim ((a, ac), bc) \sim (a, (ac, bc)) \sim (a, c) \sim 1.$$

■

Characterisation of UFDs

To determine whether a domain is a UFD without explicit factorisation, we rely on two properties: the Noetherian property (ensuring factorisation terminates) and the primal property of irreducibles (ensuring uniqueness).

Theorem 5.1. ***Properties of UFDs.***
Let R be a UFD. Then:

1. **Ascending Chain Condition (ACC) for Principal Ideals:** Any chain of principal ideals $(a_1) \subseteq (a_2) \subseteq \dots$ must stabilize (i.e., there exists N such that $(a_n) = (a_N)$ for all $n \geq N$).
2. Every irreducible element is prime.
3. For any non-zero $a, b \in R$, a GCD exists.

定理

Proof

1. Let $(a_1) \subseteq (a_2) \subseteq \dots$ be a chain. This implies $a_{i+1} \mid a_i$. Thus a_i is a factor of a_1. Let $a_1 = up_1 \dots p_k$ be the factorization of a_1 into irreducibles. Any divisor of a_1 is associated to a sub-product of these factors. Since the number of factors is finite (k), the length of any strictly increasing chain of divisors is bounded by k. Thus the chain must stabilize.
2. Let p be irreducible and suppose $p \mid ab$. Then $ab = px$ for some x. Let $a = \prod c_i$ and $b = \prod d_j$ be factorisations into irreducibles. Then
$$\prod c_i \prod d_j = p \prod y_k,$$
where $x = \prod y_k$. By the uniqueness of factorisation in R, p must be associate to one of the factors on the left. Thus $p \sim c_i$ (implies $p \mid a$) or $p \sim d_j$ (implies $p \mid b$). Hence p is prime.
3. Let $a = u \prod p_i^{e_i}$ and $b = v \prod p_i^{f_i}$ where p_i are distinct non-associate irreducibles and exponents are non-negative. Set $g_i = \min(e_i, f_i)$. Then $d = \prod p_i^{g_i}$ is clearly a common divisor. If d' divides both, its prime factorization exponents t_i must satisfy $t_i \leq e_i$ and $t_i \leq f_i$ (by uniqueness), so $t_i \leq g_i$, implying $d' \mid d$.

■

The converse also holds, providing a powerful criteria for identifying UFDs.

Theorem 5.2. ***Equivalence of Definitions.***
Let R be an integral domain. The following are equivalent:

1. R is a Unique Factorisation Domain.
2. R satisfies the ACC for principal ideals, and every irreducible element is prime.
3. R satisfies the ACC for principal ideals, and GCDs exist for all pairs.

定理

Proof

We have proven (1) $\implies$ (2) and (1) $\implies$ (3) above. We prove the reverse implications.

(2) $\implies$ (1)*:* We prove both existence and uniqueness.

Existence: Let a be a non-unit. If a is irreducible, we are done. If not, $a = a_1 b_1$ with proper factors. If these are irreducible, done. If not, continue factoring. This generates a sequence of divisors $a, a_1, a_2, \ldots$ corresponding to ideals $(a) \subsetneq (a_1) \subsetneq (a_2) \ldots$. By ACC, this chain stabilizes, meaning the process terminates in irreducibles.

Uniqueness: Suppose $p_1 \ldots p_n = q_1 \ldots q_m$ with all factors irreducible. Since p_1 is irreducible, by hypothesis (2) it is prime. Thus $p_1 \mid q_1 \ldots q_m$, so $p_1 \mid q_j$ for some j. Reorder so $j = 1$. Since q_1 is irreducible, its only factors are units and associates. Thus $p_1 \sim q_1$.

Cancelling these (in a domain) gives $p_2 \ldots p_n \sim q_2 \ldots q_m$. By induction, $n = m$ and factors are associates.

(3) $\implies$ (2)*:* It suffices to show that if GCDs exist, irreducibles are prime. Let p be irreducible and $p \mid ab$. Suppose $p \nmid a$. Since p has no factors other than units and associates, the only common divisors of p and a are units. Thus $(p, a) \sim 1$.

By *lemma 5.1(2)*, since $(p, a) \sim 1$, we have $(p, ab) \sim (p, b)$. Since $p \mid ab$, $(p, ab) \sim p$. Thus $(p, b) \sim p$, which implies $p \mid b$. Hence p is prime.

■

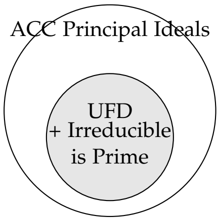

Figure 5.3: The Noetherian condition is necessary but not sufficient for a UFD.

Principal Ideal Domains are UFDs

We now connect the theory of ideals to factorization. We previously showed that in a Principal Ideal Domain (PID), irreducibles are prime. To show a PID is a UFD, we need only establish the Ascending Chain Condition.

Theorem 5.3. ***PIDs are UFDs.***
Every Principal Ideal Domain is a Unique Factorisation Domain.
定理

Proof

Let R be a PID. By *theorem 5.2*, we must show that R satisfies the ACC for principal ideals. (Recall we already proved Irreducible $\implies$ Prime for PIDs). Consider an ascending chain:

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \ldots$$

Let $I = \bigcup_{n=1}^{\infty}(a_n)$. We claim I is an ideal. If $x, y \in I$, there exist k, m such that $x \in (a_k)$ and $y \in (a_m)$. Let $N = \max(k, m)$. Then $x, y \in (a_N)$, so $x - y \in (a_N) \subseteq I$. Similarly for absorption. Since R is a PID, I is principal, so $I = (a)$ for some $a \in I$. By definition of the union, $a \in (a_N)$ for some integer N. Thus, for all $n \geq N$:

$$(a) \subseteq (a_N) \subseteq (a_n) \subseteq I = (a).$$

This forces $(a_n) = (a_N)$ for all $n \geq N$, proving stabilisation.

■

Remark.

It is important to distinguish between the existence of a GCD and the ability to express it as a linear combination (the Bezout identity). In a PID, (a, b) is generated by some d, so $d \in (a, b) \implies d = ax + by$. However, in a general UFD, this need not hold. Consider $R = \mathbb{Z}[x]$. The elements 2 and x have GCD 1. However, the ideal generated by 2 and x, $(2, x)$, is not the whole ring (elements have even constant term). Thus $1 \notin (2, x)$, so we cannot write $1 = 2f(x) + xg(x)$. Rings where the Bezout identity holds are called **Bezout domains**.

5.3 *Euclidean Domains*

We have established a hierarchy of integral domains:

Fields $\subset$ Principal Ideal Domains (PIDs) $\subset$ Unique Factorisation Domains (UFDs).

We now abstract the property of division with remainder (as seen in $\mathbb{Z}$) to define a class of rings where such a "size" function exists.

Definition 5.6. ***Euclidean Domain.***
Let R be an integral domain. R is a **Euclidean Domain** (ED) if there exists a function

$$\varphi : R \setminus \{0\} \to \mathbb{Z}_+$$

such that for any $a, b \in R$ with $a \neq 0$, there exist $q, r \in R$ satisfying:

$$b = aq + r,$$

where either $r = 0$ or $\varphi(r) < \varphi(a)$.

