MINKOWSKI THEORY AND THE CLASS NUMBER

BROOKE ULLERY

Abstract. This paper gives a basic introduction to Minkowski Theory and the class group, leading up to a proof that the class number (the order of the class group) is finite. This paper is based on Jürgen Neukirch's *Algebraic Number Theory*, but provides more detailed proofs and explanations as well as numerous examples. The goal of this paper is to present the concepts in Neukirch's book in such a way that they are more accessible to a student with a background in basic abstract algebra.

Contents

1. Integrality and Algebraic Integers

In field theory, we define an algebraic number as an element of a finite field extension of $\mathbb{Q}$. Equivalently, $\alpha \in \mathbb{C}$ is an **algebraic number** if α is a root of some nonzero polynomial $q(x) \in \mathbb{Q}[x]$. When dealing with the rings contained in algebraic extensions of $\mathbb{Q}$, we use the notion of integrality, and in particular, that of an algebraic integer. An algebraic number is an **algebraic integer** if it is a root of a monic polynomial with integer coefficients.

We now define the more general notion of integrality:

Definition 1.1. Let $R \subseteq S$ be a ring extension, where R and S are commutative rings with 1. An element $s \in S$ is **integral** over R if s is a root of a monic polynomial $a(x) \in R[x]$. The ring S is **integral** over R if all elements $s \in S$ are integral over R.

From now on, we will assume that all rings mentioned are integral domains and have a multiplicative identity 1.

We know that the algebraic closure of a field is simply the set of all elements algebraic over the field. There is an analogous definition for the integral closure of a ring extension, except that we define it with respect to a field containing the ring under consideration:

Date: August 5, 2008.

Definition 1.2. Let $R \subseteq S$ be a ring extension. The **integral closure** of R in S, denoted $\bar{R}$ is the set of all elements of S that are integral over R. That is,

$$\bar{R} = \{s \in S \mid s \text{ integral over } R\}.$$

The integral closure of a ring turns out to be a ring itself– a fact that is surprisingly nontrivial to prove. To begin, we prove a lemma that relates integrality to module theory.

Lemma 1.3. *Let R be a subring of S, and let $s \in S$ be integral over R. Then $R[s]$ is a finitely generated R-module.*

Proof. Since s is integral over R, we can find a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in R[x]$ such that $f(s) = 0$. Then we have

$$\begin{aligned} & s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0 \\ \Rightarrow \qquad & s^n = -(a_{n-1}s^{n-1} + \cdots + a_0). \end{aligned}$$

Thus, s^n (and therefore all higher powers of s) can be expressed as R-linear combinations of $s^{n-1}, \ldots, s, 1$. Thus, $R[s] = R1 + Rs + \cdots + Rs^{n-1}$, which means that $R[s]$ is a finitely generated R-module, as desired. □

In addition, note that the converse holds, but for the purposes of this paper, we will not prove it. By translating the notion of integrality into module theory, we are able to avoid discussing everything in terms of roots of monic polynomials, which tends to simplify proofs involving integrality. In fact, using the above lemma, the following proof becomes relatively simple.

Lemma 1.4. *Let $\bar{R}$ be the integral closure in a ring S of a ring R. Then $\bar{R}$ is a ring.*

Proof. Since S is a ring, we need only show that $\bar{R}$ is a subring of S, that is, that $\bar{R}$ is closed under addition and multiplication. Let x and y be elements of $\bar{R}$. Then, by the previous lemma, $R[x]$ and $R[y]$ are finitely generated R-modules. Clearly, y is integral over $R[x]$, so $(R[x])[y] = R[x, y]$ is a finitely generated $R[x]$-module. Let $p_1(x, y), \ldots, p_m(x, y)$ be a generating set for $R[x, y]$, and let $q_1(x), \ldots, q_m(x)$ be a generating set for $R[x]$. Then $R[x, y]$ is a finitely generated R-module with generating set

$$\sum_{j=1}^{n} \left(q_j(x) \sum_{i=1}^{m} p_i(x) \right).$$

$xy, x \pm y \in R[x, y]$, so they are integral over R, which means that they are contained in $\bar{R}$, as desired. Thus, $\bar{R}$ is a ring. □

Definition 1.5. Let S be a extension of a ring R. R is **integrally closed** in S if it is its own integral closure in S, that is, if $\bar{R} = R$.

When we state that a ring is integrally closed without stating in which ring, we mean that it is integrally closed in its field of fractions.

In order for an algebraic number to be an algebraic integer, it need only be a root of *some* monic polynomial with integer coefficients, as explained above. This can be a difficult condition to check, which brings us to the following lemma.

Lemma 1.6. *An algebraic number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.*

Proof. Suppose first that the minimal polynomial for α over $\mathbb{Q}$ has integer coefficients. Then by definition (since the minimal polynomial is monic), α is an algebraic integer.

Conversely, suppose that α is an algebraic integer, and let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of minimum degree with α as a root. If f were reducible in $\mathbb{Q}[x]$, then, by Gauss' Lemma, f would be reducible in $\mathbb{Z}[x]$. We would thus have two monic polynomials $g(x), h(x) \in \mathbb{Z}[x]$ of smaller degree than f such that $f(x) = g(x)h(x)$, contradicting the fact that f is of minimum degree. Thus, f must be irreducible in $\mathbb{Q}[x]$, so $f(x)$ must be the minimal polynomial for α over $\mathbb{Q}$. Thus, the minimal polynomial has integer coefficients. □

Since the only elements of $\mathbb{Q}$, with minimal polynomials having integer coefficients are the integers themselves, we immediately observe the following:

Corollary 1.7. *$\mathbb{Z}$ is integrally closed. That is, the only algebraic integers in $\mathbb{Q}$ are the integers themselves.*

2. Rings of Integers and Dedekind Domains

When we mentioned the algebraic integers in $\mathbb{Q}$ in the previous section, we were actually referring to the ring of integers of $\mathbb{Q}$, or $\mathcal{O}_{\mathbb{Q}}$. More generally, the **ring of integers** $\mathcal{O}_K$ of an algebraic field extension $K/\mathbb{Q}$ is the integral closure of $\mathbb{Z}$ in K. That is, it is the set of all algebraic integers contained in K. Of course, the example of $\mathcal{O}_{\mathbb{Q}}$ is rather uninteresting, but nontrivial extensions of $\mathbb{Q}$ have rings of integers containing more than just $\mathbb{Z}$. For instance, for $K = \mathbb{Q}[\sqrt{2}]$ we have $\sqrt{2} \in \mathcal{O}_K$. $\mathcal{O}_K$ the *ring* of integers of K, but we know that it is in fact a ring, since, as shown earlier, the integral closure of a ring is a ring itself. Moreover, we can prove something stronger: $\mathcal{O}_K$ is a Dedekind domain. We will explain and prove all this presently, but we must first provide a few definitions and lemmas that will prove very useful.

We begin by defining the discriminant, a concept upon which much of the remainder of the paper will depend.

Definition 2.1. Let L/K be a separable field extension of degree n, and let $\alpha_1, \ldots, \alpha_n$ be a K-basis. Then the **discriminant** of the basis is defined by

$$d(\alpha_1, \ldots, \alpha_n) = \left(det \begin{pmatrix} \sigma_1\alpha_1 & \sigma_2\alpha_1 & \cdots & \sigma_n\alpha_1 \\ \sigma_1\alpha_2 & \sigma_2\alpha_2 & & \vdots \\ \vdots & & \ddots & \\ \sigma_1\alpha_n & \cdots & & \sigma_n\alpha_n \end{pmatrix} \right)^2,$$

where $\sigma_1, \ldots, \sigma_n$ are the n K-embeddings of L.

