Abstract Algebra I

Groups and Rings

Course Notes — Undergraduate

Department of Mathematics

Academic Year 2025–2026

Contents

Preface

Abstract algebra is, at its heart, the study of structure. Where elementary algebra manipulates individual numbers and equations, abstract algebra isolates the *patterns* that recur across mathematics and crystallises them into axiomatic frameworks—groups, rings, fields, modules—that can then be studied in their own right.

The historical roots of the subject reach back to the early nineteenth century. Joseph-Louis Lagrange's 1770–1771 study of the permutations of the roots of polynomial equations planted the first seed. Niels Henrik Abel and Évariste Galois, working independently in the 1820s and 1830s, transformed Lagrange's observations into a profound theory linking the solvability of polynomial equations to the structure of certain groups of permutations. Galois's insight—that the key object is not the individual equation but the *group of symmetries* acting on its roots—was so far ahead of its time that decades elapsed before the mathematical community fully absorbed it.

The modern axiomatic formulation of a group emerged gradually through the work of Arthur Cayley (1854), Leopold Kronecker, and others in the second half of the nineteenth century. Ring theory crystallised somewhat later, with Richard Dedekind's ideals (1871) and Emmy Noether's revolutionary abstractions in the 1920s providing the definitive framework that we use today.

These notes cover the first semester of a two-semester undergraduate sequence in abstract algebra. The primary objects of study are **groups** and **rings**. A rough outline is as follows:

- **Chapters 1–4** develop group theory from the axioms through the Sylow theorems and group actions.
- **Chapters 5–7** introduce ring theory, ideals, quotient rings, polynomial rings, and factorisation.

Throughout, the emphasis is on *rigorous proof*: every major result is proved in full detail, and the reader is encouraged to work through the exercises at the end of each chapter.

Prerequisites. The reader is assumed to have a solid grounding in naive set theory, functions, equivalence relations, and the basic properties of the integers (divisibility, the Euclidean algorithm, modular arithmetic). Familiarity with linear algebra (matrices, determinants, vector spaces) is helpful but not strictly necessary for the first chapters.

How to use these notes. Definitions and theorems are numbered by chapter. Proofs end with the symbol $\square$. Exercises range from routine to challenging; those marked with $(\star)$ are more difficult. An index of terminology is provided at the end of the document.

Notation

Symbol	Meaning
$\mathbb{N}$	Natural numbers $\{0, 1, 2, \ldots\}$
$\mathbb{Z}$	Ring of integers
$\mathbb{Q}$	Field of rational numbers
$\mathbb{R}$	Field of real numbers
$\mathbb{C}$	Field of complex numbers
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{Z}/n\mathbb{Z}$	Integers modulo n
$(\mathbb{Z}/n\mathbb{Z})^\times$	Group of units modulo n
S_n	Symmetric group on $\{1, \ldots, n\}$
A_n	Alternating group on $\{1, \ldots, n\}$
D_n	Dihedral group of order $2n$
$\mathrm{GL}_n(K)$	General linear group over K
$\mathrm{SL}_n(K)$	Special linear group over K
$\langle S \rangle$	Subgroup (or ideal) generated by S
$\lvert G \rvert$	Order (cardinality) of a group G
$\mathrm{ord}(g)$	Order of an element g
$[G : H]$	Index of a subgroup H in G
G/N	Quotient group of G by N
$G \times H$	Direct product of G and H
$\mathrm{Hom}(G, H)$	Set of homomorphisms from G to H
$\mathrm{Aut}(G)$	Automorphism group of G
$\mathrm{Inn}(G)$	Group of inner automorphisms of G
$Z(G)$	Centre of G
$[G, G]$	Commutator (derived) subgroup of G
$N \trianglelefteq G$	N is a normal subgroup of G
$\ker \varphi$	Kernel of a homomorphism φ
$\mathrm{Im}\, \varphi$	Image of a homomorphism φ
$\cong$	Isomorphism
$\hookrightarrow$	Injective map
$\twoheadrightarrow$	Surjective map
$\circ$	Composition of functions
id_X	Identity map on X
$\lvert X \rvert$	Cardinality of a set X
$\gcd(a, b)$	Greatest common divisor
$\mathrm{lcm}(a, b)$	Least common multiple

Chapter 1

Groups — Definitions, Examples, and First Properties

1.1 Historical motivation

The concept of a *group* did not spring fully formed from a single mind; it coalesced over more than a century of mathematical activity, driven above all by the study of *symmetry* and the theory of *polynomial equations*.

Permutations and polynomial equations

In 1770, Joseph-Louis Lagrange published a landmark memoir in which he studied the permutations of the roots of a polynomial and their effect on auxiliary expressions known as *resolvents*. His key observation was that the number of distinct values taken by a rational function of the roots, when the roots are permuted, always divides the factorial $n!$ of the degree. This result, sometimes called **Lagrange's theorem on resolvents**, is a precursor of the theorem on the index of a subgroup that bears his name today (Theorem 2.3).

Augustin-Louis Cauchy systematised the theory of permutations in a series of papers beginning in 1815. He introduced the cycle notation that is still standard, proved that every permutation is a product of transpositions, and established many results about the *order* of a permutation.

The decisive leap came with Évariste Galois, who in his tragically brief career (1829–1832) created the theory that now bears his name. Galois associated to each polynomial equation a group of permutations of its roots—the *Galois group*—and showed that the equation is solvable by radicals if and only if this group has a specific structural property (solvability). His work simultaneously explained *why* the general quintic cannot be solved by radicals (a fact proved earlier by Abel) and laid the foundation for abstract group theory.

Symmetry in geometry

Independently, the study of symmetry in geometry contributed to the birth of group theory. Felix Klein's *Erlangen Programme* (1872) proposed that each geometry can be characterised by the group of transformations that preserve its structure. The symmetry

groups of regular polygons (*dihedral groups*) and polyhedra provided a rich supply of concrete, visualisable examples that helped mathematicians build intuition for the abstract concept.

Towards axiomatics

Arthur Cayley gave the first abstract definition of a group in 1854, although his formulation was not yet in the modern axiomatic style. The definition we use today—a set with a binary operation satisfying closure, associativity, identity, and inverses—was gradually refined by Kronecker, Weber, and others, reaching its definitive form by the early twentieth century.

1.2 Binary operations

Before defining a group we fix some terminology about operations on sets.

Definition 1.1 (Binary operation)**.** Let S be a non-empty set. A **binary operation** on S is a map $\star\colon S \times S \to S$. We usually write $a \star b$ instead of $\star(a, b)$.

Definition 1.2 (Associativity, commutativity)**.** A binary operation $\star$ on S is called

(i) **associative** if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$;

(ii) **commutative** if $a \star b = b \star a$ for all $a, b \in S$.

Example 1.1 (Familiar binary operations). Addition on $\mathbb{Z}$ is associative and commutative. Matrix multiplication on $M_n(\mathbb{R})$ is associative but not commutative (for $n \geq 2$). Subtraction on $\mathbb{Z}$ is neither associative nor commutative.

1.3 Definition of a group

Definition 1.3 (Group)**.** A **group** is a pair $(G, \star)$ consisting of a non-empty set G and a binary operation $\star\colon G \times G \to G$ satisfying the following axioms:

(G1) Closure. For all $a, b \in G$, $a \star b \in G$. (This is automatic from the definition of binary operation but is often stated explicitly.)

(G2) Associativity. For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.

(G3) Identity element. There exists an element $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$.

(G4) Inverse element. For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.

If moreover $a \star b = b \star a$ for all $a, b \in G$, the group is called **abelian** (or *commutative*).

Remark 1.1 (Notation). When the operation is clear from context we write ab instead of $a \star b$ and refer to the group simply as G. For abelian groups the operation is often written additively as $a + b$, with identity element denoted 0 and inverse of a denoted $-a$.

1.4 Immediate consequences of the axioms

Theorem 1.1 (Uniqueness of the identity)**.** In a group $(G, \star)$, the identity element is unique.

Proof. Suppose e and e' are both identity elements. Then $e = e \star e' = e'$, where the first equality uses the fact that e' is an identity and the second uses the fact that e is an identity. □

Theorem 1.2 (Uniqueness of inverses)**.** In a group $(G, \star)$, each element has a unique inverse.

Proof. Let $a \in G$ and suppose $b, c \in G$ both satisfy $a \star b = b \star a = e$ and $a \star c = c \star a = e$. Then

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

□

Proposition 1.1 (Inverse of a product)**.** For any a, b in a group G, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We verify directly:

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

Likewise $(b^{-1}a^{-1})(ab) = e$. By uniqueness of inverses (Theorem 1.2), $(ab)^{-1} = b^{-1}a^{-1}$. □

Proposition 1.2 (Cancellation laws)**.** Let G be a group and $a, b, c \in G$.

(i) If $ab = ac$, then $b = c$ (left cancellation).

(ii) If $ba = ca$, then $b = c$ (right cancellation).

Proof. (i) Multiply on the left by a^{-1}: $a^{-1}(ab) = a^{-1}(ac)$, so $(a^{-1}a)b = (a^{-1}a)c$, giving $eb = ec$, hence $b = c$. (ii) is analogous, multiplying on the right by a^{-1}. □

Proposition 1.3 (Unique solutions of equations)**.** In a group G, for any $a, b \in G$, each of the equations $ax = b$ and $ya = b$ has a unique solution, namely $x = a^{-1}b$ and $y = ba^{-1}$, respectively.

Proof. That $x = a^{-1}b$ is a solution is immediate: $a(a^{-1}b) = (aa^{-1})b = eb = b$. Uniqueness follows from left cancellation. The argument for y is similar. □

Proposition 1.4 (Involution of inversion)**.** For every a in a group G, $(a^{-1})^{-1} = a$.

Proof. By definition, $a^{-1} \cdot (a^{-1})^{-1} = e$. But also $a^{-1} \cdot a = e$. By uniqueness of inverses, $(a^{-1})^{-1} = a$. □

1.5 Examples of groups

Example 1.2 (The integers under addition). $(\mathbb{Z}, +)$ is an abelian group with identity 0 and inverse $-a$ for each $a \in \mathbb{Z}$. More generally, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are abelian groups under addition.

Example 1.3 (Non-zero reals under multiplication). $(\mathbb{R}^*, \times)$ is an abelian group with identity 1 and inverse $a^{-1} = 1/a$. Likewise $(\mathbb{Q}^*, \times)$ and $(\mathbb{C}^*, \times)$.

Example 1.4 (Integers modulo n). For any integer $n \geq 1$, the set $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ is an abelian group under addition modulo n, with identity $\bar{0}$ and inverse of $\bar{a}$ equal to $\overline{n-a}$.

Example 1.5 (Units modulo n). $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$ is an abelian group under multiplication modulo n. Its order is Euler's totient $\varphi(n)$.

Example 1.6 (General and special linear groups). For a field K and $n \geq 1$:

(i) $\mathrm{GL}_n(K) = \{A \in M_n(K) : \det A \neq 0\}$ is a group under matrix multiplication (non-abelian for $n \geq 2$).

(ii) $\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) : \det A = 1\}$ is a subgroup of $\mathrm{GL}_n(K)$.

Example 1.7 (The symmetric group S_n). For $n \geq 1$, the set S_n of all bijections $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ forms a group under composition of functions. Its order is $|S_n| = n!$. For $n \geq 3$ it is non-abelian.
Recall that every permutation can be written as a product of disjoint cycles, and the order of a permutation equals the least common multiple of the lengths of its disjoint cycles.

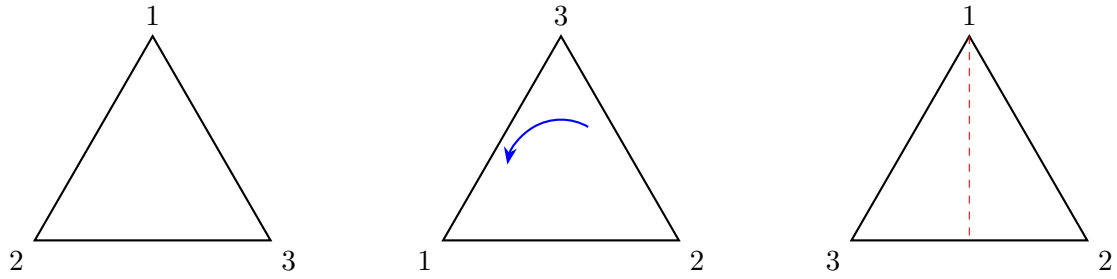
Example 1.8 (The dihedral group D_n). The **dihedral group** D_n is the group of symmetries of a regular n-gon. It has order $2n$ and is generated by a rotation r of angle $2\pi/n$ and a reflection s, subject to the relations

$$r^n = e, \quad s^2 = e, \quad srs = r^{-1}.$$

Thus $D_n = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$. For $n \geq 3$, D_n is non-abelian.

Symmetries of the equilateral triangle ($D_3 \cong S_3$).

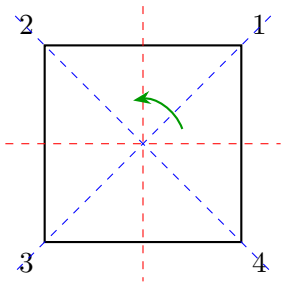
The six symmetries of the equilateral triangle are three rotations (e, r, r^2) and three reflections (s, sr, sr^2). We label the vertices 1, 2, 3 and display the effect of each symmetry.



Identity e | Rotation r: 120 | Reflection s

Symmetries of the square (D_4).

The group D_4 has order 8: four rotations (e, r, r^2, r^3) and four reflections. Below we depict the square with its axes of symmetry.



D_4: 4 axes of symmetry

Example 1.9 (The quaternion group Q_8). $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with multiplication determined by

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j.$$

It is a non-abelian group of order 8. Unlike D_4, every subgroup of Q_8 is normal.

Example 1.10 (The Klein four-group V_4). $V_4 = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$, $ab = c$, $ac = b$, $bc = a$. This is the smallest non-cyclic group. It is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1.6 Cayley tables

A *Cayley table* for a finite group $G = \{g_1, \ldots, g_n\}$ is the $n \times n$ table whose (i, j)-entry is $g_i g_j$. By the cancellation laws (Proposition 1.2), each row and each column of a Cayley table is a permutation of G (this is sometimes called the *Latin square property*).

Cayley table of $\mathbb{Z}/4\mathbb{Z}$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Cayley table of $V_4 = \{e, a, b, c\}$.

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

Cayley table of S_3. Writing $\sigma_1 = (1)$, $\sigma_2 = (12)$, $\sigma_3 = (13)$, $\sigma_4 = (23)$, $\sigma_5 = (123)$, $\sigma_6 = (132)$:

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_6	σ_1	σ_5	σ_4	σ_2
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_4	σ_2	σ_3	σ_6	σ_1
σ_6	σ_6	σ_3	σ_4	σ_2	σ_1	σ_5

1.7 Cyclic groups

Definition 1.4 (Cyclic group)**.** A group G is **cyclic** if there exists an element $g \in G$ such that $G = \langle g \rangle := \{g^n : n \in \mathbb{Z}\}$. The element g is called a **generator** of G.

Theorem 1.3 (Classification of cyclic groups)**.** Let G be a cyclic group.

(i) If G is infinite, then $G \cong (\mathbb{Z}, +)$.

(ii) If $|G| = n < \infty$, then $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

In both cases G is abelian.

Proof. Let g be a generator of G and define $\varphi\colon \mathbb{Z} \to G$ by $\varphi(k) = g^k$. This is a surjective group homomorphism (i.e. $\varphi(k+\ell) = g^{k+\ell} = g^k g^\ell = \varphi(k)\varphi(\ell)$, and every element of G is g^k for some k).

Case 1: $\ker\varphi = \{0\}$**.** Then φ is also injective, hence $G \cong \mathbb{Z}$. This is the case where $g^k \neq e$ for all $k \neq 0$, i.e. G is infinite.

Case 2: $\ker\varphi \neq \{0\}$**.** Since $\ker\varphi$ is a subgroup of $(\mathbb{Z}, +)$ and every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some $n \geq 0$, we have $\ker\varphi = n\mathbb{Z}$ for some $n \geq 1$. By the first isomorphism theorem (which we shall prove later but whose content is elementary here): $G \cong \mathbb{Z}/\ker\varphi = \mathbb{Z}/n\mathbb{Z}$.

More explicitly, the elements $e, g, g^2, \ldots, g^{n-1}$ are all distinct (for if $g^i = g^j$ with $0 \leq i < j < n$, then $g^{j-i} = e$ with $0 < j - i < n$, contradicting the minimality of n), and every element of G equals g^k for some $0 \leq k < n$ (write $k = qn + r$ with $0 \leq r < n$; then $g^k = g^{qn+r} = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r$). Hence $|G| = n$ and the map $\bar{k} \mapsto g^k$ is a well-defined isomorphism $\mathbb{Z}/n\mathbb{Z} \to G$.

In both cases, G is abelian because $g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$. □

1.8 Order of an element

Definition 1.5 (Order of an element)**.** Let G be a group and $g \in G$. The **order** of g, denoted $\operatorname{ord}(g)$, is the smallest positive integer n such that $g^n = e$, if such n exists. If no such n exists, we say g has **infinite order** and write $\operatorname{ord}(g) = \infty$.

Proposition 1.5 (Order and cyclic subgroup)**.** Let $g \in G$.

(i) $\operatorname{ord}(g) = |\langle g \rangle|$ (where $|\langle g \rangle|$ may be ∞).

(ii) If $\operatorname{ord}(g) = n < \infty$, then $g^k = e$ if and only if $n \mid k$.

Proof. (i) By Theorem 1.3, $\langle g \rangle$ is cyclic and isomorphic to $\mathbb{Z}$ (if g has infinite order) or to $\mathbb{Z}/n\mathbb{Z}$ (if g has order n). In either case, $\operatorname{ord}(g) = |\langle g \rangle|$.

(ii) Write $k = qn + r$ with $0 \le r < n$. Then $g^k = (g^n)^q g^r = g^r$. So $g^k = e$ iff $g^r = e$ iff $r = 0$ (by minimality of n) iff $n \mid k$. □

Proposition 1.6 (Order of powers)**.** Let $g \in G$ with $\operatorname{ord}(g) = n < \infty$. Then for any integer k,

$$\operatorname{ord}(g^k) = \frac{n}{\gcd(n, k)}.$$

Proof. Set $d = \gcd(n, k)$ and $m = n/d$. We need to show $\operatorname{ord}(g^k) = m$.

First, $(g^k)^m = g^{km} = g^{k \cdot n/d}$. Since $d \mid k$, write $k = d\ell$; then $km = d\ell \cdot n/d = \ell n$, so $(g^k)^m = g^{\ell n} = (g^n)^\ell = e$. Hence $\operatorname{ord}(g^k)$ divides m.

Conversely, suppose $(g^k)^t = g^{kt} = e$. Then $n \mid kt$, i.e. $\frac{n}{d} \mid \frac{k}{d}t$, i.e. $m \mid \frac{k}{d}t$. Since $\gcd(m, k/d) = 1$ (because $\gcd(n/d, k/d) = 1$), we get $m \mid t$. Hence $\operatorname{ord}(g^k) \ge m$.

Therefore $\operatorname{ord}(g^k) = m = n/\gcd(n, k)$. □

Definition 1.6 (Order of a group)**.** The **order** of a finite group G, denoted $|G|$, is its cardinality. If G is infinite, we write $|G| = \infty$.

1.9 Direct products

Definition 1.7 (Direct product)**.** Let $(G, \star)$ and $(H, \diamond)$ be groups. Their **direct product** is the set $G \times H = \{(g, h) : g \in G,\ h \in H\}$ equipped with the componentwise operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2,\ h_1 \diamond h_2).$$

Proposition 1.7 (Direct product is a group)**.** $G \times H$ is a group with identity (e_G, e_H) and $(g, h)^{-1} = (g^{-1}, h^{-1})$. If G and H are both abelian, so is $G \times H$. Moreover, $|G \times H| = |G| \cdot |H|$ when both are finite.

Proof. Each axiom is verified componentwise:

- *Closure*: $(g_1 g_2, h_1 h_2) \in G \times H$ since $g_1 g_2 \in G$ and $h_1 h_2 \in H$.
- *Associativity*: follows from associativity in each factor.

- *Identity*: $(e_G, e_H) \cdot (g, h) = (e_G g, e_H h) = (g, h)$, and similarly on the right.
- *Inverse*: $(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$.

The remaining claims follow directly. □

Remark 1.2 (Iterated direct products). The construction extends to any finite number of groups: $G_1 \times G_2 \times \cdots \times G_k$. By associativity of the Cartesian product, there is no ambiguity.

Proposition 1.8 (Order in a direct product)**.** Let $(g, h) \in G \times H$ with $\operatorname{ord}(g) = m$ and $\operatorname{ord}(h) = n$ both finite. Then $\operatorname{ord}((g, h)) = \operatorname{lcm}(m, n)$.

