THE CLASS NUMBER THEOREM

TIMUR AKMAN-DUFFY

Abstract. In basic number theory we encounter the class group (also known as the ideal class group). This group measures the extent that a ring fails to be a principal ideal domain. If the group is finite, we call the order of the group the class number. Not every ring will have a class number, but the class number theorem states that class group of the ring of of algebraic integers in an algebraic number field is finite. In this paper we present a proof of this theorem by building the foundations needed. Although there are less lengthy proofs to the class number theorem, this method establishes a solid understanding the class number theorem and number theoretic aspects of the class group.

Contents

The class group is a useful notion in number theory. It can be thought as providing a "measurement" on a ring, which tells us how far the ring is from being a principal ideal domain and, consequently, degree of the failure of unique factorization (since every principal ideal domain is a unique factorization domain). In the case that this group is finite, the order of the group is defined as the class number. A class number of 1 indicates that a ring is a principal ideal domain, with larger numbers indicating a higher degree of failure for unique factorization. Understanding the class group yields useful insights into basic number theory and the structure of various types of rings.

The primary goal of this paper is to define and prove the class number theorem, which states, "the class group of the ring of algebraic integers in an algebraic number field is finite." In doing so, we will also define the objects that class groups study and the tools needed for the proof. This paper does not offer any original material, but aims to clearly explain the class number theorem and closely related topics to a person with a knowledge of abstract algebra.

We begin by defining localization, which will be useful in later proofs and concepts. From there, we will construct Dedekind rings and explain algebraic number fields. These will be a prime focus of the paper and are the subject of the class number theorem. We will then describe determinants and lattices, which are the tools we need to finally prove the class number theorem.

1. Localization

Definition 1.1. Let R be an integral domain. A nonempty subset S of R is a *multiplicative set* if S does not contain 0 and S contains the product of any two elements in S.

Proposition 1.2. *Let R be an integral domain and S a multiplicative set in R. There is a ring, denoted R_S, which contains a subring isomorphic to R and also contains multiplicative inverses of every element of S. R_S is generated by R and s^{-1}, where $s \in S$.*

The above statement may be made clearer if R_S is defined as such:

$$R_S = \{r/s : r \in R, s \in S\} \tag{1.3}$$

with the equivalence relation on $R \times S$ defined as (r, s) is equivalent to (q, t) if $rt = qs$. We define 1 as $1 = s/s$ and we define 0 as $0 = 0/s$.

Notice R_S is an integral domain.

Definition 1.4. R_S, as constructed above, is called the *localization* of R at S.

It should be noted that r/s is the equivalence class of (r, s).

We can localize an integral domain with respect to any multiplicative set, but for our purposes we will only focus on localization at prime ideals. The following proposition displays an important correspondence between prime ideals of integral domains and their localizations.

Proposition 1.5. *Let R be an integral domain, and S be a multiplicative set in R. There is a one-to-one correspondence between the prime ideals of R which have empty intersection with S and the prime ideals of R_S. The prime ideal $\mathfrak{p}$ of R corresponds to the ideal $\mathfrak{p}R_S$ of R_S.*

When we consider localization at a prime ideal $\mathfrak{p}$, we are allowing R to be an integral domain and S to be the set of elements $s \in R$ such that $s \notin \mathfrak{p}$. Notice that, since $\mathfrak{p}$ is a prime ideal, S is a multiplicative set.

For the sake of convenience, we will write $R_\mathfrak{p}$ to represent $R_{R-\mathfrak{p}}$.

Proposition 1.6. *Let $\mathfrak{p}$ be a prime ideal of R. Then $R_\mathfrak{p}$ has only one maximal ideal, which is $\mathfrak{p}R_\mathfrak{p}$*

The proof follows from Proposition 1.5.

2. Dedekind Rings

Definition 2.1. A *discrete valuation ring*, or DVR, is is a principal ideal domain with only one maximal ideal.

Notice that every field is a DVR, but not every DVR must be a field. For the rest of the paper, every DVR we refer to will not be a field.

Theorem 2.2. *Let R be a DVR (that is not a field) and let $\pi \in R$ such that the unique maximal ideal $\mathfrak{p} = \pi R$. R has the following properties.*
(i) R is a notherian ring.
(ii) Every nonzero $x \in R$ has the form $x = u\pi^k$, where k is a nonnegative integer and u is a unit in R.
(iii) Every nonzero ideal has the form $R\pi^k$, where k is a nonnegative integer.
(iv) R is integrally closed. In other words, if we look at the field of fractions of R, call it S, then every element of S that is integral over R is an element of R.
(v) $\mathfrak{p}$ is the only nonzero prime ideal of R.

Proof. (i) PIDs are notherian.
(ii) R is a PID, and thus a UFD. Thus, since R is not a field, it can only have one prime element up to unit multiples.
(iii) Follows from (ii) and the fact that all ideals in R are principal.
(iv) Every UFD is integrally closed.
(v) Since R is not a field, π and $\mathfrak{p}$ are not zero. Since $\mathfrak{p}$ is a nonzero maximal ideal, it is prime. By (iii), all ideals have the form $R\pi^k$, so there are no other prime ideals. □

Definition 2.3. A ring R is a *Dedekind ring* if it is a notherian integral domain such that the localization $R_\mathfrak{p}$ is a DVR for every prime ideal $\mathfrak{p}$ of R.

Theorem 2.4. *If R is a Dedekind ring, then R_S is a Dedekind ring.*

Dedekind rings have many interesting properties, especially with regards to ideals.