When we are referring to the discriminant of a basis of $\mathcal{O}_K$, we simply call it the **discriminant of the algebraic number field** K, and we denote it by d_K. Similarly, we denote the discriminant of the basis of an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ by $d(\mathfrak{a})$. We need not specify the basis in these cases because these rings admit integral bases (a term that we will define shortly) and the discriminant is independent of the choice of integral basis.

We must also now define two other important concepts, the trace and the norm, but we will define them only in the context of finite separable extensions since those will be the only extensions we will be dealing with from now on.

Definition 2.2. Let L/K be a separable extension of degree n and let $\sigma_1, \ldots, \sigma_n$ be the n K-embeddings of L. Let $x \in L$. Then we have

(1) The trace of x is defined as

$$Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i x.$$

(2) The norm of x is defined as

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i x.$$

Our goal in this section, as described earlier, is to show that $\mathcal{O}_K$ is a Dedekind domain. In order to do this, we first return to module theory.

Definition 2.3. Let R be a ring, and let M be an R-module. M is a **free R-module** on the subset C of M if for all $x \in M$, such that $x \neq 0$, there exist unique elements $r_1, \ldots, r_n \in R$ and unique $c_1, \ldots, c_n \in C$, for some positive integer n, such that $x = r_1c_1 + r_2c_2 + \ldots + r_na_n$. We call C a **set of free generators** for M. For commutative R, the cardinality of C is called the **rank** of M.

In the special case where A is an integrally closed integral domain with K as its field of fractions, and L/K is a finite, separable field extension with B as the integral closure of A in L, then B is a free A-module if and only if (by the definition above) B contains a set of free generators, $D = \{\omega_1, \omega_2, \ldots, \omega_n\}$. However, in this particular situation, we call D an **integral basis** of B over A. We notice that D is automatically a K-basis of L, so that n is equal to the degree $[L : K]$ of the field extension. To more clearly illustrate the concept of an integral basis, we give the classic example in number theory of the ring of integers in quadratic extensions of $\mathbb{Q}$, the first part of which is based on an example given in Dummit and Foote's *Abstract Algebra*:

Example 2.4. Let K be a quadratic extension of $\mathbb{Q}$. Then $K = \sqrt{D}$ for some squarefree integer D. Let d be the discriminant of the quadratic number field K, and let $\{1, \omega\}$ be an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$, so that $\mathcal{O}_K = \mathbb{Z}[\omega]$. We will first show that

$$\omega = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod 4 \\ \sqrt{D}, & \text{if } D \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

It is clear that ω is integral over $\mathbb{Z}$ in both cases, satisfying

$$\omega^2 - \omega + (1 - D)/4 = 0$$

in the first case and

$$\omega^2 - D = 0$$

in the second. Thus, ω is indeed an algebraic integer, which means that $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$.

Now we show that $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$. Let $\alpha \in K$, so that $\alpha = a + b\sqrt{D}$, where $a, b \in \mathbb{Q}$. Let α be an algebraic integer. If $b = 0$, then $\alpha \in \mathbb{Q}$, so $\alpha \in \mathbb{Z} \subseteq \mathbb{Z}[\omega]$. Thus, we can assume that $b \neq 0$. Then, the minimal polynomial for α is

$$\begin{aligned} m(x) &= \left[x - \left(a - b\sqrt{D}\right)\right]\left[x - \left(a + b\sqrt{D}\right)\right] \\ &= x^2 - 2ax + (a^2 - b^2D). \end{aligned}$$

By Lemma 1.6, we know that $2a$ and $a^2 - b^2D$ are both integers, giving us

$$4(a^2 - b^2D) = (2a)^2 - (2b)^2D \in \mathbb{Z}.$$

Since $2a$ is an integer, $(2a)^2$ must be an integer, so $(2b)^2D = 4b^2D$ is an integer as well. Since D is an integer, it must be divisible by the denominator of $(2b)^2$. Since D is squarefree, this means that $(2b)^2$ has a denominator equal to one. That is, $(2b)^2$ is an integer, so $2b$ is an integer as well. Thus, we can write $a = x/2$ and $b = y/2$, where $x, y \in \mathbb{Z}$. Now, suppose

$$a^2 - b^2D \equiv z \pmod 4.$$

Then

$$\begin{aligned} & \left(\frac{x}{2}\right)^2 - \left(\frac{y}{2}\right)^2 D \equiv z \pmod 4 \\ \Rightarrow \quad & x^2 - y^2D \equiv 4z \pmod 4 \equiv 0 \pmod 4 \\ \Rightarrow \quad & x^2 \equiv y^2D \pmod 4. \end{aligned}$$

We recall from elementary number theory that an integer i is odd if and only if $i^2 \equiv 1 \pmod 4$ and i is even if and only if $i^2 \equiv 0 \pmod 4$. We also know that D is not divisible by 4. Thus we have two cases:

Case 1: $D \equiv 1 \pmod 4$. Then $x^2 \equiv y^2 \equiv 0$ or $1 \pmod 4$, so x and y are either both even or both odd. Suppose both are even. Then

$$\begin{aligned} \alpha = a + b\sqrt{D} &= \frac{x}{2} + \frac{y}{2}\sqrt{D} \\ &= \frac{x}{2} + \frac{y\sqrt{D}}{2} + \frac{y}{2} - \frac{x}{2} \\ &= \frac{x-y}{2} + y\left(\frac{1+\sqrt{D}}{2}\right) \\ &= \frac{x-y}{2} + y\omega. \end{aligned}$$

Since x and y are of the same parity, $x-y$ is even, so $(x-y)/2 \in \mathbb{Z}$. Thus, $\alpha \in \mathbb{Z}[\omega]$, as desired.

Case 2: $D \equiv 2$ or $3 \pmod 4$. Then $x^2 \equiv 2y^2$ or $3y^2 \pmod 4$. The only way this holds is if $x \equiv y \equiv 0 \pmod 4$, which implies that x and y are both even. Thus, $a, b \in \mathbb{Z}$, so $\alpha \in \mathbb{Z}[\omega]$, and we are done.

Now it is simple to show that

$$d = \begin{cases} D, & \text{if } D \equiv 1 \pmod 4 \\ 4D, & \text{if } D \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

First, suppose $D \equiv 1 \pmod 4$. Then, using our formula for the discriminant, we have

$$\begin{aligned} d &= \left(det \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}\right)^2 \\ &= \left[\left(\frac{1+\sqrt{D}}{2}\right) - \left(\frac{1-\sqrt{D}}{2}\right)\right]^2 = \left(-\sqrt{D}\right)^2 = D. \end{aligned}$$

Now suppose $D \equiv 2$ or $3 \pmod 4$. Then

$$\begin{aligned} d &= \left(det\begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}\right)^2 \\ &= \left(-\sqrt{D} - \sqrt{D}\right)^2 = \left(-2\sqrt{D}\right)^2 = 4D, \end{aligned}$$

as desired.

Now we consider again an arbitrary ring of integers of a finite extension, $\mathcal{O}_K$. It is clear that $\mathcal{O}_K$ is a $\mathbb{Z}$-module. However, it turns out that $\mathcal{O}_K$ is actually a *free* $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. The crucial step in showing this is to prove that $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$–the result then being immediate from the structure theorem for finitely generated abelian groups. We will omit the proof of this, but it can be found on pages 12-13 of Neukirch. However, using this fact, we are able to prove the statement we set out to prove at the beginning of the section, that $\mathcal{O}_K$ is a Dedekind domain.

Definition 2.5. A **Dedekind domain** is a noetherian, integrally closed integral domain in which every nonzero prime ideal is maximal.

