AN EXPLORATION OF MINKOWSKI THEORY AND ITS APPLICATIONS

DANIEL COMEAUX

Abstract. This is a paper that examines the area of number theory laid out by Herman Minkowski in his explorations of the "geometry of numbers," here referred to as Minkowski Theory. It assumes the reader will have a basic familiarity with algebraic concepts, such as groups, rings, fields, extensions, etc. If the reader is unfamiliar with these, Dummit and Foote is a useful explanatory resource. After a discussion of the necessary preliminaries (algebraic concepts, gaussian integers, integrality, ideals, and lattices), we establish the framework of Minkowski's Lattice Point Theorem, as well as its implications in Minkowski Theory. We then use these results to prove the finiteness of the ideal class group and Dirichlet's Unit Theorem, and as a conclusion make a logical jump to consider the extension of Dedekind domains. This paper is based on *Algebraic Number Theory* by Jurgen Neukirch, but provides additional examples and expands upon the often dense proofs presented in his book. Explanations of concepts were drawn from Dummit and Foote, Lang, and Ash.

Contents

Date: August 24, 2012.

1. Preliminaries

1.1. **Basic Algebra.** Readers comfortable with algebraic concepts such as modules, embeddings, and extensions may skip to subsection 1.2.

Definition 1.1. Consider a ring R. From now on, assume than any such R contains the nontrivial multiplicative identity, i.e. $1 \neq 0, 1 \in R$. An *R-module* (technically a left R-module, but we will only consider left and not right modules) is a set M paired with some binary operation $+$ on M under which M is an abelian group, as well as some map $R \times M \to M$ denoted $(r, m) \mapsto rm$ for all $r \in R$ and for all $m \in M$ with the following conditions:

(i) $(r+s)m = rm + sm$ for all $r, s \in R, m \in M$
(ii) $(rs)m = r(sm)$ for all $r, s \in R, m \in M$
(iii) $r(m+n) = rm + rn$ for all $r \in R, m, n \in M$
(iv) $1m = m$ for all $m \in M$

Note that this object is actually a more general form of the familiar notion of the vector space, itself a special case of modules where the foundational ring is actually a field. Just as in our considerations of vector spaces, we can consider subsets of modules that inherit the properties of their parent modules, denoted as submodules.

Definition 1.2. With R a ring and M an R-module, a subgroup N of M which is closed under the action of ring elements (i.e. $rn \in N$, for $r \in R$ and $n \in N$) is known as a *R-submodule* of M.

Other terms that are likely familiar to most but may be unfamiliar to some include:

Definition 1.3. The field $\overline{F}$ is known as an *algebraic closure* of F if both $\overline{F}$ is algebraic over F and $\overline{F}$ contains all elements algebraic over F.

Definition 1.4. We say that a field K is *algebraically closed* if each polynomial with coefficients in this K has a root in K.

Definition 1.5. Consider two fields K and L. An embedding of K in L is a homomorphism $\sigma\colon K \to L$. A *K-embedding* is an embedding of L in the closure of K which maps any element of K to itself.

Definition 1.6. A *separable extension* of a field is a field extension $K|F$ in which the minimal polynomial for each element of K is separable over F, i.e. this polynomial has no multiple roots (as they are all distinct) in an algebraic closure of K. See [3] pp. 178, 243.

1.2. **Relevant Algebra.** In this paper, we will often consider the trace, norm, and discriminant of various elements. These operations are likely familiar, but the interpretations we will work with may be novel to the reader. For clarity, the definitions are listed below.

Definition 1.7. Considering the field extension $L|K$, the *trace* of an element $x \in L$ is defined to be the trace of the endomorphism

$$T_x\colon L \to L \text{ with } T_x(\alpha) = x\alpha$$

of the K-vector space L:

$$Tr_{L|K}(x) = Tr(T_x). \tag{1.8}$$

Fact 1.9. If $L|K$ is a separable extension and $\sigma\colon L \to \overline{K}$ varies over different K-embeddings of L into an algebraic closure $\overline{K}$ of K then

$$Tr_{L|K}(x) = Tr(T_x) = \sum_{\sigma} \sigma x \tag{1.10}$$

Definition 1.11. Considering the same field extension and endomorphism, the *norm* is characterized as

$$N_{L|K}(x) = \det(T_x)$$

Fact 1.12. If $L|K$ is a separable extension and $\sigma\colon L \to \overline{K}$ varies over different K-embeddings of L into an algebraic closure $\overline{K}$ of K then

$$N_{L|K}(x) = \det(T_x) = \prod_{\sigma} \sigma x \tag{1.13}$$

Definition 1.14. The *discriminant* of a basis $\alpha_1, \ldots, \alpha_n$, where the basis (a K-basis, i.e. some linearly independent points $\alpha_i \in L$ such that when multiplied by coefficients in K, they span L) of some separable extension $L|K$ is defined to be $d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i(\alpha_j)))^2$ where σ_i with $i = 1, \ldots, n$ is variant over K-embeddings $L \to \overline{K}$.

Remark 1.15. Alternatively, we may write $d(\alpha_1, \ldots, \alpha_n) = \det(Tr_{L|K}(\alpha_i\alpha_j))$.

2. Gaussian Integers

Before we begin our discussion of general algebraic number fields, we will consider one of the most standard such fields $\mathbb{Q}[i]$ and its ring of integers, $\mathbb{Z}[i]$. This ring is normally known as the Gaussian Integers:

Definition 2.1. A *Gaussian Integer* is an element of $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ where i is $\sqrt{-1}$.

While a familiarity with the concept of prime numbers is expected, it will be useful to consider an alternate characterization than that normally given in elementary instruction.

Definition 2.2. If for all $a, b \in \mathbb{Z}$ such that $p \mid ab$ we have that either $p \mid a$ or $p \mid b$, then p is prime.

Definition 2.3. A is said to be a *Euclidean Domain* if there is a norm N on A, i.e. a function $N\colon A \to \mathbb{N} \cup 0$ with $N(0) = 0$ such that for any $a, b \in A$ with $b \neq 0$ there are $q, r \in A$ with $a = qb + r$ and $r = 0$ or $N(r) < N(b)$.

We can now show:

Proposition 2.4. *The ring $\mathbb{Z}[i]$ is a Euclidean Domain.*

Proof. In order to show this result, we will show that $\mathbb{Z}[i]$ is Euclidean with respect to the Euclidean norm function, $N\colon \alpha \mapsto |\alpha|^2$. We must prove that there exist gaussian integers δ, ϵ such that $\alpha = \delta\beta + \epsilon$ and $|\epsilon|^2 < |\beta|^2$. Through algebraic manipulation, it will be enough to prove the existence of $\delta \in \mathbb{Z}[i]$ with $|\frac{\alpha}{\beta} - \delta| < 1$.

Now note that the gaussian integers form a lattice in the complex plane (defined more fully later), with each point having integer coordinates from the basis $(1, i)$ serving as a lattice point. We know that $\frac{\alpha}{\beta}$ is complex and thus lies in some square of the lattice. At most, it is half the distance of the diagonal of the lattice mesh from at least one lattice point, i.e. a distance of $\frac{1}{2}\sqrt{2}$. Thus, choose the point that minimizes the distance and we have $\delta \in \mathbb{Z}[i]$ such that $|\frac{\alpha}{\beta} - \delta| \leq \frac{1}{2}\sqrt{2} < 1$ as we wanted. □

Therefore, as the ring is Euclidean, it belongs to a larger class of Principal Ideal Domains (discussed later at 4.5), which we know by [1] p. 273. Since an ED is a PID, it is also a Unique Factorization Domain, i.e. it possesses the property of unique factorization (see [1] p. 287). This property, while very desirable, is not universally possessed, as shown in section 4.

Definition 2.5. Consider a ring A. An element u of A such that there is some $v \in A$ with $uv = vu = 1$ is known as a *unit*. Notationally, the set of units in A is denoted A^*.

Definition 2.6. If we have $a \in A$ with $a \neq 0$ and not a unit, then a is called *irreducible* in A if whenever $a = bc$ with $b, c, \in A$, at least one of b or c must be a unit in A.

Definition 2.7. An n^{th} *root of unity* in $\mathbb{C}$ is a complex number z satisfying the equation $z^n = 1$.

Now, we return to our considerations of $\mathbb{Z}[i]$.

Lemma 2.8. *For any α in $\mathbb{Z}[i]$, α is a unit if and only if $N(\alpha) = 1$*

Proof. Let α be a unit. By definition, some $\beta \in \mathbb{Z}[i]$ exists such that $\alpha\beta = 1$. Thus, we have that $\beta = \frac{1}{\alpha}$. Since $\beta \in \mathbb{Z}[i]$, we know that β must be of the form $x + iy$ for $x, y \in \mathbb{Z}$, giving us $1, -1, i, -i$ as the only solutions. For each of these $\alpha, N(\alpha) = 1$ and we are done.