Theorem 2.5. *Every nonzero prime ideal of a Dedekind ring R is a maximal ideal.*

Proof. Assume not. Then there exist distinct, nonzero prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$, such that $\mathfrak{p}_1 \subset \mathfrak{p}_2$. By Proposition 1.5, $\mathfrak{p}_1 R_{p_2} \subset \mathfrak{p}_2 R_{\mathfrak{p}_2}$ is a chain distinct prime ideals in $R_{\mathfrak{p}_2}$. But $R_{\mathfrak{p}_2}$ is a DVR, and thus only has one nonzero prime ideal. Contradiction. □

Theorem 2.6. *Let $\mathfrak{U}$ be a nonzero ideal of a Dedekind ring R. Then $\mathfrak{U} = \mathfrak{p}_1^{a_1} ... \mathfrak{p}_n^{a_n}$, where $\mathfrak{p}_1, ..., \mathfrak{p}_n$ are distinct prime ideals uniquely determined by $\mathfrak{U}$ and $a_1, ..., a_n$ are positive integers uniquely determined by $\mathfrak{U}$.*

We do not necessarily have unique factorization into irreducible elements in Dedekind domains (we will use an example to show this in the next section). However, the previous Theorem shows that, by using prime ideals, we can establish a notion of unique factorization in Dedekind rings. This gives the number theoretic feel to Dedekind rings.

3. Algebraic Number Fields

Our goal in this paper is to prove that the class group is finite for the *ring of algebraic integers* in an *algebraic number field*. In this section, we will define these terms and their relation to Dedekind rings.

Definition 3.1. Given a ring R and a ring extension S, an element of S is *integral* over R if it is the root of a monic polynomial with coefficients in R.

Definition 3.2. A ring R is *integrally closed* if every element of S that is integral over R is an element of R.

Definition 3.3. The *integral closure* of a ring R is the set of all elements of S that are integral over R.

Definition 3.4. An *algebraic number field* is a finite dimensional extension field, call it L, of the rational number field $\mathbb{Q}$.

Definition 3.5. An element of an algebraic number field, $l \in L$, is an *algebraic integer* if l is integral over the ring of integers $\mathbb{Z}$.

Proposition 3.6. *Consider a Dedekind ring R with quotient field K. Let L be a finite dimensional extension field of K. The integral closure of R in L will result in a Dedekind ring.*

Notice that, since $\mathbb{Z}$ is a Dedekind ring, the ring of algebraic integers in an algebraic number field is also a Dedekind ring.

It is a fact that the ring of algebraic integers can be computed if given a primitive element. For the proof, please refer to page 47 of Janusz [1].

We will now show that a Dedekind ring does not necessarily have unique factorization into irreducibles. In other words, not every Dedekind ring is a UFD.

Example 3.7. Consider $\mathbb{Z}[\sqrt{-5}]$. By Proposition 3.6, it is a Dedekind ring. Notice that, in $\mathbb{Z}[\sqrt{-5}]$,

$$21 = 3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

We want to show that these both are irreducible factorizations of 21. Let us define a norm such that

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

We know an element x is a unit if $N(x) = 1$. Thus, we can clearly see that 1 and -1 are the only units.

Obviously 3 and 7 are irreducible. Let's assume $1 + 2\sqrt{-5}$ is not irreducible (the exact same argument will work for $1 - 2\sqrt{-5}$). Then $1 + 2\sqrt{-5} = xy$. But $N(1 + 2\sqrt{-5}) = 21$. So $N(x)N(y) = 21$. Thus the possible values for $N(x)$ are $1, 3, 7$, or 21. But, by the definition of the norm, $N(x) \neq 3, 7$. Thus either x or y must be a unit. Contradiction. Hence $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind ring that is not a UFD.

4. Fractional Ideals and Class Groups

In order to understand class groups, we must define what a fractional ideal is. Unless otherwise specified, let R be a Dedekind ring and K be the quotient field of R.

Definition 4.1. A *fractional ideal* of a Dedekind Ring R is a nonzero finitely generated R-submodule of K.

Definition 4.2. If $\mathfrak{M}$ is a fractional ideal of R, then $\mathfrak{M}^{-1}$ is the set $\{x \in K : x\mathfrak{M} \subseteq R\}$. $\mathfrak{M}^{-1}$ is called the *inverse* of $\mathfrak{M}$.

Definition 4.3. A *regular element* is a nonzero element of a ring that is neither a right nor a left zero divisor.

Definition 4.4. A *regular ideal* is an ideal of a ring that contains a regular element of the ring.

Proposition 4.5. *A fractional ideal is, up to a constant, a regular ideal.*

Proof. We know that a fractional ideal is finitely generated. Consider a fractional ideal $\mathfrak{a}$ which is generated by $\{a_1, ..., a_n\}$ of a ring R. We can pick elements $b_1, ..., b_n \in K$ and a regular element d such that $d = a_1b_1d + ... + a_nb_nd \in \mathfrak{a}$. Thus $\mathfrak{a}$ contains a regular element, and therefore it is a regular ideal. □

From this Proposition, we can see that all nonzero fractional ideals are invertible.

Notice that $\mathfrak{M}$ need not be contained in R. Consider the following example:

Example 4.6. For simplicity, let's consider the ring of integers, $\mathbb{Z}$. $\mathbb{Z}$ is a PID, so by definition it is a Dedekind ring. Consider $\frac{1}{2}\mathbb{Z}$. By definition this is a fractional ideal, but it is not contained in $\mathbb{Z}$.

We also note that every ideal in a Dedekind ring is finitely generated, thus every ideal in a Dedekind ring is a fractional ideal.

Now we know enough about fractional ideals to define what a class group is. However, we will observe some basic properties about fractional ideals first, which will be relevant later.