We recall from module theory that an R-module is **noetherian** if every submodule is finitely generated, and, similarly, a ring R is called **noetherian** if it is a noetherian R-module. We recognize that there are numerous equivalent definitions of noetherian, but the ones mentioned are the most useful to us.

Theorem 2.6. *If $K/\mathbb{Q}$ is a finite extension of rank n, then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. First we will show that $\mathcal{O}_K$ is noetherian. As stated previously, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. Thus, an ideal I of $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of rank at *most* n. We can thus find a set of $\mathbb{Z}$-generators $\{a_1, \ldots, a_m\}$ for I, where $m \leq n$. Since $\mathbb{Z} \subseteq \mathcal{O}_K$, our set of generators for I, $\{a_1, \ldots, a_m\}$, is also a set of $\mathcal{O}_K$-generators. Thus, every ideal of $\mathcal{O}_K$ is finitely generated as a $\mathcal{O}_K$-submodule, which implies that $\mathcal{O}_K$ is a noetherian ring.

We know that $\mathcal{O}_K$ is integrally closed since it is the integral closure of $\mathbb{Z}$ in K.

Now all that remains to be shown is that every nonzero prime ideal $\mathfrak{p} \neq 0$ of $\mathcal{O}_K$ is maximal. We first need to show that $\mathfrak{p} \cap \mathbb{Z}$ is prime in $\mathbb{Z}$. Suppose $\mathfrak{p} \cap \mathbb{Z}$ is trivial, and let $\alpha \in \mathfrak{p}$. Then, since α is integral over $\mathbb{Z}$, we can find a monic polynomial $f \in \mathbb{Z}[x]$ of minimum degree, such that $f(x) = x^s + c_{s-1}x^{s-1} + \ldots + c_0$, and $f(\alpha) = 0$. Then we have

$$\begin{aligned} & \alpha^s + c_{s-1}\alpha^{s-1} + \ldots + c_0 = 0 \\ \Rightarrow \quad & \alpha^s + c_{s-1}\alpha^{s-1} + \ldots + c_1\alpha = -c_0. \end{aligned}$$

In the above equation, the summands on the left-hand side are all multiples of α, so they are in $\mathfrak{p}$. Also, ideals are closed under addition, so the sum, and thus $-c_0$, is in $\mathfrak{p}$ as well. By the minimality of the degree of f, c_0 must be nonzero, so $\mathfrak{p}$ contains a nonzero integer, which contradicts our assumption that $\mathfrak{p} \cap \mathbb{Z}$ is trivial. Since $\mathbb{Z}$ is a PID, we thus know that $\mathfrak{p} \cap \mathbb{Z}$ is a principal ideal in $\mathbb{Z}$. That is, $\mathfrak{p} \cap \mathbb{Z} = (\beta)$, for some $\beta \in \mathbb{Z}$. β must be prime in $\mathbb{Z}$, because if $\beta = xy$, such that $x, y \in \mathbb{Z}$ are non-units, then, since $\mathfrak{p}$ is prime, x or y must be in $\mathfrak{p}$ and thus in $\mathfrak{p} \cap \mathbb{Z}$. However,

(xy) is a proper subset of both (x) and (y). Thus, $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime ideal (p) in $\mathbb{Z}$, and since $\mathbb{Z}$ is a PID, (p) must be maximal in $\mathbb{Z}$.

Now we consider the quotient ring $\mathcal{O}_K/\mathfrak{p}$ in order to show that $\mathcal{O}_K/\mathfrak{p}$ is a field and thus that $\mathfrak{p}$ is maximal in $\mathcal{O}_K$. Let $\beta \in \mathcal{O}_K$ and let

$$g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \mathbb{Z}[x]$$

such that $g(\beta) = 0$. Then, clearly, $g(\bar{\beta}) = \bar{0}$, where the bar notation denotes the passage into the quotient ring $\mathcal{O}_K/\mathfrak{p}$. Now, let g' denote the image of g in $(\mathbb{Z}/p\mathbb{Z})[x]$. We will write the elements of $(\mathbb{Z}/p\mathbb{Z})$, for now, using coset notation. We have

$$\begin{aligned} g'(\bar{\beta}) &= (1+p\mathbb{Z})\bar{\beta}^n + (b_{n-1}+p\mathbb{Z})\bar{\beta}^{n-1} + \cdots + (b_0 + p\mathbb{Z}) \\ &= g(\bar{\beta}) + p\mathbb{Z}(\bar{\beta}^n + \bar{\beta}^{n-1} + \cdots + 1) \\ &= \bar{0} + p\mathbb{Z}(\bar{\beta}^n + \bar{\beta}^{n-1} + \cdots + 1), \end{aligned}$$

which is in $\mathfrak{p}$, and is thus equal to $\bar{0}$. Therefore, $\mathcal{O}_K/\mathfrak{p}$ is integral over $(\mathbb{Z}/p\mathbb{Z})$. Since $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, we know that $\mathcal{O}_K/\mathfrak{p}$ is an integral domain, so in order to show that $\mathcal{O}_K/\mathfrak{p}$ is a field, we only need to show that every nonzero element is a unit. Again we consider $\bar{\beta}$, an arbitrary element of $\mathcal{O}_K/\mathfrak{p}$. We know that

$$\begin{aligned} & g'(\bar{\beta}) = \bar{\beta}^n + \bar{b}_{n-1}\bar{\beta}^{n-1} + \cdots + \bar{b}_0 = \bar{0} \\ \Rightarrow \quad & -\bar{\beta}(\bar{\beta}^{n-1} + \bar{b}_{n-1}\bar{\beta}^{n-2} + \cdots + \bar{b}_1) = \bar{b}_0. \end{aligned}$$

Since $p\mathbb{Z}$ is maximal in $\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})$ is a field. Thus $\bar{b}_0$ has a multiplicative inverse, so we can write

$$\begin{aligned} -\bar{\beta}(\bar{\beta}^{n-1} + \bar{b}_{n-1}\bar{\beta}^{n-2} + \cdots + \bar{b}_1)\bar{b}_0^{-1} &= \bar{b}_0\bar{b}_0^{-1} \\ &= 1. \end{aligned}$$

Thus, $\bar{\beta}$ is a unit, and since $\bar{\beta}$ was an arbitrary element of $\mathcal{O}_K/\mathfrak{p}$, we know that $\mathcal{O}_K/\mathfrak{p}$ is a field. Therefore, $\mathfrak{p}$ is maximal, making $\mathcal{O}_K$ a Dedekind domain. □

3. Ideals of Dedekind Domains

Although the ring of integers $\mathcal{O}_K$ of an extension of $\mathbb{Q}$ can be thought of as a generalization of the integers, one very large difference is that $\mathcal{O}_K$ is not necessarily a unique factorization domain. However, in the next few sections we will introduce a method to check "how badly" a given Dedekind domain fails to have unique factorizations. For now, consider the example of $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$.

Example 3.1. Let $K = \mathbb{Q}\left(\sqrt{-5}\right)$. We recall from Example 2.4 that $-5 \equiv 3 \pmod 4$ so that $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-5}\right]$. Now, we see that 6 can be factored into irreducibles in two ways (up to associates):

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

Thus, $\mathcal{O}_K$ is not a unique factorization domain.

The absence of unique factorization of *elements* of $\mathcal{O}_K$ leads us to consider multiplication of *ideals*. We define the addition and multiplication of ideals $\mathfrak{a}$ and $\mathfrak{b}$ as follows:

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\}$$

and

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a},\, b_i \in \mathfrak{b} \text{ and } n \in \mathbb{Z}^+ \right\}$$

We say that $\mathfrak{a}$ **divides** $\mathfrak{b}$, or $\mathfrak{a}|\mathfrak{b}$, if $\mathfrak{b} \subseteq \mathfrak{a}$.