If $\alpha = a + bi$ we have that $a^2 + b^2 = 1$. Since a and b are integers, we know that either $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$, yielding the above units. □

Hence, the group of units of the ring $\mathbb{Z}[i]$ consists of the fourth roots of unity, $\mathbb{Z}[i]^* = [1, -1, i, -i]$.

Also using this lemma, we can prove the following result:

Theorem 2.9. *For all prime numbers $p \neq 2$ we have, for a, b in $\mathbb{Z}$,*

$$p = a^2 + b^2 \text{ if and only if } p \equiv 1 \mod 4.$$

Proof. Assuming that $p = a^2 + b^2$, it is clear that $p \equiv 1 \mod 4$ since any perfect square a is either congruent to 0 mod 4 or 1 mod 4, and any prime p could not be congruent to 0 mod 4 or 2 mod 4.

Now assume that $p \equiv 1 \mod 4$. We must show that it is not a prime element in $\mathbb{Z}[i]$. This suffices because, if it is not prime, then we have some $p = \alpha\beta$ where α and β are non-units in the gaussian integers. Now, use the norm function

$$N(x + iy) = (x + iy)(x - iy) = x^2 + y^2$$

and thus $p^2 = N(\alpha)N(\beta)$ with $N(\alpha), N(\beta) \neq 1$, so we have, with $\alpha = a + bi$

$$p = N(\alpha) = a^2 + b^2$$

Note that the congruence $-1 \equiv x^2 \bmod p$ has a solution, $x = (2n)!$. Now, by Wilson's Theorem we know that

$$-1 \equiv (p-1)! \bmod p$$

and thus

$$\begin{aligned} -1 \equiv (p-1)! &= [(1)(2)\dots(2n)][(p-1)(p-2)\dots(p-2n)] \\ &\equiv [(2n)!][(-1)^{2n}(2n)!] = [(2n)!]^2 \bmod p. \end{aligned}$$

Hence, $p|x^2 + 1 = (x+i)(x-i)$. However, since $\frac{x}{p} \pm \frac{i}{p}$ is not in $\mathbb{Z}[i]$, p does not divide $x + i$ or $x - i$ and is thus not prime in $\mathbb{Z}[i]$. Thus, we are done. □

Definition 2.10. Two elements $b, c \in A$ are *associated* if they differ by only a unit factor; this is denoted $b \sim c$

Every element associated to an irreducible element is also irreducible. Given this, it is possible to prove the following (the result is interesting, but the proof is omitted for brevity. It relies on the above proofs).

Fact 2.11. The prime elements π of $\mathbb{Z}[i]$, up to associates, are:

(1) $\pi = 1 + i$
(2) $\pi = a + bi$ with $a^2 + b^2 = p, p \equiv 1 \bmod 4, a > |b| > 0$
(3) $\pi = p, p \equiv 3 \bmod 4$.

Remark 2.12. In general, irreducibility does not necessarily imply primality or vice versa. However, in the case of Principal Ideal Domains (defined at 4.5), a nonzero element is prime if and only if it is irreducible (see [1] p.284). The failure of this statement in some non-PID is clear. For example, consider $\mathbb{Z}[\sqrt{-5}] = R$, and consider one of its elements, 3. 3 is irreducible in this ring (shown in a method similar to that employed in section 4), but 3 is not prime since $(2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$ is divisible by 3 but neither of the factors is divisible by 3 in the ring.

As we mentioned earlier, $\mathbb{Z}[i]$ serves as the ring of algebraic integers of $\mathbb{Q}[i]$ (defined below at 4.2). We now prove this:

Proposition 2.13. *$\mathbb{Z}[i]$ consists only of those elements of the extension field $\mathbb{Q}(i)$ of $\mathbb{Q}$ which satisfy, with $a, b \in \mathbb{Z}$, a monic polynomial equation $x^2 + ax + b$.*

Proof. Any element $\alpha \in \mathbb{Q}(i)$ is of the form $\alpha = c + id$ with $c, d \in \mathbb{Z}$ and is a zero of the polynomial

$$x^2 + ax + b \in \mathbb{Q}[x] \text{ with } a = -2c, b = c^2 + d^2$$

If $c, d \in \mathbb{Q}$ then $a, b \in \mathbb{Q}$. Also, if $a, b \in \mathbb{Z}$, then $2c, 2d \in \mathbb{Z}$.

Note that $(2c)^2 + (2d)^2 = 4b \equiv 0 \bmod 4$. Since b is an integer and squares are always $\equiv 0$ or $\equiv 1$, $(2c)^2 \equiv (2d)^2 \equiv 0 \bmod 4$, c and d are integers and we are done. □

Thus, we have examined the units, prime elements, and unique factorization of this special case. If all algebraic number fields behaved in this manner, there would be no need to proceed. However, they do not - unique factorization fails, units behave unpredictably, and prime elements take a different form than in this case.

In the following pages, we will establish the foundations necessary to consider the general subject of algebraic number fields.

3. Integrality

We now proceed to define the more specifically applicable terms to our exploration of Minkowski Theory.

Definition 3.1. An *algebraic number field* is a finite field extension K of $\mathbb{Q}$, i.e. the *degree* (or *index*) of $K|\mathbb{Q}$, normally denoted $[K\colon \mathbb{Q}]$ and representing the dimension of K as a vector space over $\mathbb{Q}$, is finite. The elements of such a K are known as *algebraic numbers*, and if these are zeroes of monic polynomials $f(x) \in \mathbb{Z}[x]$ they are called *integral*.

Definition 3.2. A *subring* S of the ring R is a subgroup of R that is closed under multiplication, and contains the multiplicative identity 1.

Definition 3.3. Let $A \subseteq B$ be an extension of rings (where A is a subring of B). An element $b \in B$ is called *integral* over A if it satisfies a monic equation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad n \geq 1$$

with coefficients $a_i \in A$. This definition can be generalized to the ring B, which is called *integral* over A if all elements $b \in B$ are integral over A.

Definition 3.4. If we have some $\beta_1, \ldots, \beta_n \in B$ with the property that each $b \in B$ can be expressed uniquely as a linear combination $b = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$ with coefficients $\alpha_i \in A$, then we call this set an *integral basis* of B over A. Note that this integral basis is automatically a basis of $L|K$ as above, n is equal to the degree $[L\colon K]$. If such an integral basis exists, then B is a *free A-module* of rank n

In order to ensure that the concept of an integral basis is clear, we have included the following example, discussing the integral basis of $\mathbb{Q}(\sqrt[3]{2})$.

Example 3.5. $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$ is an integral basis for $\mathbb{Q}(\sqrt[3]{2})$. Since $\mathbb{Q}(\sqrt[3]{2})$ is a degree 3 extension of $\mathbb{Q}$, it must have an integral basis of size 3. We will now show that $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ are linearly independent over $\mathbb{Q}$, as suppose not. Then we have some $a, b, c \in \mathbb{Q}$ such that $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 = 0$, but then $a = -\sqrt[3]{2}(b + c\sqrt[3]{2}) \in \mathbb{Q}$ i.e. $-\sqrt[3]{2}(b + c\sqrt[3]{2}) = \frac{p}{q}$ with $p, q \in \mathbb{Z}$. Thus we have $p = -q\sqrt[3]{2}(b + c\sqrt[3]{2}) = -bq\sqrt[3]{2} - cq\sqrt[3]{2}^2 = -d\sqrt[3]{2} - e\sqrt[3]{2}^2 \in \mathbb{Z}$ for some $d, e \in \mathbb{Q}$. Thus we have $-\sqrt[3]{2}(d + e\sqrt[3]{2}) \in \mathbb{Z}$, but $-\sqrt[3]{2}f \in \mathbb{Z}$ only when f is some integer multiple of $\sqrt[3]{2}^2$ or such a multiple plus $\frac{1}{\sqrt[3]{2}}$. Since neither case holds, we can conclude that $p \notin \mathbb{Z}$, a contradiction. So $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$ is linearly independent. Moreover, it spans the set since it is a linearly independent set of size 3 in an extension of degree 3, due to basic properties of bases. Hence, it serves as an integral basis for the set it spans, namely $\mathbb{Q}(\sqrt[3]{2})$.

While the following result is not proved here, the transitivity of integrality is useful for our considerations and will be employed several times in the coming pages.

Proposition 3.6. *If $A \subseteq B \subseteq C$ are two ring extensions, C is integral over B, B is integral over A, then C is integral over A.*

Proof. See [2] □

3.7-3.9 may seem tangential; however, they will serve a crucial role in later proofs.