Proof. $(g, h)^k = (g^k, h^k) = (e_G, e_H)$ iff $g^k = e_G$ and $h^k = e_H$, iff $m \mid k$ and $n \mid k$, iff $\operatorname{lcm}(m, n) \mid k$. The smallest positive such k is $\operatorname{lcm}(m, n)$. □

1.10 Exercises

Exercise 1.1 (Uniqueness of the identity revisited). Let G be a group and $a \in G$. Show that if $a^2 = a$, then $a = e$.

Exercise 1.2 (Abelian criterion). Show that a group G is abelian if and only if $(ab)^2 = a^2 b^2$ for all $a, b \in G$.

Exercise 1.3 (Order of conjugates). Let G be a group and $a, g \in G$. Show that $\operatorname{ord}(gag^{-1}) = \operatorname{ord}(a)$.

Exercise 1.4 (Order in $\mathbb{Z}/n\mathbb{Z}$). Let $n \geq 1$ and $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Show that $\operatorname{ord}(\bar{a}) = n/\gcd(n, a)$. Deduce that $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$.

Exercise 1.5 (Generators of $\mathbb{Z}/12\mathbb{Z}$). List all generators of $\mathbb{Z}/12\mathbb{Z}$. Verify that $|\{k : 1 \leq k \leq 12, \gcd(k, 12) = 1\}| = \varphi(12) = 4$.

Exercise 1.6 ($D_3 \cong S_3$). Write out the Cayley table of D_3 (using $\{e, r, r^2, s, sr, sr^2\}$) and verify that it coincides with that of S_3 under a suitable bijection.

Exercise 1.7 (Centre of D_n). Show that the centre of D_n is $\{e\}$ if n is odd, and $\{e, r^{n/2}\}$ if n is even.

Exercise 1.8 (Quaternion subgroups). List all subgroups of Q_8 and show that each is normal.

Exercise 1.9 (When is $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ cyclic?). Show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m, n) = 1$. *(Hint: use Proposition 1.8.)*

Exercise 1.10 (Finite groups of even order). Let G be a finite group of even order. Show that G contains an element of order 2. *(Hint: pair each element with its inverse.)*

Exercise 1.11 ($(\star)$ Automorphisms of $\mathbb{Z}/n\mathbb{Z}$). Show that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercise 1.12 ($(\star)$ Product of orders in abelian groups). Let G be a finite abelian group and $a, b \in G$ with $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. Show that $\mathrm{ord}(ab) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

Chapter summary

- A **group** $(G, \star)$ satisfies four axioms: closure, associativity, existence of an identity, and existence of inverses.
- The identity element and inverses are **unique**; the **cancellation laws** hold; the inverse of a product is the product of inverses in reverse order.
- Key examples include $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$, $\mathrm{GL}_n(K)$, S_n, D_n, Q_8, and V_4.
- Every **cyclic group** is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$.
- The **order** of an element g equals $|\langle g \rangle|$, and $g^k = e \iff \mathrm{ord}(g) \mid k$.
- The **direct product** $G \times H$ is a group under componentwise operations; $\mathrm{ord}(g, h) = \mathrm{lcm}(\mathrm{ord}\, g, \mathrm{ord}\, h)$.

Chapter 2

Subgroups, Normal Subgroups, and Quotients

2.1 Subgroups

Definition 2.1 (Subgroup)**.** Let $(G, \star)$ be a group. A non-empty subset $H \subseteq G$ is a **subgroup** of G, written $H \leq G$, if $(H, \star)$ is itself a group under the same operation.

Remark 2.1 (Trivial subgroups). Every group G has at least two subgroups: the **trivial subgroup** $\{e\}$ and G itself. A subgroup H with $\{e\} \subsetneq H \subsetneq G$ is called **proper**.

The following criterion simplifies the verification that a subset is a subgroup.

Theorem 2.1 (Subgroup criterion — one-step test)**.** Let G be a group and H a non-empty subset of G. Then $H \leq G$ if and only if for all $a, b \in H$, $ab^{-1} \in H$.

Proof. ($\Rightarrow$) If H is a subgroup, then $b \in H$ implies $b^{-1} \in H$ (inverses exist in H), and then $ab^{-1} \in H$ (closure in H).

($\Leftarrow$) Suppose the condition holds. We verify the group axioms for $(H, \star)$.

Step 1. Identity. Since $H \neq \emptyset$, choose any $a \in H$. Then $aa^{-1} = e \in H$.

Step 2. Inverses. For any $b \in H$, we have $e \in H$ (from Step 1) and so $eb^{-1} = b^{-1} \in H$.

Step 3. Closure. For any $a, b \in H$, we have $b^{-1} \in H$ (from Step 2) and so $a(b^{-1})^{-1} = ab \in H$.

Step 4. Associativity. Inherited from G.

Hence $(H, \star)$ is a group, so $H \leq G$. □

Theorem 2.2 (Subgroup criterion — two-step test)**.** Let G be a group and H a non-empty subset of G. Then $H \leq G$ if and only if the following two conditions hold:

(i) For all $a, b \in H$, $ab \in H$ (closure).

(ii) For all $a \in H$, $a^{-1} \in H$ (closed under inverses).

Proof. If (i) and (ii) hold, then for $a, b \in H$ we have $b^{-1} \in H$ by (ii) and $ab^{-1} \in H$ by (i), so the one-step criterion (Theorem 2.1) is satisfied. The converse is immediate. □

Proposition 2.1 (Subgroup criterion for finite subsets)**.** Let G be a group and H a non-empty *finite* subset of G that is closed under the group operation. Then $H \leq G$.

Proof. We must show H is closed under inverses. Let $a \in H$. If $a = e$, then $a^{-1} = e \in H$. Otherwise, consider the elements $a, a^2, a^3, \ldots$. Since H is finite and closed, all of these lie in H, and by the pigeonhole principle there exist $i < j$ with $a^i = a^j$. By cancellation, $a^{j-i} = e$ with $j - i \geq 1$. If $j - i = 1$, then $a = e$, contradiction. So $j - i \geq 2$ and $a^{-1} = a^{j-i-1} \in H$ (since $j - i - 1 \geq 1$ and H is closed under multiplication). □

2.2 Examples of subgroups

Example 2.1 (Subgroups of $(\mathbb{Z}, +)$). The subgroups of $(\mathbb{Z}, +)$ are precisely the sets $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ for $n \geq 0$. Indeed, every subgroup of $\mathbb{Z}$ is cyclic (a fact we now prove).

Proposition 2.2 (Subgroups of $\mathbb{Z}$ are cyclic)**.** Every subgroup of $(\mathbb{Z}, +)$ has the form $n\mathbb{Z}$ for some $n \geq 0$.

Proof. Let $H \leq \mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Otherwise, H contains some non-zero element, and since H is closed under negation, H contains a positive integer. Let n be the smallest positive integer in H. Clearly $n\mathbb{Z} \subseteq H$ (since H is a subgroup and $n \in H$).

Conversely, let $m \in H$ and write $m = qn + r$ with $0 \leq r < n$ (division algorithm). Then $r = m - qn \in H$. By minimality of n and the fact that $0 \leq r < n$, we must have $r = 0$. Hence $m \in n\mathbb{Z}$, so $H \subseteq n\mathbb{Z}$. □

Example 2.2 (The special linear group). $\mathrm{SL}_n(K) \leq \mathrm{GL}_n(K)$: the identity matrix has determinant 1; if $\det A = \det B = 1$, then $\det(AB^{-1}) = \det A / \det B = 1$.

Example 2.3 (The alternating group A_n). $A_n = \{\sigma \in S_n : \sigma \text{ is even}\}$ is a subgroup of S_n of index 2 (hence $|A_n| = n!/2$). The verification uses the fact that the product of two even permutations is even and the inverse of an even permutation is even.

Example 2.4 (Centre of a group). The **centre** of G is $Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$. This is a subgroup: $e \in Z(G)$; if $z_1, z_2 \in Z(G)$, then for all $g \in G$, $(z_1 z_2^{-1})g = z_1(z_2^{-1}g) = z_1(gz_2^{-1}) = (z_1 g)z_2^{-1} = (gz_1)z_2^{-1} = g(z_1 z_2^{-1})$, where we used $z_2 g = gz_2 \Rightarrow z_2^{-1} g = g z_2^{-1}$.

Proposition 2.3 (Intersection of subgroups)**.** If $\{H_i\}_{i \in I}$ is any family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. Let $H = \bigcap_{i \in I} H_i$. Since $e \in H_i$ for all i, $e \in H$, so $H \neq \emptyset$. If $a, b \in H$, then $a, b \in H_i$ for all i, hence $ab^{-1} \in H_i$ for all i, hence $ab^{-1} \in H$. By Theorem 2.1,

$H \leq G$. □

Definition 2.2 (Subgroup generated by a subset)**.** For a subset $S \subseteq G$, the subgroup **generated by** S is $\langle S \rangle = \bigcap \{H \leq G : S \subseteq H\}$. This is the smallest subgroup of G containing S. Explicitly, $\langle S \rangle = \{s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} : k \geq 0,\ s_i \in S,\ \varepsilon_i \in \{1, -1\}\}$.

2.3 Cosets and Lagrange's theorem

Definition 2.3 (Cosets)**.** Let $H \leq G$ and $g \in G$. The **left coset** of H by g is

$$gH = \{gh : h \in H\}.$$

The **right coset** is $Hg = \{hg : h \in H\}$. The **index** of H in G is the number of distinct left cosets of H in G, denoted $[G : H]$.

Lemma 2.1 (Properties of cosets)**.** Let $H \leq G$ and $a, b \in G$.

(i) $aH = bH$ if and only if $a^{-1}b \in H$.

(ii) If $aH \cap bH \neq \emptyset$, then $aH = bH$.

(iii) The map $H \to aH$ defined by $h \mapsto ah$ is a bijection.

(iv) The left cosets of H in G partition G.

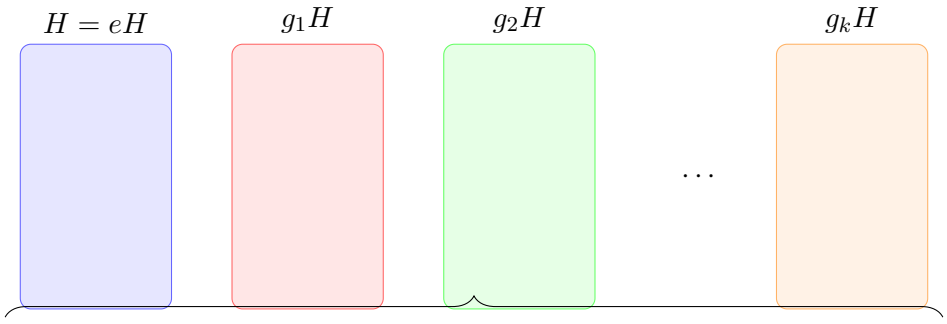
Proof. (i) $aH = bH$ iff $a^{-1}(aH) = a^{-1}(bH)$ iff $H = a^{-1}bH$ iff $a^{-1}b \in H$ (since $e \in H$, $a^{-1}b = a^{-1}b \cdot e \in a^{-1}bH = H$; conversely, if $a^{-1}b \in H$ then $a^{-1}bH = H$ since H is a subgroup).

(ii) Suppose $c \in aH \cap bH$. Then $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$, so $a^{-1}b = h_1 h_2^{-1} \in H$. By (i), $aH = bH$.

(iii) The map $h \mapsto ah$ is injective by left cancellation and surjective by construction. Hence $|aH| = |H|$.

(iv) Every $g \in G$ lies in the coset gH (since $g = ge \in gH$), and by (ii) any two cosets are either equal or disjoint. Hence the distinct cosets form a partition of G. □

Illustration: coset partition. The following diagram depicts a group G partitioned into left cosets of a subgroup H.



$$G = H \sqcup g_1H \sqcup g_2H \sqcup \cdots \sqcup g_kH$$

Theorem 2.3 (Lagrange's theorem)**.** Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$, and

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

Proof. By Lemma 2.1(iv), the distinct left cosets of H form a partition of G:

$$G = g_1 H \sqcup g_2 H \sqcup \cdots \sqcup g_k H$$

where $k = [G : H]$ and the union is disjoint. By Lemma 2.1(iii), each coset $g_i H$ has exactly $|H|$ elements. Therefore

$$|G| = \sum_{i=1}^{k} |g_i H| = k \cdot |H| = [G : H] \cdot |H|.$$

In particular, $|H|$ divides $|G|$. □

Corollary 2.1 (Order of an element divides order of the group)**.** If G is a finite group and $g \in G$, then $\mathrm{ord}(g)$ divides $|G|$. In particular, $g^{|G|} = e$.

Proof. $\mathrm{ord}(g) = |\langle g \rangle|$ (Proposition 1.5), and $\langle g \rangle \leq G$, so by Lagrange's theorem $\mathrm{ord}(g) \mid |G|$. Writing $|G| = \mathrm{ord}(g) \cdot m$, we get $g^{|G|} = (g^{\mathrm{ord}(g)})^m = e^m = e$. □

Corollary 2.2 (Groups of prime order are cyclic)**.** If $|G| = p$ is prime, then G is cyclic, and every element $g \neq e$ generates G.

Proof. Let $g \in G$ with $g \neq e$. Then $\mathrm{ord}(g) > 1$ and $\mathrm{ord}(g) \mid p$ (Corollary 2.1). Since p is prime, $\mathrm{ord}(g) = p = |G|$, so $\langle g \rangle = G$. □

Corollary 2.3 (Fermat–Euler theorem)**.** If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, a group of order $\varphi(n)$. By Corollary 2.1, $\bar{a}^{\varphi(n)} = \bar{1}$. □

Corollary 2.4 (Multiplicativity of the index)**.** If $K \leq H \leq G$ with $[G : K] < \infty$, then $[G : K] = [G : H] \cdot [H : K]$.

Proof. Let $\{g_i H\}_{i=1}^{m}$ be the distinct left cosets of H in G (so $m = [G : H]$), and let $\{h_j K\}_{j=1}^{r}$ be the distinct left cosets of K in H (so $r = [H : K]$). We claim that $\{g_i h_j K : 1 \leq i \leq m,\ 1 \leq j \leq r\}$ is the complete list of distinct left cosets of K in G.

For any $g \in G$, there exists i with $g \in g_i H$, so $g = g_i h$ for some $h \in H$. Then there exists j with $h \in h_j K$, so $g = g_i h_j k$ for some $k \in K$, hence $gK = g_i h_j K$. This shows every left coset of K appears in the list.

To see they are distinct, suppose $g_i h_j K = g_s h_t K$. Then $g_i h_j$ and $g_s h_t$ lie in the same left coset of K, so $(g_s h_t)^{-1}(g_i h_j) \in K \subseteq H$. Hence g_i and g_s lie in the same coset of H, giving $i = s$. Then $h_t^{-1} h_j \in K$, giving $j = t$.

Therefore $[G : K] = mr = [G : H] \cdot [H : K]$. □

2.4 Normal subgroups

Definition 2.4 (Normal subgroup)**.** A subgroup N of G is **normal**, written $N \trianglelefteq G$, if $gNg^{-1} = N$ for every $g \in G$, where $gNg^{-1} = \{gng^{-1} : n \in N\}$.

Theorem 2.4 (Characterisations of normality)**.** Let $N \leq G$. The following are equivalent:

(i) $N \trianglelefteq G$.

(ii) $gNg^{-1} \subseteq N$ for all $g \in G$.

(iii) $gN = Ng$ for all $g \in G$ (i.e. left cosets equal right cosets).

(iv) N is the kernel of some group homomorphism $G \to H$.

Proof. **(i)⇒(ii)** is trivial.

(ii)⇒(i). We need to show $N \subseteq gNg^{-1}$ for every g. Let $n \in N$. By hypothesis applied with g replaced by g^{-1}, we have $g^{-1}ng = (g^{-1})n(g^{-1})^{-1} \in N$, say $g^{-1}ng = n'$. Then $n = gn'g^{-1} \in gNg^{-1}$.

(i)⇔(iii). For any $g \in G$: $gN = Ng$ iff for every $n \in N$ there exists $n' \in N$ with $gn = n'g$, i.e. $gng^{-1} = n' \in N$. Thus $gN = Ng$ for all g iff $gNg^{-1} \subseteq N$ for all g, which by (ii)⇔(i) is equivalent to $N \trianglelefteq G$.

(iv)⇒(i). If $N = \ker \varphi$ for some homomorphism $\varphi\colon G \to H$, then for $n \in N$ and $g \in G$, $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g)e_H\varphi(g)^{-1} = e_H$, so $gng^{-1} \in \ker \varphi = N$.

(i)⇒(iv) will follow once we construct the quotient group (Theorem 2.5): N is the kernel of the canonical projection $\pi\colon G \to G/N$. □

Example 2.5 (Normal subgroups).

(i) Every subgroup of an abelian group is normal (since $gng^{-1} = n$ for all g, n).

(ii) $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$ (kernel of the determinant homomorphism $\det\colon \mathrm{GL}_n(K) \to K^*$).

(iii) $A_n \trianglelefteq S_n$ (kernel of the sign homomorphism $\varepsilon\colon S_n \to \{+1, -1\}$).

(iv) Any subgroup of index 2 is normal (since $gH = G \setminus H = Hg$ for $g \notin H$).

(v) $Z(G) \trianglelefteq G$ for any group G.

2.5 Quotient groups

The central construction of this section is the *quotient group* G/N. We build it in detail.

Definition 2.5 (Set of cosets)**.** Let $N \trianglelefteq G$. The **set of left cosets** of N in G is $G/N = \{gN : g \in G\}$.

Theorem 2.5 (Quotient group)**.** Let $N \trianglelefteq G$. Then G/N is a group under the operation

$$(aN) \cdot (bN) = (ab)N.$$

Moreover, the **canonical projection** $\pi\colon G \to G/N$ defined by $\pi(g) = gN$ is a surjective group homomorphism with $\ker \pi = N$.

Proof. We proceed step by step.

Step 1: Well-definedness. We must show that the product $(aN)(bN) := (ab)N$ does not depend on the choice of representatives a and b. Suppose $aN = a'N$ and $bN = b'N$. Then $a' = an_1$ and $b' = bn_2$ for some $n_1, n_2 \in N$. We need $(ab)N = (a'b')N$, i.e. $(ab)^{-1}(a'b') \in N$.

Compute:

$$(ab)^{-1}(a'b') = b^{-1}a^{-1} \cdot an_1bn_2 = b^{-1}n_1bn_2 = (b^{-1}n_1b) \cdot n_2.$$

Since $N \trianglelefteq G$, $b^{-1}n_1b \in N$, and since $n_2 \in N$ and N is closed, $(b^{-1}n_1b)n_2 \in N$. Hence $(ab)N = (a'b')N$.

Step 2: Associativity. $((aN)(bN))(cN) = (abN)(cN) = (ab)cN = a(bc)N = (aN)(bcN) = (aN)((bN)(cN))$.

Step 3: Identity. The coset $eN = N$ satisfies $(eN)(gN) = gN = (gN)(eN)$.

Step 4: Inverses. $(gN)(g^{-1}N) = gg^{-1}N = eN = N$, so $(gN)^{-1} = g^{-1}N$.

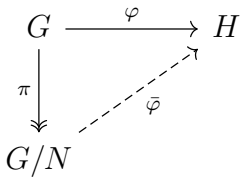
Canonical projection. $\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b)$, so π is a homomorphism. It is surjective by definition. $\ker \pi = \{g \in G : \pi(g) = N\} = \{g \in G : gN = N\} = \{g \in G : g \in N\} = N$. □

Remark 2.2 (Normality is necessary). The proof of well-definedness uses $N \trianglelefteq G$ in an essential way: we needed $b^{-1}n_1b \in N$. If N is not normal, the product of cosets is not well-defined, and G/N is merely a set, not a group.

Example 2.6 (Quotient $\mathbb{Z}/n\mathbb{Z}$). $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ (since $\mathbb{Z}$ is abelian), and the quotient group $\mathbb{Z}/n\mathbb{Z}$ is precisely the cyclic group of order n we encountered in Example 1.4. The canonical projection $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sends $k \mapsto \bar{k}$.

Example 2.7 (Quotient S_n/A_n). $A_n \trianglelefteq S_n$ with $[S_n : A_n] = 2$. The quotient $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ consists of two cosets: the even permutations A_n and the odd permutations.

Commutative diagram: canonical projection.



This diagram will become central when we prove the first isomorphism theorem (Chapter 3): if $\varphi\colon G \to H$ is a homomorphism with $N \subseteq \ker \varphi$, there is a unique homomorphism $\bar{\varphi}\colon G/N \to H$ such that $\bar{\varphi} \circ \pi = \varphi$.

2.6 The centre and the commutator subgroup

Definition 2.6 (Commutator)**.** For $a, b \in G$, the **commutator** of a and b is $[a, b] = aba^{-1}b^{-1}$.

Definition 2.7 (Commutator subgroup)**.** The **commutator subgroup** (or **derived subgroup**) of G is

$$[G, G] = \langle [a, b] : a, b \in G \rangle.$$

Proposition 2.4 (Properties of the commutator subgroup)**.** Let G be a group.