While $\mathcal{O}_K$ does not necessarily have unique factorization into irreducible elements, we will find that every ideal of $\mathcal{O}_K$ admits a unique factorization into prime ideals. In fact, this statement holds for any Dedekind domain $\mathcal{O}$ in general. We will prove this statement shortly, but first we must state some prerequisite lemmas.

Lemma 3.2. *Let $\mathcal{O}$ be a Dedekind domain. If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}$, then there exist nonzero prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ such that $\mathfrak{a}|\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n$, that is,*

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Proof. Let $\mathfrak{M}$ be the set of ideals that do *not* satisfy this condition. Suppose $\mathfrak{M}$ is nonempty. $\mathfrak{M}$ is a partially ordered set with respect to inclusion, and since $\mathcal{O}$ is noetherian, every ascending chain of ideals is eventually stationary. Thus, by Zorn's lemma, $\mathfrak{M}$ admits a maximal element $\mathfrak{b}$. $\mathfrak{b}$ cannot be prime, so there exist two elements $b_1, b_2 \in \mathcal{O}$) such that $b_1b_2 \in \mathfrak{b}$ but $b_1, b_2 \notin \mathfrak{b}$. Let $\mathfrak{b}_1 = (b_1) + \mathfrak{b}$ and $\mathfrak{b}_2 = (b_2) + \mathfrak{b}$. 0 is obviously an element of both (b_1) and (b_2), so $\mathfrak{b} \subseteq \mathfrak{b}_1$ and $\mathfrak{b}_2$, but $b_1, b_2 \notin \mathfrak{b}$, so $\mathfrak{b} \subsetneq \mathfrak{b}_1$ and $\mathfrak{b} \subsetneq \mathfrak{b}_2$. Let $c \in \mathfrak{b}_1\mathfrak{b}_2$. Then

$$\begin{aligned} c &= \sum_{i=1}^{n} (w_ib_1 + x_i)(y_ib_2 + z_i) \\ &= \sum_{i=1}^{n} (w_iy_ib_1b_2 + z_iw_ib_i + x_iy_ib_2 + x_iz_i) \end{aligned}$$

for some $n \in \mathbb{Z}^+$ where $w_i, y_i \in \mathcal{O}$ and $x_i, z_i \in \mathfrak{b}$. $b_1b_2 \in \mathfrak{b}$, so $w_iy_ib_1b_2 \in \mathfrak{b}$, and $x_i, z_i \in \mathfrak{b}$, so $z_iw_ib_i, x_iy_ib_2, x_iz_i \in \mathfrak{b}$, since $\mathfrak{b}$ is an ideal. Thus, $c \in \mathfrak{b}$ so $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{b}$. Since $\mathfrak{b}$ is maximal, both $\mathfrak{b}_1$ and $\mathfrak{b}_2$ contain a product of prime ideals. The product of those products is contained in $\mathfrak{b}_1\mathfrak{b}_2$, which is contained in $\mathfrak{b}$, a contradiction. Therefore, $\mathfrak{M}$ must be empty, which means our assertion holds. □

In the next lemma, we define the inverse of an ideal.

Lemma 3.3. *Let $\mathfrak{p}$ be a prime ideal of a Dedekind domain $\mathcal{O}$. Let K be the field of fractions of $\mathcal{O}$. We define*

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\}.$$

Then for every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}$, we have

$$\mathfrak{a}\mathfrak{p}^{-1} := \left\{ \sum_i a_ix_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1} \right\} \neq \mathfrak{a}.$$

Proof. Let $a \in \mathfrak{p}$, $a \neq 0$, and $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ are prime ideals and r is as small as possible. Suppose none of the $\mathfrak{p}_i$ were contained in $\mathfrak{p}$. Then for all i there would exist $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ such that $a_1 \cdots a_r \in \mathfrak{p}$. But $\mathfrak{p}$ is prime, a contradiction. Thus, one of the $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$. Since $\mathfrak{p}_1$ is maximal, we know that $\mathfrak{p}_1 = \mathfrak{p}$. Since r is as small as possible, we know that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \nsubseteq (a)$. Thus, there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin (a) = a\mathcal{O}$. Thus, $a^{-1}b \notin \mathcal{O}$. However, $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq (a)$, so $b\mathfrak{p} \subseteq a\mathcal{O}$, which implies that $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$. Thus, by the definition of $\mathfrak{p}^{-1}$, we have $a^{-1}b \in \mathfrak{p}^{-1}$. Thus, $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Now, let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}$ and $\alpha_1, \ldots, \alpha_n$ a system of generators of $\mathfrak{a}$. Assume $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Then for every $x \in \mathfrak{p}^{-1}$, we have

$$x\alpha_i = \sum_j a_{ij}\alpha_j,$$

where $a_{ij} \in \mathcal{O}$. Define A as the matrix $xI - (a_{ij})$. Then, by a theorem on page 6 of Neukirch (we omit the proof since it involves mostly basic linear algebra manipulations), we have that $\det(A)\alpha_1 = \det(A)\alpha_2 = \cdots = \det(A)\alpha_n = 0$. Thus, since not all a_i can be zero, we know that $\det(A) = 0$. $\det(A)$ (replacing the x with X is a monic polynomial in $\mathcal{O}[X]$. Thus, x is integral over $\mathcal{O}$. Since $\mathcal{O}$ is a Dedekind domain, it is by definition integrally closed, so $x \in \mathcal{O}$. Therefore, $\mathfrak{p}^{-1} \subseteq \mathcal{O}$. We also know that $\mathcal{O} \subseteq \mathfrak{p}^{-1}$. Thus, $\mathfrak{p}^{-1} = \mathcal{O}$, a contradiction. □

Now we are able to prove the unique factorization of Dedekind domain ideals.

Theorem 3.4. *Let $\mathcal{O}$ be a Dedekind domain, and let $\mathfrak{a} \neq 0$ be a proper ideal of $\mathcal{O}$. Then $\mathfrak{a}$ admits a factorization*

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

into nonzero prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ of $\mathcal{O}$ which is unique up to the order of the factors.

Proof. First we prove that such a factorization exists. Let $\mathfrak{M}$ be the set of all nonzero proper ideals that do *not* admit such a factorization. Suppose $\mathfrak{M}$ is nonempty. Then, just as in Lemma 3.2, there exists a maximal (with respect to inclusion) element $\mathfrak{a}$ in $\mathfrak{M}$. $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{p}$. Since $\mathcal{O} \subseteq \mathfrak{p}^{-1}$, we have

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}.$$

By Lemma 3.3, we have $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$. Thus, since $\mathfrak{p}$ is a maximal ideal, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Since $\mathcal{O}$ is commutative, we know that $\mathfrak{p}$ is prime, so $\mathfrak{a} \neq \mathfrak{p}$. Thus, $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$. Since $\mathfrak{a}$ is maximal in $\mathfrak{M}$ and $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$, $\mathfrak{a}\mathfrak{p}^{-1}$ must admit a factorization into prime ideals:

$$\mathfrak{a}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

But then we have

$$\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p},$$

which is a factorization into prime ideals, a contradiction. Thus, every nonzero proper ideal of $\mathcal{O}$ can be factored into nonzero prime ideals.