Definition 4.7. A fractional ideal $\mathfrak{M}$ is *invertible* if $\mathfrak{M}\mathfrak{M}^{-1} = R$.

We will use what we set up in Example 4.6 to illustrate this definition.

Example 4.8. Let $\mathfrak{M} = \frac{1}{2}\mathbb{Z}$. By definition, $\mathfrak{M}^{-1} = \{2n : n \in \mathbb{N}\}$ Hence $\mathfrak{M}\mathfrak{M}^{-1} = \mathbb{Z}$. Thus $\mathfrak{M}$ is invertible.

In the previous example, it is easy to see that every nonzero fractional ideal of $\mathbb{Z}$ is invertible. This leads us into the following lemma, which we will state without proof.

Lemma 4.9. *An integral domain R is a Dedekind ring if and only if every nonzero ideal of R is invertible.*

4.1. **Class Groups.** Using the basic concepts of fractional ideals we just learned, we can define a class group. First, let us define some symbols.

$\mathbf{I}(R)$ represents the collection of all fractional ideals of R. We will call it the *ideal group* of R.

$\mathbf{P}(R)$ represents the collection of all principal ideals of R. Notice it is a subgroup of $\mathbf{I}(R)$.

We can now define a class group.

Definition 4.10. A *class group*, represented by $\mathbf{C}(R)$, is the quotient

$$\mathbf{C}(R) = \mathbf{I}(R)/\mathbf{P}(R). \tag{4.11}$$

Notice that if R is a PID, then $\mathbf{C}(R) = 1$. In other words, the class group is of order 1.

We can interpret $\mathbf{C}(R)$ to be a measure of how far R is from being a PID. Notice that, if we have a class group of order 1, we know that it is a UFD. Thus, we can also interpret the class number as the extent to which unique factorization into irreducible elements fails in R.

We will prove that $\mathbf{C}(R)$ is finite if R is the ring of algebraic integers in an algebraic number field. However, $\mathbf{C}(R)$ does not have to be finite for arbitrary Dedekind rings.

5. Determinants, Traces, and Norms

In this section, we will regard K as a field and L as a finite dimensional extension field of K.

Definition 5.1. Each element $a \in L$ gives rise to a function $r_a : L \to L$ such that

$$r_a : y \to ya.$$

If we select a basis $u_1, ..., u_n$ for L over K, then we can construct a matrix for r_a, call it $[b_{ij}]$, where

$$r_a(u_i) = u_i a = \sum_j b_{ij} u_j.$$

This composite mapping is called the *regular representation* of L over K.

Obviously our choice of basis will change the matrix. However, regardless of our basis, the *trace* and *determinant* will remain the same.

Definitions 5.2. (1) The *trace* of L over K is the function $T_{L/K}(x) = trace(r_x)$.
(2) The *norm* of L over K is the function $N_{L/K}(x) = det(r_x)$.

Remark 5.3. Unless otherwise specified, we will use $T(x)$ for $T_{L/K}(x)$ and $N(x)$ for $N_{L/K}(x)$.

Proposition 5.4. *Let $x, y \in L$ and $a \in K$. Then:*
(i) $T(x + y) = T(x) + T(y)$.
(ii) $T(ax) = aT(x)$.
(iii) $N(xy) = N(x)N(y)$.
(iv) $N(ax) = a^n N(x)$ where $n = [L : K]$, the dimension of L over K.
(v) Let E be a subfield of L that contains K. Then $T_{L/K}(x) = T_{E/K}(T_{L/E}(x))$ for all $x \in L$.

Proof. (i) through (iv) are straightforward. (v) requires some work, and we will prove it here. Pick a basis E over K, $a_1, ..., a_k$, and a basis L over E, $b_1, ..., b_m$. Let $x \in L$ and $y \in E$. Then

$$xb_i = \sum_j \beta_{ij}(x) b_j, yb_p = \sum_q \alpha_{pq}(y) a_q,$$

where $\beta_{ij}(x) \in E$ and $\alpha_{pq}(y) \in K$. Then

$$T_{E/K}(y) = \sum_p \alpha_{pp}(y), T_{L/E}(x) = \sum_i \beta_{ii}(x).$$

Notice also that $a_i b_j$ give a basis of L over K,

$$xa_s b_t = \sum_j a_s \beta_{tj}(x) b_j = \sum_j \sum_i \alpha_{si}(\beta tj(x)) a_i b_j.$$

Thus,

$$T_{L/K}(x) = \sum_i \sum_p \alpha_{pp}(\beta_{ii}(x)) = T_{E/K}(T_{L/E}(x)).$$

□

When dealing with Galois groups and separable extensions, useful properties emerge. Let $K \subseteq L \subseteq F$ be a chain of separable extensions such that F is Galois over K. Define the Galois group F over K by $G = G(F/K)$ and the Galois group F over L by $H = G(F/L)$. Notice that H is the subgroup of G that fixes L elementwise.

Let

$$\sigma_1 H, \sigma_2 H, ..., \sigma_n H$$

be the distinct cosets of H in G. $n = [L : K]$ and σ_i are the distinct injections over K of L into a normal extension of K. If we consider $x \in L$ with described notation above, the following properties hold.

Proposition 5.5. *(i)* $T_{L/K}(x) = \sigma_1(x) + ... + \sigma_n(x)$.
(ii) $N_{L/K} = \sigma_1(x)...\sigma_n(x)$.

