AN INTRODUCTION TO CLASS GROUPS

ROY EDUARDO YARANGA ALMEIDA

Abstract. We study the ideal class group in the context of algebraic number theory. We begin by establishing the fundamental tools of divisibility, irreducible and prime elements, structurally analyzing the causes behind the failure of unique factorization in general integral domains. Next, the concept of a Dedekind domain is presented to illustrate how the treatment by means of ideals recovers the uniqueness of factorization. By rigorously implementing these algebraic tools in the ring of integers $\mathcal{O}_K$ of a number field K, we lay the groundwork for introducing the ideal class group $\mathcal{C}_K$, which quantifies the "distance" between $\mathcal{O}_K$ and a unique factorization domain. Finally, we address the fundamental theorem of the finiteness of the class number by means of the Minkowski bound.

1. Introduction

Modern algebraic number theory was born in the nineteenth century from the attempt to solve classical problems in number theory, among them Fermat's Last Theorem and the higher reciprocity laws. For decades, mathematicians had successfully used extensions of the rational numbers, such as the Gaussian integers $\mathbb{Z}[i]$, where the property of unique factorization remained unchanged. However, as they moved into more general cyclotomic and quadratic fields, they encountered an unexpected and profound obstacle: the collapse of unique factorization of elements into prime factors within these new rings of integers.

This phenomenon became apparent in the work of Gabriel Lamé and Ernst Kummer. In his search for a proof of Fermat's theorem for arbitrary prime exponents, Kummer identified that the loss of unique factorization prevented progress in the traditional proofs. To remedy this deficiency, he introduced the concept of "ideal numbers." These were not elements of the field in the conventional sense, but rather abstract entities that acted as invisible prime factors, formally restoring unique divisibility. Using this approach, Kummer was able to prove Fermat's theorem for a broad class of exponents, called regular primes.

Despite Kummer's success, his approach depended on cyclotomic fields and lacked a general axiomatic foundation. Richard Dedekind revolutionized the

Date: 20-06-2026.

discipline by introducing a purely structural perspective, defining "ideals" as subsets of a ring closed under addition and external multiplication. With this, Dedekind proved that in rings of integers—the modern Dedekind domains—every nonzero proper ideal factors uniquely as a product of prime ideals, restoring at the level of ideals the uniqueness that was lost for elements.

The historical development of these ideas is widely documented and analyzed. For an in-depth analysis of this period and its conceptual motivations, one may consult the texts of Edwards [1] and Kleiner [2].

2. Foundations of Algebraic Number Theory

Before defining a Dedekind domain, we need the basic language of divisibility, irreducible and prime elements, and the elementary theory of ideals.

2.1. **Domains and Units.**

Definition 2.1 (Integral domain)**.** An *integral domain* is a commutative ring D with identity 1_D and with no zero divisors: if $\alpha, \beta \in D$ satisfy $\alpha\beta = 0$, then $\alpha = 0$ or $\beta = 0$.

Proposition 2.2 (Cancellation Law)**.** *Let D be an integral domain and let $\alpha, \beta, \gamma \in D$ with $\alpha \neq 0$. If $\alpha\beta = \alpha\gamma$, then $\beta = \gamma$.*

Proof. Since $\alpha\beta = \alpha\gamma$, we have $\alpha\beta - \alpha\gamma = \alpha(\beta - \gamma) = 0$. Since D is an integral domain and $\alpha \neq 0$, the absence of zero divisors forces $\beta - \gamma = 0$, that is, $\beta = \gamma$. ■

The cancellation just proved is the tool that allows one to translate injectivity into surjectivity when the domain is finite, as the following result shows.

Lemma 2.3. *Every finite integral domain is a field.*

Proof. Let D be a finite integral domain and let $\alpha \in D$ be nonzero. Consider the map $\varphi_\alpha : D \to D$ given by $\varphi_\alpha(x) = \alpha x$. This map is injective: if $\alpha x = \alpha y$, then by the Cancellation Law, $x = y$. Since D is finite, every injective map from D to itself is also surjective. In particular, there exists $\beta \in D$ such that $\varphi_\alpha(\beta) = \alpha\beta = 1_D$, so α is a unit. Since α was an arbitrary nonzero element of D, every nonzero element of D is a unit, and therefore D is a field. ■

Definition 2.4 (Divisibility)**.** For $\alpha, \beta \in D$, we say that α *divides* β, written $\alpha \mid \beta$, if there exists $\gamma \in D$ such that $\beta = \alpha\gamma$.

Definition 2.5 (Units)**.** An element $\alpha \in D$ is a *unit* if there exists $\beta \in D$ such that $\alpha\beta = 1_D$. The set of units is denoted U_D.

Definition 2.6 (Associates)**.** Elements $\alpha, \beta \in D$ are *associates*, written $\alpha \sim \beta$, if there exists $u \in U_D$ such that $\alpha = u\beta$.