(i) $[G, G] \trianglelefteq G$.

(ii) $G/[G, G]$ is abelian.

(iii) If $N \trianglelefteq G$, then G/N is abelian if and only if $[G, G] \subseteq N$.

Thus $[G, G]$ is the smallest normal subgroup such that the quotient is abelian.

Proof. (i) For any $g \in G$ and any commutator $[a, b] = aba^{-1}b^{-1}$,

$$g[a, b]g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1},\, gbg^{-1}] \in [G, G].$$

Since conjugation maps generators to generators, it maps $[G, G]$ to itself.

(ii) In $G/[G, G]$, the cosets $\overline{a} = a[G, G]$ and $\overline{b} = b[G, G]$ satisfy $\overline{a}\,\overline{b}\,\overline{a}^{-1}\overline{b}^{-1} = \overline{aba^{-1}b^{-1}} = \overline{[a, b]} = \overline{e}$ (since $[a, b] \in [G, G]$). Hence $\overline{a}\,\overline{b} = \overline{b}\,\overline{a}$.

(iii) G/N is abelian iff $(aN)(bN) = (bN)(aN)$ for all a, b iff $abN = baN$ for all a, b iff $a^{-1}b^{-1}ab \in N$ for all a, b iff $[a, b] \in N$ for all a, b iff $[G, G] \subseteq N$ (since $[G, G]$ is generated by all commutators). □

Proposition 2.5 (The centre is normal)**.** For any group G, $Z(G) \trianglelefteq G$.

Proof. We already verified $Z(G) \leq G$ in Example 2.4. For normality, let $z \in Z(G)$ and $g \in G$. Then $gzg^{-1} = zgg^{-1} = z \in Z(G)$. Hence $gZ(G)g^{-1} \subseteq Z(G)$ for all g, so $Z(G) \trianglelefteq G$. □

Example 2.8 (Centres of familiar groups). (i) $Z(S_n) = \{e\}$ for $n \geq 3$.

(ii) $Z(\mathrm{GL}_n(K)) = \{\lambda I : \lambda \in K^*\}$ (scalar matrices).

(iii) $Z(D_n) = \{e\}$ if n is odd; $Z(D_n) = \{e, r^{n/2}\}$ if n is even.

(iv) $Z(Q_8) = \{1, -1\}$.

2.7 Simple groups

Definition 2.8 (Simple group)**.** A group G is **simple** if $|G| > 1$ and the only normal subgroups of G are $\{e\}$ and G itself.

Proposition 2.6 (Abelian simple groups)**.** An abelian group is simple if and only if it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Proof. If $G \cong \mathbb{Z}/p\mathbb{Z}$, then $|G| = p$ and by Lagrange's theorem the only subgroups have order 1 or p, so G is simple.

Conversely, if G is abelian and simple, let $g \in G$, $g \neq e$. Then $\langle g \rangle \trianglelefteq G$ (every subgroup of an abelian group is normal) and $\langle g \rangle \neq \{e\}$, so by simplicity $\langle g \rangle = G$, i.e. G is cyclic. Write $G \cong \mathbb{Z}/n\mathbb{Z}$. If n is not prime, say $n = ab$ with $1 < a, b < n$, then $\langle \bar{a} \rangle$ is a proper non-trivial subgroup, contradicting simplicity. Hence n is prime. □

Theorem 2.6 (Simplicity of A_n for $n \geq 5$)**.** For $n \geq 5$, the alternating group A_n is simple.

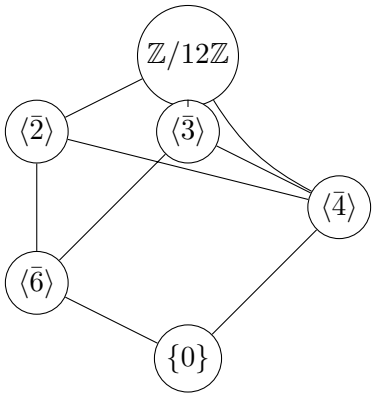
This is a deep result whose proof requires significant preparation (in particular, knowledge of the conjugacy classes of A_n). We shall return to it after developing the necessary tools. The key idea is to show that every non-trivial normal subgroup of A_n must contain a 3-cycle, and then to show that A_n is generated by 3-cycles.

Remark 2.3 (Historical significance). The simplicity of A_n for $n \geq 5$ is the group-theoretic fact underlying the unsolvability of the general polynomial equation of degree ≥ 5 by radicals. Galois's proof of this unsolvability rests precisely on the observation that A_5 is simple (hence not solvable).

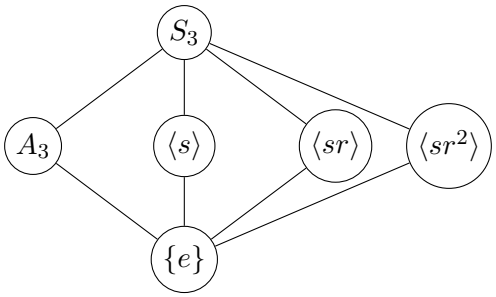
2.8 Subgroup lattices

The subgroups of a group, partially ordered by inclusion, form a *lattice*. The following diagrams depict the subgroup lattices of several small groups.

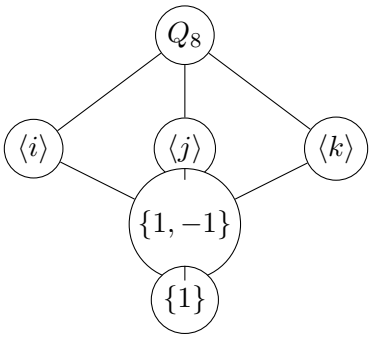
Subgroup lattice of $\mathbb{Z}/12\mathbb{Z}$.



Subgroup lattice of $D_3 \cong S_3$.



Subgroup lattice of Q_8.



2.9 Exercises

Exercise 2.1 (Subgroup test practice). Show that $H = \{2^n : n \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Q}^*, \times)$.

Exercise 2.2 (Centre computation). Compute $Z(Q_8)$ and $Z(D_4)$.

Exercise 2.3 (Subgroups of $\mathbb{Z}/20\mathbb{Z}$). List all subgroups of $\mathbb{Z}/20\mathbb{Z}$ and draw the subgroup lattice.

Exercise 2.4 (Index-2 subgroups are normal). Let $H \leq G$ with $[G : H] = 2$. Prove that $H \trianglelefteq G$.

Exercise 2.5 (Normality and products). Let $N \trianglelefteq G$ and $H \leq G$. Show that $NH = \{nh : n \in N,\, h \in H\}$ is a subgroup of G. Is HN also a subgroup?

Exercise 2.6 (Commutator subgroup of S_3). Show that $[S_3, S_3] = A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Exercise 2.7 (Quotient computation). Determine $(\mathbb{Z}/12\mathbb{Z})/\langle \bar{4} \rangle$ up to isomorphism.

Exercise 2.8 (Centre of a quotient). Let G be a group with $Z(G) = \{e\}$. Does it follow that $Z(G/N) = \{N\}$ for every $N \trianglelefteq G$? Prove or give a counterexample.

Exercise 2.9 ($G/Z(G)$ cyclic implies G abelian). Let G be a group. Show that if $G/Z(G)$ is cyclic, then G is abelian. *(Hint: write every element as $g^k z$ for $z \in Z(G)$.)*

Exercise 2.10 (Cauchy's theorem for abelian groups). Let G be a finite abelian group and p a prime dividing $|G|$. Prove that G contains an element of order p. *(Hint: induction on $|G|$; pick any $g \neq e$ and consider $G/\langle g\rangle$ or $\langle g\rangle$.)*

Exercise 2.11 ($(\star)$ Normal subgroups of S_n). Show that for $n \geq 5$, the only normal subgroups of S_n are $\{e\}$, A_n, and S_n. *(Hint: use the simplicity of A_n.)*

Exercise 2.12 ($(\star)$ Infinite index). Show that $\mathbb{Z}$ has no subgroup of finite index other than those of the form $n\mathbb{Z}$ ($n \geq 1$). Conversely, verify that $[\mathbb{Z} : n\mathbb{Z}] = n$.

Chapter summary

- A non-empty subset H of G is a **subgroup** iff $ab^{-1} \in H$ for all $a, b \in H$ (one-step test).
- **Lagrange's theorem**: if G is finite and $H \leq G$, then $|H|$ divides $|G|$ and $|G| = [G : H] \cdot |H|$.
- Corollaries: $\operatorname{ord}(g) \mid |G|$; groups of prime order are cyclic; the Fermat–Euler theorem.
- A subgroup N is **normal** ($N \trianglelefteq G$) iff $gNg^{-1} = N$ for all g iff left cosets equal right cosets iff N is the kernel of a homomorphism.
- For $N \trianglelefteq G$, the **quotient** G/N is a group under the well-defined operation $(aN)(bN) = (ab)N$.
- The **centre** $Z(G)$ is a normal subgroup; the **commutator subgroup** $[G, G]$ is the smallest normal subgroup with abelian quotient.
- A group is **simple** if it has no non-trivial proper normal subgroups. Abelian simple groups are exactly $\mathbb{Z}/p\mathbb{Z}$; A_n is simple for $n \geq 5$.

Chapter 3

Homomorphisms and Isomorphism Theorems

Having established the foundations of group theorysubgroups, cosets, and quotient groups-swe now turn to the maps that relate one group to another. Group homomorphisms are the structure-preserving functions that lie at the heart of algebra. The four isomorphism theorems provide the fundamental links between quotient groups, normal subgroups, and homomorphic images.

3.1 Group Homomorphisms

Definition 3.1 (Group homomorphism)**.** Let $(G, \cdot)$ and $(H, *)$ be groups. A function $f : G \to H$ is called a *group homomorphism* if

$$f(a \cdot b) = f(a) * f(b) \qquad \text{for all } a, b \in G.$$

Proposition 3.1 (Identity is preserved)**.** Let $f : G \to H$ be a group homomorphism. Then $f(e_G) = e_H$.

Proof. We have

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G).$$

Multiplying both sides on the left by $f(e_G)^{-1}$ yields $e_H = f(e_G)$, as desired. □

Proposition 3.2 (Inverses are preserved)**.** Let $f : G \to H$ be a group homomorphism. Then for every $a \in G$,

$$f(a^{-1}) = f(a)^{-1}.$$

Proof. Compute

$$f(a) * f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H.$$

Likewise $f(a^{-1}) * f(a) = e_H$. Hence $f(a^{-1})$ is the (unique) inverse of $f(a)$ in H. □

Proposition 3.3 (Image of a power)**.** Let $f : G \to H$ be a group homomorphism.

Then for every $a \in G$ and $n \in \mathbb{Z}$,

$$f(a^n) = f(a)^n.$$

Proof. For $n \geq 0$ the statement follows by induction on n using $f(a^{n+1}) = f(a \cdot a^n) = f(a) * f(a^n)$. For $n < 0$ write $a^n = (a^{-1})^{-n}$ and apply the result for positive exponents together with Proposition 3.2. □

3.2 Kernel and Image

Definition 3.2 (Kernel and image)**.** Let $f\colon G \to H$ be a group homomorphism.

1. The *kernel* of f is $\operatorname{Ker} f = \{g \in G : f(g) = e_H\}$.
2. The *image* of f is $\operatorname{Im} f = \{f(g) : g \in G\}$.

Theorem 3.1 (Kernel is a normal subgroup)**.** Let $f\colon G \to H$ be a group homomorphism. Then $\operatorname{Ker} f \trianglelefteq G$.

Proof. **Subgroup.** Since $f(e_G) = e_H$, we have $e_G \in \operatorname{Ker} f$, so $\operatorname{Ker} f \neq \varnothing$. Let $a, b \in \operatorname{Ker} f$. Then

$$f(ab^{-1}) = f(a) * f(b^{-1}) = f(a) * f(b)^{-1} = e_H * e_H^{-1} = e_H,$$

so $ab^{-1} \in \operatorname{Ker} f$. By the subgroup criterion, $\operatorname{Ker} f \leq G$.

Normality. Let $g \in G$ and $k \in \operatorname{Ker} f$. Then

$$f(gkg^{-1}) = f(g) * f(k) * f(g^{-1}) = f(g) * e_H * f(g)^{-1} = e_H,$$

so $gkg^{-1} \in \operatorname{Ker} f$. Therefore $g(\operatorname{Ker} f)g^{-1} \subseteq \operatorname{Ker} f$ for all $g \in G$, and $\operatorname{Ker} f \trianglelefteq G$. □

Theorem 3.2 (Image is a subgroup)**.** Let $f\colon G \to H$ be a group homomorphism. Then $\operatorname{Im} f \leq H$.

Proof. Since $f(e_G) = e_H$, we have $e_H \in \operatorname{Im} f$. Let $h_1, h_2 \in \operatorname{Im} f$, say $h_1 = f(g_1)$ and $h_2 = f(g_2)$. Then

$$h_1 h_2^{-1} = f(g_1) * f(g_2)^{-1} = f(g_1) * f(g_2^{-1}) = f(g_1 g_2^{-1}) \in \operatorname{Im} f.$$

By the subgroup criterion, $\operatorname{Im} f \leq H$. □

Proposition 3.4 (Injectivity and the kernel)**.** A group homomorphism $f\colon G \to H$ is injective if and only if $\operatorname{Ker} f = \{e_G\}$.

Proof. ($\Rightarrow$) If f is injective and $f(g) = e_H = f(e_G)$, then $g = e_G$, so $\operatorname{Ker} f = \{e_G\}$.

($\Leftarrow$) Suppose $\operatorname{Ker} f = \{e_G\}$ and $f(a) = f(b)$. Then $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$, so $ab^{-1} \in \operatorname{Ker} f = \{e_G\}$ and $a = b$. □

3.3 Types of Homomorphisms

Definition 3.3 (Monomorphism, epimorphism, isomorphism)**.** Let $f\colon G \to H$ be a group homomorphism.

1. f is a *monomorphism* if f is injective.
2. f is an *epimorphism* if f is surjective.
3. f is an *isomorphism* if f is bijective. We write $G \cong H$.
4. f is an *endomorphism* if $H = G$.
5. f is an *automorphism* if f is an isomorphism and $H = G$.

Proposition 3.5 (Inverse of an isomorphism)**.** If $f\colon G \to H$ is a group isomorphism, then $f^{-1}\colon H \to G$ is also a group isomorphism.

Proof. Let $h_1, h_2 \in H$. Write $h_i = f(g_i)$. Then $f^{-1}(h_1h_2) = f^{-1}(f(g_1)f(g_2)) = f^{-1}(f(g_1g_2)) = g_1g_2 = f^{-1}(h_1)\, f^{-1}(h_2)$. Since f^{-1} is bijective by definition, it is an isomorphism. □

3.4 Important Examples of Homomorphisms

Example 3.1 (Determinant). The map $\det\colon \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R}^*, \cdot)$ is a group homomorphism because $\det(AB) = \det(A)\det(B)$. Its kernel is $\mathrm{SL}_n(\mathbb{R}) = \{A : \det A = 1\}$, and its image is $\mathbb{R}^*$. Hence det is an epimorphism and $\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$.

Example 3.2 (Sign homomorphism). The signature map $\varepsilon\colon S_n \to \{+1, -1\}$ satisfies $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Its kernel is the alternating group Alt_n, confirming $\mathrm{Alt}_n \trianglelefteq S_n$ and $[S_n : \mathrm{Alt}_n] = 2$.

Example 3.3 (Exponential map). The map $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}^*_{>0}, \cdot)$, $x \mapsto e^x$, is a group isomorphism. Indeed $e^{x+y} = e^x e^y$, bijectivity follows from the existence of the logarithm, and $\operatorname{Ker}\exp = \{0\}$.

Example 3.4 (Canonical projection). Let $N \trianglelefteq G$. The map $\pi\colon G \to G/N$ defined by $\pi(g) = gN$ is a surjective group homomorphism with $\operatorname{Ker}\pi = N$. This map is called the *canonical projection* (or *natural homomorphism*).

Example 3.5 (Reduction modulo n). For any positive integer n, the map $\rho\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a}$, is a surjective group homomorphism with $\operatorname{Ker}\rho = n\mathbb{Z}$.

3.5 The First Isomorphism Theorem

Theorem 3.3 (First Isomorphism Theorem)**.** Let $f\colon G \to H$ be a group homomorphism. Then

$$G/\operatorname{Ker} f \;\cong\; \operatorname{Im} f.$$

More precisely, the map $\bar{f}\colon G/\operatorname{Ker} f \to \operatorname{Im} f$ defined by $\bar{f}(g\operatorname{Ker} f) = f(g)$ is a well-defined group isomorphism.

Proof. Write $K = \operatorname{Ker} f$.

Well-definedness. If $gK = g'K$, then $g' = gk$ for some $k \in K$. Hence $f(g') = f(gk) = f(g)f(k) = f(g)\,e_H = f(g)$, so $\bar{f}$ is well-defined.

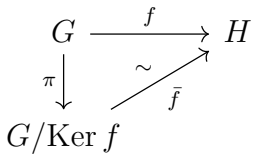
Homomorphism. $\bar{f}(gK \cdot g'K) = \bar{f}(gg'K) = f(gg') = f(g)f(g') = \bar{f}(gK)\,\bar{f}(g'K)$.

Injectivity. If $\bar{f}(gK) = e_H$, then $f(g) = e_H$, hence $g \in K$ and $gK = K = e_{G/K}$. By Proposition 3.4, $\bar{f}$ is injective.

Surjectivity. Every element of $\operatorname{Im} f$ has the form $f(g) = \bar{f}(gK)$.

Therefore $\bar{f}$ is an isomorphism $G/K \xrightarrow{\sim} \operatorname{Im} f$. □

The situation is summarized by the following commutative diagram:



where π is the canonical projection and $f = \bar{f} \circ \pi$.

Corollary 3.1. If $f\colon G \to H$ is a surjective homomorphism, then $G/\operatorname{Ker} f \cong H$.

Proof. When f is surjective, $\operatorname{Im} f = H$. Apply Theorem 3.3. □

Example 3.6. By Example 3.1, $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ is surjective with kernel $\mathrm{SL}_n(\mathbb{R})$. The First Isomorphism Theorem gives $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

Example 3.7. The surjection $\rho\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ has kernel $n\mathbb{Z}$, so $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$a tautology that nonetheless illustrates the theorem.

3.6 The Second Isomorphism Theorem

Theorem 3.4 (Second Isomorphism Theorem Diamond Theorem)**.** Let G be a group, $H \leq G$, and $N \trianglelefteq G$. Then

1. $HN = \{hn : h \in H,\, n \in N\}$ is a subgroup of G.
2. $H \cap N \trianglelefteq H$.
3. $HN/N \;\cong\; H/(H \cap N)$.

Proof. **(1)** We verify that $HN \leq G$. Clearly $e = e \cdot e \in HN$. If h_1n_1, $h_2n_2 \in HN$, then

$$(h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1} \cdot (h_2n_1n_2^{-1}h_2^{-1}).$$

Since $N \trianglelefteq G$, the element $h_2n_1n_2^{-1}h_2^{-1} \in N$, so the product lies in HN. Hence $HN \leq G$. Moreover $N \trianglelefteq HN$ because $N \trianglelefteq G$ and $N \subseteq HN$.

(2) and (3) Define $\varphi\colon H \to HN/N$ by $\varphi(h) = hN$. This is the restriction of the canonical projection $\pi\colon G \to G/N$ to H.

Homomorphism: $\varphi(h_1h_2) = h_1h_2N = (h_1N)(h_2N) = \varphi(h_1)\varphi(h_2)$.

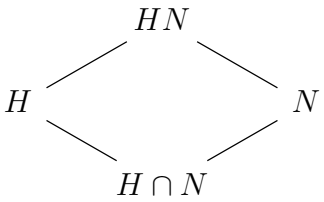
Surjectivity: Let $hnN \in HN/N$. Since $n \in N$, we have $hnN = hN = \varphi(h)$.

Kernel: $\operatorname{Ker}\varphi = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N$.

In particular $H \cap N \trianglelefteq H$ (it is the kernel of a homomorphism from H). By the First Isomorphism Theorem (Theorem 3.3),

$$H/(H \cap N) = H/\operatorname{Ker}\varphi \;\cong\; \operatorname{Im}\varphi = HN/N. \qquad \square$$

The name "Diamond Theorem" comes from the lattice diagram:



3.7 The Third Isomorphism Theorem

Theorem 3.5 (Third Isomorphism Theorem)**.** Let G be a group with $N \trianglelefteq G$ and $H \trianglelefteq G$ such that $N \subseteq H$. Then $H/N \trianglelefteq G/N$ and

$$(G/N)\big/(H/N) \;\cong\; G/H.$$

Proof. Define $\psi\colon G/N \to G/H$ by $\psi(gN) = gH$.

Well-definedness. If $gN = g'N$, then $g^{-1}g' \in N \subseteq H$, so $gH = g'H$ and ψ is well-defined.