Definition 5.6. Let R be a Dedekind ring with quotient field K. L is the finite dimensional separable extension field of K, and R' is the integral closure of R in L. Let $x_1, ..., x_n$ be a basis of L over K. The *discriminant* of the basis is

$$\Delta(x_1, ..., x_n) = det[T_{L/K}(x_i x_j)]. \tag{5.7}$$

Definition 5.8. Using the notation given in Definition 5.6, if all $x_i \in R'$, then $T_{L/K}(x_i x_j) \in R$, thus $\Delta(x_1, ..., x_n) \in R$. We can let $x_1, ..., x_n$ range over all bases of L over K that lie in R'. Taking the discriminants of these bases generates an ideal $\Delta(R'/R)$, called the *discriminant ideal* of R' over R.

We state a useful Lemma that shows a discriminant ideal can be determined locally.

Lemma 5.9. *Let R be a Dedekind ring with quotient field K. Let R' be the integral closure of R in L, and let S be a multiplicative set in R. Then*

$$\Delta(R'_S/R_S) = \Delta(R'/R)_S. \tag{5.10}$$

6. Lattices

What we learn in this section will be integral in proving the class number theorem.

Unless otherwise stated, V is an n-dimensional $\mathbb{R}$ Euclidean space.

Definition 6.1. An abelian subgroup $\mathcal{L}$ of a real vector space V is called a *lattice* if

$$\mathcal{L} = \mathbb{Z}v_1 + ... + \mathbb{Z}v_r. \tag{6.2}$$

Definition 6.3. A lattice $\mathcal{L}$ is called a *full lattice* if r from Equation 6.2 is the dimension of of V over $\mathbb{R}$.

If we are looking at full lattices, then there is a very natural set of vectors to choose for our lattice, namely, the basis vectors for V.

Definition 6.4. Let $v_1, ..., v_n$ be a basis for V and $\mathcal{L}$ a full lattice. Then we call the set

$$T = \{r_1 v_1 + ... + r_n v_n : 0 \leq r_i < 1, 1 \leq i \leq n\}. \tag{6.5}$$

the *fundamental parallelepiped* for $\mathcal{L}$.

Consider such a parallelepiped. Notice that each vector of the basis v_i can be written as

$$v_i = \sum_j \alpha_{ij} u_j.$$

where $u_1, ..., u_n$ is the orthonormal basis of V.

Definition 6.6. The *volume* of $\mathcal{L}$ is defined as

$$vol(T) = |det[\alpha_{ij}]|. \tag{6.7}$$

It is a fact that, regardless of what basis is chosen for a given V, the volume of the resulting fundamental parallelepiped is does not vary. This can be seen in Janusz [1], page 63.

Lemma 6.8. *Let $\mathcal{L}$ be a full lattice in V. Let T be a fundamental parallelepiped of $\mathcal{L}$. Then the translates, $\lambda + T$, where $\lambda \in \mathcal{L}$, are pairwise disjoint and cover V.*

Proof. Let $v_1, ..., v_n$ be our basis for V. Then we can write any $v \in V$ as $v = \sum_i s_i v_i$, where $s_i \in \mathbb{R}$.

We can express s_i as $s_i = n_i + r_i$, where $n_i \in \mathbb{Z}$ and $0 \leq r_i < 1$. Thus $v = \sum_i n_i v_i + \sum_i r_i v_i$, so we have expressed v as the sum of an element of $\mathcal{L}$ and and element of T. Thus the translates cover V.

Now let's prove they are pairwise disjoint. Suppose $\lambda_1 + T$ and $\lambda_2 + T$ have a common point. Then

$$\lambda_1 - \lambda_2 \in \mathcal{L} \bigcap T.$$

But $\mathcal{L} \bigcap T = 0$, since $\mathbb{Z}v_i \neq r_i v_i$. Thus $\lambda_1 = \lambda_2$, and we conclude the translates are pairwise disjoint. □

Definition 6.9. A *sphere* in V is the set

$$U(m) = \{r_1 v_1 + ... + r_n v_n : r_1^2 + ... + r_n^2 \leq m^2\} \tag{6.10}$$

where $v_1, ..., v_n$ is a basis for V.

Definition 6.11. A subset of V is *bounded* if it is contained in some sphere.

Theorem 6.12. *An additive subgroup $\mathcal{L}$ of V is a lattice if and only if every sphere contains only a finite number of points in $\mathcal{L}$.*

Proof. $\Rightarrow$ Let $\mathcal{L}$ be a lattice with basis vectors $v_1, ..., v_r$. (In the case that $r < n$, we can extend this set to the basis $v_1, ..., v_n$ and replace $\mathcal{L}$ with $\sum_i \mathbb{Z}v_i$.) By definition, any sphere is contained in $U(m)$ using basis vectors $v_1, ..., v_n$. So let's examine $\mathcal{L} \cap U(m)$. Consider the vector $\sum_i n_i v_i \in \mathcal{L} \cap U(m)$. Then each $n_i \in \mathbb{Z}$ and $|n_i| \leq m$ by Definition 6.9. Thus, only finite many n_i are contained in the intersection, so the sphere only contains a finite number of points in $\mathcal{L}$.
$\Leftarrow$ We will use induction on the dimension n of V. Let $V = \mathbb{R}v_1$, which has dimension 1. There are two cases:
(i) $\mathcal{L} = 0$. Then it is a lattice.
(ii) $\mathcal{L} \neq 0$. Let $r_1 v_1$ be a nonzero element of $\mathcal{L}$. Thus $U(|r_1|)$ has at least one element and a finite number of elements from $\mathcal{L}$. Now select $r > 0$ such that $v = rv_1 \in \mathcal{L}$ and r is minimal with respect to this. Thus $\mathcal{L} \supseteq \mathbb{Z}v$.