定義

The function φ is often called a Euclidean valuation or norm.

Theorem 5.4. ***ED implies PID.***
Every Euclidean Domain is a Principal Ideal Domain. Consequently, every Euclidean Domain is a Unique Factorisation Domain.

定理

Proof

Let R be a Euclidean Domain and I be a non-zero ideal of R.
We must show that I is generated by a single element. Let $S = \{\varphi(x) \mid x \in I \setminus \{0\}\} \subseteq \mathbb{N}_+$. By the Well-Ordering Principle of the integers, S contains a minimal element. Let $a \in I$ be an element such that $\varphi(a)$ is minimal in S. We claim $I = (a)$. Since $a \in I$, clearly $(a) \subseteq I$. Conversely, let $b \in I$. Since R is an ED, there exist $q, r \in R$ such that $b = aq + r$, with $r = 0$ or $\varphi(r) < \varphi(a)$. Rearranging, we have $r = b - aq$. Since $b \in I$ and $a \in I$, and I is an ideal, $r \in I$. If $r \neq 0$, then $\varphi(r)$ would be defined. However, $\varphi(r) < \varphi(a)$ would contradict the minimality of $\varphi(a)$ in the set of norms of non-zero elements of I. Therefore, we must have $r = 0$. Thus $b = aq$, implying $b \in (a)$. Hence $I = (a)$, so R is a PID. The fact that R is a UFD follows immediately from *theorem* 5.3.

■

Example 5.4. Gaussian Integers. The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (where $i^2 = -1$) is a Euclidean Domain.

範例

Solution

We define the function $\varphi : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ by the norm map:

$$\varphi(a + bi) = a^2 + b^2 = |a + bi|^2.$$

Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. We perform the division in the field of fractions $\mathbb{Q}(i)$:

$$\frac{\alpha}{\beta} = x + yi, \quad \text{where } x, y \in \mathbb{Q}.$$

Let x_0, y_0 be the integers closest to x and y respectively. That is, $|x - x_0| \leq \frac{1}{2}$ and $|y - y_0| \leq \frac{1}{2}$. Set $q = x_0 + y_0 i \in \mathbb{Z}[i]$. Then

$$\frac{\alpha}{\beta} = q + \delta, \quad \text{where } \delta = (x - x_0) + (y - y_0)i.$$

The distance satisfies $|\delta|^2 = (x - x_0)^2 + (y - y_0)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Now, set $r = \alpha - \beta q = \beta\delta$. Clearly $r \in \mathbb{Z}[i]$. If $r \neq 0$, we calculate its size:

$$\varphi(r) = |r|^2 = |\beta\delta|^2 = |\beta|^2|\delta|^2 \leq |\beta|^2 \cdot \frac{1}{2} = \frac{1}{2}\varphi(\beta).$$

Since $\varphi(\beta) > 0$, we have $\varphi(r) < \varphi(\beta)$. Thus $\mathbb{Z}[i]$ is an ED.

■

This result confirms that arithmetic in $\mathbb{Z}[i]$ supports a Euclidean algorithm, allowing us to compute greatest common divisors effectively. This structure is essential in Number Theory, particularly for characterising sums of two squares.

5.4 *Gaussian Integers and the Two-Square Problem*

We apply the general theory of Unique Factorisation Domains to the specific case of the Gaussian integers, $\mathbb{Z}[i]$. This ring provides the natural setting for solving the classical number theoretic problem of representing integers as sums of two squares.

Definition 5.7. ***Gaussian Integers.***
The ring of **Gaussian integers**, denoted $\mathbb{Z}[i]$, is the subring of complex numbers given by:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \quad \text{where } i^2 = -1.$$

Its prime elements are referred to as **Gaussian primes**. We employ the norm function defined in the previous section:

$$N(a + bi) = a^2 + b^2 = (a + bi)(a - bi).$$

定義

Recall from example 5.4 that $\mathbb{Z}[i]$ is a Euclidean Domain, and thus by *theorem* 5.4, it is a Principal Ideal Domain and a Unique Factorisation Domain.

Units and Primes

We first characterise the invertible elements and the prime elements of this ring.

Lemma 5.2. ***Units of Gaussian Integers.***
The group of units of the Gaussian integers is cyclic of order 4:

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\}.$$

引理

Proof

An element $\alpha \in \mathbb{Z}[i]$ is a unit if and only if it divides 1, which implies $N(\alpha) \mid N(1) = 1$. Since the norm is a non-negative integer, we must have $N(a+bi) = a^2 + b^2 = 1$. The only integer solutions are $(\pm 1, 0)$ and $(0, \pm 1)$, corresponding to the stated elements.

■

The classification of Gaussian primes reveals a deep connection between the algebraic structure of $\mathbb{Z}[i]$ and modular arithmetic in $\mathbb{Z}$.

Theorem 5.5. ***Classification of Gaussian Primes.***
Let p be a rational prime (i.e., a prime in $\mathbb{Z}$).

1. If $p = 2$, then p ramifies in $\mathbb{Z}[i]$:

$$2 = -i(1+i)^2.$$

   The element $1+i$ is a Gaussian prime.
2. If $p \equiv 3 \pmod 4$, then p remains prime in $\mathbb{Z}[i]$ (it is inert).
3. If $p \equiv 1 \pmod 4$, then p splits into the product of two distinct conjugate Gaussian primes:

$$p = \pi\bar{\pi},$$

   where π is not associate to $\bar{\pi}$.

Consequently, the Gaussian primes are exactly the associates of $1+i$, the rational primes $q \equiv 3 \pmod 4$, and the factors π of rational primes $p \equiv 1 \pmod 4$.

定理

Proof

We establish this classification through the following steps.

Rational primes and Gaussian norms. Let π be a Gaussian prime. Since $\pi \mid N(\pi)$ and $N(\pi)$ is an integer, π divides some rational prime p. Since p is a prime in $\mathbb{Z}$, its decomposition in $\mathbb{Z}[i]$ is of the form $p = \pi_1 \dots \pi_k$. Taking norms, $N(p) = p^2 = N(\pi_1) \dots N(\pi_k)$. Since $N(\pi_j) > 1$, there are two possibilities for any factor π:

- $N(\pi) = p^2$. Then $\pi \sim p$, meaning p remains prime in $\mathbb{Z}[i]$.
- $N(\pi) = p$. Then $p = \pi\bar{\pi}$ (since $p = N(\pi)$).

The case $p = 2$. We observe $2 = (1+i)(1-i)$. Since $1 - i = -i(1+i)$, we have $2 \sim (1+i)^2$. Since $N(1+i) = 2$, which is prime in $\mathbb{Z}$, $1+i$ must be irreducible (and hence prime) in $\mathbb{Z}[i]$.