Homomorphism. $\psi(gN \cdot g'N) = \psi(gg'N) = gg'H = (gH)(g'H) = \psi(gN)\,\psi(g'N)$.

Surjectivity. For any $gH \in G/H$, we have $\psi(gN) = gH$.

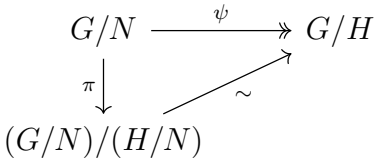
Kernel.

$$\operatorname{Ker}\psi = \{gN \in G/N : gH = H\} = \{gN : g \in H\} = H/N.$$

Hence $H/N \trianglelefteq G/N$. The First Isomorphism Theorem gives

$$(G/N)\big/(H/N) = (G/N)/\operatorname{Ker}\psi \;\cong\; G/H. \qquad \square$$

Diagrammatically:



Example 3.8. Take $G = \mathbb{Z}$, $N = 6\mathbb{Z}$, $H = 2\mathbb{Z}$. Then $N \subseteq H$, $G/N \cong \mathbb{Z}/6\mathbb{Z}$, $H/N \cong 2\mathbb{Z}/6\mathbb{Z} \cong \{0, 2, 4\} \leq \mathbb{Z}/6\mathbb{Z}$, and $G/H \cong \mathbb{Z}/2\mathbb{Z}$. The Third Isomorphism Theorem gives $(\mathbb{Z}/6\mathbb{Z})/(\{0, 2, 4\}) \cong \mathbb{Z}/2\mathbb{Z}$.

3.8 The Correspondence Theorem

The Correspondence Theorem (sometimes called the Fourth Isomorphism Theorem or the Lattice Isomorphism Theorem) describes the subgroup structure of a quotient group.

Theorem 3.6 (Correspondence Theorem)**.** Let $N \trianglelefteq G$ and let $\pi\colon G \to G/N$ be the canonical projection. There is a bijection

$$\{H : N \subseteq H \leq G\} \overset{1\text{-}1}{\longleftrightarrow} \{K : K \leq G/N\}$$

given by $H \mapsto H/N$ and $K \mapsto \pi^{-1}(K)$. Moreover:

1. $H_1 \subseteq H_2$ if and only if $H_1/N \subseteq H_2/N$.
2. $H_1 \trianglelefteq H_2$ if and only if $H_1/N \trianglelefteq H_2/N$.
3. If $H_1 \leq H_2$, then $[H_2 : H_1] = [H_2/N : H_1/N]$.

Proof. **Maps are well-defined.** If $N \subseteq H \leq G$, then $N \trianglelefteq H$ (since $N \trianglelefteq G$) and $H/N \leq G/N$. Conversely, if $K \leq G/N$, then $\pi^{-1}(K)$ is a subgroup of G containing N (since $\pi^{-1}(\{eN\}) \supseteq N$).

The maps are inverse to each other. For $N \subseteq H \leq G$: $\pi^{-1}(H/N) = \{g \in G : gN \in H/N\} = \{g \in G : g \in HN\} = H$ (since $N \subseteq H$ implies $HN = H$). For $K \leq G/N$: $\pi^{-1}(K)/N = \{gN : g \in \pi^{-1}(K)\} = \{\pi(g) : \pi(g) \in K\} = K$.

Inclusion preservation (1). $H_1 \subseteq H_2$ implies $H_1/N \subseteq H_2/N$ trivially. Conversely, if $H_1/N \subseteq H_2/N$ and $h \in H_1$, then $hN \in H_1/N \subseteq H_2/N$, so $h \in H_2 N = H_2$.

Normality (2). $H_1 \trianglelefteq H_2$ if and only if $h_2 H_1 h_2^{-1} \subseteq H_1$ for all $h_2 \in H_2$. Passing to cosets modulo N (using the canonical projection), this holds if and only if $(h_2N)(H_1/N)(h_2N)^{-1} \subseteq H_1/N$ for all $h_2 N \in H_2/N$, which is $H_1/N \trianglelefteq H_2/N$.

Index (3). The map $H_2/H_1 \to (H_2/N)/(H_1/N)$ given by $h_2 H_1 \mapsto (h_2N)(H_1/N)$ is a well-defined bijection; one can verify this directly, or apply the Third Isomorphism Theorem. □

3.9 Automorphism Groups

Definition 3.4 (Automorphism group)**.** The set of all automorphisms of a group G, denoted $\mathrm{Aut}(G)$, forms a group under composition. That is,

$$\mathrm{Aut}(G) = \{\varphi\colon G \to G : \varphi \text{ is an isomorphism}\}.$$

Definition 3.5 (Inner automorphism)**.** For $g \in G$, the map $\iota_g\colon G \to G$ defined by $\iota_g(x) = gxg^{-1}$ is an automorphism, called the *inner automorphism* induced by g. The

set of all inner automorphisms is denoted $\mathrm{Inn}(G)$.

Theorem 3.7 ($\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$)**.** $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$, and $\mathrm{Inn}(G) \cong G/Z(G)$.

Proof. Define $\Phi\colon G \to \mathrm{Aut}(G)$ by $\Phi(g) = \iota_g$.

Homomorphism. For all $x \in G$, $\Phi(gh)(x) = \iota_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \iota_g(\iota_h(x)) = (\Phi(g) \circ \Phi(h))(x)$.

Image and kernel. $\operatorname{Im}\Phi = \mathrm{Inn}(G)$ by definition. $\operatorname{Ker}\Phi = \{g \in G : gxg^{-1} = x\ \forall x\} = Z(G)$.

By the First Isomorphism Theorem, $\mathrm{Inn}(G) \cong G/Z(G)$. In particular $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Normality. Let $\varphi \in \mathrm{Aut}(G)$ and $\iota_g \in \mathrm{Inn}(G)$. For any $x \in G$,

$$(\varphi \circ \iota_g \circ \varphi^{-1})(x) = \varphi(g\,\varphi^{-1}(x)\,g^{-1}) = \varphi(g)\,x\,\varphi(g)^{-1} = \iota_{\varphi(g)}(x).$$

Hence $\varphi \circ \iota_g \circ \varphi^{-1} = \iota_{\varphi(g)} \in \mathrm{Inn}(G)$. Therefore $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

Example 3.9 ($\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$). Every automorphism of $\mathbb{Z}/n\mathbb{Z}$ is determined by the image of the generator $\bar{1}$. An endomorphism $\varphi_k\colon \bar{1} \mapsto \bar{k}$ is an automorphism if and only if $\bar{k}$ is also a generator, which happens if and only if $\gcd(k, n) = 1$. Therefore

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times},$$

the group of units modulo n, which has order $\varphi(n)$ (Euler's totient function).

Example 3.10 ($\mathrm{Aut}(S_3)$). Since $Z(S_3) = \{e\}$, we have $\mathrm{Inn}(S_3) \cong S_3/Z(S_3) \cong S_3$, so $|\mathrm{Inn}(S_3)| = 6$. Any automorphism must send elements of order 2 to elements of order 2 and elements of order 3 to elements of order 3. There are three transpositions and two 3-cycles. An automorphism is determined by its effect on the generators, say (1 2) and (1 2 3). A careful count shows $|\mathrm{Aut}(S_3)| = 6$, hence $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$.

3.10 Exercises

Exercise 3.1. Let $f\colon G \to H$ be a group homomorphism and let $g \in G$ with $\mathrm{ord}(g) = n < \infty$. Show that $\mathrm{ord}(f(g))$ divides n.

Exercise 3.2. Let $f\colon G \to H$ be a group homomorphism. Prove that if G is cyclic, then $\operatorname{Im} f$ is cyclic.

Exercise 3.3. Let $f\colon G \to H$ be a homomorphism with G finite. Show that $|\operatorname{Im} f| = [G : \operatorname{Ker} f]$.

Exercise 3.4. Prove that if $f\colon G \to H$ is a surjective homomorphism and G is abelian, then H is abelian.

Exercise 3.5. Show that the composition of two group homomorphisms is a group homomorphism.

Exercise 3.6. Determine $\mathrm{Aut}(\mathbb{Z})$ and show it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Exercise 3.7. Let $N \leq G$. Show that $N \trianglelefteq G$ if and only if N is the kernel of some group homomorphism defined on G.

Exercise 3.8. Let $G = S_4$, $H = \langle(1\ 2\ 3\ 4)\rangle$, and $N = V_4$ (the Klein four-group). Verify the Second Isomorphism Theorem by computing HN, $H \cap N$, HN/N, and $H/(H \cap N)$ explicitly.

Exercise 3.9. Let $G = \mathbb{Z}/12\mathbb{Z}$, $H = \langle\bar{3}\rangle$, $N = \langle\bar{6}\rangle$. Verify the Third Isomorphism Theorem explicitly.

Exercise 3.10. Prove that if $\gcd(m, n) = 1$, then $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Exercise 3.11. Use the Correspondence Theorem to list all subgroups of $\mathbb{Z}/12\mathbb{Z}$ by considering the subgroups of $\mathbb{Z}$ containing $12\mathbb{Z}$.

Exercise 3.12. Prove that G is abelian if and only if $\mathrm{Inn}(G) = \{\mathrm{id}\}$.

Chapter Summary

- A **group homomorphism** $f\colon G \to H$ satisfies $f(ab) = f(a)f(b)$ and automatically preserves identity and inverses.
- The **kernel** $\ker f$ is always a normal subgroup of G; the **image** $\mathrm{Im}\, f$ is always a subgroup of H. Injectivity is equivalent to $\ker f = \{e\}$.
- The **First Isomorphism Theorem** states $G/\ker f \cong \mathrm{Im}\, f$.
- The **Second Isomorphism Theorem** (Diamond): if $H \leq G$ and $N \trianglelefteq G$, then $HN/N \cong H/(H \cap N)$.
- The **Third Isomorphism Theorem**: if $N \subseteq H \trianglelefteq G$ with both normal in G, then $(G/N)/(H/N) \cong G/H$.
- The **Correspondence Theorem** establishes a lattice-preserving bijection between subgroups of G/N and subgroups of G containing N.
- The **automorphism group** $\mathrm{Aut}(G)$ contains $\mathrm{Inn}(G) \cong G/Z(G)$ as a normal subgroup.

Chapter 4

Group Actions and Sylow Theorems

Group actions provide a powerful framework for studying groups through their effect on sets. By allowing a group to "act" on various mathematical objects, we unlock counting techniques (Burnside's lemma), structural theorems (p-group theory), and the celebrated Sylow theorems, which give remarkably precise information about the subgroup structure of finite groups.

4.1 Group Actions

Definition 4.1 (Group action)**.** Let G be a group and X a set. A *(left) group action* of G on X is a map $G \times X \to X$, written $(g, x) \mapsto g \cdot x$, satisfying:

1. $e \cdot x = x$ for all $x \in X$,
2. $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$.

We say that G *acts on* X and call X a *G-set*.

Proposition 4.1 (Equivalent formulation)**.** A left action of G on X is equivalent to a group homomorphism $\varphi \colon G \to \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ denotes the symmetric group on X.

Proof. Given an action $G \times X \to X$, define $\varphi(g) \colon X \to X$ by $\varphi(g)(x) = g \cdot x$. The axioms ensure that $\varphi(g)$ is a bijection (with inverse $\varphi(g^{-1})$) and $\varphi(gh) = \varphi(g) \circ \varphi(h)$, so φ is a homomorphism into $\mathrm{Sym}(X)$.

Conversely, given $\varphi \colon G \to \mathrm{Sym}(X)$, define $g \cdot x = \varphi(g)(x)$. The homomorphism property ensures the action axioms hold. □

Definition 4.2 (Faithful action and kernel)**.** The *kernel* of the action is $\operatorname{Ker} \varphi = \{g \in G : g \cdot x = x \ \forall x \in X\}$. The action is *faithful* (or *effective*) if $\operatorname{Ker} \varphi = \{e\}$.

Example 4.1 (Left multiplication). Every group G acts on itself by left multiplication: $g \cdot x = gx$. This action is faithful. The associated homomorphism $G \to \mathrm{Sym}(G)$ is injective; this is the content of *Cayley's theorem*.

Example 4.2 (Conjugation). G acts on itself by conjugation: $g \cdot x = gxg^{-1}$. The kernel of this action is the center $Z(G)$.

Example 4.3 (Action on cosets). Let $H \leq G$. Then G acts on $G/H = \{gH : g \in G\}$ by left multiplication: $g \cdot (aH) = (ga)H$.

Example 4.4 (Conjugation on subgroups). G acts on the set of subgroups of G by conjugation: $g \cdot H = gHg^{-1}$. The stabilizer of H under this action is the normalizer $N_G(H)$.

4.2 Orbits and Stabilizers

Definition 4.3 (Orbit and stabilizer)**.** Let G act on X and let $x \in X$.

1. The *orbit* of x is $\mathcal{O}_x = G \cdot x = \{g \cdot x : g \in G\}$.
2. The *stabilizer* of x is $G_x = \mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$.

Proposition 4.2 (Stabilizer is a subgroup)**.** For any $x \in X$, $G_x \leq G$.

Proof. $e \cdot x = x$ so $e \in G_x$. If $g, h \in G_x$, then $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x)$. Now $h \cdot x = x$ implies $h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) = (h^{-1}h) \cdot x = x$, so $(gh^{-1}) \cdot x = g \cdot x = x$. Hence $gh^{-1} \in G_x$. □

Proposition 4.3 (Orbits partition X)**.** The orbits of the action form a partition of X.

Proof. Define $x \sim y$ iff $y = g \cdot x$ for some $g \in G$. This is an equivalence relation: reflexivity by $e \cdot x = x$; symmetry by $y = g \cdot x \Rightarrow x = g^{-1} \cdot y$; transitivity by $y = g \cdot x$, $z = h \cdot y \Rightarrow z = (hg) \cdot x$. The equivalence classes are precisely the orbits. □

Theorem 4.1 (Orbit-Stabilizer Theorem)**.** Let G be a group acting on a set X, and let $x \in X$. Then the map $gG_x \mapsto g \cdot x$ is a well-defined bijection from G/G_x to $\mathcal{O}_x$. In particular, if G is finite,

$$|\mathcal{O}_x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

Proof. Define $\Phi \colon G/G_x \to \mathcal{O}_x$ by $\Phi(gG_x) = g \cdot x$.

Well-definedness. If $gG_x = g'G_x$, then $g^{-1}g' \in G_x$, so $(g^{-1}g') \cdot x = x$, hence $g' \cdot x = g \cdot ((g^{-1}g') \cdot x) = g \cdot x$ (using the action axiom $(g(g^{-1}g')) \cdot x = g' \cdot x$ also confirms this; more directly, $g' \cdot x = g \cdot ((g^{-1}g') \cdot x) = g \cdot x$).

Surjectivity. By definition, every element of $\mathcal{O}_x$ has the form $g \cdot x = \Phi(gG_x)$.

Injectivity. If $\Phi(gG_x) = \Phi(g'G_x)$, then $g \cdot x = g' \cdot x$, so $(g^{-1}g') \cdot x = x$, meaning $g^{-1}g' \in G_x$ and $gG_x = g'G_x$.

Since Φ is a bijection, $|\mathcal{O}_x| = |G/G_x| = [G : G_x]$. When G is finite, Lagrange's theorem gives $[G : G_x] = |G|/|G_x|$. □

Definition 4.4 (Fixed points)**.** The set of *fixed points* of the action is

$$X^G = \{x \in X : g \cdot x = x \ \forall g \in G\}.$$

An element $x \in X^G$ has orbit $\mathcal{O}_x = \{x\}$.

4.3 The Class Equation

Theorem 4.2 (Class Equation)**.** Let G be a finite group acting on a finite set X. Let $x_1, \ldots, x_r$ be representatives of the distinct orbits of size > 1. Then

$$|X| = |X^G| + \sum_{i=1}^{r} [G : G_{x_i}].$$

Proof. The orbits partition X (Proposition 4.3):

$$|X| = \sum_{\mathcal{O}} |\mathcal{O}|.$$

Each orbit of size 1 contributes one element to X^G, and each orbit of size > 1 has size $[G : G_{x_i}]$ by the Orbit-Stabilizer Theorem (Theorem 4.1). Splitting the sum gives the result. □

Corollary 4.1 (Class equation for conjugation)**.** When G acts on itself by conjugation, the class equation becomes

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)],$$

where $g_1, \ldots, g_r$ are representatives of the conjugacy classes of size > 1, and $C_G(g) = \{h \in G : hg = gh\}$ is the centralizer of g.

Proof. Under conjugation, $G_g = C_G(g)$ and $X^G = Z(G)$. Apply Theorem 4.2. □

4.4 Burnside's Lemma

Definition 4.5 (Fixed-point set of an element)**.** For $g \in G$, denote $X^g = \{x \in X : g \cdot x = x\}$, the set of elements of X fixed by g.

Theorem 4.3 (Burnside's Lemma)**.** Let G be a finite group acting on a finite set X. The number of orbits is

$$|\text{orbits}| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. Count the pairs $(g, x) \in G \times X$ with $g \cdot x = x$ in two ways.

Counting by g: $\sum_{g \in G} |X^g|$.

Counting by x: $\sum_{x\in X} |G_x|$.

By the Orbit-Stabilizer Theorem, $|G_x| = |G|/|\mathcal{O}_x|$. Hence

$$\sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \sum_{x\in X} \frac{1}{|\mathcal{O}_x|}.$$

For each orbit $\mathcal{O}$, the sum $\sum_{x\in\mathcal{O}} 1/|\mathcal{O}| = 1$. Therefore

$$\sum_{x\in X} \frac{1}{|\mathcal{O}_x|} = (\text{number of orbits}).$$

Combining: $\sum_{g\in G} |X^g| = |G| \cdot |\text{orbits}|$, giving the result. □

Example 4.5 (Coloring a square). How many distinct necklaces can be made with 4 beads, each of k colors, where two necklaces are the same if one is a rotation of the other?
The cyclic group $C_4 = \{e, r, r^2, r^3\}$ acts on the set of k^4 colorings.

- $|X^e| = k^4$ (identity fixes everything),
- $|X^r| = k$ (all beads must be the same color),
- $|X^{r^2}| = k^2$ (opposite beads must match),
- $|X^{r^3}| = k$ (same as r).

By Burnside's lemma, the number of distinct necklaces is

$$\frac{1}{4}\big(k^4 + k + k^2 + k\big) = \frac{k^4 + k^2 + 2k}{4}.$$

For $k = 2$, this gives $(16 + 4 + 4)/4 = 6$ distinct necklaces.

Example 4.6 (Coloring a cube). How many ways can the faces of a cube be colored with k colors, up to rotational symmetry? The rotation group of the cube has 24 elements. Applying Burnside's lemma (partitioning the rotations by type: identity, face rotations, vertex rotations, edge rotations) yields

$$\frac{1}{24}\big(k^6 + 6k^3 + 3k^4 + 8k^2 + 6k^2\big) = \frac{k^6 + 3k^4 + 12k^3 + 8k^2}{24} \cdot \frac{24}{24}.$$

For $k = 2$, one obtains 10 essentially different colorings.

4.5 Conjugacy Classes and the Center

Definition 4.6 (Conjugacy class)**.** The *conjugacy class* of $g \in G$ is $\mathrm{Cl}(g) = \{hgh^{-1} : h \in G\}$. This is the orbit of g under the conjugation action.

Remark 4.1. The conjugacy classes partition G. An element g lies in $Z(G)$ if and only if $|\mathrm{Cl}(g)| = 1$. By the Orbit-Stabilizer Theorem, $|\mathrm{Cl}(g)| = [G : C_G(g)]$.

Theorem 4.4 (Center of a p-group is nontrivial)**.** Let p be a prime and let G be a finite group of order p^n with $n \geq 1$. Then $Z(G) \neq \{e\}$.

Proof. Apply the class equation (Corollary 4.1):

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Since $|G| = p^n$, each index $[G : C_G(g_i)]$ divides p^n and is > 1, hence $p \mid [G : C_G(g_i)]$ for each i. Since $p \mid |G|$, we deduce $p \mid |Z(G)|$. In particular $|Z(G)| \geq p > 1$. □

Theorem 4.5 (Groups of order p^2 are abelian)**.** Let p be a prime. Every group of order p^2 is abelian.

Proof. Let $|G| = p^2$. By Theorem 4.4, $Z(G) \neq \{e\}$, so $|Z(G)| \in \{p, p^2\}$.

If $|Z(G)| = p^2$, then $G = Z(G)$ and G is abelian.

If $|Z(G)| = p$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic (every group of prime order is cyclic). Let $G/Z(G) = \langle gZ(G) \rangle$. Then every element of G can be written $g^i z$ for some i and $z \in Z(G)$. For any two elements $g^i z_1$ and $g^j z_2$:

$$(g^i z_1)(g^j z_2) = g^{i+j} z_1 z_2 = g^j g^i z_2 z_1 = (g^j z_2)(g^i z_1),$$

since $z_1, z_2 \in Z(G)$. Hence G is abelian, contradicting $|Z(G)| = p < p^2 = |G|$.