Proposition 2.7. *The relation $\sim$ is an equivalence relation on D, and U_D is an abelian group under multiplication.*

Proof. Reflexivity. Given $a \in D$, the equality $a = 1_D \cdot a$ shows that $a \mid a$, whence $a \sim a$.

Symmetry. The very definition of $a \sim b$ requires $a \mid b$ and $b \mid a$ simultaneously; this condition is symmetric in a and b, so $a \sim b$ implies $b \sim a$.

Transitivity. Let $a \sim b$ and $b \sim c$. Then $a \mid b$, say $b = ax$ for some $x \in D$, and $b \mid c$, say $c = by$ for some $y \in D$. Substituting, $c = by = (ax)y = a(xy)$, so $a \mid c$. The same argument applied to $c \mid b$ and $b \mid a$ gives $c \mid a$. Hence $a \sim c$, and $\sim$ is an equivalence relation.

For the second assertion, we verify that $(U_D, \cdot)$ is an abelian group. First, $1_D \in U_D$ because 1_D is its own inverse. If $u, v \in U_D$ have inverses $u^{-1}, v^{-1} \in D$, the commutativity of D gives

$$(uv)(u^{-1}v^{-1}) = (uu^{-1})(vv^{-1}) = 1_D,$$

so $uv \in U_D$: this is closure. The inverse u^{-1} of any $u \in U_D$ also satisfies $u^{-1}u = 1_D$, hence $u^{-1} \in U_D$, and every element of U_D has an inverse inside U_D. Finally, associativity and commutativity of multiplication in U_D are inherited directly from D, since U_D is a subset closed under the same operation. This completes the verification that U_D is an abelian group. ■

Definition 2.8 (Field of fractions)**.** The *field of fractions* of D is the field F formed by the elements $\alpha\beta^{-1}$ with $\alpha, \beta \in D$, $\beta \neq 0$. We identify D with its isomorphic image inside F.

2.2. **Irreducibles and Primes.** The distinction between irreducible and prime elements, which coincides in $\mathbb{Z}$, is the starting point for understanding why unique factorization may fail in an arbitrary integral domain.

Definition 2.9 (Irreducible)**.** A nonzero nonunit element $\pi \in D$ is *irreducible* if, whenever $\pi = \alpha\gamma$, one of α, γ is a unit.

Definition 2.10 (Prime)**.** A nonzero nonunit element $\pi \in D$ is *prime* if, whenever $\pi \mid \alpha\gamma$, then $\pi \mid \alpha$ or $\pi \mid \gamma$.

Theorem 2.11. *Every prime element of D is irreducible.*

Proof. Let $\pi \in D$ be prime and suppose that $\pi = \alpha\gamma$. Then, in particular, $\pi \mid \alpha\gamma$, so $\pi \mid \alpha$ or $\pi \mid \gamma$. Without loss of generality, suppose that $\pi \mid \alpha$. Then there exists $\delta \in D$ such that $\alpha = \pi\delta$. It follows that $\pi = \alpha\gamma = \pi\delta\gamma$, so, by the Cancellation Law, $1_D = \delta\gamma$, which shows that γ is a unit. Therefore π is irreducible. ■

Definition 2.12 (Unique factorization domain)**.** D is a *factorization domain* if every nonzero nonunit element can be written as a finite product of irreducibles. If this representation is unique up to order and associates, then D is a *unique factorization domain* (UFD).

Theorem 2.13. *Let D be a factorization domain. Then D is a UFD if and only if every irreducible element of D is prime.*

Proof. ($\Rightarrow$) Suppose that every factorization into irreducibles in D is unique up to units and order, and let $p \in D$ be irreducible. To show that p is prime, suppose $p \mid xy$, so $xy = ps$ for some $s \in D$. Factor each of x, y, s into irreducibles:

$$x = u\prod_{i=1}^{m} x_i, \qquad y = v\prod_{i=1}^{n} y_i, \qquad s = w\prod_{i=1}^{k} s_i,$$

with $u, v, w \in U_D$ units and each x_i, y_i, s_i irreducible. The equality $xy = ps$ becomes

$$uv\prod_{i=1}^{m} x_i \prod_{i=1}^{n} y_i = pw\prod_{i=1}^{k} s_i.$$

The left-hand side is a factorization into irreducibles of the same element, and the right-hand side displays p as one of its irreducible factors (up to the unit w). By uniqueness of factorization, p must coincide, up to associates, with one of the x_i or with one of the y_j; that is, $p \mid x$ or $p \mid y$. We conclude that p is prime.