Definition 3.7. The set of elements $\overline{A} = \{b \in B \mid b \text{ integral over } A\}$ in some ring extension $A \subseteq B$ is known as the *integral closure* of A in B, and A is called *integrally closed* in B if we have that $A = \overline{A}$.

Lemma 3.8. *Consider the integrally closed integral domain A, its field of fractions K, and its integral closure B in the finite separable extension $L|K$. If we let $\alpha_1, \ldots, \alpha_n$ be some basis of $L|K$ contained in B, i.e. with $\alpha_i \in B$ and spanning $L|K$ with coefficients in K, with discriminant $d = d(\alpha_1, \ldots, \alpha_n)$, then we will have that $dB \subseteq A\alpha_1 + \cdots + A\alpha_n$*

Proof. Note that the concept of a field of fractions will be clarified later (section 7.1). To prove this, we will show that if $\alpha \in B$ then we have that

$$d\alpha \in A\alpha_1 + \cdots + A\alpha_n$$

So if $\alpha = k_1\alpha_1 + \cdots + k_n\alpha_n \in B, k_j \in K$, then these k_j are a solution of the following system of linear equations: $Tr_{L|K}(\alpha_i\alpha) = \sum_j Tr_{L|K}(\alpha_i\alpha_j)k_j$. Moreover, since we know that $Tr_{L|K} \in A$, each such k_j is the quotient of an element of A given by the value $d = \det(Tr_{L|K}(\alpha_i\alpha_j))$. Multiplying, we obtain that $dk_j \in A$, and since A is integrally closed, $d\alpha \in A\alpha_1 + \cdots + A\alpha_n$. □

Proposition 3.9. *If $L|K$ is separable and A is a principal ideal domain, then every finitely generated B-submodule $M \neq 0$ of L is a free A-module of rank $[L\colon K]$. More practically, B admits an integral basis over A.*

Proof. See [2] □

4. Ideals

4.1. **Preliminaries.** In section 2, we considered the ring of integers $\mathbb{Z}[i]$ of $\mathbb{Q}[i]$. But what do we call the more generalized ring of integers of some algebraic number field, an extension $K|\mathbb{Q}$? How do we define this ring of integers?

Definition 4.1. Consider an extension field $K|\mathbb{Q}$. Recall that if $\alpha \in K$ is an algebraic integer, it is the solution of some monic polynomial with coefficients in $\mathbb{Z}$. The ring of all such α, i.e. the integral closure of $\mathbb{Z}$ in K is called the *ring of integers* of K and is denoted $\mathcal{O}_K$.

Our discussion will now require a motivating example. Unlike the rings $\mathbb{Z}$ and $\mathbb{Z}[i]$, the ring $\mathcal{O}_K$ of integers of an algebraic number field K does not inherently possess a general uniqueness of prime factorization. For example, consider $\mathbb{Q}(\sqrt{-47})$. Its ring of integers is $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{-47})$, which we know by [1], p. 229. Now consider

$$54 = (2)(3^3) = (\frac{13 + \sqrt{-47}}{2})(\frac{13 - \sqrt{-47}}{2})$$

Unlike in Z or $Z[i]$, each of these factors is irreducible in $\mathcal{O}_K$. We will show this by contradiction. So suppose that $2 = ab$ where a and b are non-units. Therefore, we have $2 = ab$ which gives us that $4 = N_{K|\mathbb{Q}}(a)N_{K|\mathbb{Q}}(b)$. This implies that, without loss of generality, $N_{K|\mathbb{Q}}(a) = \pm 2$, but remember that we have

$$N_{K|\mathbb{Q}}(x + y(\frac{1}{2})(1 + \sqrt{-47})) = ((x + \frac{1}{2}y) + y\sqrt{-47})((x + \frac{1}{2}y) - y\sqrt{-47})$$

which simplifies to $x^2 + xy + 12y^2 = \pm 2$, and this has no integral solutions, so at least one of a or b is a unit. The other factors can be similarly proven to be irreducible. It is because of this failure of unique factorization that we have instead begun our discussion of ideals, with which we attempt to solve the problem of unique factorization in integer rings of algebraic number fields. The underlying intuition behind this progression is that each of these irreducible factors is a product of ideal prime numbers, such that

$$2 = P_1P_2, 3 = P_3P_4, (\frac{13 + \sqrt{-47}}{2}) = P_1P_3, (\frac{13 - \sqrt{-47}}{2}) = P_2P_4$$

and thus we have $P_1P_2P_3P_4 = 54$. Before we establish prime ideals, however, we must define the concept of ideals in general and outline their basic properties.

Definition 4.2. Let R be a commutative ring, and I a subgroup (an abelian group under addition) of this R. Such an I is an *ideal* of R if, for all r in R and a in I, ar is contained in I.

Definition 4.3. For any r in a ring R, we will denote (r) as the smallest ideal of R containing r, and this is the ideal *generated* by r. An ideal generated by only one element is a *principal ideal*, and an ideal generated by a finite number of elements is a *finitely generated ideal*

Hence, in the ring of integers of $\mathbb{Q}$, which is $\mathbb{Z}$, the ideal generated by 1 is $(1) = \mathbb{Z}$, the ideal generated by 2 is all even numbers, by 3 is all multiples of 3, etc. Also, note that if an ideal is generated by, for example, 2 and 3, this is actually the same as (1) as we can subtract 2 from 3 to obtain the principal ideal $(1) = \mathbb{Z}$.

Definition 4.4. An ideal B in R is a *prime ideal* if $B \neq R$ and when, with $a, b \in R$, we have $ab \in B$ then either a, b or both are elements of B.

Definition 4.5. A *Principal Ideal Domain* is an integral domain in which every ideal is principal.

Also, note that if a given domain is Euclidean, it is automatically a Principal Ideal Domain. Hence, $\mathbb{Z}[i]$ is a Principal Ideal Domain, in addition to being Euclidean.

Definition 4.6. An ideal C in R is a *maximal ideal* if $C \neq R$ and the only ideals of R containing C are itself and the whole ring, i.e. C and R.

Note that if C is an ideal of R such that R/C is a field, then C is maximal, and in any Principal Ideal Domain, a nonzero prime ideal is maximal.

Definition 4.7. A commutative ring R with an identity is *noetherian* if each of its ideals is finitely generated.

Definition 4.8. A noetherian, integrally closed integral domain in which each nonzero prime ideal is also maximal is known as a *Dedekind Domain*.

We now establish basic operation on ideals:

Remark 4.9. Take $A, B \in \mathcal{O}$ where $\mathcal{O}$ is an arbitrary Dedekind Domain.

(1) The divisibility relation $A|B$ is defined by $B \subseteq A$

(2) Summation (or union) of ideals is defined by $A + B = \{a + b \mid a \in A, b \in B\}$, i.e. the smallest ideal containing both A and B, or the greatest common divisor.

(3) Intersection of ideals is defined by the least common multiple of A and B.
(4) The product of ideals is defined by $AB = \{\sum_i a_i b_i \mid a_i \in A, b_i \in B\}$

4.2. **Results.** We can now prove the following facts about $\mathcal{O}_K$.

Theorem 4.10. *The ring $\mathcal{O}_K$ is noetherian, integrally closed, and every prime ideal $P \neq 0$ in $\mathcal{O}_K$ is a maximal ideal.*

Proof. We know that $\mathcal{O}_K$ is noetherian because each ideal A is a finitely generated $\mathbb{Z}$-module by 3.6. Thus, it is a finitely generated $\mathcal{O}_K$-module, or noetherian.

As it is the integral closure of $\mathbb{Z}$ in K, it is integrally closed by results proved in section 3.

Finally, we must show that each prime ideal $P \neq 0$ is a maximal ideal. We know that $P \cap \mathbb{Z}$ is a nonzero prime ideal (p_0) in $\mathbb{Z}$, since it is clearly prime and if $y \in P, y \neq 0$, and $y^n + a_1 y^{n-1} + \cdots + a_n = 0$ (with $a_i \in \mathbb{Z}, a_n \neq 0$) then $a_n \in P \cap \mathbb{Z}$. We also know that the integral domain $\overline{\mathcal{O}} = \mathcal{O}_K/P$ is generated from $A = \mathbb{Z}/p_0\mathbb{Z}$ by adjoining algebraic elements, and this is thus a field, since $A[\alpha] = A(\alpha)$ if α is algebraic. Thus P is maximal. □

We will now consider ideals on an arbitrary Dedekind domain $\mathcal{O}$.