Therefore $|Z(G)| = p^2$ and G is abelian. □

4.6 Cauchy's Theorem

Theorem 4.6 (Cauchy's Theorem)**.** Let G be a finite group and let p be a prime dividing $|G|$. Then G contains an element of order p.

Proof. Let $X = \{(g_1, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\}$. Note that $|X| = |G|^{p-1}$: the first $p-1$ entries may be chosen freely, and g_p is then determined as $g_p = (g_1 \cdots g_{p-1})^{-1}$.

The cyclic group $\mathbb{Z}/p\mathbb{Z}$ acts on X by cyclic permutation:

$$\bar{1} \cdot (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1).$$

This is well-defined because if $g_1 \cdots g_p = e$, then $g_2 \cdots g_p g_1 = g_1^{-1}(g_1 \cdots g_p) g_1 = g_1^{-1} e g_1 = e$.

Each orbit has size 1 or p (since $|\mathbb{Z}/p\mathbb{Z}| = p$ is prime). An orbit has size 1 if and only if $g_1 = g_2 = \cdots = g_p$, which means $g_1^p = e$.

The orbit of $(e, e, \ldots, e)$ has size 1, so there is at least one fixed point. Since $|X| = |G|^{p-1}$ and $p \mid |G|$, we have $p \mid |X|$. The fixed points are the orbits of size 1, and the remaining elements are partitioned into orbits of size p. Hence

$$|X| \equiv |\text{fixed points}| \pmod{p},$$

so $p \mid |\text{fixed points}|$. Since there is at least one fixed point $(e, \dots, e)$, there are at least p fixed points. A fixed point different from $(e, \dots, e)$ gives an element $g \neq e$ with $g^p = e$, hence $\text{ord}(g) = p$. □

4.7 Sylow Subgroups

Definition 4.7 (Sylow p-subgroup)**.** Let G be a finite group and p a prime. Write $|G| = p^n m$ where $p \nmid m$ and $n \geq 1$. A subgroup $P \leq G$ is called a *Sylow p-subgroup* if $|P| = p^n$. The set of all Sylow p-subgroups of G is denoted $\text{Syl}_p(G)$, and we write $n_p = |\text{Syl}_p(G)|$.

Definition 4.8 (p-subgroup)**.** A *p-subgroup* of G is any subgroup whose order is a power of p.

4.8 The First Sylow Theorem

Theorem 4.7 (First Sylow Theorem Existence)**.** Let G be a finite group and p a prime dividing $|G|$. Then G contains a Sylow p-subgroup.

Proof. We prove the stronger statement: for every $0 \leq k \leq n$ (where $|G| = p^n m$), G has a subgroup of order p^k. The proof is by strong induction on $|G|$.

Base case. If $|G| = 1$, the statement holds vacuously.

Inductive step. Let $|G| = p^n m$ with $n \geq 1$. Consider the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Case 1: $p \mid |Z(G)|$. By Cauchy's theorem (Theorem 4.6), $Z(G)$ contains an element z of order p. The subgroup $N = \langle z \rangle$ is normal in G (since $z \in Z(G)$). Consider G/N, which has order $|G|/p = p^{n-1}m$. By induction, G/N has a subgroup $\bar{H}$ of order p^{k-1} for each $1 \leq k \leq n$. By the Correspondence Theorem (Theorem 3.6), $\bar{H} = H/N$ for some $H \leq G$ with $N \subseteq H$. Then $|H| = |\bar{H}| \cdot |N| = p^{k-1} \cdot p = p^k$.

Case 2: $p \nmid |Z(G)|$. Then there exists a conjugacy class of size $[G : C_G(g_i)]$ with $p \nmid [G : C_G(g_i)]$. Since $p^n \mid |G|$ and $|G| = [G : C_G(g_i)] \cdot |C_G(g_i)|$, we get $p^n \mid |C_G(g_i)|$. Since $C_G(g_i)$ is a proper subgroup of G (because $g_i \notin Z(G)$), by induction $C_G(g_i)$ has a subgroup of order p^k for each $0 \leq k \leq n$. This subgroup is also a subgroup of G.

In both cases, G has subgroups of order p^k for all $0 \leq k \leq n$. In particular, G has a subgroup of order p^n. □

4.9 The Second Sylow Theorem

Lemma 4.1. Let P be a Sylow p-subgroup of G, and let Q be any p-subgroup of G. If $Q \subseteq N_G(P)$, then $Q \subseteq P$.

Proof. Since $Q \subseteq N_G(P)$, the product QP is a subgroup of G (because $P \trianglelefteq N_G(P)$). Moreover $|QP| = |Q| \cdot |P|/|Q \cap P|$. Since Q and P are both p-subgroups, $|QP|$ is a power of p. But $P \subseteq QP$ and P is a Sylow p-subgroup (maximal p-subgroup), so $QP = P$ and therefore $Q \subseteq P$. □

Theorem 4.8 (Second Sylow Theorem Conjugacy)**.** Any two Sylow p-subgroups of a finite group G are conjugate.

Proof. Let P and Q be Sylow p-subgroups of G. Let Q act on $G/P = \{gP : g \in G\}$ by left multiplication. Consider the orbits of this action. We have $|G/P| = [G : P] = m$ where $|G| = p^n m$ and $p \nmid m$.

Since Q is a p-group, every orbit has size a power of p. Since the total number of cosets is m and $p \nmid m$, there must exist an orbit of size 1, say $\{gP\}$.

This means $qgP = gP$ for all $q \in Q$, i.e., $g^{-1}qg \in P$ for all $q \in Q$, hence $g^{-1}Qg \subseteq P$. Since $|g^{-1}Qg| = |Q| = |P| = p^n$, we conclude $g^{-1}Qg = P$, so $Q = gPg^{-1}$. □

4.10 The Third Sylow Theorem

Theorem 4.9 (Third Sylow Theorem Counting)**.** Let G be a finite group of order $p^n m$ with $p \nmid m$. Then

1. $n_p \equiv 1 \pmod{p}$,
2. $n_p \mid m$.

Proof. Let $\mathcal{S} = \mathrm{Syl}_p(G)$, so $n_p = |\mathcal{S}|$. Fix a Sylow p-subgroup $P \in \mathcal{S}$.

Proof that $n_p \mid m$: G acts on $\mathcal{S}$ by conjugation. By the Second Sylow Theorem (Theorem 4.8), this action is transitive (there is a single orbit). By the Orbit-Stabilizer Theorem, $n_p = |\mathcal{S}| = [G : G_P]$ where $G_P = N_G(P)$ is the stabilizer of P under conjugation. Since $P \subseteq N_G(P)$, we have $p^n \mid |N_G(P)|$, so $n_p = |G|/|N_G(P)| \mid |G|/p^n = m$.

Proof that $n_p \equiv 1 \pmod{p}$: Let P act on $\mathcal{S}$ by conjugation. The fixed points of this action are those $Q \in \mathcal{S}$ with $P \subseteq N_G(Q)$. By Lemma 4.1, this implies $P \subseteq Q$, and since $|P| = |Q| = p^n$, we get $P = Q$.

Therefore P is the unique fixed point. All other orbits under the P-action have size divisible by p (since P is a p-group). Hence

$$n_p = |\mathcal{S}| \equiv 1 \pmod{p}.$$

□

Corollary 4.2 (Normality criterion)**.** A Sylow p-subgroup P of G is normal in G if and only if $n_p = 1$.

Proof. $P \trianglelefteq G$ iff $gPg^{-1} = P$ for all g, iff P is the unique Sylow p-subgroup, iff $n_p = 1$. □

4.11 Applications of the Sylow Theorems

Theorem 4.10 (Groups of order pq)**.** Let $p < q$ be distinct primes. Then:

1. Every group of order pq has a unique (hence normal) Sylow q-subgroup.
2. If $p \nmid (q-1)$, then every group of order pq is cyclic.
3. If $p \mid (q-1)$, then there exists a non-abelian group of order pq, and it is unique up to isomorphism.

Proof. Let $|G| = pq$.

(1) By the Third Sylow Theorem, $n_q \mid p$ and $n_q \equiv 1 \pmod{q}$. Since $p < q$, the only possibility is $n_q = 1$. Hence there is a unique Sylow q-subgroup Q, and $Q \trianglelefteq G$.

(2) Similarly $n_p \mid q$ and $n_p \equiv 1 \pmod{p}$, so $n_p \in \{1, q\}$. If $p \nmid (q-1)$, then $q \not\equiv 1 \pmod{p}$, forcing $n_p = 1$. Let P be the unique Sylow p-subgroup. Then $P \cap Q = \{e\}$ (since $\gcd(p,q) = 1$), $|PQ| = pq = |G|$, and both are normal, so $G \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

(3) If $p \mid (q-1)$, then $n_p = q$ is possible. One can construct the non-abelian group as a semidirect product $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ using a nontrivial homomorphism $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ (which exists since $p \mid (q-1)$). Uniqueness follows from the fact that all nontrivial homomorphisms $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ yield isomorphic semidirect products. □

Example 4.7 (Classification of groups of order 15). We have $15 = 3 \cdot 5$ with $p = 3 < q = 5$. Since $3 \nmid (5-1) = 4$, Theorem 4.10(2) applies: every group of order 15 is cyclic. Thus $\mathbb{Z}/15\mathbb{Z}$ is the unique group of order 15 (up to isomorphism).

Theorem 4.11 (No simple group of order 12)**.** There is no simple group of order 12.

Proof. Let $|G| = 12 = 2^2 \cdot 3$. We have $n_3 \mid 4$ and $n_3 \equiv 1 \pmod{3}$, so $n_3 \in \{1, 4\}$.

Case 1: $n_3 = 1$. The unique Sylow 3-subgroup is normal, so G is not simple.

Case 2: $n_3 = 4$. Then G acts by conjugation on the four Sylow 3-subgroups, giving a homomorphism $\varphi\colon G \to S_4$. The kernel $K = \ker \varphi$ is a normal subgroup of G.

If $K = G$, every element normalizes every Sylow 3-subgroup, so each is normal, contradicting $n_3 = 4$.

If $K = \{e\}$, then G embeds into S_4. The four Sylow 3-subgroups contribute $4 \times 2 = 8$ elements of order 3 (they pairwise intersect trivially since each has order 3). The remaining $12 - 8 = 4$ elements must include the identity and form the unique Sylow 2-subgroup (of order 4). Hence $n_2 = 1$, and this Sylow 2-subgroup is normal in G, so G is not simple.

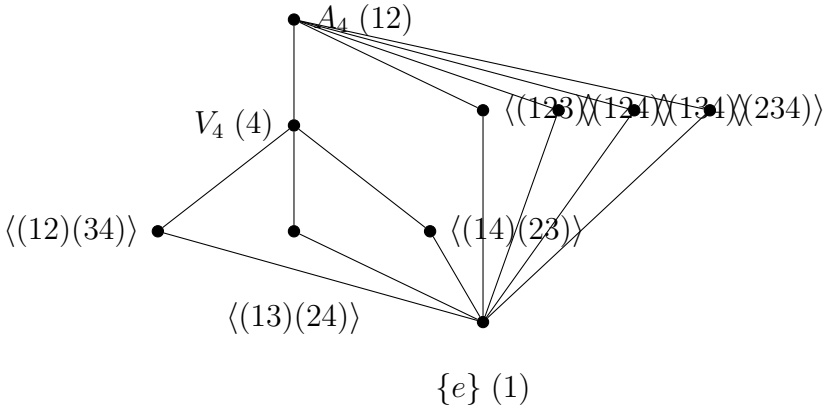
If $\{e\} \subsetneq K \subsetneq G$, then K is a nontrivial proper normal subgroup, so G is not simple.

In all cases, G is not simple. □

Example 4.8 (Groups of order p^2q). Let p and q be distinct primes with $p > q$. Consider $|G| = p^2q$. Then $n_p \mid q$ and $n_p \equiv 1 \pmod{p}$. Since $p > q$, the only divisor of q that is $\equiv 1 \pmod{p}$ is 1. Hence $n_p = 1$ and G has a normal Sylow p-subgroup.

4.12 Subgroup Lattice with Sylow Subgroups

As an illustration, consider $G = A_4$ of order $12 = 2^2 \cdot 3$. The Sylow 2-subgroup is the Klein four-group $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$, which is normal ($n_2 = 1$). There are $n_3 = 4$ Sylow 3-subgroups, each of order 3.



In this lattice, V_4 (the unique Sylow 2-subgroup) is normal in A_4, while each $\langle(abc)\rangle$ is a Sylow 3-subgroup.

4.13 Exercises

Exercise 4.1. Verify that the conjugation action of S_3 on itself satisfies the action axioms. List all orbits (conjugacy classes) of S_3.

Exercise 4.2. Let D_4 (the dihedral group of order 8) act on the set $\{1, 2, 3, 4\}$ of vertices of a square. For each vertex, determine the orbit and stabilizer, and verify the Orbit-Stabilizer Theorem.

Exercise 4.3. Use Burnside's lemma to count the number of distinct necklaces with 6 beads and 2 colors, under the action of the cyclic group C_6.

Exercise 4.4. Use Burnside's lemma to determine the number of distinct ways to color the faces of a regular tetrahedron with 3 colors, up to rotational symmetry.

Exercise 4.5. Let G be a group of order p^3 where p is prime. Show that $|Z(G)| \in \{p, p^2, p^3\}$ and that $G/Z(G)$ cannot be cyclic of order p^2.

Exercise 4.6. Let G be a finite group of even order. Use Cauchy's theorem to show that G contains an element of order 2.

Exercise 4.7. Let $|G| = 20 = 2^2 \cdot 5$. Determine the possible values of n_5 and n_2. Show that G has a normal Sylow 5-subgroup.

Exercise 4.8. Show that there is no simple group of order 30.

Exercise 4.9. Show that there is no simple group of order $56 = 2^3 \cdot 7$.

Exercise 4.10. Let $P \in \mathrm{Syl}_p(G)$. Show that $P \trianglelefteq N_G(P)$ and that $N_G(N_G(P)) = N_G(P)$.

Exercise 4.11. Let P be a Sylow p-subgroup of a finite group G. Show that $[G : P] \equiv 1 \pmod{p}$ is not necessarily true, but $[N_G(P) : P] \not\equiv 0 \pmod{p}$.

Exercise 4.12. Use the Sylow theorems to classify all groups of order 6 up to isomorphism. (There are exactly two: $\mathbb{Z}/6\mathbb{Z}$ and S_3.)

Exercise 4.13. Let G be a group of order $48 = 2^4 \cdot 3$. Suppose $n_2 = 3$. Show that there exist two distinct Sylow 2-subgroups P_1, P_2 with $|P_1 \cap P_2| \geq 4$.

Exercise 4.14. Let G act on a set X. Show that the kernel of the action is the largest normal subgroup of G contained in every stabilizer G_x, $x \in X$.

Chapter Summary

- A **group action** of G on X is equivalent to a homomorphism $G \to \mathrm{Sym}(X)$.
- **Orbits** partition X; the **Orbit-Stabilizer Theorem** gives $|\mathcal{O}_x| = [G : G_x]$.
- The **Class Equation** $|X| = |X^G| + \sum [G : G_{x_i}]$ is a fundamental counting tool.
- **Burnside's Lemma**: the number of orbits equals $\frac{1}{|G|} \sum_g |X^g|$.
- The center of a **p-group** is nontrivial; groups of order p^2 are abelian.
- **Cauchy's Theorem**: if $p \mid |G|$, then G has an element of order p.
- **Sylow's Theorems**: if $|G| = p^n m$ with $p \nmid m$, then
  1. Sylow p-subgroups (of order p^n) exist.
  2. All Sylow p-subgroups are conjugate.
  3. $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.
- Applications include classifying groups of small order and proving non-simplicity results.

Chapter 5

Rings

5.1 Basic definitions

Definition 5.1 (Ring)**.** A **ring** is a triple $(R, +, \cdot)$ where R is a non-empty set equipped with two binary operations, addition $+ \colon R \times R \to R$ and multiplication $\cdot \colon R \times R \to R$, satisfying the following axioms:

(i) $(R, +)$ is an abelian group, with identity element denoted 0_R (or simply 0);

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

$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

(iii) Multiplication distributes over addition: for all $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Definition 5.2 (Ring with unity, commutative ring)**.** A ring R is said to be a **ring with unity** (or a **unital ring**) if there exists an element $1_R \in R$ (called the **unity** or **multiplicative identity**) such that

$$1_R \cdot a = a \cdot 1_R = a \quad \text{for all } a \in R.$$

A ring R is **commutative** if $a \cdot b = b \cdot a$ for all $a, b \in R$.

Throughout this text, *all rings are assumed to be unital* unless stated otherwise. We write ab for $a \cdot b$ when no ambiguity arises.

Proposition 5.1 (Elementary properties of rings)**.** Let R be a ring. For all $a, b \in R$:

(i) $0 \cdot a = a \cdot 0 = 0$;

(ii) $(-a) \cdot b = a \cdot (-b) = -(ab)$;

(iii) $(-a)(-b) = ab$;

(iv) If R has unity 1_R, then $(-1_R) \cdot a = -a$.

Proof. **(i)** We have $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Adding $-(0 \cdot a)$ to both sides yields $0 = 0 \cdot a$. The identity $a \cdot 0 = 0$ follows by the same argument using right distributivity.

(ii) We compute $(-a)b + ab = (-a+a)b = 0 \cdot b = 0$ by (i). Therefore $(-a)b = -(ab)$. Similarly, $a(-b) + ab = a(-b+b) = a \cdot 0 = 0$, so $a(-b) = -(ab)$.

(iii) By (ii), $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, since $-(-x) = x$ in any abelian group.

(iv) By (ii), $(-1_R)a = -(1_R \cdot a) = -a$. □

Proposition 5.2 (Uniqueness of unity)**.** If a ring R has a unity, it is unique.

Proof. Suppose 1 and $1'$ are both unities of R. Then $1 = 1 \cdot 1' = 1'$, since $1'$ is a right identity and 1 is a left identity. □

5.2 Examples of rings

Example 5.1 (Classical rings). The following are commutative rings with unity:

(a) $(\mathbb{Z}, +, \cdot)$, the ring of integers.

(b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, the fields of rationals, reals, and complex numbers.

(c) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ for any integer $n \geq 1$, the ring of integers modulo n.

(d) For a field K, the polynomial ring $K[X]$ with the usual addition and multiplication of polynomials.

Example 5.2 (Matrix rings). For a field K and an integer $n \geq 1$, the set $M_n(K)$ of $n \times n$ matrices with entries in K forms a ring with unity (the identity matrix I_n). For $n \geq 2$, this ring is *not* commutative. For instance, in $M_2(\mathbb{R})$,

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

Example 5.3 (Gaussian integers). The set $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a commutative ring with unity 1, called the ring of **Gaussian integers**. Addition and multiplication are inherited from $\mathbb{C}$.

Example 5.4 (Rings of algebraic integers). For a square-free integer d, the set

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

is a commutative ring with unity. The ring operations follow from the relation $(\sqrt{d})^2 = d$.

Example 5.5 (Formal power series). For a field K, the set $K[[X]]$ of formal power

series

$$K[[X]] = \left\{ \sum_{n=0}^{\infty} a_n X^n : a_n \in K \right\}$$

is a commutative ring with unity, where addition and multiplication are defined by

$$\sum a_n X^n + \sum b_n X^n = \sum (a_n + b_n) X^n, \qquad \left(\sum a_n X^n\right)\left(\sum b_n X^n\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n.$$

The polynomial ring $K[X]$ embeds naturally into $K[[X]]$.

Example 5.6 (Group ring). Let R be a commutative ring with unity and G a finite group. The **group ring** $R[G]$ consists of all formal sums $\sum_{g \in G} a_g\, g$ with $a_g \in R$, equipped with addition

$$\sum_{g \in G} a_g\, g + \sum_{g \in G} b_g\, g = \sum_{g \in G} (a_g + b_g)\, g$$

and multiplication induced by the group operation and extended by linearity:

$$\left(\sum_{g \in G} a_g\, g \right) \left(\sum_{h \in G} b_h\, h \right) = \sum_{g,h \in G} a_g b_h\, (gh).$$

The unity of $R[G]$ is $1_R \cdot e_G$, where e_G is the identity of G.

5.3 Zero divisors, integral domains, and units

Definition 5.3 (Zero divisor)**.** Let R be a ring. A non-zero element $a \in R$ is called a **left zero divisor** if there exists a non-zero $b \in R$ with $ab = 0$, and a **right zero divisor** if there exists a non-zero $c \in R$ with $ca = 0$. An element that is both a left and right zero divisor is simply called a **zero divisor**.
In a commutative ring, left and right zero divisors coincide, and we speak simply of zero divisors.

Example 5.7. In $\mathbb{Z}/6\mathbb{Z}$, we have $\bar{2} \cdot \bar{3} = \bar{0}$, so $\bar{2}$ and $\bar{3}$ are zero divisors. In $M_2(\mathbb{R})$, the matrices $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ satisfy $AB = 0$, so they are zero divisors.