Now pick $sv \in \mathcal{L}$, such that $s \in \mathbb{R}$. We can write $s = m + q$, where $m \in \mathbb{Z}$ and $0 \leq q < 1$. We know $qv = qrv_1 \in \mathcal{L}$. But r is minimal, so $0 \leq qr < r$ implies $q = 0$. Thus $\mathcal{L} \subseteq \mathbb{Z}v$, and therefore $\mathcal{L} = \mathbb{Z}v$.

Now we will consider $n > 1$. By the induction hypothesis, we can assume that $\mathcal{L}$ is not contained in any proper subspace of V. So we can write $\mathbb{R}\mathcal{L} = V$, which means we can select a basis of V contained in $\mathcal{L}$. We will represent this basis as $v_1, ..., v_n$. Let V_0 be the subspace spanned by $v_1, ..., v_{n-1}$. By induction, we know $\mathcal{L}_0 = \mathcal{L} \cap V_0$ is a full lattice in V_0.

Now pick a basis of $\mathcal{L}_0$ represented by $w_1, ..., w_{n-1}$. We can make this a basis of V by adding one element, $w_1, ..., w_{n-1}, v_n$. Hence, any element of $\mathcal{L}$ can be written as such:

$$\lambda = \sum_{i}^{n-1} r_i w_i + r_n v_n. \tag{6.13}$$

Since it is a lattice, if $r_n \in \mathbb{Z}$, then $r_i \in \mathbb{Z}$ for all i. If we subtract an element of $\mathcal{L}_0$ from such λ we may obtain an element such that $|r_i| < 1$ if $1 \leq i \leq n-1$.

Notice that there are a only finite number of $\lambda \in \mathcal{L}$ where $|r_n|$ is bounded above. Pick λ such that $0 < r_n$ and r_n is minimal. Call this w_n. Then $w_1, ..., w_n$ is a basis for V. For a general element $\lambda' \in \mathcal{L}$, we can write

$$\lambda' = \sum_{1}^{n} a_i wi, a_i \in \mathbb{R}.$$

We want to show that this is a lattice. If we can show that all the a_i are integers, we will be done. Let's explore the two cases.
(1) We can subtract an integer multiple of w_n such that $a_n = 0$. Thus $\lambda' \in \mathcal{L}_0$, and thus $\mathcal{L}$ is a lattice.
(2) We can subtract an integer multiple of w_n such that $0 < |a_n| < 1$. Then we can subtract an element of $\mathcal{L}_0$ so that $|a_i| < 1$ for all $1 \leq i \leq n-1$. But then we will have an element in the form of Equation 6.13 where the coefficient of v_n is $0 < a_n r_n < r_n$. This contradictions our choice of a minimal r_n. Thus this case cannot occur.

This completes the proof. □

Definition 6.14. A set X in V is *convex* if, for all $x, y \in X, (x+y)/2 \in X$.

Definition 6.15. A set X in V is *centrally symmetric* if, for all $x \in X, -x \in X$.

Lemma 6.16. *Let T be a fundamental parallelepiped of $\mathcal{L}$. If Y is a bounded subset of V and the translates $\lambda + Y$, $\lambda \in \mathcal{L}$, are disjoint, then $vol(Y) \leq vol(T)$*

Proof. We are given that Y is bounded, so it is contained in some sphere. By Theorem 6.12, this sphere only contains a finite number of points in $\mathcal{L}$. Thus, there can only be finitely many λ such that $(\lambda + T) \bigcap Y$ is nonempty.

By Lemma 6.16, we know that all the nonempty intersections are pairwise disjoint and cover Y, so

$$vol(Y) = \sum_{\lambda} vol[(\lambda + T) \bigcap Y].$$

Notice

$$(\lambda + T) \bigcap Y = [T \bigcap (Y - \lambda)] + \lambda.$$

Thus

$$vol[(\lambda + T) \bigcap Y] = vol[[T \bigcap (Y - \lambda)] + \lambda] = vol[T \bigcap (Y - \lambda)].$$

$Y - \lambda$ is a translate of Y, and by the Lemma we know that the translates of Y are disjoint. However, we do not know if $\sum_{\lambda} vol[T \bigcap (Y - \lambda)]$ covers T, as the assumptions of of Lemma 6.16 are not met. Thus, we can only claim that $\sum_{\lambda} vol[T \bigcap (Y - \lambda)] \leq vol(T)$. But $vol(Y) = \sum_{\lambda} vol[T \bigcap (Y - \lambda)]$. Hence $vol(Y) \leq vol(T)$. □

Theorem 6.17 (Minkowski's Theorem)**.** *Let $\mathcal{L}$ be a full lattice in vector space V where V is dimension n over $\mathbb{R}$. Let X be a bounded, centrally symmetric, convex subset of V. If $vol(X) > 2^n vol(\mathcal{L})$, then X contains a nonzero point of $\mathcal{L}$.*

Proof. Let's consider X as given above. We will construct the set $\frac{1}{2}X$ such that

$$\frac{1}{2}X = \left\{ \frac{1}{2}x : x \in X \right\}.$$

The volume of the set is

$$vol\left[\frac{1}{2}X\right] = vol(2^{-1}X) = 2^{-n} vol(X) > vol(\mathcal{L}).$$

By Lemma 6.16, if the translates of $\frac{1}{2}X$ were disjoint, then $vol[\frac{1}{2}X] \leq vol(\mathcal{L})$. Since this is not the case, we can assume there exist $\lambda_1 \neq \lambda_2$ such that

$$\frac{1}{2}x + \lambda_1 = \frac{1}{2}y + \lambda_2,$$

where $x, y \in X$. By simple manipulation, we conclude that

$$(x - y)/2 = \lambda_2 - \lambda_1 \neq 0.$$

Thus there exists a nonzero point of $\mathfrak{L}$ that is in X. □

Before we move on, we will state a quick proposition about the volume of a centrally symmetric, convex subsets in an n-dimensional $\mathbb{R}$ vector space. This will help us in the next section.