Lemma 4.11. *For every ideal $A \neq 0$ of $\mathcal{O}$ there exist nonzero prime ideals $P_1, \ldots, P_n$ such that $A \supseteq P_1 \ldots P_n$.*

Proof. We prove this by contradiction. Suppose that the set Φ of ideals without such nonzero prime ideals is nonempty, i.e. there are ideals $B \neq 0$ of $\mathcal{O}$ such that they do not contain any products of nonzero prime ideals. Since $\mathcal{O}$ is noetherian, every ascending chain of ideals becomes stationary. Thus, Φ has a maximal element A_0, as if it did not, there would be an infinite chain of ideals in contradiction to our hypothesis. Since A_0 is not a prime ideal, we can find some b_1 and b_2 in $\mathcal{O}$ such that neither b_1 nor b_2 are in A, but their product $b_1 b_2$ is in A.

Now set $A_1 = (b_1) + A_0$ and $A_2 = (b_2) + A_0$. $A_0 \subsetneq A_1$ and $A_0 \subsetneq A_2$ and $A_1 A_2 \subseteq A_0$. Since A_0 is the maximal element of Φ and A_1 and A_2 are both proper supersets of A_0, both A_1 and A_2 contain a product of prime ideals. However, the product of these products is contained in A_0, so A_0 contains a product of prime ideals, a contradiction. □

We now define the inverse operation on prime ideals. We can also prove that any ideal multiplied by an inverse prime ideal is not equal to itself:

Lemma 4.12. *Let P be a prime ideal of $\mathcal{O}$ and define*

$$P^{-1} = \{x \in K \mid xP \subset \mathcal{O}\}$$

Then we have $AP^{-1} := \{\sum_i a_i x_i \mid a_i \in A, x_i \in P^{-1}\} \neq A$ for all ideals $A \neq 0$.

Proof. Let $s \in P, s \neq 0$ and $P_1 P_2 \ldots P_r \subset (s) \subset P$, minimizing r. P_1 is contained in P which implies that $P_1 = P$ since P_1 is a maximal ideal. Now, since $P_2 \ldots P_r \nsubseteq (s)$, there exists $t \in P_2 \ldots P_r$ with $t \notin s\mathcal{O}$, which implies that $s^{-1}t \notin \mathcal{O}$. We also have, however, that $tP \subseteq (s)$ giving that $s^{-1}tp \subseteq \mathcal{O}$, hence giving us that $s^{-1}t \in P^{-1}$, and therefore $P^{-1} \neq \mathcal{O}$.

Following [2], assume that $AP^{-1} = A$, and thus $P^{-1} = \mathcal{O}$ which contradicts our previous statement. □

We can now resolve the problem of unique factorization encountered earlier. We say that Euclidean domains are contained within the larger domain of Unique Factorization Domains [UFDs], which have unique factorization at the element level. However, our next consideration will be of a special type of non-UFD domains that have unique factorization at the ideal level.

Theorem 4.13. *Every ideal A of $\mathcal{O}$ which differs from* (0) *and* (1) *admits a factorization $A = P_1 \dots P_r$ into nonzero prime ideals P_i of $\mathcal{O}$ which is unique up to the order of the factors.*

Proof. First we show the existence of such a prime ideal factorization. Similar to our proof above, let Φ be the set of all ideals different from (0) and (1) which do not admit a prime ideal decomposition. Suppose it is nonempty, then there is some maximal element A in Φ, itself contained in a maximal ideal P. We know that $\mathcal{O} \subseteq P^{-1}$, and thus $A \subseteq AP^{-1} \subseteq PP^{-1} \subseteq \mathcal{O}$.

By the previous lemma, $A \subsetneq AP^{-1}$ and $P \subsetneq PP^{-1} \subseteq \mathcal{O}$. Since P is a maximal ideal, $PP^{-1} = \mathcal{O}$. Also, we know that A is maximal in Φ so since $AP^{-1} \neq \mathcal{O}$, AP^{-1} admits some prime ideal decomposition $AP^{-1} = P_1 \dots P_r$. Since $A = AP^{-1}P = P_1 \dots P_r P$, A admits a prime ideal decomposition, a contradiction.

Now, we aim to show such a factorization is unique. Let $A = P_1 P_2 \dots P_r = Q_1 Q_2 \dots Q_s$ be two prime ideal factorizations of A. Without loss of generality, P_1 divides Q_1, and since P_1 is maximal, $P_1 = Q_1$. Now multiply this by P^{-1} and then $P_2 \dots P_r = Q_2 \dots Q_s$. Continuing, $r = s$ and each P and Q can match, i.e. with renumbering $P_i = Q_i$. □

The following theorem will be employed later and is thus included for completeness. However, its proof is not instructive relative to our discussions.

Theorem 4.14. Chinese Remainder Theorem. *Let $A_1, \dots, A_n$ be ideals in a ring $\mathcal{O}$ such that $A_i + A_j = \mathcal{O}$ for $i \neq j$. Then, if $A = \bigcap_{i=1}^{n} A_i$, one has $\mathcal{O}/A \equiv \bigoplus_{i=1}^{n} \mathcal{O}/A_i$*

Proof. See [2]. □

5. Lattices

While we considered the motivating example of $\mathbb{Q}[i]$, we mentioned the concept of a lattice in the complex plane. In that case, the lattice was merely the integral points spanned by the basis $(1, i)$. However, we will now extend this definition to that of all algebraic number fields.

Definition 5.1. Consider V, an n-dimensional $\mathbb{R}$-vector space. A subgroup in V of the form $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$ with linearly independent vectors $v_1, \dots, v_m$ of V is known as a *lattice*. We call $(v_1, \dots, v_m)$ a *basis*.

Note that although the lattices which we will consider will be over real vector spaces, this definition can be generalized to lattices over $\mathbb{C}$, for example, or for any field. In the above definition, replace $\mathbb{R}$ with some arbitrary field K, and

thus V is an n-dimensional vector space over K. Instead of $\mathbb{Z}$, we will use some $\beta = (b_1, \ldots, b_n)$, a K-basis for V. Now for some ring R in K, the lattice is

$$\Gamma = \{\sum_{i=1}^{n} r_i b_i \mid r_i \in R, b_i \in B\}$$

Definition 5.2. The set $\Phi = \{x_1 v_1 + \cdots + x_m v_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$ is known as the *fundamental mesh* of the lattice, and the lattice is said to be a *complete* lattice if $m = n$.

For example, in the case of the first lattice we considered, the basis was $(1, i)$ and therefore the fundamental mesh was $\{x_1 + ix_2 \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$. This is equivalent to the square of edge 1 in the complex plane with its lower left corner on the origin; though it is only a fraction of the entirety, we can learn a great deal about the lattice by examining the fundamental mesh.

Several useful properties of lattices are as follows:

Proposition 5.3. *A subgroup $\Gamma \subseteq V$ is a lattice if and only if it is discrete*

Proof. See [2]. The discreteness of an arbitrary lattice is clear from the definition. Briefly, in the other direction, the proof proceeds as follows: assuming that Γ is discrete, the proof continues by showing that Γ is closed. Then, considering the subspace V_0 of V spanned by Γ, a basis of V_0 of size m and contained in Γ is chosen to form a complete lattice Γ_0. After proving that $(\Gamma : \Gamma_0)$ is finite, the proof uses this fact and the main theory on finitely generated abelian groups to conclude that Γ is indeed a lattice. □

Lemma 5.4. *A lattice Γ in V is complete if and only if there exists some bounded subset $M \subseteq V$ such that the collection of all translates $M + \gamma, \gamma \in \Gamma$, covers the entire space V.*

Proof. If $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ is complete then taking M to be the fundamental mesh Φ is sufficient.

To prove in the other direction, let M be such a bounded subset. Let V' be the subspace which is spanned by Γ. We must show that $V = V'$. Take $v \in V$ and we will show that it belongs to V'. $V = \bigcup_{\gamma \in \Gamma} (M + \gamma)$, so with $v \in V$, $a_v \in M$ and $\gamma_v \in \Gamma \subseteq V'$, we have$vv = a_v + \gamma_v$. Now divide this by v and take its limit going to ∞, then we have

$$v = \lim_{v \to \infty} \frac{1}{v} a_v + \lim_{v \to \infty} \frac{1}{v} \gamma_v = \lim_{v \to \infty} \frac{1}{v} \gamma_v \in V'$$

since M is bounded and V' is closed. □

Remark 5.5. In general, it will be useful to understand the volume of a lattice. This may seem nonintuitive, as we have shown a lattice is necessarily a discrete set. We will consider another measure of its volume, best thought of as the volume of the parallelepiped spanned by the fundamental mesh. This volume is calculated as

$$vol(\Phi) = |\det A|,$$

with A equivalent to (a_{ik}), i.e. the matrix of the base change from the identity to $v_1, \ldots, v_n$ so that $v_i = \sum_k a_{ik} e_k$. Equivalently, we can write that

$$vol(\Phi) = [\det(\langle v_i, v_j \rangle)]^{1/2} = vol(\Gamma).$$

With the following definitions, we will finally be ready to discuss the underlying concepts of Minkowski Theory.