($\Leftarrow$) Now suppose that every irreducible element of D is prime, and let

$$u\,p_1 \cdots p_m = v\,q_1 \cdots q_n, \qquad m \geq n \geq 1,\ u, v \in U_D,$$

be two factorizations into irreducibles of the same element. We proceed by induction on m. If $m = 1$, then necessarily $n = 1$ and there is nothing to prove. Suppose uniqueness is valid for factorizations of length less than m. Since q_n divides the product $u\,p_1 \cdots p_m$ and q_n is prime (by hypothesis), q_n must divide one of the factors p_i; since q_n is not a unit, this forces $q_n \mid p_i$ for some i, that is, p_i and q_n are associates. Reordering, we may assume $i = m$, so $p_m = q_n z$ for some unit z. Cancelling p_m from both sides by means of the Cancellation Law gives

$$u\,p_1 \cdots p_{m-1} = z^{-1} v\,q_1 \cdots q_{n-1}.$$

By the induction hypothesis, $m - 1 = n - 1$, and after reordering, each p_i ($i < m$) is associated to some q_j. Together with $p_m \sim q_n$, this completes the induction. ∎

Theorem 2.13 locates exactly the cause of the failure of unique factorization: it fails if and only if there exist irreducibles that are not prime. This

obstruction, at the level of elements, is what ideal theory corrects at another structural level.

Definition 2.14 (Ideal)**.** An *ideal* of D is a nonempty subset $\mathfrak{a} \subseteq D$ such that $\alpha, \beta \in \mathfrak{a} \Rightarrow \alpha + \beta \in \mathfrak{a}$, and $\alpha \in \mathfrak{a}$, $r \in D \Rightarrow r\alpha \in \mathfrak{a}$.

Definition 2.15 (Ideal generated by a set)**.** If $S \subseteq D$, the *ideal generated by* S, denoted (S), is the smallest ideal of D that contains S. If $S = \{\alpha_1, \ldots, \alpha_n\}$ is finite, we write $(\alpha_1, \ldots, \alpha_n) = \{r_1\alpha_1 + \cdots + r_n\alpha_n : r_i \in D\}$. An ideal is *finitely generated* if it is of this form for some finite set.

Definition 2.16 (Principal and proper ideal)**.** $\mathfrak{a}$ is *principal* if $\mathfrak{a} = (\alpha) := \{r\alpha : r \in D\}$ for some $\alpha \in D$. If $\mathfrak{a} \neq D$, then $\mathfrak{a}$ is *proper*.

Definition 2.17 (Prime ideal)**.** A proper ideal $\mathfrak{p} \subsetneq D$ is *prime* if $\alpha\beta \in \mathfrak{p}$ implies $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$.

Definition 2.18 (Product of ideals)**.** For ideals $\mathfrak{a}, \mathfrak{b}$ of D,

$$\mathfrak{ab} = \left\{ \sum_{j=1}^{n} \alpha_j\beta_j : n \in \mathbb{N},\ \alpha_j \in \mathfrak{a},\ \beta_j \in \mathfrak{b} \right\}.$$

Definition 2.19 (Division of ideals)**.** A nonzero ideal $\mathfrak{a}$ *divides* $\mathfrak{b}$, written $\mathfrak{a} \mid \mathfrak{b}$, if there exists an ideal $\mathfrak{c}$ with $\mathfrak{b} = \mathfrak{ac}$.

Lemma 2.20 (To Divide Is To Contain)**.** *If $\mathfrak{a} \mid \mathfrak{b}$ for ideals of D, then $\mathfrak{b} \subseteq \mathfrak{a}$.*

Proof. Since $\mathfrak{a} \mid \mathfrak{b}$, by definition there exists an ideal $\mathfrak{h}$ of D such that $\mathfrak{b} = \mathfrak{ah}$. But, by the definition of ideal, $\mathfrak{b} = \mathfrak{ah} \subseteq \mathfrak{a}D \subseteq \mathfrak{a}$, as required. ∎

Definition 2.21 (Maximal ideal)**.** A proper ideal $\mathfrak{m} \subsetneq D$ is *maximal* if there is no ideal $\mathfrak{a}$ with $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq D$.

Theorem 2.22. *$\mathfrak{p} \subsetneq D$ is prime if and only if $D/\mathfrak{p}$ is an integral domain.*

Proof. Suppose that $\mathfrak{p}$ is a prime ideal of D. Then $D/\mathfrak{p}$ is a commutative ring with multiplicative identity $1_D + \mathfrak{p}$ and additive identity $0_D + \mathfrak{p}$. We must verify that $D/\mathfrak{p}$ has no zero divisors. If $\alpha, \beta \in D$ are such that $(\alpha + \mathfrak{p})(\beta + \mathfrak{p}) = 0_D + \mathfrak{p} = \mathfrak{p}$, then $\alpha\beta + \mathfrak{p} = \mathfrak{p}$, so $\alpha\beta \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$, that is, $\alpha + \mathfrak{p} = 0_D + \mathfrak{p}$ or $\beta + \mathfrak{p} = 0_D + \mathfrak{p}$. We have shown that $D/\mathfrak{p}$ has no zero divisors, so it is an integral domain.

