An Introduction to Class Groups

Roy Yaranga
r.yaranga.almeida@gmail.com

Euler Circle

July 10, 2026

Introduction and Historical Context

- While attempting to solve Fermat's Last Theorem, Ernst Kummer analyzed the factorization in rings of integers of cyclotomic fields $\mathbb{Q}(\zeta_p)$ and discovered that unique factorization into irreducible elements failed (specifically for $p = 23$).
- To restore arithmetic order, Kummer introduced so-called "ideal numbers", which allowed for the recovery of a notion of unique divisibility.
- Richard Dedekind translated Kummer's ideal numbers into concrete collections of elements of a ring, formally coining the modern concept of an **ideal** and extending this study to general number fields.

Preliminaries and the Failure of Unique Factorization

Preliminaries: Group Structures

Definition 1.1 (Group)

*A **group** is a non-empty set G together with a binary operation $\cdot : G \times G \to G$ that satisfies the following axioms:*

1. *Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.*
2. *Identity element: There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.*
3. *Inverse element: For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

Definition 1.2 (Abelian Group)

*A group $(G, \cdot)$ is **abelian** if the binary operation satisfies the commutative property, that is, $a \cdot b = b \cdot a$ for all $a, b \in G$.*

Preliminaries: Rings and Subrings

Definition 1.3 (Ring)

A **ring** *is a non-empty set R together with two binary operations $+$ and $\cdot$ such that $(R, +)$ is an abelian group, the operation $\cdot$ is associative and distributive with respect to $+$. We will assume that every ring R is commutative and possesses an identity element denoted by $1_R \neq 0_R$.*

Definition 1.4 (Subring)

A **subring** *of R is a subset $S \subseteq R$ that is a ring under the same operations of R and contains the identity element 1_R.*

Preliminaries: Ideals and Quotient Rings

Definition 1.5 (Ideal)

A non-empty subset $I \subseteq R$ *is an* **ideal** *of* R *if* $(I, +)$ *is an additive subgroup of* R *and satisfies that for all* $r \in R$ *and* $a \in I$*, it holds that* $r \cdot a \in I$*.*

Definition 1.6 (Quotient Ring)

Given an ideal I *of a ring* R*, the* **quotient ring** R/I *is the set of cosets* $R/I = \{r + I \mid r \in R\}$*, which constitutes a ring under the operations of addition and multiplication defined by:*

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I \quad \textit{and} \quad (r_1 + I)(r_2 + I) = r_1 r_2 + I$$

Preliminaries: Fields, Subfields and Extensions

Definition 1.7 (Field)

A commutative ring with identity F is a **field** *if $1_F \neq 0_F$ and every non-zero element possesses a multiplicative inverse.*

Definition 1.8 (Subfield)

A **subfield** *of F is a subring $E \subseteq F$ that is a field under the inherited operations.*

Definition 1.9 (Field Extension)

A **field extension***, denoted by L/F, consists of a field L containing a subfield F.*

Preliminaries: Dimension and Field of Fractions

Definition 1.10 (Degree of an Extension)

The **degree** *(or dimension) of a field extension L/F, denoted by $[L : F]$, is the dimension of L viewed as a vector space over the base field F:*

$$[L : F] = \dim_F(L)$$

Definition 1.11 (Field of Fractions)

Given an integral domain D, its **field of fractions***, denoted by $Frac(D)$, is the smallest field containing D up to isomorphism, whose elements are of the form $\frac{a}{b}$ with $a, b \in D$ and $b \neq 0$.*

Preliminaries: Domains, Units and Associates

Definition 1.12 (Integral Domain)

A commutative ring with identity D is an **integral domain** *if for any $a, b \in D$, the condition $a \cdot b = 0$ implies that $a = 0$ or $b = 0$.*

Definition 1.13 (Unit)

An element $a \in D$ is a **unit** *if it possesses a multiplicative inverse in D, that is, there exists $\beta \in D$ such that $a\beta = 1_D$. The set of all units of D is denoted by $D^\times$.*