The splitting condition. A rational prime p splits (i.e., is not prime in $\mathbb{Z}[i]$) if and only if $p = \pi\bar{\pi}$ for some $\pi = a + bi$.

$$p = \pi\bar{\pi} \iff p = a^2 + b^2 \iff p \text{ is a sum of two squares.}$$

By standard modular arithmetic, $a^2 + b^2 \equiv 0, 1, 2 \pmod 4$. Thus, if $p \equiv 3 \pmod 4$, p cannot be written as a sum of two squares, so p must remain prime in $\mathbb{Z}[i]$.

Conversely, suppose $p \equiv 1 \pmod 4$. By Euler's Criterion, the Legendre symbol satisfies:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$

Thus, the congruence $x^2 \equiv -1 \pmod p$ has an integer solution x. This implies $p \mid x^2 + 1 = (x+i)(x-i)$. If p were prime in $\mathbb{Z}[i]$, then $p \mid (x+i)$ or $p \mid (x-i)$. However, $\frac{x+i}{p} = \frac{x}{p} + \frac{1}{p}i$ is not in $\mathbb{Z}[i]$. Contradiction.

Therefore, p is not prime in $\mathbb{Z}[i]$, so it must split as $p = \pi\bar{\pi}$.

■

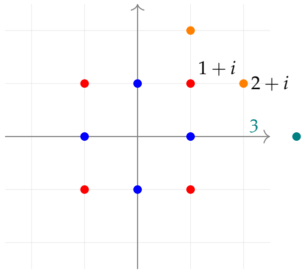

Figure 5.4: Lattice of $\mathbb{Z}[i]$. Units (blue), primes above 2 (red), and primes above 5 (orange).

Sum of Two Squares

The algebraic structure of $\mathbb{Z}[i]$ provides a complete solution to the problem of determining which integers can be written as a sum of two squares. An integer n is a sum of two squares if and only if $n = N(\alpha)$ for some $\alpha \in \mathbb{Z}[i]$.

Theorem 5.6. ***Sum of Two Squares.***
Let n be a positive integer with prime factorisation

$$n = 2^k \prod_{j=1}^{s} p_j^{\beta_j} \prod_{m=1}^{t} q_m^{\gamma_m},$$

where $p_j \equiv 1 \pmod 4$ and $q_m \equiv 3 \pmod 4$.

1. The integer n can be written as a sum of two squares if and only if the exponent γ_m is even for all $m = 1, \ldots, t$.
2. If this condition holds, the number of distinct representations $n = x^2 + y^2$ (distinguishing signs and order) is given by:

$$r_2(n) = 4\prod_{j=1}^{s}(\beta_j + 1).$$

定理

Proof

We analyse the factorisation of n in $\mathbb{Z}[i]$. We substitute the rational primes with their Gaussian factorisations:

- $2 = -i(1+i)^2$.
- $p_j = \pi_j \bar{\pi}_j$ (split).
- q_m remains prime (inert).

Thus, the unique factorisation of n in $\mathbb{Z}[i]$ (up to units) is:

$$n \sim (1+i)^{2k} \prod_{j=1}^{s} (\pi_j \bar{\pi}_j)^{\beta_j} \prod_{m=1}^{t} q_m^{\gamma_m}.$$

An integer n is a sum of two squares if and only if $n = \alpha\bar{\alpha} = N(\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. Let $\alpha = u(1+i)^{k'} \prod \pi_j^{e_j} \bar{\pi}_j^{f_j} \prod q_m^{h_m}$. Then the norm is:

$$N(\alpha) = 2^{k'} \prod p_j^{e_j+f_j} \prod q_m^{2h_m}.$$

Matching this with the factorisation of n:

1. The exponent of q_m in n is $\gamma_m = 2h_m$. Thus, γ_m must be even for a solution to exist.
2. The exponent of p_j is $\beta_j = e_j + f_j$.
3. The exponent of 2 is $k = k'$.

If the condition on γ_m is met, we construct α. For each split prime p_j, we must choose exponents e_j, f_j such that $e_j + f_j = \beta_j$. There are $\beta_j + 1$ choices for the pair (e_j, f_j) (specifically, $e_j \in \{0, \ldots, \beta_j\}$). For the inert primes q_m, the exponent h_m is fixed as $\gamma_m/2$. For the ramified prime 2, the exponent is fixed as k. Finally, there are 4 choices for the unit $u \in \{1, -1, i, -i\}$. By the uniqueness of factorisation in $\mathbb{Z}[i]$, distinct choices of exponents and units yield distinct Gaussian integers α. Thus, the total number of solutions is $4\prod(\beta_j + 1)$.

■

Example 5.5. Representations of 45 and 49.

- $n = 45 = 3^2 \cdot 5$. The prime $3 \equiv 3 \pmod 4$ has even exponent, and $5 \equiv 1 \pmod 4$. Thus solutions exist. The number of solutions is $4(1+1) = 8$. They are $(\pm 3)^2 + (\pm 6)^2 = 9 + 36 = 45$ and $(\pm 6)^2 + (\pm 3)^2$.
- $n = 49 = 7^2$. Here $7 \equiv 3 \pmod 4$ has even exponent. Number of solutions is $4(1) = 4$. Solutions are $(\pm 7)^2 + 0^2$.
- $n = 21 = 3 \cdot 7$. Exponents are odd for primes $\equiv 3 \pmod 4$. No solution.

範例

5.5 Exercises

1. **Divisibility and LCM in a UFD.** Let R be a Unique Factorisation Domain. For non-zero elements $a, b, c \in R$, prove:

   (a) The product relates to the GCD and LCM via associates: $ab \sim (a, b)[a, b]$.

   (b) If $a \mid bc$ and $(a, b) \sim 1$, then $a \mid c$.

2. **Ideal Arithmetic in a PID.** Let R be a Principal Ideal Domain. Prove the following properties of ideals generated by $a, b \in R$:

   (a) The intersection corresponds to the LCM: $(a) \cap (b) = ([a, b])$.

   (b) The intersection equals the product, $(a) \cap (b) = (a)(b)$, if and only if a and b are coprime (i.e., $(a, b) \sim 1$).

   (c) The linear Diophantine equation $ax + by = c$ has a solution $(x, y) \in R^2$ if and only if the GCD (a, b) divides c.

3. **Polynomial Rings over Non-Fields.** Let D be an integral domain that is not a field. Prove that the polynomial ring $D[X]$ is not a Principal Ideal Domain.

Consider the ideal generated by X and a non-unit constant.

4. **Properties of Associates.** Let R be an integral domain and let $a, b \in R \setminus \{0\}$ be associates ($a \sim b$). Prove:

   (a) If a is irreducible, then b is irreducible.

   (b) If a is prime, then b is prime.

5. **Prime vs. Irreducible Quotients.** Let a be a non-zero element in a PID D.

   (a) Prove that if a is a prime element, then the quotient ring $D/(a)$ is a field.

   (b) Prove that if a is not a prime element (and not a unit), then $D/(a)$ is not an integral domain.

6. **Classifying Quadratic Rings.** Determine which of the following rings are Principal Ideal Domains (PIDs) and which are Euclidean Domains (EDs). Justify your answers.