Conversely, if $D/\mathfrak{p}$ is an integral domain, then $\alpha\beta \in \mathfrak{p}$ implies that

$$(\alpha + \mathfrak{p})(\beta + \mathfrak{p}) = \alpha\beta + \mathfrak{p} = 0_D + \mathfrak{p}.$$

Since $D/\mathfrak{p}$ has no zero divisors, $\alpha + \mathfrak{p} = 0_D + \mathfrak{p}$ or $\beta + \mathfrak{p} = 0_D + \mathfrak{p}$, that is, $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$, so $\mathfrak{p}$ is a prime ideal of D. ∎

Theorem 2.23. *$\mathfrak{m} \subsetneq D$ is maximal if and only if $D/\mathfrak{m}$ is a field.*

Proof. Suppose that $\mathfrak{m}$ is a maximal ideal of D. Since D is a commutative ring with identity, so is $D/\mathfrak{m}$. Let $\alpha + \mathfrak{m} \neq 0_D + \mathfrak{m}$ be a nonzero element of $D/\mathfrak{m}$, that is, $\alpha \notin \mathfrak{m}$. Then the ideal $\mathfrak{m} + (\alpha)$ properly contains $\mathfrak{m}$ (because $\alpha \in \mathfrak{m} + (\alpha)$ but $\alpha \notin \mathfrak{m}$), so, by the maximality of $\mathfrak{m}$, $\mathfrak{m} + (\alpha) = D$. Therefore there exist $m \in \mathfrak{m}$ and $r \in D$ such that

$$1_D = m + r\alpha.$$

Passing to the quotient, $1_D + \mathfrak{m} = r\alpha + \mathfrak{m} = (r + \mathfrak{m})(\alpha + \mathfrak{m})$, that is, $r + \mathfrak{m}$ is the multiplicative inverse of $\alpha + \mathfrak{m}$ in $D/\mathfrak{m}$. Since $\alpha + \mathfrak{m}$ was an arbitrary nonzero element, every nonzero element of $D/\mathfrak{m}$ has an inverse, so $D/\mathfrak{m}$ is a field.

Conversely, suppose that $D/\mathfrak{m}$ is a field. First note that a ring R with identity is a field if and only if its only ideals are (0) and R: if R is a field and $J \neq (0)$ is an ideal, there exists a nonzero element $\beta \in J$, and since β is invertible, $1_R = \beta\beta^{-1} \in J$, hence $J = R$; conversely, if the only ideals of R are (0) and R, and $\beta \in R$ is nonzero, then $(\beta) = R$, so there exists $\gamma \in R$ with $\gamma\beta = 1_R$, and β is invertible.

Now, if $\mathfrak{m} \subseteq I \subseteq D$ for a D-ideal I, then $I/\mathfrak{m}$ is an ideal of $D/\mathfrak{m}$. Since $D/\mathfrak{m}$ is a field, by the preceding paragraph $I/\mathfrak{m} = (0)$ or $I/\mathfrak{m} = D/\mathfrak{m}$, that is, $I = \mathfrak{m}$ or $I = D$. Therefore $\mathfrak{m}$ is maximal. ■

Corollary 2.24. *Every nonzero maximal ideal of D is prime.*

Proof. Let $\mathfrak{m}$ be a nonzero maximal ideal of D. By Theorem 2.23, $D/\mathfrak{m}$ is a field. Every field is, in particular, an integral domain, since it has no zero divisors. Thus $D/\mathfrak{m}$ is an integral domain, and by Theorem 2.22, $\mathfrak{m}$ is a prime ideal of D. ■

2.3. **Noetherian Domains.**

Definition 2.25 (ACC, Noetherian domain)**.** D satisfies the *ascending chain condition* (ACC) if every chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ stabilizes. An integral domain satisfying the ACC is called *Noetherian*.

Lemma 2.26. *D is Noetherian if and only if every ideal of D is finitely generated.*

Proof. Suppose that every D-ideal is finitely generated, and let

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots$$

be an ascending chain of ideals. The union $\mathfrak{a} = \bigcup_{i=1}^{\infty} \mathfrak{a}_i$ is also a D-ideal: if $\alpha, \beta \in \mathfrak{a}$, then $\alpha \in \mathfrak{a}_i$ and $\beta \in \mathfrak{a}_j$ for some i, j, and taking $k = \max\{i, j\}$ gives $\alpha, \beta \in \mathfrak{a}_k$, so $\alpha + \beta \in \mathfrak{a}_k \subseteq \mathfrak{a}$; similarly, if $r \in D$, then $r\alpha \in \mathfrak{a}_i \subseteq \mathfrak{a}$. Since every D-ideal is finitely generated, there exist $\alpha_1, \ldots, \alpha_d \in D$ such that $\mathfrak{a} = (\alpha_1, \ldots, \alpha_d)$. For each $j = 1, \ldots, d$, there exists k_j such that $\alpha_j \in \mathfrak{a}_{k_j}$.