Proposition 6.18. *Let $n = r + 2s$, where r, s are nonnegative. We will represent points in the n-dimensional $\mathbb{R}$ vector space V by the usual n-tuples. For a positive real number, t, define a set*

(6.19)

$$X_t = \{(x_1, ..., x_r, y_1, z_1, ..., y_s, z_s) : |x_1| + ... + |x_r| + 2\sqrt{y_1^2 + z_1^2} + ... + 2\sqrt{y_s^2 + z_s^2} < t\}$$

where all the coordinates are real. Then

$$vol(X_t) = \frac{2^{r-s}\pi^s t^n}{n!}.$$

For proof, see page 66 of Janusz [1].

7. The Class Number Theorem

Finally, we have the tools necessary to prove what we are interested in:

Theorem 7.1. *The class group of the ring of algebraic integers in an algebraic number field is finite.*

We will prove this Theorem by first proving several related propositions. Once we have these tools, the final proof will be quite straightforward.

First, we will define our terms. We denote our algebraic number field by K and the ring of algebraic integers in K by R. $\mathbf{C}(R)$ will represent the class group of the ring of algebraic integers, as defined in Section 4. E will be a normal extension of $\mathbb{Q}$ which contains K. The Galois group of $E/\mathbb{Q}$, usually written as $G(E/\mathbb{Q})$, will be written as G for simplicity. Similarly, $H = G(E/K)$.

We will let $\sigma_1, ..., \sigma_n$ represent all the distinct cosets, σH, in G. Thus, n is the degree of K over $\mathbb{Q}$ and σ_i are the embeddings of K into $\mathbb{C}$.

Notice that, for all i, $\sigma_i(K)$ either lies in the real field or it has a complex root. Let's organize them based on where they lie. We will choose all the σ_i such that $\sigma_i(K)$ lies in the real field $\mathbb{R}$. We will label them $\sigma_1, ..., \sigma_r$. (Note: r may equal 0.)

For the remaining $n - r$ cosets, notice we have $\sigma_j \neq \overline{\sigma_j}$. Thus, there must be an even number of cosets remaining. We can organize them as such:

$$\sigma_{r+1}, ..., \sigma_{r+s}, \overline{\sigma_{r+1}}, ..., \overline{\sigma_{r+s}}.$$

Hence, $n = r + 2s$. This should look quite familiar (see Proposition 6.18).

From this, we can compute actual vectors in $\mathbb{R}^n$. Let's consider the function $v^* : K \to \mathbb{R}^r \times \mathbb{C}^s$ defined as, for $x \in K$,

$$v^*(x) = (\sigma_1(x), ..., \sigma_r(x), ..., \sigma_{r+s}(x)).$$

We can define $\mathbb{C}$ as a two dimensional $\mathbb{R}$ vector space. Thus, we can write $\mathbb{C}^s$ as a 2s dimensional $\mathbb{R}$ vector space as such: For $x \in K$, we write

(7.2)

$$v(x) = (\sigma_1(x), ..., \sigma_r(x), Re(\sigma_{r+1}(x)), Im(\sigma_{r+1}(x)), ..., Re(\sigma_{r+s}(x)), Im(\sigma_{r+s}(x))).$$

Now we make a computation that will be useful for future theorems.

Lemma 7.3. *Pick basis $a_1, ..., a_n$ of K over $\mathbb{Q}$. Let $M = [v(a_m)]$ (where $v(x)$ is defined as above) be an $n \times n$ matrix with row m equal to $v(a_m)$. Now define D to be the $n \times n$ matrix such that row m equals*

$$\sigma_1(a_m), ..., \sigma_r(a_m), \sigma_{r+1}(a_m), ..., \sigma_{r+s}(a_m), \overline{\sigma_{r+1}}(a_m), ..., \overline{\sigma_{r+s}(a_m)}.$$

Then

$$det(M) = (-2i)^{-s} det(D)$$

where $i^2 = -1$.

Proof. The proof is essentially row and column manipulation. In matrix D add columns $r+1$ and $r+2$ together in order to obtain, in row k, the entry $2Re(\sigma_{r+1}(a_k))$. We will now multiply column $r+1$ by $\frac{1}{2}$. Subtract this from column $r+2$ to obtain the entry $-iIm(\sigma_{r+1}(a_k))$.

Repeat this with all the conjugate columns. Now we have a matrix that is almost the same M, with the only difference being a factor of 2 in s columns and a factor of $-i$ in s columns. Thus, the determinants $det(M)$ and $det(D)$ differ by a factor of $(-2i)^{-s}$, which is what we wanted. □

Definition 7.4. Let $\mathfrak{U}$ be a fractional ideal of R. The discriminant $\Delta(\mathfrak{U}/\mathbb{Z})$ of $\mathfrak{U}$ is the ideal of $\mathbb{Z}$ generated by $\Delta(a_1, ..., a_n)$, where $(a_1, ..., a_n)$ run through all the bases of K over $\mathbb{Q}$ contained in $\mathfrak{U}$.