Definition 1.14 (Associated Elements)

Two elements $a, b \in D$ are **associates** *($a \sim b$) if there exists a unit $u \in D^\times$ such that $a = ub$.*

Prime and Irreducible Elements

Let D be an integral domain and let $p \in D \setminus (D^\times \cup \{0\})$ be a non-zero and non-unit element:

Definition 1.15 (Irreducible Element)

*p is **irreducible** if whenever $p = ab$ with $a, b \in D$, it implies that $a \in D^\times$ or $b \in D^\times$.*

Definition 1.16 (Prime Element)

*p is **prime** if whenever $p \mid ab$ with $a, b \in D$, it implies that $p \mid a$ or $p \mid b$.*

Proposition 1.17

If an element $p \in D$ is prime, then it is irreducible.

Unique Factorization Domains (UFD)

Definition 1.18 (Unique Factorization Domain)

An integral domain D is a **UFD** *if the following conditions are satisfied:*

1. *Every element $x \in D \setminus (D^{\times} \cup \{0\})$ can be expressed as a finite product of irreducible elements $x = p_1 p_2 \cdots p_s$.*
2. *If $p_1 \cdots p_s = q_1 \cdots q_r$ are two factorizations into irreducibles, then $s = r$ and there exists a permutation $\pi \in S_s$ such that $p_i \sim q_{\pi(i)}$ for all $i = 1, \ldots, s$.*

Theorem 1.19

An integral domain D in which every non-zero and non-unit element factorizes into irreducibles is a UFD if and only if every irreducible element in D is prime.

Number Fields and Algebraic Integers

Definition 1.20 (Number Field)

A **number field** K *is a field extension of finite degree over the rational numbers, that is,* $[K:\mathbb{Q}] < \infty$.

Definition 1.21 (Algebraic Number and Algebraic Integer)

An element $\alpha \in \mathbb{C}$ *is an* **algebraic number** *if it is a root of a non-zero polynomial in* $\mathbb{Q}[x]$. *It is an* **algebraic integer** *if it is a root of a monic polynomial in* $\mathbb{Z}[x]$:

$$g(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \mathbb{Z}[x]$$

Definition 1.22 (The Ring of Integers $\mathcal{O}_K$)

Given a number field K, *the set* $\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}$ *is defined. This set constitutes an integral domain.*

The Failure of Unique Factorization in $\mathbb{Z}[\sqrt{-5}]$

Let $K = \mathbb{Q}(\sqrt{-5})$ with ring of integers $D = \mathbb{Z}[\sqrt{-5}]$. The norm is defined by $N(a + b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z}$. We observe two distinct factorizations for the number 6:

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

- The element 2 is irreducible: If $2 = \alpha\beta$, then $4 = N(\alpha)N(\beta)$. Since the equation $a^2 + 5b^2 = 2$ lacks integer solutions, the norms of the factors must be 1 or 4, forcing one of them to be a unit in $D^\times$.
- The element 2 is not prime: It is clear that $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. However, it can be shown that $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$.

Dedekind Domains and Ideals

Prime Ideals and Principal Ideals

Definition 2.1 (Prime Ideal)

A proper ideal $\mathfrak{p} \subsetneq R$ *is a* **prime ideal** *if for any* $a, b \in R$, *the condition* $a \cdot b \in \mathfrak{p}$ *implies that* $a \in \mathfrak{p}$ *or* $b \in \mathfrak{p}$.

Definition 2.2 (Principal Ideal)

An ideal I *of* R *is* **principal** *if it is generated by a single element* $a \in R$, *which we denote by* $I = (a) = \{r \cdot a \mid r \in R\}$.