Let $n = \max\{k_1, \dots, k_d\}$. Then, since $\mathfrak{a}_{k_j} \subseteq \mathfrak{a}_n$ for each j (because $k_j \leq n$), we have $(\alpha_1, \dots, \alpha_d) \subseteq \mathfrak{a}_n$, which implies $\mathfrak{a} \subseteq \mathfrak{a}_n$. Since also $\mathfrak{a}_n \subseteq \mathfrak{a}$, it follows that $\mathfrak{a}_n = \mathfrak{a} = \mathfrak{a}_j$ for all $j \geq n$. Thus the chain stabilizes and D satisfies the ACC, that is, D is Noetherian.

Conversely, suppose that D is Noetherian and that $\mathfrak{a}$ is a D-ideal that is not finitely generated. Then $\mathfrak{a} \neq (0)$, so there exists $\alpha_1 \in \mathfrak{a}$ with $\alpha_1 \neq 0$, and $(\alpha_1) \subsetneq \mathfrak{a}$. Since $\mathfrak{a} \neq (\alpha_1)$ (because $\mathfrak{a}$ is not finitely generated, in particular it is not generated by a single element), there exists $\alpha_2 \in \mathfrak{a}$ with $\alpha_2 \notin (\alpha_1)$, so $(\alpha_1) \subsetneq (\alpha_1, \alpha_2) \subsetneq \mathfrak{a}$. Continuing inductively in this way, we obtain a strictly ascending chain of ideals

$$(\alpha_1) \subsetneq (\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq (\alpha_1, \dots, \alpha_n) \subsetneq \cdots \subsetneq \mathfrak{a},$$

which never stabilizes, contradicting the fact that D is Noetherian. Therefore every D-ideal is finitely generated. ■

Corollary 2.27. *If D is Noetherian, every nonempty collection of ideals of D has a maximal element, and every proper ideal is contained in some maximal ideal.*

Proof. Let $\mathcal{T}$ be a nonempty collection of D-ideals, and suppose, seeking a contradiction, that $\mathcal{T}$ has no maximal element. Then, for each $\mathfrak{a} \in \mathcal{T}$, there exists $\mathfrak{b} \in \mathcal{T}$ with $\mathfrak{a} \subsetneq \mathfrak{b}$. Starting from any $\mathfrak{a}_1 \in \mathcal{T}$ and applying this repeatedly, we construct a strictly ascending chain

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \cdots$$

of ideals in $\mathcal{T}$, which never stabilizes, contradicting that D is Noetherian. Therefore $\mathcal{T}$ has a maximal element.

For the second assertion, let $\mathfrak{a}$ be a proper ideal of D, and let $\mathcal{T}$ be the collection of all proper ideals of D containing $\mathfrak{a}$. Since $\mathfrak{a} \in \mathcal{T}$, $\mathcal{T} \neq \varnothing$, so by what we have just proved $\mathcal{T}$ has a maximal element $\mathfrak{m}$. If there were a D-ideal I with $\mathfrak{m} \subsetneq I \subsetneq D$, then $\mathfrak{a} \subseteq \mathfrak{m} \subsetneq I$ would show that $I \in \mathcal{T}$, contradicting the maximality of $\mathfrak{m}$ in $\mathcal{T}$. Therefore $\mathfrak{m}$ is a maximal ideal of D containing $\mathfrak{a}$. ■

Definition 2.28 (Principal ideal domain)**.** D is a *principal ideal domain* (PID) if every ideal of D is principal.

Proposition 2.29. *Every PID is Noetherian.*

Proof. Since D is a PID, every D-ideal $\mathfrak{a}$ is principal, that is, $\mathfrak{a} = (\alpha)$ for some $\alpha \in D$; in particular, $\mathfrak{a}$ is finitely generated (by the single element α). By Lemma 2.26, D is a Noetherian domain. ■

Proposition 2.30. *Every PID is a UFD.*

Proof. We first show that D is a factorization domain, that is, that every nonzero nonunit element of D is a finite product of irreducibles. Let S be the

set of nonzero nonunit elements of D that do not admit such a factorization, and suppose, seeking a contradiction, that $S \neq \varnothing$. Since D is a PID, by Proposition 2.29, D is Noetherian, so by Corollary 2.27 the collection of ideals $\{(\alpha) : \alpha \in S\}$ has a maximal element (m), with $m \in S$.