   (a) $\mathbb{Z}[\sqrt{-2}]$

   (b) $\mathbb{Z}[\sqrt{-3}]$

   (c) The ring of polynomials in two variables, $\mathbb{R}[X, Y]$

   (d) $\mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$ (the Eisenstein integers)

7. **GCD Preservation in Extensions.** Let D be a PID and E be an integral domain such that D is a subring of E. Let $a, b \in D \setminus \{0\}$. Let d be a GCD of a and b computed in D. Prove that d remains a GCD of a and b when considered as elements of the larger ring E.

Use the Bezout identity available in the PID D.

8. **Unique Representations.** Let p be an odd prime such that $p \equiv 1$

$\pmod 4$. Prove that if (a, b) is an integer solution to the Diophantine equation $x^2 + y^2 = p$, then the complete set of integer solutions is given by $(\pm a, \pm b)$ and $(\pm b, \pm a)$.

9. **Gaussian Factorisation.** Perform the factorisation into irreducible elements for the following in the ring $\mathbb{Z}[i]$:

   (a) The integer 60.

   (b) The Gaussian integer $81 + 8i$.

10. **Sum of Squares Solutions.** Determine all integer solutions (x, y) to the equation $x^2 + y^2 = 585$.

First find the prime factorisation of 585 in $\mathbb{Z}$, then apply the method of Gaussian integers.

11. **Generalised Quadratic Forms.** Using the methods developed for $\mathbb{Z}[i]$ (Euclidean domains and norms), investigate the following Diophantine problems:

   (a) For a positive integer n, determine the necessary and sufficient conditions for the equation $x^2 + 2y^2 = n$ to have integer solutions. Derive a formula for the number of such solutions.

For (a): Work in the ring $\mathbb{Z}[\sqrt{-2}]$.

   (b) For a positive integer n, determine the conditions for the equation $x^2 + xy + y^2 = n$ to have integer solutions, and find the number of solutions.

For (b): Work in the ring of Eisenstein integers $\mathbb{Z}[\omega]$ where $\omega = \frac{-1+\sqrt{-3}}{2}$, noting that $x^2 + xy + y^2 = N(x - \omega y)$.

6
Polynomials

We now narrow our focus to a specific and crucial class of rings: polynomial rings. While we introduced the definition of $R[X]$ in *definition* 1.4, we now investigate their arithmetic properties in greater depth. Throughout this chapter, unless specified otherwise, R denotes a commutative ring.

6.1 Degree and Arithmetic

We begin by formalising the "size" of a polynomial.

> **Definition 6.1.** ***Degree and Leading Coefficient.***
> Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ be a non-zero polynomial in $R[X]$ with $a_n \neq 0$.
> 1. The integer n is the **degree** of f, denoted $\deg f$.
> 2. The coefficient a_n is the **leading coefficient** of f.
> 3. If $a_n = 1$, the polynomial f is called **monic**.
>
> For the zero polynomial $f(X) = 0$, we adopt the convention $\deg 0 = -\infty$. Elements of R (regarded as polynomials of degree ≤ 0) are called **constant polynomials**.
>
> 定義

The behaviour of the degree function under addition and multiplication is governed by the structural properties of the coefficient ring R.

> **Proposition 6.1.** ***Degree Properties.***
> Let $f, g \in R[X]$. Then:
> 1. $\deg(f+g) \leq \max(\deg f, \deg g)$.
> 2. $\deg(fg) \leq \deg f + \deg g$.
>
> Equality holds in (2) if the leading coefficient of either f or g is not a zero divisor in R. In particular, if R is an integral domain, equality always holds.
>
> 命題

> *Proof*
>
> This follows directly from the definition of polynomial multiplication. The leading term of the product is the product of the leading terms, provided this product is non-zero. The details are left as an exercise.
>
> ■

When the coefficient ring is an integral domain, the polynomial ring inherits this property. Furthermore, the units of the polynomial ring are constrained to the units of the base ring.

> **Proposition 6.2.** ***Units in Polynomial Rings.***
> Let D be an integral domain. Then $D[X]$ is an integral domain, and the group of units is exactly the group of units of D:
>
> $$U(D[X]) = U(D).$$
>
> 命題

> *Proof*
>
> Let $f, g \in D[X]$ be non-zero. Since D is a domain, the product of the leading coefficients of f and g is non-zero. Thus the leading coefficient of fg is non-zero, implying $fg \neq 0$. Hence $D[X]$ has no zero divisors.
> Now, suppose $f \in U(D[X])$. Then there exists $g \in D[X]$ such that $fg = 1$. Applying the degree formula for domains:
>
> $$\deg(fg) = \deg f + \deg g = \deg 1 = 0.$$
>
> Since degrees are non-negative for non-zero polynomials, we must have $\deg f = \deg g = 0$. Thus f and g are constant polynomials in D, and their product is 1. Therefore $f \in U(D)$. The reverse inclusion $U(D) \subseteq U(D[X])$ is immediate.
>
> ■

6.2 *The Division Algorithm and Roots*

While $R[X]$ is not generally a Euclidean Domain (unless R is a field), a division algorithm exists provided the divisor has a "nice" leading coefficient.

> **Proposition 6.3.** ***Polynomial Division.***
> Let $f, g \in R[X]$. If the leading coefficient of g is a unit in R, then there exist unique polynomials q (quotient) and r (remainder) in $R[X]$ such that:
>
> $$f(X) = q(X)g(X) + r(X), \quad \text{with } \deg r < \deg g.$$

命題

Proof

The existence is proven by induction on $\deg f$, mirroring the standard long division of polynomials over a field. Uniqueness follows from the fact that the leading coefficient of g is not a zero divisor.

■

This result yields the fundamental link between the algebra of polynomials and the values they take.

Corollary 6.1. *Remainder Theorem.* Let $f \in R[X]$ and let $c \in R$. Then there exists a unique polynomial $q \in R[X]$ such that

$$f(X) = q(X)(X - c) + f(c).$$

Consequently, c is a root of f (i.e., $f(c) = 0$) if and only if $(X - c)$ divides $f(X)$.

推論

Proof

Apply the polynomial division proposition with $g(X) = X - c$. Since the leading coefficient of g is 1 (a unit), there exist unique q, r with $f(X) = q(X)(X - c) + r(X)$, where $\deg r < 1$. Thus r is a constant. Evaluating at $X = c$:

$$f(c) = q(c)(c - c) + r = r.$$

Thus $f(X) = q(X)(X - c) + f(c)$. The equivalence follows immediately.

■

This allows us to bound the number of roots a polynomial may possess, a property that distinguishes integral domains from general rings.

Corollary 6.2. *Roots in Integral Domains.* Let D be an integral domain and let E be an integral domain containing D. A non-zero polynomial $f \in D[X]$ has at most $\deg f$ distinct roots in E.