Definition 5.6. A subset X of V is called *centrally symmetric*, if, given any point $x \in X$, the point $-x$ also belongs to X.

Definition 5.7. A subset X of V is called *convex* if, given any two points $x, y \in X$, the whole line segment $\{ty + (1-t)x \mid 0 \leq t \leq 1\}$ is contained in X.

Theorem 5.8. Minkowski's Lattice Point Theorem. *Let Γ be a complete lattice in the euclidean vector space V and X a centrally symmetric and convex subset of V. Now suppose that vol$(X) > 2^n$vol(Γ). Then X contains at least one nonzero lattice point $\gamma \in \Gamma$.*

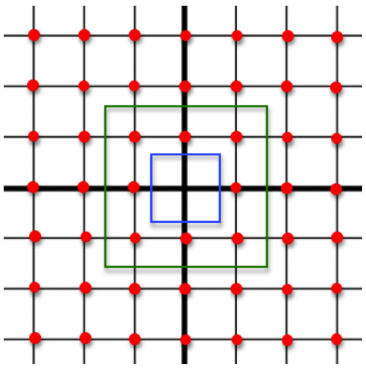

FIGURE 1. Picture Proof

First, we will demonstrate the intuition behind this theorem. Consider the case where $V = \mathbb{R}^2$, and then the lattice points are as pictured above (with distance 1 between each point on the axes). Any centrally symmetric and convex subset of V will be centered on the origin, for example the squares pictured above. In this case, vol$(\Gamma) = 1$. Note that the blue square has a volume of approximately 3, whereas the green square has a volume of approximately 9.

Now, vol(Blue Square) $= 3 <$ 4vol(γ), but vol(Green Square) $= 9 >$ 4vol(γ). According to the theorem, this would imply that the green square contains at least one nonzero lattice point, and in fact it does.

Proof. It will suffice for us to show that we can find two distinct lattice points $\gamma_1, \gamma_2 \in \Gamma$ such that

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$$

So we choose some element in this intersection, and we obtain, with $x_1, x_2 \in X$ that $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$ is such an element. Define

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

Now note that this γ is the center of the line segment joining x_2 and $-x_1$ (part of X through central symmetry) and thus contained in $X \cap \Gamma$ (through convexity).

Now, suppose that we cannot find such lattice points, i.e. that the sets $\frac{1}{2}X + \gamma$

are pairwise disjoint for all $\gamma \in \Gamma$. Then the same property would hold for the intersections $\Phi \cap (\frac{1}{2}X + \gamma)$ since an intersection can only remove elements of a set. Then we have

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

However, remember that we can translate $\Phi \cap (\frac{1}{2}X + \gamma)$ by γ, or in this case, $-\gamma$, which yields the set $(\Phi - \gamma) \cap \frac{1}{2}X$. Note that this set has the same volume as the initial set. Also, $\Phi - \gamma, \gamma \in \Gamma$ cover the entire space V since with the addition of one γ, we have the fundamental mesh and its lattice translate. In particular they cover the set $\frac{1}{2}X$. This yields the inequality chain:

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

but this violates our initial hypothesis. Thus, two such lattice points exist, and X contains at least one nonzero lattice point. □

6. Minkowski Theory

Essentially, the intuition behind Minkowski Theory is the interpretation of degree n algebraic number fields $K|\mathbb{Q}$ as points in some n-dimensional space. The results of the theory are based upon the above Lattice Point Theorem, but before we can derive the desired results, we must discuss the definitions of Minkowski Space and its associated operations. First among these is the space $K_{\mathbb{C}}$, based upon a family of complex embeddings.

Definition 6.1. $K_{\mathbb{C}}$ is a $\mathbb{C}$-vector space defined by a function j which maps from K to this $K_{\mathbb{C}}$:

$$j \colon K \to K_{\mathbb{C}} = \prod_{\tau} \mathbb{C}, \quad a \mapsto ja = (\tau a)$$

where τ are the n complex embeddings $\tau \colon K \to \mathbb{C}$. Thus, $j(a) = (\tau_1 a, \tau_2 a, \ldots, \tau_n a)$ is some element of $K_{\mathbb{C}}$.

Remark 6.2. $K_{\mathbb{C}}$ is equipped with the *hermitian scalar product* $\langle x, y \rangle = \sum_{\tau} x_\tau \overline{y}_\tau$

Having defined this $K_{\mathbb{C}}$, we now restrict it as follows:

Definition 6.3. The *Minkowski Space* is the Euclidean vector space

$$K_{\mathbb{R}} = K_{\mathbb{C}}^{+} = [\prod_{\tau} \mathbb{C}]^{+}$$

where the points in $K_{\mathbb{R}}$ are the points $(z_\tau) \in K_{\mathbb{C}}$ such that $z_{\overline{\tau}} = \overline{z}_\tau$.

Remark 6.4. The scalar product in the Minkowski Space is known as the canonical metric, and it is denoted $\langle\ ,\ \rangle \colon K_{\mathbb{R}} \times K_{\mathbb{R}} \to K_{\mathbb{R}}$.

Remark 6.5. We can more explicitly describe Minkowski spaces. Note that of the n embeddings τ, the embeddings into $\mathbb{C}$ of K, we have some which already map to $\mathbb{R}$. We will denote the real embeddings as $\rho_1, \ldots, \rho_r \colon K \to \mathbb{R}$. The remaining embeddings are complex, and come in pairs, denoted $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s \colon K \to \mathbb{C}$. Thus $n = r + 2s$ and

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

We now want to be able to consider the relation of the Minkowski Space to $\mathbb{R}^n$.

Proposition 6.6. *There exists an isomorphism*

$$f\colon K_{\mathbb{R}} \to \prod_{\tau} \mathbb{R} = \mathbb{R}^{r+2s} = \mathbb{R}^n$$

$$f\colon (z_\tau) \mapsto (x_\tau)$$

with $x_\rho = z_\rho, \quad x_\sigma = Re(z_\sigma), \quad x_{\overline{\sigma}} = Im(z_\sigma)$. *This isomorphism transforms the canonical metric into the scalar product* $(x, y) = \sum_{\tau} \alpha_\tau x_\tau y_\tau$ *with* $\alpha_\tau = 1$ *or* 2 *if* τ *is real or complex, respectively.*

Proof. The map is an isomorphism as it is clearly injective and surjective, as well as structure preserving. Now to prove the claim in regards to scalar products, take $z = (z_\tau) = (x_\tau + iy_\tau)$ and $z' = (z'_\tau) = (x'_\tau + iy'_\tau) \in K_{\mathbb{R}}$. First, consider $\langle z, z' \rangle$ when τ is real. We have $(z, z') = z_\rho \overline{z}'_\rho = x_\rho x'_\rho$ which fits our proposition. Now given that $y_\sigma = x_{\overline{\sigma}}, x_\sigma = y_{\overline{\sigma}}, y'_\sigma = x'_{\overline{\sigma}}$, and $x'_\sigma = y'_{\overline{\sigma}}$,

$$z_\sigma \overline{z}'_\sigma + z_{\overline{\sigma}} \overline{z}'_{\overline{\sigma}} = z_\sigma \overline{z}'_\sigma + \overline{z}_\sigma z'_\sigma = 2\mathrm{Re}(z_\sigma \overline{z}'_\sigma) = 2(x_\sigma x'_\sigma + x_{\overline{\sigma}} x'_{\overline{\sigma}}).$$

□

Remark 6.7. Since this scalar product takes the canonical measure from $K_{\mathbb{R}}$ to $\mathbb{R}^{r+2s}$, it differs from the standard Lebesgue measure by the relation

$$\mathrm{vol}_{\mathrm{canonical}}(X) = 2^s \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)).$$

Now we show an alternative method for determining the volume of the fundamental mesh, and thus a lattice:

Proposition 6.8. *If* $A \neq 0$ *is an ideal of* $\mathcal{O}_K$ *then* $\Gamma = jA$ *is a complete lattice in* $K_{\mathbb{R}}$ *with fundamental mesh of volume*

$$vol(\Gamma) = \sqrt{|d_K|}(\mathcal{O}_K\colon A).$$

Proof. Let $a_1, \ldots, a_n$ be a $\mathbb{Z}$-basis of A, and thus $\Gamma = \mathbb{Z}ja_1 + \cdots + \mathbb{Z}ja_n$. Now choose a numbering of our embeddings $\tau\colon K \to \mathbb{C}$, $\tau_1, \ldots, \tau_n$, and then form a matrix $B = (\tau_s a_i)$. Using [2] 2.12,

$$d(A) = d(a_1, \ldots, a_n) = (\det B)^2 = (\mathcal{O}_K\colon A)^2 d(\mathcal{O}_K) = (\mathcal{O}_K\colon A)^2 d_K.$$

However,

$$(\langle ja_i, ja_k \rangle) = (\sum_{s=1}^{n} \tau_s a_i \overline{\tau}_s a_k) = B\overline{B}^t.$$

We conclude:

$$\mathrm{vol}(\Gamma) = |\det(\langle ja_i, ja_k \rangle)|^{1/2} = |\det B| = \sqrt{|d_K|}(\mathcal{O}_K\colon A).$$

□

The following result relies heavily on the above proofs, and will be an important tool as we proceed.