Proposition 7.5. *Let our terms be as they were in the definition above. Let* $M = [v(a_i)]$. *Then*

$$\Delta(\mathfrak{U}/\mathbb{Z}) = (-4)^s det(M)^2 \tag{7.6}$$

Proof. Pick a matrix D as defined in Lemma 7.3. Consider DD^t. By Proposition 5.5(i), the i, j entry of the matrix is $T_{K/\mathbb{Q}}(a_i a_j)$. Thus

$$det(DD^t) = det(D)^2 = \Delta(\mathfrak{U}/\mathbb{Z}).$$

Also, by Definition 7.3,

$$det(D)^2 = (-4)^s det(M)^2.$$

This leads to the result

$$\Delta(\mathfrak{U}/\mathbb{Z}) = (-4)^s det(M)^2.$$

□

Proposition 7.7. $\Delta(\mathfrak{U}/\mathbb{Z}) = \mathcal{N}(\mathfrak{U})^2 \Delta(R/\mathbb{Z})$ *where* $\mathcal{N}(\mathfrak{U})$ *is the number of elements of* $R/\mathfrak{U}$.

Proof. It is sufficient to prove that the the equation holds after localization at every maximal ideal of $\mathbb{Z}$. Let p be prime and $S = \mathbb{Z} - p\mathbb{Z}$. Let $\mathfrak{U}_S = aR_S$ for some $a \in R_S$.

Pick a basis of R over $\mathbb{Z}$, $x_1, ..., x_n$. We know this is still a basis of R_S over $\mathbb{Z}_S$. Then $ax_1, ..., ax_n$ is a $\mathbb{Z}_S$ basis of $\mathfrak{U}_S$.

Using Definition 5.1, we can construct a regular representation mapping $r_a : y \to ya$ with respect to the basis $x_1, ..., x_n$. We will call the resulting matrix ρ_a. Thus

$$T_{K/\mathbb{Q}}(ax_i ax_j) = \rho_a [T_{K/\mathbb{Q}}(x_i x_j)] \rho_a^t.$$

We know that $N_{K/\mathbb{Q}}(a) = det(\rho_a)$, so

$$\Delta(ax_1, ..., ax_n) = N_{K/\mathbb{Q}}(a)^2 \Delta(x_1, ..., x_n).$$

Lastly, we need the equation

$$N_{K/\mathbb{Q}}(\mathfrak{U}_S) = N_{K/\mathbb{Q}}(a)\mathbb{Z}_S = \mathcal{N}\mathbb{Z}_S.$$

Combining the three previous equations, we obtain the equation

$$\Delta(\mathfrak{U}_S/\mathbb{Z}_S) = \mathcal{N}(\mathfrak{U}_S)^2 \Delta(R_S/\mathbb{Z}_S). \tag{7.8}$$

By Lemma 5.9 the result follows. □

Theorem 7.9. *Let* $\mathfrak{U}$ *be a nonzero ideal in* R, *the ring of algebraic integers. Let* $v : K \to \mathbb{R}^n$ *be as in Equation 7.2. Then* $v(\mathfrak{U})$ *is a full lattice, and its volume is* $2^{-s}|\Delta(R/\mathbb{Z})|^{1/2}\mathcal{N}(\mathfrak{U})$.

Proof. First, we want to show that $v(\mathfrak{U})$ is a full lattice. Begin by picking a $\mathbb{Z}$ basis of $\mathfrak{U}$, $a_1, ..., a_n$. Clearly, $v(a_1), ..., v(a_n)$ is a $\mathbb{Z}$ basis of $v(\mathfrak{U})$. Thus, the vectors $v(a_1), ..., v(a_n)$ are linearly independent, and we can conclude that $v(\mathfrak{U})$ is a full lattice.

Now, we will compute the volume. Construct a matrix M such that row i equals $v(a_i)$. Then $det(M)$ equals the volume of the lattice. By Proposition 7.5,

$$det(M) = 2^{-s}|\Delta(\mathfrak{U}/\mathbb{Z})|^{1/2}. \tag{7.10}$$

By Proposition 7.7, we know

$$\Delta(\mathfrak{U}/\mathbb{Z}) = \mathcal{N}(\mathfrak{U})^2\Delta(R/\mathbb{Z}).$$

If we substitute this into Equation 7.10, we obtain the result

$$det(M) = 2^{-s}|\Delta(R/\mathbb{Z})|^{1/2}\mathcal{N}(\mathfrak{U}).$$

□

Theorem 7.11. *Let $\mathfrak{U}$ be a nonzero ideal of R. Then there exists an element $a \in \mathfrak{U}, a \neq 0$, such that*

$$|N_{K/\mathbb{Q}}(a)| \leq (n!/n^n)(4/\pi)^s|\Delta(R/\mathbb{Z})|^{1/2}\mathcal{N}(\mathfrak{U}).$$

Proof. Let the set X_t be as in Equation 6.19. Then X_t is a centrally symmetric convex subset of $\mathbb{R}^n$, which allows us to use what we learned in the previous section. By Proposition 6.18, we see that

$$vol(X_t) = \frac{2^{r-s}\pi^s t^n}{n!}. \tag{7.12}$$

By Theorem 7.9, we know

$$v(\mathfrak{U}) = 2^{-s}|\Delta(R/\mathbb{Z})|^{1/2}\mathcal{N}(\mathfrak{U}). \tag{7.13}$$

By Theorem 6.17, if $vol(X_t) > 2^n vol(\mathfrak{U})$, then X_t contains a nonzero point of $v(\mathfrak{U})$. We see, by Equations 7.12 and 7.13, that this inequality holds if

$$t^n = \epsilon + n!\left(\frac{2^{n-r}}{\pi^s}\right)\mathcal{N}(\mathfrak{U})|\Delta_R|^{1/2}. \tag{7.14}$$

As ϵ approaches zero, we will get a point in $X_t \cap v(\mathfrak{U})$. By Theorem 6.12, we know that the lattice contains a finite number of points in any sphere. Thus even if $\epsilon = 0$, the intersection contains a nonzero point. Assume t is selected as in Equation 7.14, where $\epsilon = 0$. Pick a nonzero $a \in \mathfrak{U}$ such that

$$v(a) = (\sigma_1(a), ..., \sigma_r(a), Re(\sigma_{r+1}(a)), Im(\sigma_{r+1}(a)), ...) = (x_1, ..., x_r, y_1, z_1, ..., y_s, z_s)$$

is in X_t.