推論

Proof

We proceed by induction on $n = \deg f$. If $n = 0$, f is a non-zero constant and has no roots. Suppose the result holds for degree $n - 1$. If f has no roots in E, the statement is trivial. If f has a root $c_1 \in E$, then by corollary 6.1, $f(X) = (X - c_1)q_1(X)$ for some $q_1 \in E[X]$. Note that $\deg q_1 = n - 1$. If $c_2 \in E$ is another distinct root, then

$$0 = f(c_2) = (c_2 - c_1)q_1(c_2).$$

Since E is an integral domain and $c_2 \neq c_1$, we must have $q_1(c_2) = 0$. Thus, any other root of f is a root of q_1. By the inductive hypothesis, q_1 has at most $n - 1$ roots. Therefore, f has at most $1 + (n-1) = n$ roots.

■

Remark.

The commutativity of the ring E is essential. For instance, in the ring of quaternions $\mathbb{H}$ (which is a non-commutative division ring), the polynomial $X^2 + 1$ has infinitely many roots of the form $ai + bj + ck$ where $a^2 + b^2 + c^2 = 1$.

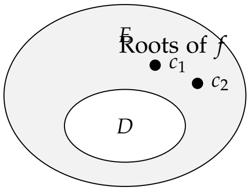

Figure 6.1: A polynomial over D may factor further in a larger domain E.

Rational Roots

When solving polynomial equations, it is often useful to test for roots in the field of fractions. The following proposition restricts the possible candidates for such roots.

Proposition 6.4. ***Rational Root Test.***
Let D be a Unique Factorisation Domain (UFD) and let F be its field of fractions. Let $f(X) = \sum_{i=0}^{n} a_i X^i \in D[X]$ with $a_n \neq 0$. If $u = \frac{c}{d} \in F$ (where $c, d \in D$ and $(c, d) \sim 1$) is a root of f, then:

$$c \mid a_0 \quad \text{and} \quad d \mid a_n.$$

命題

Proof

Since $f(c/d) = 0$, we substitute and clear the denominator by multiplying by d^n:

$$a_n \left(\frac{c}{d}\right)^n + \cdots + a_1 \left(\frac{c}{d}\right) + a_0 = 0 \implies \sum_{i=0}^{n} a_i c^i d^{n-i} = 0.$$

Isolating the terms divisible by c and d respectively:

1. $a_n c^n = -d\left(a_{n-1}c^{n-1} + \cdots + a_0 d^{n-1}\right)$. Thus $d \mid a_n c^n$. Since c and d are coprime, $d \mid a_n$.
2. $a_0 d^n = -c\left(a_n c^{n-1} d^{n-1} + \cdots + a_1 d^{n-1}\right)$. Thus $c \mid a_0 d^n$. Since $(c, d) \sim 1$, $c \mid a_0$.

■

6.3 *Derivatives and Multiplicity*

We can detect multiple roots algebraically using formal differentiation.

Definition 6.2. ***Formal Derivative.***
Let $f(X) = \sum_{k=0}^{n} a_k X^k \in D[X]$. The **formal derivative** of f, denoted $f'(X)$, is defined by:

$$f'(X) = \sum_{k=1}^{n} k a_k X^{k-1} = n a_n X^{n-1} + \cdots + a_1.$$

定義

It is a routine verification that the standard rules of differentiation (linearity and the product rule) apply:

$$(f+g)' = f' + g', \quad (fg)' = f'g + fg'.$$

Definition 6.3. ***Multiplicity.***
Let $c \in E$ be a root of $f \in D[X]$. We say c is a root of **multiplicity** n if:

$$f(X) = (X-c)^n g(X)$$

where $g(c) \neq 0$.

定義

Theorem 6.1. ***Roots and Derivatives.***
Let $D \subseteq E$ be integral domains and let $f \in D[X]$ have a root $c \in E$.

1. If c is a root of multiplicity n, then $f(c) = f'(c) = \cdots = f^{(n-1)}(c) = 0$ and $f^{(n)}(c) \neq 0$.
2. If D has characteristic zero, the converse holds: if the first $n-1$ derivatives vanish at c but the n-th does not, then c has multiplicity n.
3. If D is a field and $\gcd(f, f') = 1$, then f has no multiple roots in any extension E.

定理

Proof

1. Suppose $f(X) = (X-c)^n g(X)$. Differentiating using the product rule:

   $$f'(X) = n(X-c)^{n-1}g(X) + (X-c)^n g'(X) = (X-c)^{n-1}\left[ng(X) + (X-c)g'(X)\right].$$

   Thus c is a root of f' of multiplicity at least $n - 1$. Repeating this argument inductively, we find that derivatives up to order $n-1$ vanish at c. The n-th derivative involves a term $n!g(c)$ plus terms vanishing at c. Since E is a domain, $f^{(n)}(c) \neq 0$ (assuming appropriate characteristic or checking the specific expansion).
2. Conversely, expand $f(X)$ as a polynomial in $(X - c)$ (Taylor expansion):

   $$f(X) = b_0 + b_1(X-c) + \cdots + b_m(X-c)^m.$$

Evaluating the derivatives at c yields $f^{(k)}(c) = k!b_k$. If $f^{(k)}(c) = 0$ for $k < n$ and $f^{(n)}(c) \neq 0$, then $b_0 = \cdots = b_{n-1} = 0$ and $b_n \neq 0$. Thus

$$f(X) = (X - c)^n \left[b_n + b_{n+1}(X - c) + \ldots\right],$$

so c has multiplicity n.

3. If $\gcd(f, f') = 1$, there exist polynomials a, b such that $af + bf' = 1$. If c were a multiple root (multiplicity ≥ 2), then $f(c) = 0$ and $f'(c) = 0$, implying $1 = 0$, a contradiction.

■

6.4 Gauss's Lemma and Unique Factorisation

We now address a fundamental question: if D is a Unique Factorisation Domain, is the polynomial ring $D[X]$ also a UFD? While $D[X]$ is generally not a PID (as seen with $\mathbb{Z}[X]$), it turns out that the UFD property is preserved. The bridge between factorisation in $D[X]$ and the typically simpler factorisation in $F[X]$ (where F is the field of fractions) is provided by Gauss's Lemma.

Throughout this section, let D be a Unique Factorisation Domain and let F be its field of fractions.

Content and Primitive Polynomials

To compare polynomials over D with those over F, we separate the "scalar" factors from the polynomial part.

Definition 6.4. ***Content and Primitive Polynomials.***
Let $f(X) = \sum_{i=0}^{n} a_i X^i \in D[X]$ be a non-zero polynomial.

1. The **content** of f, denoted $c(f)$, is the greatest common divisor of its coefficients:
$$c(f) = \gcd(a_0, a_1, \ldots, a_n).$$
Since D is a UFD, this GCD exists and is unique up to multiplication by a unit.
2. The polynomial f is called **primitive** if $c(f) \sim 1$ (i.e., the coefficients are coprime).

定義

Remark.

Any non-zero polynomial $f \in D[X]$ can be written as $f(X) = c(f)f_1(X)$, where f_1 is a primitive polynomial. This decomposition is unique up to units: if $f = cg$ with g primitive, then $c \sim c(f)$ and $g \sim f_1$.

The interaction between content and multiplication is described by Gauss's Lemma.