Theorem 6.9. *Let $A \neq 0$ be an integral ideal of K, and let $c_\tau > 0$, with $\tau \in Hom(K, \mathbb{C})$, be real numbers such that we have*

$$c_\tau = c_{\overline{\tau}} \qquad \text{and} \qquad \prod_\tau c_\tau > \Delta(\mathcal{O}_K : A),$$

with $\Delta = (\frac{2}{\pi})^s \sqrt{|d_k|}$. Then there exists $a \in A, a \neq 0$ such that

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

Proof. Consider the set $X = \{(z_\tau) \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$ which is centrally symmetric and convex. Note that its volume, denoted $\mathrm{vol}(X)$, can be calculated by the isomorphism we defined in 6.6. By 6.7, we have that

$$\mathrm{vol}(X) = 2^s \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)) = 2^s \mathrm{vol}_{\mathrm{Lebesgue}}(\{(x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\rho| < c_\rho,\ x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2\})$$

so

$$\mathrm{vol}(X) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s} \pi^s \prod_\tau c_\tau.$$

Now we apply 6.8:

$$\mathrm{vol}(X) = 2^{r+s} \pi^s \prod_\tau c_\tau > 2^{r+s} \pi^s (\frac{2}{\pi})^s \sqrt{|d_K|} (\mathcal{O}_K : A) = 2^n \mathrm{vol}(\Gamma)$$

and we are done. Hence, there is some lattice point $ja \in X, a \neq 0, a \in A, jA \in \Gamma$, and furthermore $|\tau a| < c_\tau$. □

The following is a necessary lemma for Theorem 6.11, but its proof is not instructive for our purposes.

Lemma 6.10. *Consider the convex, centrally symmetric set*

$$X = \{(z_\tau) \in K_\mathbb{R} \mid \sum_\tau |z_\tau| < t\}.$$

X has volume $vol(X) = 2^r \pi^s \frac{t^n}{n!}$.

Proof. See [2], III.2.15. □

We now prove the existence of an upper bound for the norm of some element of any nonzero ideal of a ring of integers $\mathcal{O}_K$.

Theorem 6.11. *In every ideal $A \neq 0$ of $\mathcal{O}_K$, there exists an $a \in A, a \neq 0$ such that*

$$|N_{K|\mathbb{Q}}(a)| \leq M(\mathcal{O}_K : A),$$

where M is referred to as the Minkowski Bound *and $M = \frac{n!}{n^n} (\frac{4}{\pi})^s \sqrt{|d_K|}$.*

Proof. We proceed in a manner similar to Theorem 6.9, using 6.10. Consider the set $X = \{(z_\tau) \in K_\mathbb{R} \mid \sum_\tau |z_\tau| < t\}$ which has volume $2^r \pi^s \frac{t^n}{n!}$. Since X is convex and centrally symmetric, we know by the Minkowski Lattice Point Theorem that some $a \in A$ is a lattice point of Γ, and we also know that $\mathrm{vol}(X) = 2^r \pi^s \frac{t^n}{n!} > 2^n \mathrm{vol}(\Gamma)$, where $\mathrm{vol}(\Gamma) = 2^- s \sqrt{|d_K|} (\mathcal{O}_K : A)$. So now, using the known inequality between arithmetic and geometric means,

$$\frac{1}{n} \sum_\tau |z_\tau| \geq (\prod_\tau |z_\tau|)^(1/n)$$

we see that

$$|N_{K|\mathbb{Q}}(a)| = \prod_{k=1}^{r}|\rho_k(a)|\prod_{k=1}^{s}|\sigma_k(a)^2| \leq n^{-n}(\sum_{k=1}^{r}|\rho_k(a)| + 2\sum_{k=1}^{r}|\sigma_k(a)|)^n$$

which, given the conditions for elements of X, and substituting for t^n is

$$|N_{K|\mathbb{Q}}(a)| \leq \frac{t^n}{n^n} \leq \frac{2^n 2^{-s}\sqrt{|d_K|}(\mathcal{O}_K\colon A)n!}{2^r\pi^s n^n} = (\frac{2}{\pi})^s\frac{\sqrt{|d_K|}(\mathcal{O}_K\colon A)}{n^n} \leq (\frac{4}{\pi})^s\frac{\sqrt{|d_K|}(\mathcal{O}_K\colon A)}{n^n}$$

□

Example 6.12. The Minkowski bound for $\mathbb{Q}[\sqrt{-5}]$ can be calculated using the above. $n = 2$ since $\mathbb{Q}[\sqrt{-5}]$ is a quadratic extension, therefore of degree 2. Also, $s = 1$ because for each real embedding, we have exactly one corresponding pair of complex embeddings. The discriminant is -20, and as the ring of integers for this field is $\mathcal{O}_K = \mathbb{Z}[1, \sqrt{-5}]$, there exists some $a \neq 0, a \in A$ (with $A \neq 0$) of $\mathcal{O}_K$ such that $|N_{K|\mathbb{Q}}(a)| \leq \frac{4}{\pi}\sqrt{5}(\mathcal{O}_K\colon A)$.

There also exists a multiplicative version of Minkowski theory. Similar to the homomorphism j from K to $K_{\mathbb{C}}$, we now examine the restriction

$$j\colon K^* \to K_{\mathbb{C}}^* = \prod_{\tau}\mathbb{C}^*.$$

This multiplicative group $K_{\mathbb{C}}^*$ admits the homomorphism $N\colon K_{\mathbb{C}}^* \to \mathbb{C}^*$ which can be calculated by taking the product of the coordinates. Note that $N \circ j$ is the usual norm of $K|\mathbb{Q}$.

Since we are building a lattice, we must use logarithms to pass from multiplicative to additive groups. Take $l\colon \mathbb{C}^* \to \mathbb{R}, z \mapsto \log|z|$. This map induces the surjective homomorphism $l\colon K_{\mathbb{C}}^* \to \prod_{\tau}\mathbb{R}$, and this gives us a commutative diagram.

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{l} & \prod_{\tau}\mathbb{R} \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{C}^* & \xrightarrow{l} & \mathbb{R} \end{array}$$

As we did previously, we restrict these operations to elements fixed under conjugation. Note that in the below diagram, the plus sign in the exponent of the term on the upper right, $[\prod_{\tau}\mathbb{R}]^+$, restricts the term inside the brackets to elements fixed under complex conjugation. This notation will be employed similarly from now on.

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\prod_{\tau}\mathbb{R}]^+ \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array}$$

Furthermore, we can explicitly describe $[\prod_{\tau}\mathbb{R}]^+$ using our existing terminology as follows.

$$[\prod_{\tau}\mathbb{R}]^+ = \prod_{\rho}\mathbb{R} \times \prod_{\sigma}[\mathbb{R} \times \mathbb{R}]^+$$

Note that the second factor can be identified with $\mathbb{R}$ by the map $(x, x) \mapsto 2x$, which gives us an isomorphism $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$. Thus, the trace now becomes a map from $\mathbb{R}^{r+s}$ to $\mathbb{R}$ as we expect, and $l\colon K_\mathbb{R}^* \to \mathbb{R}^{r+s}$ is explicitly given by the equation

$$l(x) = (\log|x_{\rho_1}|, \dots, \log|x_{\rho_r}|, \log|x_{\sigma_1}|^2, \dots, \log|x_{\sigma_s}|^2)$$

with $x \in K_\mathbb{R}^* \subseteq \prod_\tau \mathbb{C}^*$ since $x = (x_\tau)$

7. Class Numbers

7.1. **Preliminaries.** We are now ready to apply the results gained through our exploration of Minkowski Theory, first by proving the finiteness of the ideal class group. Before we proceed, however, we must establish the preliminary definitions and foundations of this group.

Definition 7.1. Consider the field of fractions K of $\mathcal{O}$, a Dedekind domain. A *fractional ideal* of K is a finitely generated $\mathcal{O}$-submodule $A \neq 0$ of K.