Definition 2.3 (PID)

An integral domain D *is a* **PID** *if every ideal in* D *is a principal ideal.*

Noetherian Domains and Product of Ideals

Definition 2.4 (Noetherian Ring)

A commutative ring R is **Noetherian** *if it satisfies the ascending chain condition: for any sequence of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq R$, there exists an integer $N \geq 1$ such that $I_n = I_N$ for all $n \geq N$.*

Definition 2.5 (Product of Ideals)

Given two ideals I, J of R, the **product of ideals** *$I \cdot J$ is the ideal generated by all products of elements of I and J:*

$$I \cdot J = \left\{ \sum_{k=1}^{m} a_k b_k \;\middle|\; a_k \in I,\ b_k \in J,\ m \in \mathbb{Z}^+ \right\}$$

Integral Elements and Integral Closure

Definition 2.6 (Integral Element)

Given an integral domain D and a field extension L containing D, an element $\alpha \in L$ is **integral** *over D if it is a root of a monic polynomial with coefficients in the polynomial ring $D[x]$.*

Definition 2.7 (Integrally Closed Domain)

An integral domain D is **integrally closed** *if every element of its field of fractions $Frac(D)$ that is integral over D necessarily belongs to the domain $D itself$.*

Dedekind Domains and the FTA for Ideals

Definition 2.8 (Dedekind Domain)

An integral domain D is a **Dedekind Domain** *if it is Noetherian, integrally closed in its field of fractions $Frac(D)$, and every non-zero prime ideal is a maximal ideal.*

Theorem 2.9 (Fundamental Theorem of Arithmetic for Ideals)

Let $\mathcal{O}_K$ be the ring of integers of a number field. Every non-zero proper ideal $I \subsetneq \mathcal{O}_K$ can be expressed uniquely, up to the order of the factors, as a finite product of prime ideals:

$$I = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_g^{a_g}$$

Restoration of Arithmetic in $\mathbb{Z}[\sqrt{-5}]$

We define the following prime ideals (understood as subsets of elements) in the domain $D = \mathbb{Z}[\sqrt{-5}]$:

$$\mathfrak{p}_2 = (2, 1+\sqrt{-5}) = \{2r_1 + (1+\sqrt{-5})r_2 \mid r_1, r_2 \in D\}$$
$$\mathfrak{p}_3 = (3, 1+\sqrt{-5}) = \{3r_1 + (1+\sqrt{-5})r_2 \mid r_1, r_2 \in D\}$$
$$\mathfrak{p}_3' = (3, 1-\sqrt{-5}) = \{3r_1 + (1-\sqrt{-5})r_2 \mid r_1, r_2 \in D\}$$

Computing the product of these algebraic ideals as sets yields:

$$(2) = \mathfrak{p}_2^2, \quad (3) = \mathfrak{p}_3 \cdot \mathfrak{p}_3'$$
$$(1+\sqrt{-5}) = \mathfrak{p}_2 \cdot \mathfrak{p}_3, \quad (1-\sqrt{-5}) = \mathfrak{p}_2 \cdot \mathfrak{p}_3'$$

The non-unique factorization of elements $(6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}))$ is completely reconciled into a unique factorization of prime ideals:

$$(6) = \mathfrak{p}_2^2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_3'$$

The Ideal Class Group

Fractional Ideals

Definition 3.1 (Fractional Ideal)

Let K be a number field and $\mathcal{O}_K$ its ring of integers. A **fractional ideal** *of $\mathcal{O}_K$ is a non-empty subset $I \subseteq K$ that is an additive subgroup of K, is closed under multiplication by elements of $\mathcal{O}_K$ ($\alpha x \in I$ for all $\alpha \in \mathcal{O}_K$ and $x \in I$), and for which there exists a non-zero element $d \in \mathcal{O}_K \setminus \{0\}$ such that $dI \subseteq \mathcal{O}_K$.*

Arithmetic Interpretation

A fractional ideal represents an ordinary ideal of $\mathcal{O}_K$ whose elements have been divided by a fixed common denominator d. The set of all non-zero fractional ideals is denoted as $\mathcal{I}_K$.

Proof: Group Structure of $\mathcal{I}_K$ (Part 1)

Theorem 3.2

The set $\mathcal{I}_K$ is an abelian group under ideal multiplication.