Definition 5.4 (Integral domain)**.** A commutative ring R with unity $1_R \neq 0_R$ is called an **integral domain** if it has no zero divisors, that is, for all $a, b \in R$:

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

Example 5.8. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i]$, and $K[X]$ (for any field K) are integral domains. The ring $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

Proposition 5.3 (Cancellation in integral domains)**.** Let R be an integral domain. For all $a, b, c \in R$ with $a \neq 0$:

$$ab = ac \implies b = c.$$

Proof. If $ab = ac$, then $a(b - c) = 0$. Since R is an integral domain and $a \neq 0$, we must have $b - c = 0$, hence $b = c$. □

Definition 5.5 (Unit, group of units)**.** An element a of a ring R (with unity) is called a **unit** (or **invertible element**) if there exists $b \in R$ such that $ab = ba = 1_R$. The element b is unique and is denoted a^{-1}. The set of all units of R is denoted $U(R)$ (or $R^\times$) and forms a group under multiplication, called the **group of units** of R.

Example 5.9. (a) $U(\mathbb{Z}) = \{1, -1\}$.

(b) $U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{a} : \gcd(a, n) = 1\}$, with $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$ (Euler's totient).

(c) $U(K[X]) = K^\times = K \setminus \{0\}$ for any field K.

(d) $U(M_n(K)) = \mathrm{GL}_n(K)$, the general linear group.

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

(f) A field K is precisely a commutative ring with unity in which $U(K) = K \setminus \{0\}$.

Proposition 5.4. In a ring with unity, a unit is never a zero divisor.

Proof. Suppose $a \in R$ is a unit and $ab = 0$. Then $b = 1 \cdot b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Similarly for left zero divisors. □

Proposition 5.5 (Finite integral domains are fields)**.** Every finite integral domain is a field.

Proof. Let R be a finite integral domain with $|R| = n$ and let $a \in R \setminus \{0\}$. Consider the map $\varphi_a \colon R \to R$ defined by $\varphi_a(r) = ar$. This map is injective: if $ar_1 = ar_2$ then $a(r_1 - r_2) = 0$, and since $a \neq 0$ and R is an integral domain, $r_1 = r_2$. Since R is finite, an injective map from R to itself is surjective. In particular, there exists $b \in R$ with $ab = 1_R$. By commutativity, $ba = ab = 1_R$, so a is a unit. □

Corollary 5.1. $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime.

Proof. If p is prime and $\bar{a}\bar{b} = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$, then $p \mid ab$, so $p \mid a$ or $p \mid b$ (Euclid's lemma), meaning $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. Hence $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. Being finite, it is a field by Proposition 5.5. Conversely, if $p = mn$ with $1 < m, n < p$, then $\bar{m}\bar{n} = \bar{0}$ with $\bar{m}, \bar{n} \neq \bar{0}$, so $\mathbb{Z}/p\mathbb{Z}$ has zero divisors and is not a field. □

5.4 Ideals

Definition 5.6 (Ideal)**.** Let R be a ring. A non-empty subset $I \subseteq R$ is called:

- a **left ideal** if I is an additive subgroup of R and $ra \in I$ for all $r \in R$, $a \in I$;
- a **right ideal** if I is an additive subgroup of R and $ar \in I$ for all $a \in I$, $r \in R$;
- a **(two-sided) ideal** if I is both a left and a right ideal.

In a commutative ring, all three notions coincide.

Proposition 5.6 (Ideal test)**.** A non-empty subset I of a commutative ring R is an ideal if and only if:

(i) for all $a, b \in I$, $a - b \in I$;

(ii) for all $r \in R$ and $a \in I$, $ra \in I$.

Proof. Condition (i) is exactly the subgroup criterion for $(I, +)$: since $I \neq \varnothing$, pick $a \in I$; then $0 = a - a \in I$; then $-b = 0 - b \in I$ for all $b \in I$; then $a + b = a - (-b) \in I$. Together with (ii), this gives an ideal. Conversely, both conditions are necessary by the definition of an ideal. □

Definition 5.7 (Principal ideal, generated ideal)**.** Let R be a commutative ring with unity.

(i) For $a \in R$, the **principal ideal generated by** a is

$$(a) = aR = \{ar : r \in R\}.$$

(ii) More generally, for $a_1, \ldots, a_n \in R$, the **ideal generated by** $a_1, \ldots, a_n$ is

$$(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} r_i a_i : r_i \in R \right\}.$$

This is the smallest ideal of R containing $a_1, \ldots, a_n$.

Example 5.10. (a) In $\mathbb{Z}$, every ideal is principal: the ideals of $\mathbb{Z}$ are exactly $n\mathbb{Z} = (n)$ for $n \geq 0$.

(b) In $K[X]$, every ideal is principal (proved later in Chapter 7).

(c) $\{0\} = (0)$ and $R = (1)$ are ideals of any ring R, called the **trivial ideals**.

(d) An ideal I of R satisfies $I = R$ if and only if I contains a unit.

(e) In $\mathbb{Z}[X]$, the ideal $(2, X) = \{f \in \mathbb{Z}[X] : f(0) \text{ is even}\}$ is not principal.

5.5 Operations on ideals

Proposition 5.7 (Operations on ideals)**.** Let I and J be ideals of a commutative ring R.

(i) The **intersection** $I \cap J$ is an ideal of R.

(ii) The **sum** $I + J = \{a + b : a \in I, b \in J\}$ is an ideal of R. It is the smallest ideal containing both I and J.

(iii) The **product** IJ is the ideal generated by all products ab with $a \in I$, $b \in J$:

$$IJ = \left\{ \sum_{k=1}^{n} a_k b_k : n \geq 1,\ a_k \in I,\ b_k \in J \right\}.$$

We have $IJ \subseteq I \cap J$.

Proof. **(i)** $I \cap J$ is non-empty since $0 \in I \cap J$. If $a, b \in I \cap J$, then $a - b \in I$ (since I is an ideal) and $a - b \in J$ (since J is an ideal), so $a - b \in I \cap J$. For $r \in R$ and $a \in I \cap J$, we have $ra \in I$ and $ra \in J$, hence $ra \in I \cap J$.

(ii) $I + J$ is non-empty since $0 = 0 + 0 \in I + J$. If $a_1 + b_1, a_2 + b_2 \in I + J$ (with $a_i \in I$, $b_i \in J$), then $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$. For $r \in R$ and $a + b \in I + J$, $r(a + b) = ra + rb \in I + J$ since $ra \in I$ and $rb \in J$.

(iii) It is straightforward to verify that IJ, as defined, is an ideal. For the inclusion $IJ \subseteq I \cap J$: each generator ab with $a \in I$, $b \in J$ satisfies $ab \in I$ (since I is an ideal and $b \in R$) and $ab \in J$ (since J is an ideal and $a \in R$). So $ab \in I \cap J$, and since $I \cap J$ is an ideal (by (i)), all finite sums of such products also lie in $I \cap J$. □

Example 5.11. In $\mathbb{Z}$: $(m) + (n) = (\gcd(m, n))$, $(m) \cap (n) = (\operatorname{lcm}(m, n))$, and $(m)(n) = (mn)$.

5.6 Prime ideals

Definition 5.8 (Prime ideal)**.** An ideal P of a commutative ring R is **prime** if $P \neq R$ and for all $a, b \in R$:

$$ab \in P \implies a \in P \text{ or } b \in P.$$

Theorem 5.1 (Characterization of prime ideals)**.** Let R be a commutative ring with unity and let P be an ideal of R. Then P is a prime ideal if and only if the quotient ring R/P is an integral domain.

Proof. Recall that the quotient ring R/P has elements $\bar{r} = r + P$ and satisfies $\bar{r}\bar{s} = \overline{rs}$, and R/P is non-trivial (i.e., $\bar{0} \neq \bar{1}$) if and only if $P \neq R$.

($\Rightarrow$) Suppose P is prime. Then $P \neq R$, so R/P is a non-trivial commutative ring with unity $\bar{1}$. Suppose $\bar{a}\bar{b} = \bar{0}$ in R/P. Then $\overline{ab} = \bar{0}$, so $ab \in P$. Since P is prime, $a \in P$ or $b \in P$, i.e., $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. Hence R/P is an integral domain.

($\Leftarrow$) Suppose R/P is an integral domain. Then R/P is non-trivial, so $P \neq R$. If $ab \in P$, then $\bar{a}\bar{b} = \overline{ab} = \bar{0}$ in R/P. Since R/P has no zero divisors, $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, i.e.,

$a \in P$ or $b \in P$. Hence P is prime. □

Example 5.12. (a) In $\mathbb{Z}$, the prime ideals are (0) and (p) for p prime.

(b) In $K[X]$ (for a field K), the prime ideals are (0) and (f) for irreducible $f \in K[X]$.

5.7 Maximal ideals

Definition 5.9 (Maximal ideal)**.** An ideal M of a ring R is **maximal** if $M \neq R$ and there is no ideal I of R with $M \subsetneq I \subsetneq R$.

Theorem 5.2 (Characterization of maximal ideals)**.** Let R be a commutative ring with unity and let M be an ideal of R. Then M is a maximal ideal if and only if R/M is a field.

Proof. ($\Rightarrow$) Suppose M is maximal. Then $M \neq R$, so R/M is a non-trivial commutative ring with unity. We must show every non-zero element of R/M is a unit. Let $\bar{a} \neq \bar{0}$ in R/M, i.e., $a \notin M$. Consider the ideal $M + (a) = \{m + ra : m \in M, r \in R\}$. This is an ideal containing M and a. Since $a \notin M$, we have $M \subsetneq M + (a)$. By maximality of M, $M + (a) = R$. In particular, $1 \in M + (a)$, so there exist $m \in M$ and $r \in R$ with $1 = m + ra$. Passing to R/M:

$$\bar{1} = \bar{m} + \bar{r}\bar{a} = \bar{0} + \bar{r}\bar{a} = \bar{r}\bar{a}.$$

Hence $\bar{a}$ is a unit with inverse $\bar{r}$, and R/M is a field.

($\Leftarrow$) Suppose R/M is a field. Then R/M is non-trivial, so $M \neq R$. Let I be an ideal with $M \subseteq I \subseteq R$ and $I \neq M$. Pick $a \in I \setminus M$. Then $\bar{a} \neq \bar{0}$ in R/M. Since R/M is a field, there exists $\bar{r} \in R/M$ with $\bar{r}\bar{a} = \bar{1}$. This means $ra - 1 \in M \subseteq I$. Since $a \in I$ and I is an ideal, $ra \in I$. Then $1 = ra - (ra - 1) \in I$, so $I = R$. Hence M is maximal. □

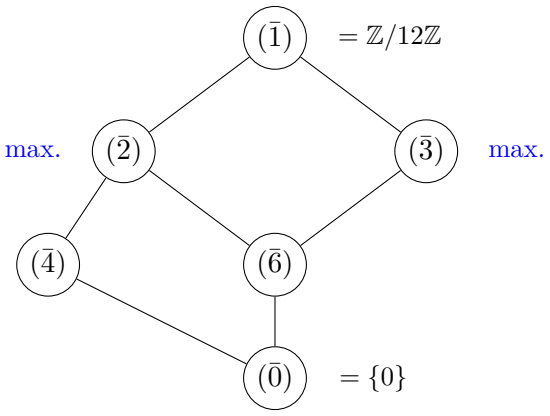
Theorem 5.3 (Maximal implies prime)**.** Every maximal ideal of a commutative ring with unity is prime.

Proof. Let M be a maximal ideal of R. By Theorem 5.2, R/M is a field. Every field is an integral domain (it has no zero divisors, since every non-zero element is a unit; see Proposition 5.4). By Theorem 5.1, M is prime. □

Remark 5.1. The converse of Theorem 5.3 is false in general. For instance, (0) is a prime ideal of $\mathbb{Z}$ (since $\mathbb{Z}$ is an integral domain) but not maximal (since $(0) \subsetneq (2) \subsetneq \mathbb{Z}$).

5.8 Ideal lattice of $\mathbb{Z}/12\mathbb{Z}$

The ideals of $\mathbb{Z}/12\mathbb{Z}$ correspond to the divisors of 12. Ordering by inclusion, they form the following lattice.



The maximal ideals are $(\bar{2})$ and $(\bar{3})$, corresponding to the prime divisors of 12. These are also the prime ideals (consistent with Theorem 5.3). The non-prime ideals are $(\bar{4})$, $(\bar{6})$, and $(\bar{0})$: for instance, $\bar{2} \cdot \bar{2} = \bar{4} \in (\bar{4})$ but $\bar{2} \notin (\bar{4})$.

5.9 Exercises

Exercise 5.1. Let R be a ring with unity. Prove that if $1_R = 0_R$, then $R = \{0\}$.

Exercise 5.2. Show that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.

Exercise 5.3. Find all the units of $\mathbb{Z}/12\mathbb{Z}$ and determine the structure of the group $U(\mathbb{Z}/12\mathbb{Z})$.

Exercise 5.4. Let R be a commutative ring. Show that the set $\mathrm{Nil}(R) = \{a \in R : a^n = 0 \text{ for some } n \geq 1\}$ is an ideal of R (the **nilradical**).

Exercise 5.5. Let I and J be ideals of a commutative ring R. Show that $I \cup J$ is an ideal if and only if $I \subseteq J$ or $J \subseteq I$.

Exercise 5.6. Prove that the ideal $(2, X)$ in $\mathbb{Z}[X]$ is not principal.

Exercise 5.7. Let R be a commutative ring and I an ideal. Show that $\sqrt{I} = \{a \in R : a^n \in I \text{ for some } n \geq 1\}$ is an ideal of R containing I (the **radical** of I). Show that $\sqrt{I} = \bigcap_{P \supseteq I} P$, where P ranges over all prime ideals containing I.

Exercise 5.8. Find all prime and maximal ideals of $\mathbb{Z}/30\mathbb{Z}$.

Exercise 5.9. Show that $U(K[[X]]) = \{f \in K[[X]] : f(0) \neq 0\}$, where K is a field.

Exercise 5.10. Let R be a commutative ring with unity, and let P be an ideal such that R/P is finite and has no zero divisors. Show that P is maximal. *(Hint: use Proposition 5.5.)*

Exercise 5.11. Let $\varphi\colon R \to S$ be a ring homomorphism and let Q be a prime ideal of S. Show that $\varphi^{-1}(Q)$ is a prime ideal of R. Is the same true for maximal ideals?

Chapter 5 Summary. A ring is an abelian group with a compatible associative multiplication. Key structures include zero divisors, units, and integral domains (commutative rings without zero divisors). Ideals generalize normal subgroups: they are additive subgroups closed under multiplication by ring elements. Ideals can be added, multiplied, and intersected. The quotient R/P is an integral domain iff P is prime, and R/M is a field iff M is maximal. Every maximal ideal is prime.

Chapter 6

Quotient Rings, Integral Domains, and Fields of Fractions

6.1 Construction of the quotient ring

Definition 6.1 (Quotient ring)**.** Let R be a ring and I an ideal of R. The **quotient ring** R/I is the set of cosets

$$R/I = \{a + I : a \in R\}$$

equipped with the operations

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I)(b + I) = ab + I.$$

Theorem 6.1 (Well-definedness of the quotient ring)**.** Let R be a ring and I an ideal of R. The operations on R/I defined above are well-defined, and R/I is a ring. If R is commutative with unity, then so is R/I (with unity $1 + I$). Moreover, the **canonical projection** $\pi\colon R \to R/I$ defined by $\pi(a) = a + I$ is a surjective ring homomorphism with kernel I.

Proof. **Well-definedness.** Suppose $a + I = a' + I$ and $b + I = b' + I$, i.e., $a - a' \in I$ and $b - b' \in I$. For addition: $(a+b)-(a'+b') = (a-a')+(b-b') \in I$, so $(a+b)+I = (a'+b')+I$. For multiplication:

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b').$$

Since I is an ideal, $(a - a')b \in I$ and $a'(b - b') \in I$, so $ab - a'b' \in I$ and $ab + I = a'b' + I$.

Ring axioms. The set R/I inherits the abelian group structure on the quotient group $(R/I, +)$, with identity $0 + I = I$. Associativity and distributivity of multiplication follow directly from those in R:

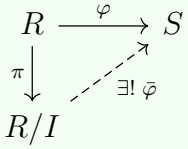
$$\begin{aligned}((a + I)(b + I))(c + I) &= (ab + I)(c + I) = (ab)c + I = a(bc) + I \\ &= (a + I)(bc + I) = (a + I)((b + I)(c + I)).\end{aligned}$$

Distributivity is checked similarly.

If R has unity 1_R, then $1_R + I$ is the unity of R/I: $(1_R + I)(a + I) = 1_R \cdot a + I = a + I$. Commutativity is inherited similarly.

Projection. $\pi(a+b) = (a+b)+I = (a+I)+(b+I) = \pi(a)+\pi(b)$ and $\pi(ab) = ab+I = (a+I)(b+I) = \pi(a)\pi(b)$. Also $\pi(1_R) = 1_R + I$. Surjectivity is clear, and $\ker\pi = \{a \in R : a+I = I\} = I$. □

Proposition 6.1 (Universal property of quotient rings)**.** Let R be a ring, I an ideal, and $\pi\colon R \to R/I$ the canonical projection. For every ring homomorphism $\varphi\colon R \to S$ with $I \subseteq \ker\varphi$, there exists a unique ring homomorphism $\bar{\varphi}\colon R/I \to S$ such that $\varphi = \bar{\varphi}\circ\pi$.



Moreover, $\bar{\varphi}$ is injective if and only if $\ker\varphi = I$, and surjective if and only if φ is surjective.

Proof. Define $\bar{\varphi}(a+I) = \varphi(a)$. This is well-defined: if $a+I = a'+I$, then $a-a' \in I \subseteq \ker\varphi$, so $\varphi(a) = \varphi(a')$. It is a ring homomorphism since φ is, and $\bar{\varphi}\circ\pi = \varphi$ by construction. Uniqueness: if $\psi\circ\pi = \varphi$, then $\psi(a+I) = \psi(\pi(a)) = \varphi(a) = \bar{\varphi}(a+I)$ for all a.

For injectivity: $\ker\bar{\varphi} = \{a+I : \varphi(a) = 0\} = \ker\varphi/I$. So $\bar{\varphi}$ is injective iff $\ker\varphi/I = \{I\}$ iff $\ker\varphi = I$. Surjectivity of $\bar{\varphi}$ is equivalent to that of φ since π is surjective. □

6.2 Isomorphism theorems for rings

Theorem 6.2 (First isomorphism theorem for rings)**.** Let $\varphi\colon R \to S$ be a ring homomorphism. Then $\ker\varphi$ is an ideal of R, $\operatorname{im}\varphi$ is a subring of S, and

$$R/\ker\varphi \cong \operatorname{im}\varphi.$$

Proof. That $\ker\varphi$ is an ideal: it is an additive subgroup (as for group homomorphisms), and if $a \in \ker\varphi$ and $r \in R$, then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\cdot 0 = 0$, so $ra \in \ker\varphi$.

Let $I = \ker\varphi$. By the universal property (Proposition 6.1), the induced map $\bar{\varphi}\colon R/I \to S$ satisfies $\bar{\varphi}(a+I) = \varphi(a)$. Since $\ker\varphi = I$, $\bar{\varphi}$ is injective. Its image is $\operatorname{im}\varphi$, so $\bar{\varphi}$ restricts to an isomorphism $R/I \xrightarrow{\sim} \operatorname{im}\varphi$. □

Theorem 6.3 (Second isomorphism theorem for rings)**.** Let R be a ring, S a subring, and I an ideal of R. Then $S+I$ is a subring of R, $S\cap I$ is an ideal of S, and

$$S/(S\cap I) \cong (S+I)/I.$$

Proof. First, $S+I = \{s+a : s \in S,\ a \in I\}$ is a subring: it is closed under subtraction $((s_1+a_1)-(s_2+a_2) = (s_1-s_2)+(a_1-a_2) \in S+I)$ and multiplication $((s_1+a_1)(s_2+a_2) = s_1s_2 + s_1a_2 + a_1s_2 + a_1a_2$; here $s_1s_2 \in S$ and the remaining terms lie in I).

That $S\cap I$ is an ideal of S is immediate.

Define $\varphi\colon S \to (S+I)/I$ by $\varphi(s) = s+I$. This is a ring homomorphism (restriction of π). It is surjective: for $s+a+I \in (S+I)/I$ (with $s \in S$, $a \in I$), we have $s+a+I = s+I = \varphi(s)$. Its kernel is $\{s \in S : s \in I\} = S\cap I$. By the first isomorphism theorem, $S/(S\cap I) \cong (S+I)/I$. □

Theorem 6.4 (Third isomorphism theorem for rings)**.** Let R be a ring and $I \subseteq J$ ideals of R. Then J/I is an ideal of R/I, and

$$(R/I)/(J/I) \cong R/J.$$

Proof. That $J/I = \{a + I : a \in J\}$ is an ideal of R/I: for $a + I \in J/I$ and $r + I \in R/I$, $(r + I)(a + I) = ra + I \in J/I$ since $ra \in J$.