Proposition 7.2. *The fractional ideals form an abelian group, the* ideal group *which we will denote J_K of K. The identity element is $(1) = \mathcal{O}$ and we define the inverse of A to be $A^{-1} = \{x \in K \mid xA \subseteq \mathcal{O}\}$*

Proof. Associativity, commutativity, and the fact that $A(1) = A$ are clear.

For some prime ideal P, we know that $P \subsetneq PP^{-1}$ by 4.12. Thus, since P is maximal, $PP^{-1} = \mathcal{O}$. Thus, if $A = P_1 \dots P_r$ is an integral ideal, then $B = P_1^{-1} \dots P_r^{-1}$ is an inverse, and thus $BA = \mathcal{O}$ implies that $B \subseteq A^{-1}$.

Also, if $xA \subseteq \mathcal{O}$ then $xAB \subseteq B$, showing that $x \in B$ since $AB = \mathcal{O}$. Therefore, $B = A^{-1}$.

Finally, if A is some arbitrary fractional ideal and $C \in \mathcal{O}$ is a nonzero ideal such that $CA \subseteq \mathcal{O}$ then $(CA)^{-1} = C^{-1}A^{-1}$ is the inverse of CA, which implies that $AA^{-1} = \mathcal{O}$. □

We now generalize 4.13 into the broader category of fractional ideals.

Corollary 7.3. *Every fractional ideal A admits a unique representation as a product $A = \prod_p p^{v_p}$, where $v_p \in \mathbb{Z}$ and $v_p = 0$ for almost all p. Namely, this implies that J_K is the free abelian group on the set of nonzero prime ideals p of $\mathcal{O}$.*

Proof. See [2] I.3.9 for the proof that A is a quotient of two integral ideals B and C. Uniqueness comes from 4.13. □

Similarly, we must generalize the concept of principal ideals.

Definition 7.4. The fractional principal ideals $(A) = A\mathcal{O}$ with $A \in K^*$ are a subgroup of the ideals J_K, and we will denote this subgroup P_K.

With fractional ideals established, it is now logical for us to consider the result of modding out the fractional principal ideals from the ideal group, since $J_K \supset P_K$.

Definition 7.5. The quotient group $Cl_K = J_K/P_K$ is known as the *ideal class group*, or *class group* of K.

Definition 7.6. The *absolute norm* of an ideal A in the ring $\mathcal{O}_K$ is $\mathcal{N}(A) = (\mathcal{O}_K : A)$

7.2. **Results.**

Proposition 7.7. *Let A be an ideal of a ring $\mathcal{O}_K$, and let $p_1, \ldots, p_r$ be prime ideals of this $\mathcal{O}_K$. If $A = p_1^{v_1} \ldots p_r^{v_r}$, is the prime factorization of an ideal $A \neq 0$, then $\mathcal{N}(A) = \mathcal{N}(p_1)^{v_1} \ldots \mathcal{N}(p_r)^{v_r}$*

Proof. See [2]. The proof is based upon the Chinese Remainder Theorem. □

With this, we can finally apply Minkowski Theory to the problem of the ideal class group.

Theorem 7.8. *The ideal class group $Cl_K = J_K/P_K$ is finite. We will denote its order as $h_K = (J_K \colon P_K)$ and call it the* class number *of K.*

Proof. If $P \neq 0$ is a prime ideal of $\mathcal{O}_K$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$, then $\mathcal{O}_K/P$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ of arbitrary degree $f \geq 1$. Further, $\mathcal{N}(P) = p^f$, since $(p\mathbb{Z} \colon \mathbb{Z}) = p$. Now, for a given p, only finitely many such prime ideals P exist because $P|(p)$. Thus we have only finitely many P for each p and there are only finitely many prime ideals P with bounded absolute norm.

Now, since each integral ideal admits some representation $A = P_1^{v_1} \ldots P_r^{v_r}$ with $v_i > 0 \ \forall \ i$ and since $\mathcal{N}(A) = \mathcal{N}(P_1)^{v_1} \ldots \mathcal{N}(P_r)^{v_r}$, we can conclude that there are only finitely many ideals A of $\mathcal{O}_K$ with a bounded absolute norm $\mathcal{N}(A) < M$.

Therefore, to show our claim, it will be enough to show that each class $[A] \in Cl_K$ contains some integral ideal A_1 satisfying the inequality

$$\mathcal{N}(A_1) \leq M = (\frac{2}{\pi})^s \sqrt{|d_K|}.$$

So we will choose some arbitrary A in the class, along with $b \in \mathcal{O}_K, b \neq 0$, such that we have $B = bA^{-1} \subseteq \mathcal{O}_K$. By the above proof of the existence of the Minkowski bound, we can choose some $\beta \in B, \beta \neq 0$ with $|N_{K|\mathbb{Q}}(\beta)| \leq M\mathcal{N}(B)$ which we can rearrange to the following

$$|N_{K|\mathbb{Q}}(\beta)|\mathcal{N}(B)^{-1} = \mathcal{N}(\beta)B^{-1} = \mathcal{N}(\beta B^{-1}) \leq M.$$

Thus, the ideal $A_1 \colon = \beta B^{-1} = \beta b^{-1} A \in [A]$ has the required property, and Cl_K is finite. □

Example 7.9. For quadratic fields with discriminant $5, 8, 11, -3, -4, -7$, and -8, the class number is 1. We know this because of Minkowski's Bound, which gives us some element of the ideal with norm less than his namesake bound. When we plug in discriminants, along with $n = 2$ because it is a quadratic field, $s = 0$ for the positive cases because there are no complex embeddings and $s = 1$ for the negative cases as there are complex embeddings, we obtain, respectively, $M \approx 1.12, 1.41, 1.66, 1.10, 1.27, 1.68$, and 1.80, all less than 2. Thus, we have that there exists some $a \in A$ for each of these ideals such that $\mathcal{N}(a) \leq M$, i.e. that $\mathcal{N}(a) \leq 1.80 < 2$, and since this must be an integer, we can only conclude that $\mathcal{N}(a) = 1$ for these discriminants, i.e. that the class number is 1.

8. Dirichlet's Unit Theorem

Having discussed the ideal class group, we can now discuss other interesting aspects of $\mathcal{O}_K$, namely the group of units $\mathcal{O}_K^*$. Although $\mathcal{O}_K^*$ itself is not necessarily finite, it contains the finite group of the roots of unity lying in K, denoted $\mu(K)$, Recall the commutative diagram from above.

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\prod_\tau \mathbb{R}]^+ \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R} \end{array}$$

Now, looking at the upper half of the diagram, we find three subgroups of note.

$\mathcal{O}_K^* = \{\epsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\epsilon) = \pm 1\}$, the group of units
$S = \{\gamma \in K_{\mathbb{R}}^* \mid N(\gamma) = \pm 1\}$ the norm-one surface
$H = \{x \in [\prod_\tau \mathbb{R}]^+ \mid Tr(x) = 0\}$, the trace-zero hyperplane

Note that our existing functions serve as homomorphisms, i.e. $j\colon \mathcal{O}_K^* \to S$ and $l\colon S \to H$ gives us a composite homomorphism, $\lambda := l \circ j\colon \mathcal{O}_K^* \to H$, and its image $\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$.

Definition 8.1. A sequence of groups and group homomorphisms, denoted by $\cdots \to X_{n-1} \overset{\alpha_n}{\to} X_n \overset{\alpha_{n+1}}{\to} X_{n+1} \to \ldots$, is said to be *exact* if, for each X_i, image α_n=ker α_{n+1}.

Proposition 8.2. *The sequence* $1 \to \mu(K) \to \mathcal{O}_K^* \overset{\lambda}{\to} \Gamma \to 0$ *is exact.*

Proof. Exactness at $\mu(K)$ and Γ is clear. Thus, we must show that $\mu(K)$ is the kernel of λ. Note that for $\zeta \in \mu(K)$ and $\tau\colon K \to \mathbb{C}$ some embedding, we can find $\log|\tau\zeta| = \log 1 = 0$, and thus $\mu(K) \subseteq \ker(\lambda)$.