Since $m \in S$, m is not irreducible (otherwise it would trivially be a product of one irreducible), so $m = \alpha\beta$ with α, β both nonunits. By Lemma 2.20, $(m) \subseteq (\alpha)$. If $(m) = (\alpha)$, then $\alpha = um$ for some unit u, and from $m = \alpha\beta = um\beta$ it follows, by the Cancellation Law (since $m \neq 0$), that $1_D = u\beta$, that is, β is a unit, a contradiction. Thus $(m) \subsetneq (\alpha)$, and by the maximality of (m) among the ideals (α'') with $\alpha'' \in S$, it follows that $\alpha \notin S$. Since α is neither zero nor a unit, α is a product of irreducibles. The same argument, interchanging the roles of α and β, shows that $(m) \subsetneq (\beta)$ and that β is also a product of irreducibles. But then $m = \alpha\beta$ is a product of irreducibles, contradicting $m \in S$. Therefore $S = \varnothing$, and D is a factorization domain.

It remains to show that every irreducible element of D is prime, and then invoke Theorem 2.13. Let $r \in D$ be irreducible, and suppose that $r \mid \alpha\beta$ with $\alpha, \beta \in D$, and that $r \nmid \alpha$. Consider the ideal (r, α); since D is a PID, $(r, \alpha) = (d)$ for some $d \in D$. In particular $d \mid r$, so by the irreducibility of r, d is either a unit or an associate of r. If d were an associate of r, then from $d \mid \alpha$ it would follow that $r \mid \alpha$, contradicting the hypothesis. Therefore d is a unit, and so $(r, \alpha) = (d) = D$. In particular, there exist $s_1, s_2 \in D$ such that

$$1_D = rs_1 + \alpha s_2.$$

Multiplying by β,

$$\beta = rs_1\beta + \alpha s_2\beta = rs_1\beta + (\alpha\beta)s_2 = r(s_1\beta) + (rt)s_2 = r(s_1\beta + ts_2),$$

where $t \in D$ is such that $\alpha\beta = rt$ (because $r \mid \alpha\beta$). Therefore $r \mid \beta$, so r is prime.

Since D is a factorization domain in which every irreducible is prime, by Theorem 2.13, D is a UFD. ■

With divisibility, ideals, and the ACC already established, we can introduce the class of domains in which factorization of ideals is indeed unique.

3. Dedekind Domains

3.1. **Integrality and Integral Closure.**

Definition 3.1 (Integral element, integral closure)**.** Let $D \subseteq S$ be an extension of integral domains. An element $\alpha \in S$ is *integral over* D if it is a root of a monic polynomial with coefficients in D. The domain D is *integrally closed in* S if every element of S integral over D already belongs to D. If F is the field of fractions of D, we say that D is *integrally closed* if it is integrally closed in F.

Theorem 3.2 (Transitivity of Integrality)**.** *Let $R \subseteq S \subseteq T$ be a tower of integral domains with S integral over R, and let $t \in T$ be integral over S. Then t is integral over R.*

3.2. **Definition of a Dedekind Domain.**

Definition 3.3 (Dedekind domain)**.** A *Dedekind domain* is an integral domain D such that: (1) D is Noetherian; (2) D is integrally closed in its field of fractions F; (3) every nonzero prime ideal of D is maximal.

3.3. **Fractional Ideals and Invertibility.** To invert ideals, we enlarge the notion of ideal beyond subsets of D.

Definition 3.4 (Fractional ideal)**.** Let D be an integral domain with field of fractions F. A nonempty subset $\mathfrak{a} \subseteq F$ is a *fractional ideal* if it is closed under addition, closed under multiplication by elements of D, and there exists a nonzero $\gamma \in D$ with $\gamma\mathfrak{a} \subseteq D$. If $\mathfrak{a} \subseteq D$, we say that $\mathfrak{a}$ is *integral*.

Theorem 3.5. *Let $\mathfrak{a}$ be a fractional ideal of D. Then $\mathfrak{a}^{-1} := \{\alpha \in F : \alpha\mathfrak{a} \subseteq D\}$ is also a nonzero fractional ideal.*

Definition 3.6 (Invertibility)**.** $\mathfrak{a}$ is *invertible* if $\mathfrak{a}^{-1}\mathfrak{a} = D$.

Theorem 3.7 (Invertibility in Dedekind Domains)**.** *If D is a Dedekind domain, every nonzero integral ideal of D is invertible.*

3.4. **Unique Factorization of Ideals.**

Corollary 3.8 (To Divide Is the Same as To Contain)**.** *Let D be a Dedekind domain and let $\mathfrak{a}, \mathfrak{b}$ be ideals of D. Then $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a}$.*

Unlike Lemma 2.20, which is valid in any integral domain, this corollary is an equivalence and is exclusive to Dedekind domains: it is invertibility (Theorem 3.7) that makes it possible to recover $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$ from $\mathfrak{b} \subseteq \mathfrak{a}$.

Theorem 3.9 (Unique Factorization of Ideals)**.** *Every nonzero proper ideal of a Dedekind domain D can be represented uniquely, up to order, as*

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_n^{a_n},$$

with the $\mathfrak{p}_i$ distinct prime ideals of D and $a_i \in \mathbb{N}$.