Proof of Closure, Associativity and Identity

- Closure: Let $I, J \in \mathcal{I}_K$. There exist elements $d_1, d_2 \in \mathcal{O}_K \setminus \{0\}$ such that $d_1 I \subseteq \mathcal{O}_K$ and $d_2 J \subseteq \mathcal{O}_K$. The product of sets $I \cdot J$ satisfies the conditions of an additive subgroup and external absorption. Furthermore, the non-zero element $d_1 d_2 \in \mathcal{O}_K$ satisfies $(d_1 d_2)(I \cdot J) = (d_1 I)(d_2 J) \subseteq \mathcal{O}_K$. Thus, $I \cdot J$ has a common denominator, so $I \cdot J \in \mathcal{I}_K$.
- Associativity and Commutativity: They are directly inherited from the associative and commutative laws of multiplication in the base field K.
- Identity Element: The ring of integers itself, viewed as the principal ideal $\mathcal{O}_K = (1)$, acts as the identity since $I \cdot \mathcal{O}_K = I$ for all $I \in \mathcal{I}_K$.

Proof: Group Structure of $\mathcal{I}_K$ (Part 2)

Proof of the Inverse Element

Given $I \in \mathcal{I}_K$, we define the inverse set as:

$$I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}$$

- Fractional Ideal Property: It is an additive subgroup and closed under external multiplication by $\mathcal{O}_K$. To find its denominator, we take any fixed and non-zero element $\alpha \in I$. By definition of I^{-1}, for all $x \in I^{-1}$ it holds that $x\alpha \in \mathcal{O}_K$. This implies that $\alpha I^{-1} \subseteq \mathcal{O}_K$, which guarantees that I^{-1} is a fractional ideal.
- Exact Inversion: By definition, $I \cdot I^{-1} \subseteq \mathcal{O}_K$, constituting an ordinary integral ideal. Since $\mathcal{O}_K$ is a Dedekind domain, the structural property of its maximal ideals and localization guarantee that this containment is actually a strict equality $I \cdot I^{-1} = \mathcal{O}_K$. ∎

The Ideal Class Group

Definition 3.3 (Principal Fractional Ideal)

A fractional ideal I is **principal** *if there exists an element $x \in K^\times$ such that $I = (x) = x\mathcal{O}_K$. The set of these ideals forms a subgroup of $\mathcal{I}_K$ which we denote by $\mathcal{P}_K$.*

Definition 3.4 (Ideal Class Group)

We define the **Ideal Class Group** *$Cl(\mathcal{O}_K)$ as the quotient group:*

$$Cl(\mathcal{O}_K) = \mathcal{I}_K / \mathcal{P}_K$$

Its order is denoted as $h_K = |Cl(\mathcal{O}_K)|$ and is called the class number or Class Number.

The Arithmetic Equivalence Theorem

Theorem 3.5 (Theorem of the Three Equivalences)

Let $\mathcal{O}_K$ be the ring of integers of a number field K. The following three statements are completely equivalent:

1. *The class number is one ($h_K = 1$).*
2. *$\mathcal{O}_K$ is a Principal Ideal Domain (PID).*
3. *$\mathcal{O}_K$ is a Unique Factorization Domain (UFD).*

Interpretation

This result formally establishes that the size and structure of the class group measure with mathematical precision the deviation of the ring from the unique factorization property.

The Finiteness of the Class Number

Theorem 3.6 (Finiteness of the Class Number)

For any number field K, the Ideal Class Group $Cl(\mathcal{O}_K)$ is a finite group, that is, $h_K < \infty$.

Minkowski's Strategy

For each number field K, there exists a constant $M_K \geq 1$ such that every ideal class in $Cl(\mathcal{O}_K)$ contains at least one representative integral ideal $J \subseteq \mathcal{O}_K$ whose norm satisfies the inequality:

$$N(J) \leq M_K$$

Since there exists only a finite number of integral ideals with norm less than or equal to any fixed constant in $\mathcal{O}_K$, the total number of equivalence classes must necessarily be finite.

Thanks

Thanks!