Now we show that the factorization is unique. Let

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

be two prime ideal factorizations of $\mathfrak{a}$. For a prime ideal $\mathfrak{p}$, we know that $\mathfrak{p}|\mathfrak{b}\mathfrak{c}$ implies that $\mathfrak{p}|\mathfrak{b}$ or $\mathfrak{p}|\mathfrak{c}$. Thus, since $\mathfrak{p}_1|\mathfrak{a}$, we know that $\mathfrak{p}_1|\mathfrak{q}_i$ for some $i \in \{1, 2, \ldots, s\}$. Without loss of generality, assume $i = 1$. Then $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. However, since $\mathfrak{q}_1$ is prime, it is also maximal, so $\mathfrak{q}_1 = \mathfrak{p}_1$. Thus,

$$\begin{aligned} & \mathfrak{p}_1^{-1}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{p}_1^{-1}\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s \\ \Rightarrow \quad & \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s \end{aligned}$$

We can continue like this, and eventually we see that $r = s$. Thus, after a reordering, we have $\mathfrak{p}_i = \mathfrak{q}_i$ for all $i \in \{1, 2, \ldots, s\}$. Thus, every nonzero proper ideal of $\mathcal{O}$ can be factored uniquely (up to ordering) into prime ideals, as desired. □

In the same way that non-field rings can be extended to a field that contains their inverses, namely the field of fractions, we can also find the inverses of ideals of a Dedekind domain by extending into the field of fractions, as shown earlier in this section. This brings us to the notion of a fractional ideal.

Definition 3.5. Let $\mathcal{O}$ be a Dedekind domain, and let K be its field of fractions. A **fractional ideal** of K is a nonzero finitely generated $\mathcal{O}$-submodule of K.

Since every fractional ideal of $\mathcal{O}$ lies in the field of fractions of $\mathcal{O}$, we can give an equivalent definition relating fractional ideals to ideals inside $\mathcal{O}$, where multiplication of fractional ideals is defined in the same way as multiplication of ideals. We state this definition as a lemma.

Lemma 3.6. *Let $\mathfrak{a} \neq 0$ be an $\mathcal{O}$-submodule of K. $\mathfrak{a}$ is a fractional ideal of K if and only if there exists a nonzero element c of $\mathcal{O}$ such that $c\mathfrak{a} \subseteq \mathcal{O}$ is an ideal of $\mathcal{O}$.*

Proof. Suppose $\mathfrak{a}$ is a fractional ideal. Then, there is a finite set of generators that generates $\mathfrak{a}$. Since $\mathfrak{a}$ is in the field of fractions of $\mathcal{O}$, we can write these generators of fractions of elements of $\mathcal{O}$. That is, we can write

$$\mathfrak{a} = \frac{a_1}{b_1}\mathcal{O} + \cdots + \frac{a_n}{b_n}\mathcal{O}$$

where $a_1, \ldots, a_n$ and $b_1, \ldots, b_n \in \mathcal{O}$. Let $c = b_1 b_2 \cdots b_n$. Clearly $c(a_i/b_i) \in \mathcal{O}$ for $i \in \{1, \ldots, n\}$. Thus, $c\mathfrak{a} \subseteq \mathcal{O}$. Also, since $b\mathfrak{a}$ is a finitely generated $\mathcal{O}$-submodule of $\mathcal{O}$, it must be an ideal of $\mathcal{O}$.

Now we prove that the converse holds. Assume there is a nonzero element c of $\mathcal{O}$ such that $c\mathfrak{a} \subseteq \mathcal{O}$ is an ideal of $\mathcal{O}$. Since $\mathcal{O}$ is noetherian, $c\mathfrak{a}$ must be a finitely generated $\mathcal{O}$-submodule of K. we know that c^{-1} is in the field of fractions K, so if we multiply every element of the generating set of $c\mathfrak{a}$ by c^{-1}, and look at the module generated by the new set, we are again left with a finitely generated $\mathcal{O}$-submodule of K, and thus a fractional ideal, as desired. □

Now that we have a notion of multiplication and of inverses, a question that naturally arises is whether or not the set of fractional ideals is a group. It is simple to check that it *is* in fact a group, called the **ideal group**, as we will show in the following lemma.

Lemma 3.7. *Let $\mathcal{O}$ be a Dedekind domain, and let K be its field of fractions. The set of fractional ideals of K forms an abelian group, the ideal group of K, denoted J_K. The identity element is $\mathcal{O} = (1)$ and the inverse of $\mathfrak{a}$ is*

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Proof. Associativity and commutativity follow from the fact that K is a field. Also, $\mathfrak{a}(1) = \mathfrak{a}$ for all $\mathfrak{a} \in J_K$. J_K is nonempty, because it contains $\mathcal{O}$. Thus, all that remains to be shown is that every fractional ideal multiplied by its "inverse" is indeed $\mathcal{O}$. We first consider a prime ideal $\mathfrak{p}$. By Lemma 3.3, $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$. Since $\mathfrak{p}$ is a prime ideal of a Dedekind domain it must be a maximal ideal, which means that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Now, let $\mathfrak{a}$ be an arbitrary nonzero ideal of $\mathcal{O}$. Then, by Theorem 3.4, we can write $\mathfrak{a}$ as a product of prime ideals, so $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Then, $\mathfrak{b} = \mathfrak{p}_n\mathfrak{p}_{n-1}\cdots\mathfrak{p}_1$ is an inverse for $\mathfrak{a}$. Since $\mathfrak{b}\mathfrak{a} = \mathcal{O}$, we know that $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Now let $x \in \mathfrak{a}^{-1}$. Then we have $x\mathfrak{a} \subseteq \mathcal{O}$ which means that $x = x\mathcal{O} = x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$. Thus, $\mathfrak{a}^{-1} = \mathfrak{b}$. Now let $\mathfrak{a}$ be an arbitrary fractional ideal. Then we can find $c \in \mathcal{O}$ such that $c\mathfrak{a}$ is an ideal of $\mathcal{O}$. The inverse of $c\mathfrak{a}$ is $c^{-1}\mathfrak{a}^{-1}$, so $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. Thus, J_K is an abelian group. □

The ideal group can be used to help us understand the structure of the original Dedekind domain itself. In fact, it will help us answer the question raised

previously about determining "to what extent" a Dedekind domain fails to have unique factorization of elements. One convenient property of Dedekind domains that makes this task a lot easier, is that a Dedekind domain is a UFD if and only if it is a principal ideal domain (PID). It tends to be much easier to check that a ring is a PID, so we will take advantage of this property. This leads us to define the concept of a fractional *principal* ideal:

Definition 3.8. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Then a fractional ideal $\mathfrak{a}$ is a **fractional principal ideal** if it is a cyclic $\mathcal{O}$-submodule of K. If a generates $\mathfrak{a}$, then we write $\mathfrak{a} = (a)$. We denote the set of fractional principal ideals of K by P_K.

Conveniently, P_K turns out to be a subgroup of J_K. The quotient group $Cl_K = J_K/P_K$ is called the **class group** of K, and the order of the group, denoted h_K is called the **class number** of K. It is clear that as the proportion of principal ideals of $\mathcal{O}$ increases, h_K increases, and $h_K = 1$ if and only if $\mathcal{O}$ is a PID. Thus, the size of the class group can be thought of as a measure of the extent to which $\mathcal{O}$ fails to be a PID, or, equivalently, a UFD. If the class group were ever infinite, however, it would be difficult to compare two Dedekind domains. However, we find that the class number is always finite for rings of integers in number fields. In the following sections we explain concepts from linear algebra and geometry which will help us prove this and will enable us to compute the class numbers of a few fields.