Although unique factorization of *elements* may fail in D (Theorem 2.13), unique factorization of *ideals* never fails in a Dedekind domain.

In fact, unique factorization of ideals makes it possible to specify exactly when factorization of *elements* is unique:

Theorem 3.10 (UFD and PID in Dedekind Domains)**.** *Let D be a Dedekind domain. Then D is a UFD if and only if D is a PID.*

This equivalence—exclusive to Dedekind domains, since in general PID implies UFD but not conversely—is what gives precise meaning to the class number that we define in Section 5.

4. The Ring of Integers

We now apply the preceding theory to the central object of algebraic number theory: the ring of integers of a number field.

4.1. Algebraic Numbers and Number Fields.

Definition 4.1 (Algebraic number, algebraic integer)**.** An *algebraic number* is an element $\alpha \in \mathbb{C}$ that is a root of some nonzero polynomial with rational coefficients. If α is a root of a *monic* polynomial with integer coefficients, it is called an *algebraic integer*.

Definition 4.2 (Number field)**.** A *number field* is a finite extension K of $\mathbb{Q}$: $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for algebraic numbers $\alpha_1, \ldots, \alpha_n$, viewed as a finite-dimensional $\mathbb{Q}$-vector space.

Definition 4.3 (Degree)**.** The *degree* of a number field K, denoted $[K : \mathbb{Q}]$, is its dimension as a $\mathbb{Q}$-vector space.

Theorem 4.4 (Primitive Element Theorem)**.** *Every number field K is a simple extension of $\mathbb{Q}$: there exists an algebraic integer α such that $K = \mathbb{Q}(\alpha)$.*

4.2. The Ring $\mathcal{O}_K$.

Definition 4.5 (Ring of integers)**.** The *ring of integers* of K, denoted $\mathcal{O}_K$, is the set of algebraic integers contained in K.

Proposition 4.6. *$\mathcal{O}_K$ is a subring of K, and $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$.*

Proposition 4.7. *The field of fractions of $\mathcal{O}_K$ is K.*

Theorem 4.8 (Existence of an Integral Basis)**.** *Every number field K of degree n over $\mathbb{Q}$ admits an* integral basis*: $\{\omega_1, \ldots, \omega_n\} \subseteq \mathcal{O}_K$ such that every element of $\mathcal{O}_K$ can be written uniquely as a $\mathbb{Z}$-linear combination of the ω_i. In particular, $\mathcal{O}_K$ is a free abelian group of rank n.*

Corollary 4.9. *$\mathcal{O}_K$ is a Noetherian domain, since by Theorem 4.8 it is finitely generated as a $\mathbb{Z}$-module.*

4.3. Structural Properties.

Lemma 4.10. *Let K be a number field and let $\mathfrak{p}$ be a nonzero ideal of $\mathcal{O}_K$. Then $\mathfrak{p} \cap \mathbb{Z}$ contains a nonzero element.*

Corollary 4.11. *If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p}$ is a finite field.*

Theorem 4.12 (Rings of Integers Are Dedekind Domains)**.** *For every number field K, the ring $\mathcal{O}_K$ is a Dedekind domain.*

The three requirements of Definition 3.3 are verified as follows:

- $\mathcal{O}_K$ is Noetherian because, by Theorem 4.8, it is finitely generated as a $\mathbb{Z}$-module.
- $\mathcal{O}_K$ is integrally closed by transitivity of integrality (Theorem 3.2): being integral over $\mathcal{O}_K$ already implies being integral over $\mathbb{Z}$, that is, being an algebraic integer.
- Every nonzero prime ideal of $\mathcal{O}_K$ is maximal by Corollary 4.11 (every finite integral domain is a field).

This theorem is the hinge of the paper: it guarantees that, although unique factorization of elements may fail in $\mathcal{O}_K$, factorization of ideals (Theorem 3.9) always holds.

5. The Ideal Class Group

Although Theorem 3.9 restores unique factorization at the level of ideals in $\mathcal{O}_K$, a natural question remains: how far is $\mathcal{O}_K$ from also having unique factorization at the level of *elements*? By Theorem 3.10, that distance is measured by the existence of ideals that are not principal. The ideal class group, which we introduce in this section, quantifies exactly that distance.

5.1. The Norm of an Ideal.

To extend the notion of size to ideals, we use the additive group structure of the ring of integers.

Definition 5.1 (Norm of an ideal)**.** The *norm* of a nonzero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ is the index of $\mathfrak{a}$ as an additive subgroup of the ring of integers:

$$N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = |\mathcal{O}_K/\mathfrak{a}|.$$

Since $\mathcal{O}_K$ is a Dedekind domain, the quotient $\mathcal{O}_K/\mathfrak{a}$ is always a finite ring, which guarantees that the norm is a natural number.