We know, from Section 5, that

$$|N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{r}|\sigma_i(a)|\prod_{j=1}^{s}|\sigma_{r+j}(a)|^2 = |x_1|...|x_r|(y_1^2+z_1^2)...(y_s^2+z_s^2).$$

We now apply the Arithmetic-Geometric Mean Inequality, which states

$$\left(\prod_i^n b_i\right)^{1/n} \leq \frac{\sum_1^n b_i}{n},$$

for nonnegative real b_i, and conclude

$$|N_{K/\mathbb{Q}}(a)|^{1/n} \leq \frac{1}{n}\left(\sum_i |x_i| + 2\sum_j \sqrt{y_j^2+z_j^2}\right) < \frac{t}{n}.$$

Replace t^n by the value given in Equation 7.14, and we are given the desired equation, $|N_{K/\mathbb{Q}}(a)| \leq (n!/n^n)(4/\pi)^s|\Delta(R/\mathbb{Z})|^{1/2}\mathcal{N}(\mathfrak{U})$. □

For the next Theorem, we need the following definition.

Definition 7.15. Two ideals, $\mathfrak{U}$ and $\mathfrak{B}$, are *equivalent* if $\mathfrak{U} = \mathfrak{B}c$ for some nonzero c. The equivalence class of $\mathfrak{U}$ is represented by $[\mathfrak{U}]$.

Theorem 7.16 (The Minkowski Bound)**.** *For any nonzero fractional ideal $\mathfrak{B}$ of R there is an $\mathfrak{U} \in [\mathfrak{B}]$ such that $\mathfrak{U} \subseteq R$ and*

$$\mathcal{N}(\mathfrak{U}) \leq (n!/n^n)(4/\pi)^s|\Delta|^{1/2}.$$

Proof. Pick $b \in \mathfrak{B}$ such that $\mathfrak{B}_1 = b\mathfrak{B}^{-1}$ is an ideal in R which lies in $[\mathfrak{B}^{-1}]$. By Theorem 7.11 there exists a nonzero $a \in \mathfrak{U}_0$ such that

$$|N_{K/\mathbb{Q}}(a)|\mathcal{N}(\mathfrak{B}_1)^{-1} \leq (n!/n^n)(4/\pi)^s|\Delta|^{1/2}.$$

Let $\mathfrak{U} = a{\mathfrak{B}_1}^{-1}$. Then $\mathfrak{U} \subseteq R$ (since $a \in \mathfrak{B}_1$). Thus

$$\mathcal{N}(\mathfrak{U}) = \mathcal{N}(a\mathfrak{B}_1^{-1}) = |N_{K/\mathbb{Q}}(a)|\mathcal{N}(\mathfrak{B}_1)^{-1}.$$

This proves the Theorem. □

Notice that the previous Theorem proves that the bound on $\mathcal{N}(\mathfrak{U})$ depends only on K. With this, we are ready to prove our main Theorem.

Theorem 7.17. *The class group of the ring of algebraic integers in an algebraic number field is finite.*

Proof. By Theorem 7.16, every class contains an integral ideal, call it $\mathfrak{U}$, such that

$$\mathcal{N}(\mathfrak{U}) \leq (n!/n^n)(4/\pi)^s|\Delta|^{1/2} = M.$$

Now all we need to prove is that there are only finitely many integral ideals such that the norm is below the fixed bound M.

We can factor $\mathfrak{U}$ into powers of prime ideals: $\mathfrak{U} = \mathfrak{B}_1^{a_1}...\mathfrak{B}_t^{a_t}$, where $\mathfrak{B}_i$ are distinct prime ideals and a_i are positive integers. Now let $p_i\mathbb{Z} = \mathbb{Z} \cap \mathfrak{B}_i$, where p_i is a positive prime. Suppose $\mathcal{N}(\mathfrak{U}) = \prod_i p_i^{f_i a_i} \leq M$ where f_i is the relative degree of $\mathfrak{B}_i$ over $\mathbb{Z}$. Notice that there must be finitely many p_i, and each p_i is only divisible by finitely many $\mathfrak{B}_j$. Thus there exist only finitely many $\mathfrak{B}_i$.

It's also clear that there are only finitely many possible a_i (since each $p_i^{f_i a_i} \leq M$). Hence there are only finitely many $\mathfrak{U}$ such that $\mathcal{N}(\mathfrak{U}) \leq M$. Thus every class group is represented by only a finite number of ideals. Thus the class group of the ring of algebraic integers in an algebraic number field is finite. □

Acknowledgments. I would like to thank my mentors Aaron Marcus and Emily Norton for sharing their knowledge and their extensive patience. I greatly appreciate their help.

References

[1] Gerald J. Janusz Algebraic Number Fields, Second Edition American Mathematical Society, 1996
[2] Anthony W. Knapp Basic Algebra Birkhauser, 2006
[3] Ian Stewart Galois Theory, Third Edition Chapman and Hall/CRC, 2004