Proposition 6.5. ***Gauss's Lemma.***
Let D be a UFD. If $f, g \in D[X]$ are non-zero polynomials, then:

$$c(fg) \sim c(f)c(g).$$

In particular, the product of two primitive polynomials is a primitive polynomial.

命題

Proof

We can write $f = c(f)f_1$ and $g = c(g)g_1$ where f_1, g_1 are primitive. Then $fg = c(f)c(g)f_1g_1$. Since content is multiplicative for scalars, $c(fg) \sim c(f)c(g)c(f_1g_1)$. Thus, it suffices to prove that if f and g are primitive, then fg is primitive (i.e., $c(fg) \sim 1$).
Let $f(X) = \sum_{i=0}^{n} a_i X^i$ and $g(X) = \sum_{j=0}^{m} b_j X^j$. Suppose, for the sake of contradiction, that fg is not primitive. Then there exists a prime element $p \in D$ that divides every coefficient of the product fg. Since f is primitive, p does not divide all coefficients a_i. Let s be the smallest index such that $p \nmid a_s$ (so $p \mid a_i$ for all $i < s$). Similarly, since g is primitive, let t be the smallest index such that $p \nmid b_t$ (so $p \mid b_j$ for all $j < t$).
Consider the coefficient of X^{s+t} in the product fg, denoted c_{s+t}:

$$c_{s+t} = \sum_{k=0}^{s+t} a_k b_{s+t-k} = \cdots + a_{s-1}b_{t+1} + a_s b_t + a_{s+1}b_{t-1} + \ldots$$

By assumption, p divides the entire coefficient c_{s+t}. We examine the terms in the sum:

- For $k < s$, $p \mid a_k$, so $p \mid a_k b_{s+t-k}$.
- For $k > s$, we have $s + t - k < t$, so $p \mid b_{s+t-k}$, implying $p \mid a_k b_{s+t-k}$.

Thus, p divides every term in the sum except possibly $a_s b_t$. Since p divides the sum c_{s+t} and all other terms, it must divide $a_s b_t$. However, p is prime and $p \nmid a_s$ and $p \nmid b_t$, which contradicts the definition of prime elements in a domain. Therefore, no such prime exists, and fg is primitive.

■

Relations with the Field of Fractions

We can view $D[X]$ as a subring of $F[X]$. Since F is a field, $F[X]$ is a Euclidean Domain (and thus a PID and UFD), and its arithmetic is well-understood. We use Gauss's Lemma to pull properties from

$F[X]$ back to $D[X]$.

$$\begin{tikzcd}
D[X] \arrow[r, hook] & F[X] \\
D \arrow[u] \arrow[r, hook] \arrow[ur, phantom, "\circlearrowleft"] & F \arrow[u]
\end{tikzcd}$$

Figure 6.2: Embeddings of polynomial rings.

Lemma 6.1. ***Associates in*** $D[X]$ ***and*** $F[X]$**.**
Let $f, g \in D[X]$ be primitive polynomials. Then f and g are associates in $D[X]$ if and only if they are associates in $F[X]$.

引理

Proof

If $f \sim g$ in $D[X]$, then $f = ug$ for some unit $u \in D^\times$. Since $D^\times \subseteq F^\times = F \setminus \{0\}$, they are associates in $F[X]$. Conversely, suppose f, g are associates in $F[X]$. Then $f = \alpha g$ for some $\alpha \in F^\times$. Write $\alpha = \frac{a}{b}$ with $a, b \in D$ and $b \neq 0$. Then $bf(X) = ag(X)$. Taking contents on both sides and using Gauss's Lemma:

$$c(bf) \sim c(ag) \implies b \cdot c(f) \sim a \cdot c(g).$$

Since f and g are primitive, $c(f) \sim 1$ and $c(g) \sim 1$. Thus $b \sim a$ in D. Therefore, $\alpha = a/b$ is a unit in D, meaning f and g are associates in $D[X]$.

■

This lemma allows us to characterise irreducible elements in $D[X]$. An element can be irreducible in $D[X]$ either because it is a prime constant, or because it is a polynomial that cannot be factored even allowing for fractions.

Lemma 6.2. ***Irreducibility Criteria.***
Let $f \in D[X]$ be a non-zero polynomial. Then f is irreducible in $D[X]$ if and only if one of the following holds:

1. $\deg f = 0$ and f is irreducible in D.
2. $\deg f > 0$, f is primitive in $D[X]$, and f is irreducible in $F[X]$.

引理

Proof

If $\deg f = 0$, then $f \in D$. The units of $D[X]$ are the units of D, so f is irreducible in $D[X]$ if and only if it is irreducible in D. Now assume $\deg f \geq 1$.

($\impliedby$) Suppose condition (2) holds. If $f = gh$ in $D[X]$, then $g, h \in F[X]$. Since f is irreducible in $F[X]$, one factor, say g, must be a unit in $F[X]$. Thus $g \in F^\times$, so $g \in D \setminus \{0\}$ (as $g \in D[X]$). We have $f = gh$. Taking contents: $c(f) = g \cdot c(h)$. Since f is primitive, $c(f) \sim 1$, which implies g is a unit in D. Thus the factorisation is trivial.

($\implies$) Suppose f is irreducible in $D[X]$ with $\deg f \geq 1$. First, $f = c(f)f_1$. If $c(f)$ is not a unit, then f is reducible (product of constant and polynomial). Thus $c(f) \sim 1$, so f is primitive. Next, suppose $f = g(X)h(X)$ is a factorisation in $F[X]$. We must show it is trivial. Write $g(X) = \frac{a}{b}g_0(X)$ and $h(X) = \frac{c}{d}h_0(X)$, where $g_0, h_0 \in D[X]$ are primitive and $a, b, c, d \in D$. Then:

$$f(X) = \frac{ac}{bd}g_0(X)h_0(X) \implies bdf(X) = acg_0(X)h_0(X).$$

By Gauss's Lemma, g_0h_0 is primitive. Comparing contents:

$$bd \cdot c(f) \sim ac \cdot c(g_0h_0) \implies bd \sim ac.$$

Thus $\frac{ac}{bd}$ is a unit $u \in D$. So $f(X) = ug_0(X)h_0(X)$ is a factorisation in $D[X]$. Since f is irreducible in $D[X]$, either g_0 or h_0 must be a unit in $D[X]$. Since $\deg f \geq 1$, the non-unit factor must have the same degree as f. Thus either $\deg g = 0$ or $\deg h = 0$, implying g or h is a unit in $F[X]$.

Thus f is irreducible in $F[X]$.

■

Polynomial Rings are UFDs

We are now equipped to prove the main theorem of this section.

Theorem 6.2. ***Polynomial UFD Theorem.***
If D is a Unique Factorisation Domain, then $D[X]$ is a Unique Factorisation Domain.

定理

We must verify the existence and uniqueness of factorisations into irreducibles.

Existence.