Theorem 5.2 (Finiteness and Multiplicativity of the Norm of Ideals)**.** *Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ be nonzero ideals. Then $N(\mathfrak{a})$ is a positive integer, and*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

5.2. Fractional Ideals of $\mathcal{O}_K$ and Invertibility.

Definition 5.3 (Fractional ideal of $\mathcal{O}_K$)**.** A *fractional ideal* of $\mathcal{O}_K$ is a nonzero $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K such that there exists a nonzero $\gamma \in \mathcal{O}_K$ with $\gamma\mathfrak{a} \subseteq \mathcal{O}_K$. A fractional ideal $\mathfrak{a}$ is *principal* if $\mathfrak{a} = (\alpha) := \alpha\mathcal{O}_K$ for some $\alpha \in K^\times$.

Since $\mathcal{O}_K$ is a Dedekind domain (Theorem 4.12), Theorem 3.7 guarantees that every nonzero integral ideal of $\mathcal{O}_K$ is invertible; this invertibility extends naturally to all fractional ideals.

Definition 5.4 (Product of fractional ideals)**.** If $\mathfrak{a}, \mathfrak{b}$ are fractional ideals of $\mathcal{O}_K$, their product is

$$\mathfrak{ab} = \left\{ \sum_{j=1}^{n} \alpha_j \beta_j : \alpha_j \in \mathfrak{a},\ \beta_j \in \mathfrak{b} \right\},$$

extending the definition of product of integral ideals from Section 2.3.

Theorem 5.5. *The set* $\mathrm{Id}(\mathcal{O}_K)$ *of all nonzero fractional ideals of* $\mathcal{O}_K$ *forms an abelian group under multiplication of ideals, with identity element* $\mathcal{O}_K$ *and with* $\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathcal{O}_K\}$ *as the inverse of* $\mathfrak{a}$*.*

5.3. **The Class Group.**

Definition 5.6 (Class group, class number)**.** The subset $P(\mathcal{O}_K) \subseteq \mathrm{Id}(\mathcal{O}_K)$ of principal fractional ideals is a subgroup. The *ideal class group* of K is the quotient group

$$C_K := \mathrm{Id}(\mathcal{O}_K)/P(\mathcal{O}_K).$$

Its order h_K is called the *class number* of K.

The class number h_K is precisely the desired measure. If $h_K = 1$, every fractional ideal is principal, and in particular every integral ideal of $\mathcal{O}_K$ is principal; that is, $\mathcal{O}_K$ is a PID (Section 2.4). By Theorem 3.10, this is equivalent to $\mathcal{O}_K$ having unique factorization of elements. When $h_K > 1$, the group C_K measures precisely how many classes of nonprincipal ideals there are, and therefore how far $\mathcal{O}_K$ is from unique factorization.

5.4. **Finiteness of the Class Number.**

We now state, without proof and following Milne and Stein, the bound that makes it possible to prove that $\mathcal{C}_K$ is finite.

Lemma 5.7 (Finiteness of Ideals of Bounded Norm)**.** *For every number field* K *and every* $M > 0$*, there are only finitely many integral ideals* $\mathfrak{a} \subseteq \mathcal{O}_K$ *such that* $N(\mathfrak{a}) \leq M$*.*

Theorem 5.8 (Minkowski Bound)**.** *For every number field* K *there exists a constant* $M_K \geq 1$*, depending only on* K*, such that every class of* $\mathcal{C}_K$ *contains at least one integral ideal representative* $\mathfrak{a} \subseteq \mathcal{O}_K$ *whose norm satisfies*

$$N(\mathfrak{a}) \leq M_K.$$

Theorem 5.9 (Finiteness of the Class Number)**.** *For every number field* K*, the class group* $\mathcal{C}_K$ *is finite; that is,* $h_K < \infty$*.*

By Lemma 5.8, there are only finitely many integral ideals of norm at most M_K. By Theorem 5.9, each class of $\mathcal{C}_K$ is represented by at least one of those

finitely many ideals. Hence $\mathcal{C}_K$ has at most as many elements as there are integral ideals of norm $\leq M_K$; in particular, it is finite.

It is worth emphasizing that, although the preceding results establish the finiteness of the class group theoretically, the explicit determination of the Minkowski bound and the execution of the complete proof of this theorem involve tools that connect the geometry of numbers with the analysis of lattices in real vector spaces. For the reader interested in studying the technical details of this proof in depth, Daniel Marcus's book *Number Fields* [3] offers a fully developed proof of the finiteness of the class number from the first principles of the geometry of Minkowski.

References

[1] H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 50, Springer-Verlag, New York, 1977.
[2] I. Kleiner, *A History of Abstract Algebra*, Birkhäuser, Boston, 2007.
[3] D. A. Marcus, *Number Fields*, Universitext, 2nd Edition, Springer, Cham, 2018.

Euler Circle, Mountain View, CA 94040
Email address: r.yaranga.almeida@gmail.com