4. Lattices and Minkowski Theory

We begin this section by introducing some concepts from linear algebra that at first may seem unrelated to the topic at hand, but our strategy is to apply linear algebra, in particular the notion of a lattice, to ideals of Dedekind domains, in order to give a sense of the size of an ideal. Doing this will enable us to bound the "size" of an ideal in order to eventually show that the class number must be finite. We begin with the definition of a lattice and describe some of its properties.

Definitions 4.1. Let V be an n-dimensional $\mathbb{R}$-vector space. A **lattice** in V is a subgroup of V of the form

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

where $v_1, \ldots, v_m$ are linearly independent vectors in V. $\{v_1, \ldots, v_m\}$ is called a **basis** for the lattice, and the set

$$\Phi = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R}, \text{ and } 0 \leq x_i < 1\}$$

is called a **fundamental mesh** of the lattice. The lattice is called **complete** if $m = n$.

Since we are working in Euclidean space, we now have available the notion of volume. Using the same V as in the previous definition, the cube spanned by an orthonormal basis has volume 1. More generally, a parallelepiped spanned by n linearly independent vectors $v_1, \ldots, v_n$, that is, Φ, has volume $\text{vol}(\Phi) = |\det A|$, where A is the base change matrix going from the orthonormal basis to $v_1, \ldots, v_n$. For short, we write $\text{vol}(\Gamma) = \text{vol}(\Phi)$. Using just these few definitions we are now able to prove Minkowski's lattice point theorem, the most important theorem having to do with lattices.

Theorem 4.2 (Minkowski's Lattice Point Theorem)**.** *Let Γ be a complete lattice in the euclidean vector space V, and let X be a centrally symmetric, convex subset of V. Suppose that*

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma).$$

Then X contains at least one nonzero lattice point $\gamma \in \Gamma$.

Proof. Let $\gamma_1, \gamma_2 \in \Gamma$, and let

$$Y = \left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

Suppose Y is nonempty. Let $y \in Y$. Then we have

$$y = \frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2,$$

for some $x_1, x_2 \in X$. Then

$$\gamma_1 - \gamma_2 = \frac{1}{2}(x_2 - x_1).$$

This is the center of the line segment joining x_2 and $-x_1$. Thus, it is an element of X. It is also the difference of two elements in Γ, a group, and it is thus also in Γ. Thus, it is an element of $\Gamma \cap X$. Therefore, it suffices to show that there exist γ_1 and γ_2 so that Y is nonempty.

Consider the collection of sets

$$\left\{\frac{1}{2}X + \gamma \mid \gamma \in \Gamma\right\}.$$

Suppose these sets are pairwise disjoint. Then the same would be true of their intersections $\Phi \cap (\frac{1}{2}X + \gamma)$ with the fundamental mesh Φ of Γ. Thus, we have

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right).$$

Translation of the set $\Phi \cap \left(\frac{1}{2}X + \gamma\right)$ by $-\gamma$ gives the set $(\Phi - \gamma \cap \frac{1}{2}X$ of equal volume. The sets $\Phi - \gamma, \gamma \in \Gamma$ cover the entire space V (this is a consequence of the completeness of Γ and is proven on pages 25 and 26 of Neukirch), so they also cover $\frac{1}{2}X$. Thus, we obtain

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{vol}(X),$$

which contradicts the hypothesis. □

Now we are ready to apply the theory of lattices to the study of algebraic number fields $K/\mathbb{Q}$ of degree n. We will first think of the field as an n-dimensional vector space, and then show that $\mathcal{O}_K$ actually forms a lattice in the vector space. First we consider a mapping j of K into a $\mathbb{Q}$-space. Let

$$j : K \to K_{\mathbb{C}} = \prod_{i=1}^{n} \mathbb{C}$$

be a function such that

$$j(x) = (\tau_1 x, \tau_2 x, \ldots, \tau_n x)$$

where $\tau_1, \tau_2, \ldots, \tau_n$ are the n complex embeddings of K into $\mathbb{C}$.

Although $K_{\mathbb{C}}$ is a $\mathbb{C}$-vector space, giving us the notion of distance, it is rather difficult to visualize geometrically. Admittedly, it would be much "nicer" if we could map K into a euclidean space without losing any information from the complex embeddings. In order to do this, we must notice three things: First, the real embeddings already map K into $\mathbb{R}$, so we can, at the moment, ignore those embeddings. Second, the complex embeddings can be thought of as embeddings into $\mathbb{R}^2$ by splitting the embedding into its real and imaginary parts. Lastly, the complex embeddings come in pairs of complex conjugates. Thus, given only half of the complex embeddings, that is, one from each pair of complex conjugates, we lose no information. This leads us to the description of the Minkowski space:

Every embedding of K into $\mathbb{C}$ is either real or complex. Let $\rho_1, \ldots, \rho_r$ be the real embeddings. As just mentioned, the complex embeddings come in pairs. Let $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s$ be the complex embeddings. From each pair of complex embeddings, we choose one fixed embedding. Then we let ρ vary over the real embeddings, and we let σ vary over the chosen complex embeddings. Then we define the **Minkowski space** $K_{\mathbb{R}}$ as

$$K_{\mathbb{R}} = \{(z_\tau) \in K_{\mathbb{C}} \mid z_\rho \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z}_\sigma\}$$

where τ varies over the n embeddings. In order to think of the Minkowski space geometrically, we point out that there is an isomorphism between $K_{\mathbb{R}}$ and $\prod_\tau \mathbb{R}$, as described above, given by the rule $(z_\tau) \mapsto (x_\tau)$, where

$$x_\rho = z_\rho, \ x_\sigma = \mathrm{Re}(z_\sigma), \text{ and } x_{\bar{\sigma}} = \mathrm{Im}(z_\sigma). \tag{4.3}$$

In order to illustrate this concept, we present a simple example.

Example 4.4. Let $K = \mathbb{Q}\left[\sqrt[3]{2}\right]$. $K/\mathbb{Q}$ is a degree 3 extension. Thus, there are three canonical embeddings of K into $\mathbb{C}$, which we will denote τ_1, τ_2, and τ_3. The maps are uniquely defined by their action on $\sqrt[3]{2}$, so we write

$$\begin{aligned}
\tau_1\left(\sqrt[3]{2}\right) &= \sqrt[3]{2}, \\
\tau_2\left(\sqrt[3]{2}\right) &= \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right), \\
\tau_3\left(\sqrt[3]{2}\right) &= \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right).
\end{aligned}$$

We see that τ_1 is a real embedding and that $\tau_2 = \bar{\tau}_3$. Thus, using the above isomorphism, the three new embeddings into $\mathbb{R}^3$ are

$$\begin{aligned}
\sigma_1\left(\sqrt[3]{2}\right) &= \sqrt[3]{2}, \\
\sigma_2\left(\sqrt[3]{2}\right) &= -\frac{\sqrt[3]{2}}{2}, \\
\sigma_3\left(\sqrt[3]{2}\right) &= \frac{\sqrt[3]{2}\sqrt{3}}{2}.
\end{aligned}$$

Now that we are able to think of K as an n-dimensional euclidean space, we can interpret the ring of integers of K and its ideals as lattices in the Minkowski space $K_{\mathbb{R}}$, using the following lemma.