Define $\varphi\colon R/I \to R/J$ by $\varphi(a + I) = a + J$. This is well-defined: if $a + I = a' + I$, then $a - a' \in I \subseteq J$, so $a + J = a' + J$. It is a surjective ring homomorphism, and $\ker \varphi = \{a + I : a \in J\} = J/I$. By the first isomorphism theorem, $(R/I)/(J/I) \cong R/J$. □

Theorem 6.5 (Correspondence theorem for rings)**.** Let R be a ring and I an ideal. There is an inclusion-preserving bijection between ideals of R/I and ideals of R containing I, given by $J \mapsto J/I$ and $\bar{J} \mapsto \pi^{-1}(\bar{J})$.

Proof. This follows from the corresponding result for groups (applied to the additive groups) together with the observation that the additional multiplicative absorption property of ideals is preserved under both π and π^{-1}. □

6.3 The Chinese Remainder Theorem

Definition 6.2 (Coprime ideals)**.** Two ideals I and J of a ring R are **coprime** (or **comaximal**) if $I + J = R$.

Theorem 6.6 (Chinese Remainder Theorem)**.** Let R be a commutative ring with unity and let $I_1, \ldots, I_n$ be pairwise coprime ideals (i.e., $I_j + I_k = R$ for all $j \neq k$). Then:

(i) $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$;

(ii) The natural ring homomorphism

$$\Phi\colon R/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

defined by $\Phi(r + \bigcap I_k) = (r + I_1, \ldots, r + I_n)$ is an isomorphism.

Proof. We first treat the case $n = 2$.

Step 1: $I_1 \cap I_2 = I_1 I_2$. We already know $I_1 I_2 \subseteq I_1 \cap I_2$ (Proposition 5.7). For the reverse inclusion: since $I_1 + I_2 = R$, there exist $a \in I_1$ and $b \in I_2$ with $a + b = 1$. For any $x \in I_1 \cap I_2$, we have

$$x = x \cdot 1 = x(a + b) = xa + xb.$$

Now $xa \in I_2 I_1 = I_1 I_2$ (since $x \in I_2$, $a \in I_1$) and $xb \in I_1 I_2$ (since $x \in I_1$, $b \in I_2$). Thus $x \in I_1 I_2$.

Step 2: The isomorphism. Define $\varphi\colon R \to R/I_1 \times R/I_2$ by $\varphi(r) = (r + I_1, r + I_2)$. This is a ring homomorphism with $\ker \varphi = I_1 \cap I_2$.

Surjectivity. Let $(r_1 + I_1, r_2 + I_2) \in R/I_1 \times R/I_2$. Since $I_1 + I_2 = R$, write $a + b = 1$

with $a \in I_1$, $b \in I_2$. Set $r = r_2a + r_1b$. Then:

$$r - r_1 = r_2a + r_1b - r_1 = r_2a + r_1(b-1) = r_2a - r_1a = (r_2 - r_1)a \in I_1,$$

so $r + I_1 = r_1 + I_1$. Similarly, $r - r_2 = r_2(a-1) + r_1b - r_2 = -r_2b + r_1b = (r_1 - r_2)b \in I_2$, so $r + I_2 = r_2 + I_2$. Hence $\varphi(r) = (r_1 + I_1, r_2 + I_2)$.

By the first isomorphism theorem, $R/(I_1 \cap I_2) \cong R/I_1 \times R/I_2$.

General case by induction. Assume the result for $n-1$ ideals. We claim that I_1 and $J = I_2 \cdots I_n$ are coprime. For each $k \geq 2$, there exist $a_k \in I_1$ and $b_k \in I_k$ with $a_k + b_k = 1$. Then

$$1 = \prod_{k=2}^{n}(a_k + b_k) = a + b_2b_3 \cdots b_n,$$

where a is a sum of terms each containing some a_k as a factor, so $a \in I_1$, and $b_2 \cdots b_n \in I_2 \cdots I_n = J$. Thus $I_1 + J = R$.

By the $n = 2$ case, $I_1 \cap J = I_1J$ and $R/(I_1 \cap J) \cong R/I_1 \times R/J$. One verifies that $I_2, \ldots, I_n$ remain pairwise coprime as ideals of R (they already are by hypothesis), so by induction $R/J \cong R/I_2 \times \cdots \times R/I_n$ and $J = I_2 \cap \cdots \cap I_n$. Combining:

$$R/(I_1 \cap \cdots \cap I_n) = R/(I_1 \cap J) \cong R/I_1 \times R/J \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

Also $I_1 \cap \cdots \cap I_n = I_1 \cap J = I_1J = I_1I_2 \cdots I_n$. □

Corollary 6.1. If $n_1, \ldots, n_k$ are pairwise coprime positive integers and $n = n_1 \cdots n_k$, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

6.4 Integral domains and characteristic

Definition 6.3 (Characteristic)**.** The **characteristic** of a ring R with unity, denoted $\operatorname{char}(R)$, is the smallest positive integer n such that $n \cdot 1_R = \underbrace{1_R + \cdots + 1_R}_{n} = 0_R$, if such n exists. If no such n exists, we set $\operatorname{char}(R) = 0$.

Proposition 6.2. The characteristic of an integral domain is either 0 or a prime number.

Proof. Let R be an integral domain with $\operatorname{char}(R) = n > 0$. Suppose $n = ab$ with $1 \leq a, b < n$. Then $0 = n \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$. Since R is an integral domain, $a \cdot 1_R = 0$ or $b \cdot 1_R = 0$, contradicting the minimality of n. Hence n is prime. □

Proposition 6.3. Let R be a ring with unity. There exists a unique ring homomorphism $\iota\colon \mathbb{Z} \to R$ (given by $\iota(n) = n \cdot 1_R$), and $\ker \iota = \operatorname{char}(R) \cdot \mathbb{Z}$. In particular:

- If $\operatorname{char}(R) = 0$, then R contains a subring isomorphic to $\mathbb{Z}$.
- If $\operatorname{char}(R) = p > 0$, then R contains a subring isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof. The map $\iota(n) = n \cdot 1_R$ is the unique ring homomorphism $\mathbb{Z} \to R$ (since any such homomorphism must send 1 to 1_R). Its kernel is the ideal $n\mathbb{Z}$ where $n = \operatorname{char}(R)$ (with the convention $0 \cdot \mathbb{Z} = \{0\}$). By the first isomorphism theorem, $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{im} \iota \subseteq R$. □

6.5 The field of fractions

Theorem 6.7 (Field of fractions)**.** Let R be an integral domain. There exists a field $\mathrm{Frac}(R)$, unique up to isomorphism, and an injective ring homomorphism $\iota\colon R \hookrightarrow \mathrm{Frac}(R)$, such that every element of $\mathrm{Frac}(R)$ can be written as $\iota(a)\iota(b)^{-1}$ for some $a \in R$ and $b \in R \setminus \{0\}$.

We give the full construction.

Construction. Consider the set $S = R \times (R \setminus \{0\})$. Define a relation on S by

$$(a, b) \sim (c, d) \iff ad = bc.$$

Lemma 6.1. The relation $\sim$ is an equivalence relation on S.

Proof. *Reflexivity.* $(a, b) \sim (a, b)$ since $ab = ba$ (by commutativity).

Symmetry. If $(a, b) \sim (c, d)$, then $ad = bc$, so $cb = da$, hence $(c, d) \sim (a, b)$.

Transitivity. Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, i.e., $ad = bc$ and $cf = de$. We must show $af = be$. Multiply the first equation by f: $adf = bcf$. Multiply the second by b: $bcf = bde$. So $adf = bde$, i.e., $d(af - be) = 0$. Since $d \neq 0$ and R is an integral domain, $af = be$. □

Denote the equivalence class of (a, b) by $\frac{a}{b}$. Let $F = S/\!\sim$ be the set of equivalence classes. Define operations on F:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Note that $bd \neq 0$ since R is an integral domain, so the right-hand sides are well-defined elements of S.

Proposition 6.4. The operations on F are well-defined.

Proof. **Addition.** Suppose $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$, i.e., $ab' = a'b$ and $cd' = c'd$. We must show $(ad + bc)(b'd') = (a'd' + b'c')(bd)$. Expand:

$$\begin{aligned}(ad + bc)(b'd') &= adb'd' + bcb'd' = ab' \cdot dd' + cd' \cdot bb' \\ &= a'b \cdot dd' + c'd \cdot bb' = a'd'bd + b'c'bd = (a'd' + b'c')bd.\end{aligned}$$

Multiplication. We must show $(ac)(b'd') = (a'c')(bd)$. We have $ac \cdot b'd' = ab' \cdot cd' = a'b \cdot c'd = (a'c')(bd)$. □

Proof of Theorem 6.7. F **is a field.** Addition is commutative and associative (verified by direct computation), with identity $\frac{0}{1}$ and additive inverse $-\frac{a}{b} = \frac{-a}{b}$. Multiplication is commutative and associative, with identity $\frac{1}{1}$. Distributivity holds:

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{a(cf + de)}{bdf} = \frac{acf + ade}{bdf}.$$

On the other hand, $\frac{ac}{bd} + \frac{ae}{bf} = \frac{acbf + aebd}{b^2df} = \frac{b(acf + ade)}{b^2df}$. Now $(acf + ade) \cdot b^2df = b(acf + ade) \cdot bdf$, so these are equal.

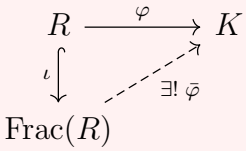
For inverses: if $\frac{a}{b} \neq \frac{0}{1}$ (i.e., $a \neq 0$), then $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \in F$.

Embedding. Define $\iota\colon R \to F$ by $\iota(a) = \frac{a}{1}$. Then $\iota(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$, $\iota(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$, and $\iota(1) = \frac{1}{1}$. Injectivity: if $\iota(a) = \frac{0}{1}$, then $a \cdot 1 = 0 \cdot 1$, so $a = 0$.

Every element $\frac{a}{b} \in F$ equals $\frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1} = \iota(a)\iota(b)^{-1}$.

Uniqueness is addressed by the universal property below. □

Theorem 6.8 (Universal property of the field of fractions)**.** Let R be an integral domain and $\iota\colon R \hookrightarrow \mathrm{Frac}(R)$ the canonical embedding. For every injective ring homomorphism $\varphi\colon R \to K$ where K is a field, there exists a unique ring homomorphism $\bar{\varphi}\colon \mathrm{Frac}(R) \to K$ such that $\bar{\varphi} \circ \iota = \varphi$.



Proof. **Definition.** For $\frac{a}{b} \in \mathrm{Frac}(R)$ (with $b \neq 0$), set $\bar{\varphi}\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1}$. Note that $\varphi(b) \neq 0$ since φ is injective and $b \neq 0$, so $\varphi(b)^{-1}$ exists in K.

Well-definedness. If $\frac{a}{b} = \frac{c}{d}$, then $ad = bc$, so $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$, hence $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$.

Ring homomorphism.

$$\bar{\varphi}\left(\frac{a}{b} + \frac{c}{d}\right) = \bar{\varphi}\left(\frac{ad+bc}{bd}\right) = \frac{\varphi(ad+bc)}{\varphi(bd)} = \frac{\varphi(a)\varphi(d) + \varphi(b)\varphi(c)}{\varphi(b)\varphi(d)}$$
$$= \frac{\varphi(a)}{\varphi(b)} + \frac{\varphi(c)}{\varphi(d)} = \bar{\varphi}\left(\frac{a}{b}\right) + \bar{\varphi}\left(\frac{c}{d}\right).$$

Multiplicativity is similar: $\bar{\varphi}\left(\frac{ac}{bd}\right) = \frac{\varphi(a)\varphi(c)}{\varphi(b)\varphi(d)}$.

Compatibility. $\bar{\varphi}(\iota(a)) = \bar{\varphi}\left(\frac{a}{1}\right) = \varphi(a)\varphi(1)^{-1} = \varphi(a)$.

Uniqueness. Any $\psi\colon \mathrm{Frac}(R) \to K$ with $\psi \circ \iota = \varphi$ must satisfy $\psi\left(\frac{a}{b}\right) = \psi(\iota(a)\iota(b)^{-1}) = \psi(\iota(a))\psi(\iota(b))^{-1} = \varphi(a)\varphi(b)^{-1} = \bar{\varphi}\left(\frac{a}{b}\right)$. □

Example 6.1. (a) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(b) $\mathrm{Frac}(K[X]) = K(X)$, the field of rational functions over K.

(c) $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

6.6 Exercises

Exercise 6.1. Show that $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Exercise 6.2. Let $R = \mathbb{Z}[X]$ and $I = (X^2+1, 5)$. Determine the structure of R/I.

Exercise 6.3. Use the Chinese Remainder Theorem to decompose $\mathbb{Z}/60\mathbb{Z}$ as a product of rings.

Exercise 6.4. Let $R = \mathbb{Z}[i]$. Determine $R/(1+i)$.

Exercise 6.5. Let R be a commutative ring with unity. Show that if R has exactly one maximal ideal, then the non-units of R form an ideal. Such a ring is called a **local ring**.

Exercise 6.6. Let $\varphi\colon R \to S$ be a surjective ring homomorphism. Show that if I is a maximal ideal of R containing $\ker\varphi$, then $\varphi(I)$ is a maximal ideal of S.

Exercise 6.7. Let R be an integral domain and $S = R \setminus \{0\}$. Verify that the construction $S^{-1}R$ (formal fractions a/s, $a \in R$, $s \in S$) with the equivalence relation $a/s \sim b/t \iff at = bs$ yields $\mathrm{Frac}(R)$. Generalize: for any multiplicative set $S \subseteq R$ (with $0 \notin S$, $1 \in S$, S closed under multiplication), construct the **localization** $S^{-1}R$.

Exercise 6.8. Show that $\mathrm{char}(\mathrm{Frac}(R)) = \mathrm{char}(R)$ for any integral domain R.

Exercise 6.9. Let R be an integral domain with $\mathrm{char}(R) = p > 0$. Show that the Frobenius map $\varphi\colon R \to R$ defined by $\varphi(a) = a^p$ is a ring homomorphism.

Exercise 6.10. Let I and J be ideals of a ring R with $I + J = R$. Show that $IJ = I \cap J$.

Exercise 6.11. Prove the following version of the CRT: if $\gcd(m, n) = 1$, then for any $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ with $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, and x is unique modulo mn. Exhibit the isomorphism explicitly for $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercise 6.12. Let K be a field and $a \in K$. Show that the evaluation map $\mathrm{ev}_a\colon K[X] \to K$, $f \mapsto f(a)$, is a surjective ring homomorphism with kernel $(X - a)$, and conclude that $K[X]/(X - a) \cong K$.

Chapter 6 Summary. The quotient ring R/I is constructed from cosets $a + I$ with well-defined operations. The first isomorphism theorem states $R/\ker\varphi \cong \mathrm{im}\,\varphi$. The Chinese Remainder Theorem decomposes $R/(I_1 \cap \cdots \cap I_n)$ into a product when the ideals are pairwise coprime. The characteristic of an integral domain is 0 or prime. Every integral domain embeds into its field of fractions $\mathrm{Frac}(R)$, which is the smallest field containing R and satisfies a universal property.

Chapter 7

Principal Ideal Domains, Euclidean Domains, and Unique Factorization Domains

7.1 Divisibility in integral domains

Throughout this chapter, R denotes a commutative ring with unity, and most results require R to be an integral domain.

Definition 7.1 (Divisibility, associates)**.** Let R be an integral domain and $a, b \in R$.

(i) We say a **divides** b (written $a \mid b$) if $b = ac$ for some $c \in R$.

(ii) Elements a and b are **associates** (written $a \sim b$) if $a = ub$ for some unit $u \in U(R)$, equivalently, $a \mid b$ and $b \mid a$.

Definition 7.2 (Irreducible and prime elements)**.** Let R be an integral domain and $p \in R \setminus (\{0\} \cup U(R))$ (i.e., p is non-zero and not a unit).

(i) p is **irreducible** if whenever $p = ab$, either $a \in U(R)$ or $b \in U(R)$.

(ii) p is **prime** if whenever $p \mid ab$, either $p \mid a$ or $p \mid b$.

Proposition 7.1 (Prime implies irreducible)**.** In an integral domain, every prime element is irreducible.

Proof. Let p be a prime element of an integral domain R, and suppose $p = ab$. Then $p \mid ab$. Since p is prime, $p \mid a$ or $p \mid b$.

Case 1: $p \mid a$. Write $a = pc$ for some $c \in R$. Then $p = ab = pcb$, so $p(1 - cb) = 0$. Since $p \neq 0$ and R is an integral domain, $cb = 1$, so $b \in U(R)$.

Case 2: $p \mid b$. By the same argument, $a \in U(R)$.

In either case, one of a, b is a unit, so p is irreducible. □

Remark 7.1. The converse is false in general: in $\mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible but not prime (see Section 7.4).

7.2 Principal ideal domains

Definition 7.3 (Principal ideal domain)**.** An integral domain R is a **principal ideal domain** (PID) if every ideal of R is principal, i.e., for every ideal I of R, there exists $a \in R$ with $I = (a)$.

Example 7.1. $\mathbb{Z}$ and $K[X]$ (for any field K) are PIDs. The ring $\mathbb{Z}[X]$ is *not* a PID (the ideal $(2, X)$ is not principal).

Theorem 7.1 (Irreducible iff prime in a PID)**.** In a principal ideal domain, an element is irreducible if and only if it is prime.

Proof. Prime implies irreducible holds in any integral domain (Proposition 7.1). We prove the converse.

Let R be a PID and let $p \in R$ be irreducible. We show that the ideal (p) is prime, which is equivalent to p being prime. Suppose $p \mid ab$, i.e., $ab \in (p)$. Assume $p \nmid a$; we must show $p \mid b$.

Consider the ideal (p, a). Since R is a PID, $(p, a) = (d)$ for some $d \in R$. Then $p \in (d)$, so $p = dc$ for some $c \in R$. Since p is irreducible, either $d \in U(R)$ or $c \in U(R)$.

Case 1: $c \in U(R)$. Then $d = pc^{-1}$, so $(d) = (p)$. This means $a \in (p)$, i.e., $p \mid a$, contradicting our assumption.

Case 2: $d \in U(R)$. Then $(d) = R$, so $(p, a) = R$. There exist $x, y \in R$ with $px + ay = 1$. Multiplying by b: $pbx + aby = b$. Now $p \mid pbx$ and $p \mid ab$ implies $p \mid aby$. Hence $p \mid (pbx + aby) = b$, as desired.

So the only consistent case is Case 2, proving $p \mid b$. □

Corollary 7.1. In a PID, the non-zero prime ideals are exactly the maximal ideals.

Proof. Let (p) be a non-zero prime ideal of a PID R. Then p is a prime element, hence irreducible. Suppose $(p) \subseteq (d)$ for some $d \in R$. Then $p = dc$, and since p is irreducible, $d \in U(R)$ (giving $(d) = R$) or $c \in U(R)$ (giving $(d) = (p)$). Hence (p) is maximal.

Conversely, every maximal ideal is prime (Theorem 5.3). □

7.3 Euclidean domains

Definition 7.4 (Euclidean domain)**.** An integral domain R is a **Euclidean domain** if there exists a function $N \colon R \setminus \{0\} \to \mathbb{N}$ (called a **Euclidean function** or **norm**) such that for all $a \in R$ and $b \in R \setminus \{0\}$, there exist $q, r \in R$ with

$$a = bq + r, \quad \text{where } r = 0 \text{ or } N(r) < N(b).$$

Example 7.2. (a) $\mathbb{Z}$ with $N(a) = |a|$.

(b) $K[X]$ (for a field K) with $N(f) = \deg f$.

(c) $\mathbb{Z}[i]$ with $N(a + bi) = a^2 + b^2$ (proved below in Theorem 7.3).

Theorem 7.2 (Every Euclidean domain is a PID)**.** Every Euclidean domain is a principal ideal domain.

Proof. Let R be a Euclidean domain with Euclidean function N, and let I be a non-zero ideal of R (the case $I = \{0\} = (0)$ is trivial). Among all non-zero elements of I, choose $d \in I$ with $N(d)$ minimal (this is possible since $\mathbb{N}$ is well-ordered).

We claim $I = (d)$. The inclusion $(d) \subseteq I$ is clear since $d \in I$ and I is an ideal. For the reverse, let $a \in I$. By the Euclidean property, write $a = dq + r$ with $r = 0$ or $N(r) < N(d)$. Since $a \in I$ and $dq \in I$ (as $d \in I$), we have $r = a - dq \in I$. If $r \neq 0$, then $r \in I \setminus \{0\}$ with $N(r) < N(d)$, contradicting the minimality of $N(d)$. Hence $r = 0$ and $a = dq \in (d)$. □

Theorem 7.3 ($\mathbb{Z}[i]$ is a Euclidean domain)**.** The ring of Gaussian integers $\mathbb{Z}[i]$, equipped with the norm $N(a + bi) = a^2 + b^2$, is a Euclidean domain.