Let $f \in D[X]$. We proceed by induction on $\deg f$. If $\deg f = 0$, $f \in D$. Since D is a UFD, f factors into irreducibles in D, which remain irreducible in $D[X]$. If $\deg f \geq 1$, write $f = c(f)f_1$ with f_1 primitive. The constant $c(f)$ factors into irreducibles in D. We focus on f_1. If f_1 is irreducible in $D[X]$, we are done. If f_1 is reducible in $D[X]$, then by *lemma* 6.2, it must be reducible in $F[X]$ (since it is primitive). Or simply, if $f_1 = gh$ with non-units in $D[X]$, then since f_1 is primitive, $\deg g \geq 1$ and $\deg h \geq 1$. Since $\deg g < \deg f$ and $\deg h < \deg f$, by the induction hypothesis, g and h factor into irreducibles. Thus f_1 (and hence f) factors into irreducibles.

証明終

Uniqueness.

Suppose f has two factorisations into irreducibles:

$$f = c_1 \dots c_r \cdot p_1(X) \dots p_s(X) = d_1 \dots d_k \cdot q_1(X) \dots q_m(X),$$

where c_i, d_j are irreducible constants (primes in D) and p_i, q_j are irreducible polynomials of degree ≥ 1. By *lemma* 6.2, the polynomials p_i, q_j are primitive in $D[X]$ and irreducible in $F[X]$. Taking contents on both sides:

$$c(f) \sim c_1 \dots c_r \sim d_1 \dots d_k.$$

Since D is a UFD, $r = k$ and the constants c_i are associated to d_j (after reordering). We can cancel the constants (up to units), leaving:

$$p_1(X) \dots p_s(X) \sim q_1(X) \dots q_m(X).$$

This equality holds in $F[X]$. Since $F[X]$ is a Euclidean Domain (hence a UFD), factorisation is unique in $F[X]$. Thus $s = m$, and after reordering, p_i is associated to q_i in $F[X]$. Since p_i and q_i are primitive in $D[X]$, the Lemma on Associates implies they are associated in $D[X]$. Thus the factorisation is unique.

証明終

Corollary 6.3. *Multivariate Polynomial UFDs*. If D is a UFD, then the polynomial ring in n variables $D[X_1, \dots, X_n]$ is a UFD.

推論

Proof

We proceed by induction on n. The base case $n = 1$ is the theorem above. For the inductive step, observe that $D[X_1, \dots, X_n] \cong (D[X_1, \dots, X_{n-1}])[X_n]$. By the inductive hypothesis, $R = D[X_1, \dots, X_{n-1}]$ is a UFD. Applying the theorem to $R[X_n]$, we conclude that the ring of n variables is a UFD.

■

Example 6.1. Structure of $\mathbb{Z}[X]$. Since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[X]$ is a UFD. Its irreducible elements are:

1. Prime numbers $p \in \mathbb{Z}$.
2. Primitive polynomials $f(X)$ that are irreducible over $\mathbb{Q}$.

For example, $2X^2 + 2 = 2(X^2 + 1)$ is not irreducible (factor 2), but $X^2 + 1$ is irreducible (primitive and irreducible over $\mathbb{Q}$).

範例

6.5 *Irreducibility Criteria*

Determining whether a polynomial is irreducible is a fundamental problem in algebra. While we have established general structural results, we now present a powerful sufficient condition for irreducibility over Unique Factorisation Domains, particularly $\mathbb{Z}$.

Theorem 6.3. ***Eisenstein's Criterion.***
Let D be a Unique Factorisation Domain and let $p \in D$ be an irreducible element. Let $f(X) = \sum_{i=0}^{n} a_i X^i \in D[X]$ be a polynomial of degree $n \geq 1$. Suppose that:
1. $p \nmid a_n$ (the leading coefficient is not divisible by p),
2. $p \mid a_i$ for all $0 \leq i < n$ (all other coefficients are divisible by p),
3. $p^2 \nmid a_0$ (the constant term is not divisible by p^2).

Then $f(X)$ is irreducible in $D[X]$ unless it is the product of a constant and a polynomial (i.e., reducible only by content). If f is primitive, then f is irreducible.

定理

Proof

Suppose $f(X) = g(X)h(X)$ where $g(X) = \sum_{j=0}^{m} b_j X^j$ and $h(X) = \sum_{k=0}^{l} c_k X^k$ are non-constant polynomials in $D[X]$. Thus $m, l < n$. Comparing the leading coefficients, $a_n = b_m c_l$. Since $p \nmid a_n$, we have $p \nmid b_m$ and $p \nmid c_l$. Comparing the constant terms, $a_0 = b_0 c_0$. Since $p \mid a_0$ but $p^2 \nmid a_0$, p must divide exactly one of b_0, c_0. Without loss of generality, assume $p \mid b_0$ and $p \nmid c_0$.

We seek a contradiction. Since $p \mid b_0$ and $p \nmid b_m$, there exists a smallest index k such that $p \nmid b_k$. Note that $0 < k \leq m < n$. Consider the coefficient of X^k in the product $f = gh$:

$$a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0.$$

Since $k < n$, by hypothesis $p \mid a_k$. By the choice of k, p divides $b_0, b_1, \ldots, b_{k-1}$. Thus p divides every term in the sum except possibly $b_k c_0$. Since $p \mid a_k$ and p divides the initial sum, it implies $p \mid b_k c_0$. However, p is prime (irreducibles are prime in a UFD), and we know $p \nmid b_k$ (by choice of k) and $p \nmid c_0$ (by assumption). This is a contradiction. Thus no such factorisation exists.

■

Remark.

The monic case $a_n = 1$ is the most common application. In this case, since f is primitive, Eisenstein's Criterion implies irreducibility in both $D[X]$ and the fraction field $F[X]$.

Example 6.2. Cyclotomic Polynomials. Let p be a prime number. The p-th cyclotomic polynomial is defined as:

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Direct application of Eisenstein is not possible since the coefficients are all 1. However, irreducibility is invariant under translation

$X \mapsto X+1$. Consider:

$$g(X) = \Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1)-1} = \frac{\sum_{k=0}^{p} \binom{p}{k} X^k - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}.$$

The coefficients are $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}, 1$. Explicitly:

$$g(X) = X^{p-1} + \binom{p}{p-1} X^{p-2} + \cdots + \binom{p}{1}.$$

Since p is prime, $p \mid \binom{p}{k}$ for $1 \leq k < p$. The constant term is $\binom{p}{1} = p$, which is divisible by p but not p^2. Thus $g(X)$ is irreducible by Eisenstein's Criterion, implying $\Phi_p(X)$ is irreducible in $\mathbb{Z}[X]$.

範例

Reducibility over $\mathbb{Z}$ and $\mathbb{Q}$

Finally, we restate the practical implication of Gauss's Lemma for integer polynomials.

Theorem 6.4. ***Integer vs Rational Irreducibility.***
Let $f \in \mathbb{Z}[X]$. Then f is irreducible in $\mathbb{Z}[X]$ if and only if:
1. f is irreducible in $\mathbb{Q}[X]$, and
2. The coefficients of f are coprime (i.e., f is primitive).