Lemma 4.5. *Let K be a finite extension of $\mathbb{Q}$, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Let j be the map from K into the Minkowski space $K_\mathbb{R}$. Then $\Gamma = j\mathfrak{a}$ is a complete lattice in $K_\mathbb{R}$, and its fundamental mesh has volume*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}(O_K : \mathfrak{a}).$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Then $\Gamma = \mathbb{Z}j\alpha_1 + \cdots + \mathbb{Z}j\alpha_n$. Let $\tau_1, \tau_2, \ldots, \tau_n$ be the embeddings of K into $\mathbb{C}$. We define the matrix

$$A = \begin{pmatrix} \tau_1\alpha_1 & \tau_2\alpha_1 & \cdots & \tau_n\alpha_1 \\ \tau_1\alpha_2 & \tau_2\alpha_2 & & \vdots \\ \vdots & & \ddots & \\ \tau_1\alpha_n & \cdots & & \tau_n\alpha_n \end{pmatrix}.$$

By the theory of finitely generated $\mathbb{Z}$-modules (which we will not prove), if $\mathfrak{b} \subseteq \mathfrak{b}'$ are two nonzero finitely generated $\mathcal{O}_K$-submodules of K, then $(\mathfrak{b}' : \mathfrak{b})$ is finite and

$$d(\mathfrak{b}) = (\mathfrak{b}' : \mathfrak{b})^2 d(\mathfrak{b}').$$

Thus, we have

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = (\det\ A)^2 = (\mathcal{O}_K : \mathfrak{a})^2 d(\mathcal{O}_K) = (\mathcal{O}_K : \mathfrak{a})^2 d_K.$$

We also know that

$$(\langle j\alpha_i, j\alpha_k \rangle) = \left(\sum_{l=1}^{n} \tau_l\alpha_i\bar{\tau}_l\alpha_k \right) = A\bar{A}^t.$$

Now we have

$$\mathrm{vol}(\Gamma) = |\det(\langle j\alpha_i, j\alpha_k \rangle)|^{1/2} = |\det\ A| = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}),$$

as desired. □

We now give an example of determining the lattice of $\mathcal{O}_K$ for a field K.

Example 4.6. Let $K = \mathbb{Q}\left[\sqrt[3]{2}\right]$, as in Example 3.4. A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is $1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2$. Let j be the canonical map from K into $\mathbb{R}^3$. Then, using the embeddings we found in Example 3.4, we have

$$\begin{aligned} j(1) &= (1,1,1), \\ j\left(\sqrt[3]{2}\right) &= \left(\sqrt[3]{2}, -\frac{\sqrt[3]{2}}{2}, \frac{\sqrt[3]{2}\sqrt{3}}{2}\right), \\ j\left(\left(\sqrt[3]{2}\right)^2\right) &= \left(\left(\sqrt[3]{2}\right)^2, \frac{\left(\sqrt[3]{2}\right)^2}{4}, \frac{3\left(\sqrt[3]{2}\right)^2}{4}\right) \end{aligned}$$

as the three basis vectors for the lattice.

In order to apply lattices of ideals to the class number, we need to first prove a theorem that is the direct result of the Minkowski Lattice Point Theorem, which will help us in finding a "bound" for ideals, as mentioned before.

Theorem 4.7. *Let $K/\mathbb{Q}$ be a finite extension, and let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}_K$. Let $c_\tau > 0$, for $\tau \in \mathrm{Hom}(K, \mathbb{C})$, be a real number such that $c_\tau = c_{\bar{\tau}}$ and*

$$\prod_\tau c_\tau > A(\mathcal{O}_K : \mathfrak{a}),$$

where $A = (2/\pi)^s\sqrt{|d_K|}$. *Then there exists a nonzero* $a \in \mathfrak{a}$ *such that*

$$|\tau a| < c_\tau \text{ for all } \tau \in \mathrm{Hom}(K, \mathbb{C}).$$

Proof. Let

$$X = \{(z_\tau) \in K_\mathbb{R} \big| |z_\tau| < c_\tau\}.$$

This set is centrally symmetric, since $|z_\tau| = |-z_\tau|$, and it is convex since if $|z_\tau|, |w_\tau| < c_\tau$, then

$$\left|\frac{1}{2}(z_\tau + w_\tau)\right| = \frac{1}{2}|z_\tau + w_\tau| \leq \frac{1}{2}|z_\tau| + \frac{1}{2}|w_\tau| \leq \max\{|z_\tau|, |w_\tau|\} < c_\tau.$$

We compute the volume using map 4.3, which we will denote f. It comes out to be 2^s times the Lebesgue-volume of the image

$$f(X) = \left\{ (x_\tau) \in \prod_\tau \mathbb{R} \middle| |x_\rho| < c_\rho, x_\sigma^2 + x_{\bar{\sigma}}^2 < c_\sigma^2 \right\}.$$

This gives

$$\mathrm{vol}(X) = 2^s \mathrm{vol}_{\text{Lebesgue}}\left(f(X)\right) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s}\pi^s \prod_\tau c_\tau.$$

Now, by Lemma 4.5, we have

$$\mathrm{vol}(X) > 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}) = 2^n \mathrm{vol}(\Gamma).$$

Thus, by Minkowski's Lattice Point Theorem, there exists a lattice point $ja \in X, a \neq 0, a \in \mathfrak{a}$. That is, $|\tau a| < c_\tau$, as desired. □

5. The Class Number

Now that we have the basic tools from Minkowski Theory, we are able to apply them to the class group, which was mentioned briefly in section 3. Before we do so, we must define the concept of the absolute norm of an ideal.

Definition 5.1. Let $K/\mathbb{Q}$ be a finite extension, and let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}_K$. The **absolute norm** of $\mathfrak{a}$ is given by

$$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}).$$

It seems reasonable that multiplicativity of the absolute norm would hold, but the proof is actually not entirely trivial. We thus state it as a lemma.

Lemma 5.2. *Let* $K/\mathbb{Q}$ *be a finite extension, and let* $\mathfrak{a} \neq 0$ *be an ideal of* $\mathcal{O}_K$. *If* $\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$ *is the prime factorization of* $\mathfrak{a}$, *then*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{v_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{v_r}.$$

Proof. By the Chinese Remainder Theorem, we have

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/{\mathfrak{p}_1}^{v_1} \oplus \cdots \oplus \mathcal{O}_K/{\mathfrak{p}_r}^{v_r}.$$

Since

$$|\mathcal{O}_K/\mathfrak{a}| = |\mathcal{O}_K/{\mathfrak{p}_1}^{v_1}| \cdots |\mathcal{O}_K/{\mathfrak{p}_r}^{v_r}|,$$

we only need to consider the case where $\mathfrak{a} = \mathfrak{p}^v$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Consider the chain

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^v.$$

We know that $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$, because otherwise we would not have unique prime factorization. Now consider the quotient ring $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Let $a \in \mathfrak{p}^i \backslash \mathfrak{p}^{i+1}$ and $\mathfrak{b} = (a)+\mathfrak{p}^{i+1}$. Then $\mathfrak{p}^{i+1} \subsetneq \mathfrak{b} \subseteq \mathfrak{p}^i$. Thus, since $\mathfrak{p}^{i+1}$ is maximal in $\mathfrak{p}^i$, we know that $\mathfrak{p}^i = \mathfrak{b}$. Thus, a mod $\mathfrak{p}^{i+1}$ is a basis for the $\mathcal{O}_K/\mathfrak{p}$-vector space $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Therefore, we have

$$\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}.$$

This means that

$$\mathfrak{N}(\mathfrak{p}^v) = (\mathcal{O}_K : \mathfrak{p}^v) = (\mathcal{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2)\cdots(\mathfrak{p}^{v-1} : \mathfrak{p}^v) = \mathfrak{N}(\mathfrak{p})^v,$$

as desired. □

Now before we get to the actual proof of the finiteness of the class number, we give one more prerequisite lemma.