Proof. The norm N is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$. (This follows from $N(z) = |z|^2$ and $|z_1 z_2| = |z_1||z_2|$.)

Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. In $\mathbb{C}$, compute $\alpha/\beta = x + yi$ with $x, y \in \mathbb{Q}$. Choose integers $m, n \in \mathbb{Z}$ closest to x and y respectively, so that $|x - m| \leq \frac{1}{2}$ and $|y - n| \leq \frac{1}{2}$. Set $q = m + ni \in \mathbb{Z}[i]$ and $r = \alpha - \beta q$.

Then $r \in \mathbb{Z}[i]$ and

$$\frac{r}{\beta} = \frac{\alpha}{\beta} - q = (x - m) + (y - n)i.$$

Hence

$$N(r) = N(\beta) \cdot N\left(\frac{r}{\beta}\right) = N(\beta)\left[(x - m)^2 + (y - n)^2\right] \leq N(\beta)\left[\frac{1}{4} + \frac{1}{4}\right] = \frac{N(\beta)}{2}.$$

In particular, either $r = 0$ or $N(r) \leq \frac{N(\beta)}{2} < N(\beta)$. □

7.4 Counterexample: $\mathbb{Z}[\sqrt{-5}]$ is not a UFD

Proposition 7.2. The ring $\mathbb{Z}[\sqrt{-5}]$ is an integral domain that is not a unique factorization domain.

Proof. $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ is a subring of a field, hence an integral domain.

Define the norm $N \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$ by $N(a + b\sqrt{-5}) = a^2 + 5b^2$. This norm is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.

Claim 1: $\alpha \in U(\mathbb{Z}[\sqrt{-5}])$ if and only if $N(\alpha) = 1$, i.e., the units are ± 1.

Proof of Claim 1. If $\alpha\beta = 1$, then $N(\alpha)N(\beta) = 1$ with $N(\alpha), N(\beta) \in \mathbb{N}$, so $N(\alpha) = 1$. Conversely, $N(a + b\sqrt{-5}) = a^2 + 5b^2 = 1$ forces $b = 0$ and $a = \pm 1$.

Claim 2: The elements 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible.

Proof of Claim 2. $N(2) = 4$. If $2 = \alpha\beta$ with neither α nor β a unit, then $N(\alpha)N(\beta) = 4$, so $N(\alpha) = N(\beta) = 2$. But $a^2 + 5b^2 = 2$ has no solution in integers. Similarly, $N(3) = 9$ would require $N(\alpha) = 3$, but $a^2 + 5b^2 = 3$ has no integer solution. For $1 \pm \sqrt{-5}$, $N(1 \pm \sqrt{-5}) = 6$, and a non-trivial factorization would require a factor of norm 2 or 3, which we have shown do not exist.

Claim 3: 2 is not prime.

Proof of Claim 3. We have $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2\cdot 3$, so $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$. But $2 \nmid (1+\sqrt{-5})$: if $1+\sqrt{-5} = 2(a+b\sqrt{-5})$, then $2a = 1$, impossible in $\mathbb{Z}$. Similarly $2 \nmid (1-\sqrt{-5})$.

Since $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are two essentially different factorizations into irreducibles (the factors in one factorization are not associates of those in the other, as can be checked via norms), $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. □

7.5 Unique factorization domains

Definition 7.5 (Unique factorization domain)**.** An integral domain R is a **unique factorization domain** (UFD) if:

(i) **Existence:** Every non-zero, non-unit element of R can be written as a product of irreducible elements.

(ii) **Uniqueness:** If $a = p_1 \cdots p_m = q_1 \cdots q_n$ are two such factorizations, then $m = n$ and, after reordering, p_i and q_i are associates for each i.

Lemma 7.1 (Ascending chain condition on principal ideals in a PID)**.** In a PID R, every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilizes, i.e., there exists N such that $I_n = I_N$ for all $n \geq N$.

Proof. Let $I = \bigcup_{n=1}^{\infty} I_n$. We verify I is an ideal: $0 \in I_1 \subseteq I$; if $a, b \in I$, then $a \in I_j$ and $b \in I_k$ for some j, k, so $a, b \in I_{\max(j,k)}$ and $a - b \in I_{\max(j,k)} \subseteq I$; if $r \in R$ and $a \in I_n$, then $ra \in I_n \subseteq I$.

Since R is a PID, $I = (d)$ for some $d \in R$. Then $d \in I$, so $d \in I_N$ for some N. For all $n \geq N$: $(d) \subseteq I_N \subseteq I_n \subseteq I = (d)$, so $I_n = (d) = I_N$. □

Theorem 7.4 (Every PID is a UFD)**.** Every principal ideal domain is a unique factorization domain.

Proof. Let R be a PID. We must establish both existence and uniqueness of factorization.

Existence of factorization. Suppose for contradiction that there exists a non-zero, non-unit element of R that cannot be written as a product of irreducibles. Let a_1 be such an element. Then a_1 is not irreducible (otherwise it is a product of one irreducible). So $a_1 = b_1 c_1$ where neither b_1 nor c_1 is a unit. At least one of b_1, c_1 is not a product of irreducibles (otherwise a_1 would be). Call it a_2; we have $(a_1) \subsetneq (a_2)$ (since $a_2 \mid a_1$ but $a_1 \nmid a_2$, for if $a_1 \mid a_2$ then the cofactor of a_2 in $a_1 = b_1 c_1$ would be a unit, contradicting our choice).

Repeating, we obtain a strictly ascending chain $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$, contradicting the ACC (Lemma 7.1).

To see that $(a_1) \subsetneq (a_2)$: say $a_1 = a_2 d$ for some non-unit d (we chose a_2 to be one of b_1, c_1, and the other factor is a non-unit d). Then $a_1 \in (a_2)$, so $(a_1) \subseteq (a_2)$. If $(a_1) = (a_2)$, then $a_2 = a_1 e$ for some $e \in R$, hence $a_1 = a_2 d = a_1 e d$, so $ed = 1$ (since R is an integral domain and $a_1 \neq 0$), meaning d is a unit—contradiction. So the inclusion is strict.

Uniqueness of factorization. Suppose $p_1p_2\cdots p_m = q_1q_2\cdots q_n$ where all p_i, q_j are irreducible. We proceed by induction on m.

Base case $m = 1$: $p_1 = q_1\cdots q_n$. Since p_1 is irreducible and this is a factorization, $n = 1$ and $p_1 = q_1$.

Inductive step: Since $p_1 \mid q_1q_2\cdots q_n$ and p_1 is irreducible (hence prime in a PID by Theorem 7.1), $p_1 \mid q_j$ for some j. After reordering, assume $p_1 \mid q_1$. Since q_1 is irreducible and p_1 is not a unit, $q_1 = up_1$ for some unit u. Then:

$$p_1p_2\cdots p_m = up_1q_2\cdots q_n.$$

Cancelling p_1 (valid since R is an integral domain):

$$p_2\cdots p_m = uq_2\cdots q_n = (uq_2)q_3\cdots q_n.$$

Note that uq_2 is irreducible (since u is a unit). By the induction hypothesis, $m-1 = n-1$ (so $m = n$) and, after reordering, $p_i \sim q_i$ for $i \geq 2$. Also $p_1 \sim q_1$, completing the proof. □

7.6 Gauss's lemma and polynomial rings over UFDs

Definition 7.6 (Content of a polynomial)**.** Let R be a UFD and $f = a_0 + a_1X + \cdots + a_nX^n \in R[X] \setminus \{0\}$. The **content** of f, denoted $c(f)$, is the gcd of the coefficients $a_0, \ldots, a_n$ (defined up to associates). We say f is **primitive** if $c(f) \sim 1$.

Lemma 7.2 (Gauss's lemma)**.** Let R be a UFD and let $f, g \in R[X]$ be primitive polynomials. Then fg is primitive.

Proof. Let $f = \sum a_iX^i$ and $g = \sum b_jX^j$. Suppose fg is not primitive. Then there exists an irreducible (hence prime, in a UFD) element $p \in R$ dividing all coefficients of fg. Since f is primitive, p does not divide all a_i; let a_s be the first coefficient not divisible by p (so $p \mid a_i$ for $i < s$). Similarly, let b_t be the first coefficient of g not divisible by p.

The coefficient of X^{s+t} in fg is

$$c_{s+t} = \sum_{i+j=s+t} a_ib_j = a_sb_t + \sum_{\substack{i+j=s+t \\ i<s}} a_ib_j + \sum_{\substack{i+j=s+t \\ i>s}} a_ib_j.$$

For $i < s$: $p \mid a_i$, so $p \mid a_ib_j$. For $i > s$: $j = s + t - i < t$, so $p \mid b_j$, hence $p \mid a_ib_j$. Thus $p \mid (c_{s+t} - a_sb_t)$. Since $p \mid c_{s+t}$ by assumption, $p \mid a_sb_t$. Since p is prime, $p \mid a_s$ or $p \mid b_t$—contradicting our choice of s and t. □

Corollary 7.2 (Content is multiplicative)**.** For $f, g \in R[X] \setminus \{0\}$ (where R is a UFD), $c(fg) \sim c(f)c(g)$.

Proof. Write $f = c(f)f_0$ and $g = c(g)g_0$ where f_0, g_0 are primitive. Then $fg = c(f)c(g)f_0g_0$, and f_0g_0 is primitive by Gauss's lemma. Hence $c(fg) \sim c(f)c(g)$. □

Theorem 7.5 (R UFD implies $R[X]$ UFD)**.** If R is a UFD, then $R[X]$ is a UFD.

Proof. Let $F = \mathrm{Frac}(R)$. Since F is a field, $F[X]$ is a Euclidean domain, hence a PID, hence a UFD.

Step 1: Irreducibles of $R[X]$. The irreducible elements of $R[X]$ are:

(a) the irreducible elements of R (viewed as constant polynomials);

(b) the primitive polynomials $f \in R[X]$ of degree ≥ 1 that are irreducible in $F[X]$.

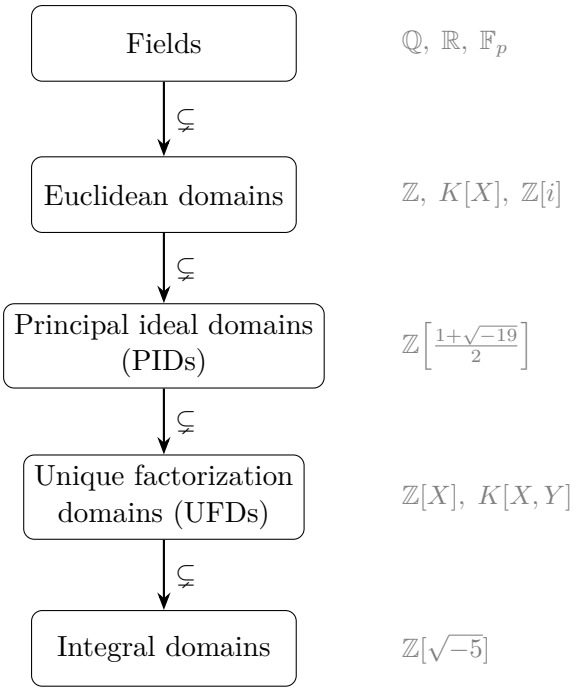
Proof that type (b) elements are irreducible in $R[X]$: Let f be primitive of degree ≥ 1 and irreducible in $F[X]$. Suppose $f = gh$ in $R[X]$. Since f is irreducible in $F[X]$ and $\deg f \geq 1$, one of g, h must be constant in $F[X]$, say $\deg h = 0$ in the factorization over $F[X]$... more carefully: writing $f = gh$ in $R[X]$, this is also a factorization in $F[X]$, so (since f is irreducible in $F[X]$) one factor, say h, must be a unit in $F[X]$, i.e., $h \in F^\times$. So $\deg h = 0$, meaning $h \in R \setminus \{0\}$. Since f is primitive, h must be a unit in R. Hence f is irreducible in $R[X]$.

Step 2: Existence of factorization. Let $f \in R[X]$ be non-zero and not a unit. Write $f = c(f) \cdot f_0$ where f_0 is primitive. Factor $c(f)$ into irreducibles in R (possible since R is a UFD). If $\deg f_0 \geq 1$, factor f_0 in $F[X]$ into irreducibles $f_0 = g_1 \cdots g_k$ (in $F[X]$). Clearing denominators: for each g_i, write $g_i = \frac{a_i}{b_i} h_i$ where $h_i \in R[X]$ is primitive and $a_i, b_i \in R \setminus \{0\}$. Then $f_0 = \frac{a_1 \cdots a_k}{b_1 \cdots b_k} h_1 \cdots h_k$. Since f_0 and $h_1 \cdots h_k$ are both primitive (by Gauss's lemma, applied inductively), we get $\frac{a_1 \cdots a_k}{b_1 \cdots b_k} \in U(R)$, so f_0 is associate to $h_1 \cdots h_k$ in $R[X]$, giving a factorization into irreducibles.

Step 3: Uniqueness. Suppose $p_1 \cdots p_m = q_1 \cdots q_n$ in $R[X]$ with each factor irreducible. The constant irreducibles (type (a)) and the primitive irreducibles (type (b)) are distinguished by degree. Comparing contents, the type (a) factors on each side must give the same product up to associates and reordering (by uniqueness in R). After cancellation, we have a product of primitive irreducibles equal on both sides. Viewing this in $F[X]$ (a UFD), the factorizations agree up to associates in $F[X]$ and reordering. Since the factors are primitive elements of $R[X]$, associates in $F[X]$ that are primitive in $R[X]$ are associates in $R[X]$. (Indeed, if $f = \frac{a}{b} g$ with f, g primitive in $R[X]$ and $\frac{a}{b} \in F^\times$, then comparing contents: $1 \sim \frac{a}{b} \cdot 1$, so $\frac{a}{b} \in U(R)$.) □

7.7 The hierarchy of integral domains

The following diagram summarizes the inclusions among the classes of integral domains studied in this chapter. Each inclusion is strict.



7.8 Eisenstein's irreducibility criterion

Theorem 7.6 (Eisenstein's criterion)**.** Let R be a UFD with field of fractions F, and let

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$$

with $n \geq 1$. Suppose there exists an irreducible element $p \in R$ such that:

(i) $p \nmid a_n$;

(ii) $p \mid a_i$ for all $i = 0, 1, \ldots, n-1$;

(iii) $p^2 \nmid a_0$.

Then f is irreducible in $F[X]$. If moreover f is primitive, then f is irreducible in $R[X]$.

Proof. By Gauss's lemma, it suffices to prove that f is irreducible in $R[X]$ (assuming f is primitive; the general case reduces to this by factoring out the content).

Suppose $f = gh$ in $R[X]$ with $g = \sum_{i=0}^{r} b_i X^i$ and $h = \sum_{j=0}^{s} c_j X^j$, where $r + s = n$, $r, s \geq 1$.

Reducing modulo p: let $\bar{f}$, $\bar{g}$, $\bar{h}$ denote the images in $(R/pR)[X]$. By conditions (i) and (ii):

$$\bar{f} = \bar{a}_n X^n.$$

So $\bar{g}\bar{h} = \bar{a}_n X^n$ in $(R/pR)[X]$. Since p is irreducible (hence prime) in R, the quotient R/pR is an integral domain (by Theorem 5.1). In an integral domain, $\bar{g}\bar{h} = \bar{a}_n X^n$ implies $\bar{g} = \bar{b}_r X^r$ and $\bar{h} = \bar{c}_s X^s$ (since R/pR is a domain, hence $(R/pR)[X]$ is a domain, and irreducible factorization of X^n forces this form). In particular, $p \mid b_0$ and $p \mid c_0$.

But then $a_0 = b_0 c_0$ gives $p^2 \mid a_0$, contradicting condition (iii). Hence no such non-trivial factorization exists. $\square$

Corollary 7.3. For any prime p, the p-th cyclotomic polynomial

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

is irreducible over $\mathbb{Q}$.

Proof. $\Phi_p(X)$ is irreducible if and only if $\Phi_p(X+1)$ is. We compute:

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

Now apply Eisenstein's criterion with the prime p: the leading coefficient is 1 (not divisible by p); $\binom{p}{k}$ is divisible by p for $1 \le k \le p-1$; and the constant term is p, not divisible by p^2. □

Example 7.3. The polynomial $f = 2X^5 + 6X^3 + 9X^2 + 15 \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 3$: $3 \nmid 2$, $3 \mid 6$, $3 \mid 9$, $3 \mid 15$, and $9 \nmid 15$.

7.9 A PID that is not Euclidean

Theorem 7.7. The ring $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\right\}$ is a PID but not a Euclidean domain.

Remark 7.2. The proof that R is a PID uses the Dedekind–Hasse criterion or the Minkowski bound in algebraic number theory. The proof that R is not Euclidean uses the theory of universal side divisors: in a Euclidean domain, there must exist an element a such that for every $b \in R$, either $a \mid b$ or there exist q, r with $b = aq + r$ and $r \in U(R)$. One shows no such element exists in R. We refer to [1] (Section 8.2) for a complete treatment.

The existence of this example confirms that the inclusion Euclidean domains $\subsetneq$ PIDs is strict.

7.10 Exercises

Exercise 7.1. Show that in a UFD, an element p is prime if and only if it is irreducible.

Exercise 7.2. Determine the units, irreducibles, and primes in $\mathbb{Z}[i]$. Show that a rational prime p factors in $\mathbb{Z}[i]$ as follows:

(a) $p = 2 = (1+i)(1-i)(-i)$, so 2 ramifies;

(b) if $p \equiv 1 \pmod 4$, then $p = \pi\bar{\pi}$ for some irreducible $\pi \in \mathbb{Z}[i]$ (splits);

(c) if $p \equiv 3 \pmod 4$, then p remains irreducible in $\mathbb{Z}[i]$ (inert).

Exercise 7.3. Let R be a PID and $a, b \in R$, not both zero. Show that $\gcd(a, b)$ exists and can be written as $\gcd(a, b) = xa + yb$ for some $x, y \in R$ (Bézout's identity).

Exercise 7.4. Show that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD. *(Hint: consider* $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$*.)*

Exercise 7.5. Show that in a UFD R, any two elements $a, b \in R$ (not both zero) have a gcd, and that $\gcd(a, b) \sim \prod p_i^{\min(\alpha_i, \beta_i)}$ where $a \sim u \prod p_i^{\alpha_i}$ and $b \sim v \prod p_i^{\beta_i}$ are the factorizations.

Exercise 7.6. Prove that X^4+1 is irreducible over $\mathbb{Q}$ but reducible modulo every prime p. *(For irreducibility, use the substitution* $X \mapsto X + 1$ *and Eisenstein.)*

Exercise 7.7. Let K be a field. Show that $K[X, Y]$ is a UFD but not a PID. *(Hint: use Theorem 7.5; show* (X, Y) *is not principal.)*

Exercise 7.8. Show that in a PID, every non-zero prime ideal is maximal.

Exercise 7.9. Use Eisenstein's criterion to show that $X^4 + 10X^2 + 1$ is irreducible over $\mathbb{Q}$... or explain why Eisenstein does not apply directly, and find another method.

Exercise 7.10. Show that $f = Y^2 - X^3 - X \in \mathbb{R}[X, Y]$ is irreducible. *(View* f *as an element of* $(\mathbb{R}[X])[Y]$ *and apply Eisenstein.)*

Exercise 7.11. Let R be a UFD and $p \in R$ irreducible. Show that $R[X]/(p) \cong (R/(p))[X]$ and deduce that if $R/(p)$ is an integral domain, then p remains irreducible in $R[X]$.

Exercise 7.12. **(Challenging.)** Show that if R is a PID and $S \subseteq R \setminus \{0\}$ is a multiplicative set, then the localization $S^{-1}R$ is also a PID.

Exercise 7.13. Determine all the ideals of $\mathbb{Z}[i]/(2+3i)$, and decide whether this quotient is a field.

Chapter 7 Summary. In an integral domain: prime implies irreducible, but not conversely in general. In a PID, the two notions coincide. Every Euclidean domain is a PID (by the division algorithm), and every PID is a UFD (via the ascending chain condition). The polynomial ring $R[X]$ over a UFD R is again a UFD (Gauss's lemma). The hierarchy Fields $\subsetneq$ Euclidean $\subsetneq$ PID $\subsetneq$ UFD $\subsetneq$ Integral domains has strict inclusions. Eisenstein's criterion provides a powerful irreducibility test.

Bibliography

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, 2004.

[2] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics 211, Springer-Verlag, 2002.

[3] M. Artin, *Algebra*, 2nd ed., Pearson, 2011.

[4] N. Jacobson, *Basic Algebra I*, 2nd ed., W. H. Freeman, 1985.

[5] N. Jacobson, *Basic Algebra II*, 2nd ed., W. H. Freeman, 1989.

[6] N. Bourbaki, *Algebra I, Chapters 1–3*, Springer-Verlag, 1989.

[7] D. Perrin, *Algèbre: cours de mathématiques de première année*, Ellipses, 1996.

Index