Equivalently, a primitive polynomial factors over $\mathbb{Z}$ if and only if it factors over $\mathbb{Q}$.

定理

This theorem assures us that searching for factors with integer coefficients is sufficient to determine reducibility over the rationals, greatly simplifying the search space by restricting coefficients to divisors of the constant and leading terms.

6.6 *Exercises*

1. **Degree Properties.** Prove *proposition* 6.1. Specifically, verify $\deg(f+g) \leq \max(\deg f, \deg g)$ and $\deg(fg) \leq \deg f + \deg g$, with equality in the latter if the leading coefficients are not zero divisors.

2. **Special Elements in Polynomial Rings.** Let R be a ring and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. Prove:
   (a) $f(x)$ is invertible (a unit) if and only if $a_0 \in U(R)$ and $a_1, \ldots, a_n$ are nilpotent.
   (b) $f(x)$ is nilpotent if and only if $a_0, a_1, \ldots, a_n$ are all nilpotent.

(c) $f(x)$ is a zero divisor if and only if there exists a non-zero $a \in R$ such that $af(x) = 0$.

3. **Monic Factors in UFDs.** Let D be a UFD with field of fractions F. Let $f(x) \in D[x]$ be a monic polynomial. Prove that every monic polynomial factor of $f(x)$ in $F[x]$ must actually lie in $D[x]$.

Apply Gauss's Lemma to the factorisation.

4. **Cyclotomic Factorisation.** Factor the polynomials $x^n - 1$ into irreducible polynomials in $\mathbb{Z}[x]$ for all $3 \leq n \leq 10$.

5. **Derivations.** Let F be a field. A linear map $d : F[x] \to F[x]$ is called a **derivation** if it satisfies the Leibniz rule: $d(fg) = d(f)g + fd(g)$ for all $f, g \in F[x]$. Find all derivations on $F[x]$.

Show that d is determined by its value on x.

6. **Sum of Conjugate Roots.** Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of odd degree. Let α and β be two distinct roots of $f(x)$ in some extension field. Prove that $\alpha + \beta \notin \mathbb{Q}$.

Recall that the **minimal polynomial** of $\theta \in E$ over F is the unique monic irreducible $p(x) \in F[x]$ such that $p(\theta) = 0$.

7. **Formal Power Series.** Let R be a ring with identity. The ring of formal power series $R[[x]]$ consists of formal sums $\sum_{n=0}^{\infty} a_n x^n$ with coefficients in R, with addition and multiplication defined analogously to polynomials (but without terminating).

   (a) Verify that $R[[x]]$ is a ring containing $R[x]$ as a subring.
   (b) Prove that $f(x) = \sum a_n x^n$ is invertible in $R[[x]]$ if and only if the constant term a_0 is a unit in R.
   (c) If F is a field, prove that $F[[x]]$ is a Principal Ideal Domain (in fact, a Euclidean Domain) with a unique maximal ideal $\mathfrak{m} = (x)$. Describe all ideals of $F[[x]]$.

8. **Ideals in Polynomial Rings.** Determine all prime ideals and maximal ideals of $\mathbb{R}[x]$ and $\mathbb{Z}[x]$.

9. **Automorphisms.** Determine the automorphism groups $\text{Aut}(\mathbb{Z}[x])$ and $\text{Aut}(\mathbb{Q}[x])$.

10. **Lagrange Interpolation.** Let D be an integral domain. Let $c_0, \ldots, c_n$ be distinct elements in D, and $d_0, \ldots, d_n$ be arbitrary elements.

    (a) Prove that there exists **at most one** polynomial $f(x) \in D[x]$ of degree $\leq n$ such that $f(c_i) = d_i$ for all i.
    (b) If D is a field, prove that such a polynomial always exists.

11. **Classification of Elements.** Determine whether the following polynomials are units or irreducible elements in the rings $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, and $\mathbb{Z}[[x]]$:

    (a) $2x + 2$
    (b) $x^2 + 1$
    (c) $x + 1$
    (d) $x^2 + 3x + 2$

12. **Reduction Modulo p.** Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. Let $\bar{f}(x) \in \mathbb{F}_p[x]$ be its reduction modulo a prime p.
    (a) Prove that if $\bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.
    (b) Does this conclusion hold if $f(x)$ is not monic? Provide a proof or counter-example.

13. **Affine Transformation.** Let F be a field and $a, b \in F$ with $a \neq 0$. Prove that $f(x)$ is irreducible in $F[x]$ if and only if $f(ax+b)$ is irreducible in $F[x]$.

14. **Coprimality over $\mathbb{Q}$ vs $\mathbb{Z}$.** Prove that two polynomials in $\mathbb{Z}[x]$ are coprime in $\mathbb{Q}[x]$ (i.e., generate the unit ideal in $\mathbb{Q}[x]$) if and only if the ideal they generate in $\mathbb{Z}[x]$ contains a non-zero integer.

15. **Generalised Eisenstein Criterion.** Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ with degree n. Suppose there exists a prime p and an integer k $(0 < k < n)$ such that:

$$p \nmid a_n, \quad p \nmid a_k, \quad p \mid a_i \text{ for } 0 \leq i \leq k-1, \quad p^2 \nmid a_0.$$

Prove that $f(x)$ must have an irreducible factor of degree at least k in $\mathbb{Z}[x]$.

Consider the Newton polygon or adapt the standard Eisenstein proof.

16. **Unique Factorisation of Primitives.** Let D be an integral domain. Let $f(x) \in D[x]$ be a non-zero polynomial with coprime coefficients (primitive). Prove that if an irreducible factorisation of $f(x)$ exists in $D[x]$, it is unique (up to units and ordering).

17. **Irreducibility of Composition.** Let $f(x) \in \mathbb{Z}[x]$ be irreducible. Is it true that $f(x^2)$ is always irreducible? If not, find a counter-example. Under what conditions is $f(x^n)$ irreducible?

18. **Rational Function Fields.** Let $F(x)$ be the field of fractions of $F[x]$ (the field of rational functions). Prove that any automorphism of $F(x)$ that fixes F is of the form $x \mapsto \frac{ax+b}{cx+d}$ with $ad - bc \neq 0$ (a Möbius transformation).

19. **Resultants.** Let $f, g \in F[x]$ be polynomials of degree m and n. The *resultant* $\mathrm{Res}(f,g)$ is the determinant of the $(m+n) \times (m+n)$ Sylvester matrix formed by their coefficients. Prove that $\mathrm{Res}(f,g) = 0$ if and only if f and g share a common factor of positive degree.

The **Sylvester matrix** of $f = \sum_{i=0}^{m} a_i x^i$ and $g = \sum_{j=0}^{n} b_j x^j$ is the $(m+n) \times (m+n)$ matrix whose rows are coefficients of $x^{n-1}f, \dots, f, x^{m-1}g, \dots, g$.

20. **Polynomials with Integer Values.** Let $f \in \mathbb{Q}[x]$. Suppose $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Prove that $f(x)$ can be written as a $\mathbb{Z}$-linear combination of the binomial polynomials $\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$.