Now let $\epsilon \in \mathcal{O}_K^*$ be in the kernel, i.e. $\lambda(\epsilon) = l(j\epsilon) = 0$. We can then conclude that $|\tau\epsilon| = 1$ for each embedding, and thus $j\epsilon = (\tau\epsilon)$ lies in some bounded domain of $K_{\mathbb{R}}$. However, remember that by 6.8, $j\epsilon$ is a point of the $K_{\mathbb{R}}$ lattice $j\mathcal{O}_K$. Thus, the kernel of λ contains finitely many elements, and, as it is a finite group, contains only roots of unity in K^* (see [2] I.7.1). Thus, $\mu(K) \supseteq \ker(\lambda)$. □

Lemma 8.3. *Up to multiplication by units, there are only finitely many elements* $\alpha \in \mathcal{O}_K$ *of a given norm* $N_{K|\mathbb{Q}}(\alpha) = \alpha$

Proof. Take some $a \in \mathbb{Z}, a > 1$. Now consider $\mathcal{O}_K/a\mathcal{O}_K$. In each of the finitely many cosets of this quotient, there exists up to multiplication by units at most one element α such that $|N(\alpha)| = a$. We know this as, if $\beta = \alpha + a\gamma, \gamma \in \mathcal{O}_K$ is another such element, we have $\frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta}\gamma \in \mathcal{O}_K$ since $\mathbb{N}(\beta)/\beta \in \mathcal{O}_K$. Also, $\frac{\beta}{\alpha} = 1 \pm \frac{N(\alpha)}{\alpha}\gamma \in \mathcal{O}_K$, which gives us that β is associated to α. Hence, up to the multiplication of units, we have at most $(\mathcal{O}_K\colon a\mathcal{O}_K)$ elements of norm $\pm a$, and it is finite as we wanted. □

Theorem 8.4. *The group* Γ *is a complete lattice in the* $(r+s-1)$*-dimensional vector space* H*. As a consequence, it is isomorphic to* $\mathbb{Z}^{r+s-1}$*.*

Proof. The proof is rather unwieldy - see [2] for full details. □

Theorem 8.5. *This is known as* Dirichlet's Unit Theorem. *The group of units* $\mathcal{O}_K^*$ *of* $\mathcal{O}_K$ *is the direct product of the finite cyclic group* $\mu(K)$ *and a free abelian group of rank* $r+s-1$*.*

Proof. By the above, we know that Γ is a free abelian group of rank $t = r+s-1$. Now, let $v_1, \ldots, v_t$ be a $\mathbb{Z}$-basis of γ, and let $\epsilon_1, \ldots, \epsilon_t \in \mathcal{O}_K$ be the preimages of

each v_i. Finally, let $A \subseteq \mathcal{O}_K^*$ be the subgroup generated by these ϵ_i. Thus, we can conclude that A is mapped isomorphically onto Γ by λ. Therefore $\mu(K) \cap A = \{1\}$, which shows $\mathcal{O}_K^* = \mu(K) \times A$. □

Remark 8.6. This implies that there exist $\epsilon_1, \ldots, \epsilon_t$ called *fundamental units* such that any other unit ϵ can be written uniquely as a product $\epsilon = \zeta \epsilon_1^{v_1} \ldots \epsilon_t^{v_t}$ where ζ is a root of unity and v_i are integers.

Example 8.7. We will now apply this result to consider the group of units of both real and imaginary quadratic field extensions. First, we will consider real quadratic field extensions. For an arbitrary $\mathbb{Q}[\sqrt{D}]$, D square-free and positive, note that $r = 2, s = 0$, and thus $r + s - 1 = 1$. For example, $\mathbb{Q}[\sqrt{3}]$ has two real embeddings, where $1 + \sqrt{3}$ can be mapped to either $1 + \sqrt{3}$ or $1 - \sqrt{3}$. This implies that the group of units of $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{3}$ is the direct product of group of the roots of unity of $\mathbb{Q}[\sqrt{3}]$, which are only 1 and -1, and a free abelian group of rank 1. Thus, the group of units is isomorphic to $\{-1, 1\} \times \mathbb{Z}$, and in this specific case, calculation shows that the group of units is $(2 + \sqrt{3})^{\mathbb{Z}}$ where the exponent $\mathbb{Z}$ refers to the integer multiples of this fundamental unit, and their respective isomorphisms to the integers ($2 + \sqrt{3}$ maps to 1, $-4 - \sqrt{3}$ maps to -2, etc.).

Now we consider the imaginary quadratic field extensions. For an arbitrary $\mathbb{Q}[\sqrt{D}]$, D square-free and negative, note that $r = 0, s = 1$, and thus $r + s - 1 = 0$ as there are no real embeddings and only one pair of complex embeddings. Thus, any imaginary quadratic field has a group of units for its ring of integers that is only composed of the group of the roots of unity, and in all cases but two, this will be $(1, -1)$. The two exception are $\mathbb{Q}[i]$ as described above, as well as $\mathbb{Q}[\sqrt{-3}]$. For more details on the latter, see [4], Chapter 6.

9. Extending Dedekind Domains

We can now take some arbitrary Dedekind domain and extend its characteristics to some related integrally closed domain.

Proposition 9.1. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, $L|K$ a finite extension of K, and $\overline{\mathcal{O}}$ the integral closure of $\mathcal{O}$ in L. Then $\overline{\mathcal{O}}$ is also a Dedekind domain.*

Proof. As in an earlier proof, we know that since $\overline{\mathcal{O}}$ is the integral closure of $\mathcal{O}$, it is also integrally closed.

The set of nonzero prime ideals $\mathcal{P}$ of $\overline{\mathcal{O}}$ is maximal. Choose some $p \in P, p \neq 0, P \in \mathcal{P}$. Given this p, we can find a polynomial

$$c_0 + c_1 p + \cdots + c_n p^n = 0 \qquad c_i \in \mathcal{O}, c_0 \neq 0$$

Therefore, $c_0 = -p(c_1 + \cdots + c_n p^{n-1}$ and $c_0 \in P \cap \mathcal{O}$. Hence, $P \cap \mathcal{O}$ is a nonzero prime ideal in $\mathcal{O}$, and since $\mathcal{O}$ is a Dedekind domain, $P \cap \mathcal{O}$ is maximal. Thus, the integral domain $\overline{\mathcal{O}}/\mathcal{P}$ is an algebraic extension of the field $\mathcal{O}/P$, and is hence a field. Thus, P is a maximal ideal.

Now we will show that $\overline{\mathcal{O}}$ is noetherian in the case that $L|K$ is a separable extension (for the inseparable case, see [2] 12.8). Take some basis of $L|K$ called $\alpha = a_1 + \cdots + a_n$ contained in $\overline{\mathcal{O}}$. The discriminant of this basis is $D = d(a_1, \ldots, a_n)$ and by [2] I.2.8 and Lemma 3.4 above, $D \neq 0$ and $\overline{\mathcal{O}} \subset \mathcal{O}a_1/D + \cdots + \mathcal{O}a_n/D$. Thus, each ideal of $\overline{\mathcal{O}}$ is contained in this same $\mathcal{O}$-module, and is thus itself a finite $\mathcal{O}$-module, i.e. it is also a finitely generated $\overline{\mathcal{O}}$-module, hence noetherian. □

Though the proof is beyond the scope of this paper, we will conclude with a very interesting identity, known as the *fundamental identity*. This identity weaves together many of the concepts discussed in this paper, and while it is not a result of Minkowski Theory, the conclusions we have drawn through the applications of Minkowski's theorems have led us to this point.

With our above notation, note that for $P \in \mathcal{O}$, we have $P\overline{\mathcal{O}} \neq \overline{\mathcal{O}}$. Moreover, if $P \neq 0$ then $P\overline{\mathcal{O}}$ decomposes into a unique product of prime ideals, $P\overline{\mathcal{O}} = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$, where $P = \mathcal{P} \cap \mathcal{O}$. This e_i is known as the *ramification index*, of $\mathcal{P}_i$ over P and the degree of the field extension $f_i = [\overline{\mathcal{O}}/\mathcal{P}_i \colon \mathcal{O}/P]$ is known as the *inertia degree* of $\mathcal{P}_i$ over P. The fundamental identity is:

If $L|K$ is separable, then

$$\sum_{i=1}^{r} e_i f_i = n = [L : K].$$

Proceeding based upon the Chinese Remainder Theorem, the proof connects the degree of the larger field extension with the product of the respective exponents of prime ideals and the degrees of each sub-field extension.

10. Acknowledgments

It is a pleasure to thank my mentor, Vaidehee Thatte, for her invaluable help on this project. In addition, I would like to thank the UChicago Department of Mathematics, and especially Dr. Peter May, for providing this wonderful opportunity, both to myself and other students - it's an extraordinary program that has developed my ability to discuss and write about mathematics. Finally, thank you to the people, far too numerous to name here, who tolerated me as I blabbed on and on about Minkowski Bounds, Class Numbers, and lattice points - I truly appreciate your patience.

References

[1] David S. Dummit and Richard M. Foote. Abstract Algebra, 3rd ed. John Wiley and Sons, Inc., 2004.

[2] Jurgen Neukirch, translated from the German by Norbert Schappacher. Algebraic Number Theory. Springer, 1999.

[3] Serge Lang. Algebra. Springer, 2002.

[4] Robert B. Ash. A Course in Algebraic Number Theory. Robert Ash, 2003. Available at http://www.math.uiuc.edu/∼r-ash/ANT.html.