Lemma 5.3. *In every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists a nonzero $a \in \mathfrak{a}$ such that*

$$\left|N_{K/\mathbb{Q}}(a)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

Proof. Given $\epsilon > 0$, we can choose positive real numbers c_τ, for $\tau \in \mathrm{Hom}(K, \mathbb{C})$, such that $c_\tau = c_{\bar{\tau}}$ and

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \epsilon.$$

Then by Theorem 4.7, we find an element $a \in \mathfrak{a}, a \neq 0$, satisfying $|\tau a| < c_\tau$. Thus

$$\left|N_{K/\mathbb{Q}}(a)\right| = \prod_\tau |\tau a| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \epsilon.$$

Since $|N_{K/\mathbb{Q}}(a)|$ is a positive integer, there exists an $a \in \mathfrak{a}, a \neq 0$, such that

$$\left|N_{K/\mathbb{Q}}(a)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

□

Now we reach the theorem that we have been building up to since the beginning of the paper.

Theorem 5.4. *Let $K/\mathbb{Q}$ be a finite extension. The class number $h_K = (J_K : P_K)$ is finite.*

Proof. Let $\mathfrak{p} \neq 0$ be a prime ideal of $\mathcal{O}_K$. By the proof of Theorem 2.6, we know that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \in \mathbb{Z}$. Thus, $\mathcal{O}/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$. Suppose the extension has degree $f \geq 1$. Then

$$\mathfrak{N}(\mathfrak{p}) = p^f.$$

Given a prime p, there are only a finite number of prime ideals such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ since this would mean that $\mathfrak{p}|(p)$. Thus, there are only finitely many prime ideals of bounded absolute norm. Let $\mathfrak{a}$ be an arbitrary ideal of $\mathcal{O}_K$. By Theorem 3.4, we can write $\mathfrak{a}$ uniquely (up to the order of the factors) as a product of prime ideals, so that

$$\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$$

where all $v_i > 0$ and by Lemma 5.2, we have

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{v_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{v_r}.$$

Thus, there are only a finite number of ideals of $\mathcal{O}_K$ with a bounded absolute norm $\mathfrak{N}(\mathfrak{a}) \leq M$.

Therefore, it will suffice to show that each ideal class, or element, $[\mathfrak{a}]$ of Cl_K contains an ideal $\mathfrak{a}_1$ of $\mathcal{O}_K$ such that

$$\mathfrak{N}(\mathfrak{a}_1) \leq M = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

In order to show this, we choose an arbitrary representative $\mathfrak{a}$ of the class and a nonzero element $\gamma \in \mathcal{O}_K$ such that $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. By Lemma 5.3, we can find a nonzero element $\alpha \in \mathfrak{b}$, such that

$$\left|N_{K/\mathbb{Q}}(\alpha)\right| \mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}\left((\alpha)\mathfrak{b}^{-1}\right) = \mathfrak{N}\left(\alpha\mathfrak{b}^{-1}\right) \leq M.$$

Thus, the ideal $\alpha\mathfrak{b}^{-1}$ has the desired property. □

As described in Section 3, when $\mathcal{O}_K$ is a PID (or, equivalently, a UFD), the class number is 1. Thus, we will give an example of the computation of the class number of a field whose ring of integers is *not* a PID.

Example 5.5. Let $K = \mathbb{Q}[\sqrt{-5}]$. From Example 2.4, since $-5 \equiv 3 \pmod 4$, we know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, and $d_K = -20$. Thus, from the proof of Theorem 5.4, we know that each ideal class contains an ideal $\mathfrak{a}$, such that

$$\mathfrak{N}(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)\sqrt{20} \approx 2.85.$$

Thus, we must find all ideals with absolute norm 2.

Suppose $\mathfrak{a}$ is an ideal such that $\mathfrak{N}(\mathfrak{a}) = 2$. Let

$$\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$$

where all $v_i > 0$, and each p_i is prime. Then

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{v_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{v_r}.$$

Since $\mathfrak{p}_i$ is prime, we know that $\mathfrak{N}(\mathfrak{p}_i)$ is an integer greater than one. Thus, $r = 1$ and $v_i = 1$, which means that $\mathfrak{a}$ is prime. Thus, $\mathfrak{a} \cap \mathbb{Z} = 2\mathbb{Z}$, so $(2) \subseteq \mathfrak{a}$.

Consider the ideal $\mathfrak{b} = (\sqrt{-5} + 1, 2)$. Clearly $(2) \subseteq \mathfrak{b}$. We will show that $\mathfrak{b}$ is not principal, and thus that it is not in the same ideal class as (2). Suppose $\mathfrak{b}$ is principal, so that $\mathfrak{b} = (b)$, for some $b \in \mathbb{Z}[\sqrt{-5}]$. Then

$$N_{K/\mathbb{Q}}(b) | N_{K/\mathbb{Q}}(2) = 4$$

and

$$N_{K/\mathbb{Q}}(b) | N_{K/\mathbb{Q}}(\sqrt{-5} + 1) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$$

. Thus, $N_{K/\mathbb{Q}}(b) = 2$. So if $b = x + y\sqrt{-5}$, then

$$N_{K/\mathbb{Q}}(b) = x^2 + 5y^2 = 2.$$

There are no integer solutions for x and y, so $\mathfrak{b}$ must not be principal. In particular, it is not equal to (1). We know $\mathfrak{b}|(2)$, so $\mathfrak{N}(\mathfrak{b})|2$. Since $\mathfrak{N}(\mathfrak{b}) \neq 1$ it must be 2.

Now let $\mathfrak{c}$ be a nonprincipal prime ideal of norm 2, so that $(2) \subseteq \mathfrak{c}$. We will show that $\mathfrak{c} = \mathfrak{b}$. We can find two elements of $\mathfrak{c} \setminus (2)$, $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$, such that

$$\begin{aligned} & (a + b\sqrt{-5}) + (c + d\sqrt{-5}) = 2 \\ \Rightarrow \quad & (a + c) + (b + d)\sqrt{-5} = 2, \end{aligned}$$

so $c = 2 - a$ and $d = -b$.

Now suppose a is odd and b is even or a is even and b is odd. Then by subtracting even multiples of $\sqrt{-5}$ and 1, respectively, from $a + b\sqrt{-5}$, we obtain $\sqrt{-5} \in \mathfrak{c}$, which means that $-5 \in \mathfrak{c}$, or $1 \in \mathfrak{c}$, a contradiction either way. Thus a and b are of the same parity. Suppose they are both even. Then $a + b\sqrt{-5} \in (2)$, a contradiction. Thus, a and b are odd. Subtracting even multiples of $\sqrt{-5}$ and 1, respectively, from $a + b\sqrt{-5}$, we obtain $\sqrt{-5} + 1 \in \mathfrak{c}$. Thus, $\mathfrak{b} \subseteq \mathfrak{c}$. Since $\mathfrak{c} \neq (1)$ and since $\mathfrak{b}$ is maximal, we have $\mathfrak{c} \in \mathfrak{b}$. Thus, $\mathfrak{c} = \mathfrak{b}$.

Therefore, there is only one nonprincipal ideal of norm 2, so there are precisely 2 ideal classes. Thus $h_K = 2$, so $Cl_K = \mathbb{Z}_2$.

6. Conclusion

Although the example we gave of finding the class group at the end of the previous section was not trivial, it was relatively simple compared to finding class groups of much higher order. In fact, the calculation of nontrivial class groups of algebraic number fields of larger discriminant is impractical to do by hand. Moreover, there is no known pattern yet in the ideal class groups of algebraic number fields– neither in size nor in structure. Neukirch states that it is believed that they behave completely unpredictably.

References

[1] D. S. Dummit and R. M. Foote. Abstract Algebra. Wiley. 2003.
[2] J. Neukirch. Algebraic Number Theory. Springer-Verlag. 1999.