MAT 7410 (Advanced Algebra II)
The Class Number

Mohammad Behzad Kang

May 1, 2020

Abstract

This is an expository paper on the class number of a finite field extension of $\mathbb{Q}$, intended as a survey of work done on the class group and class number of a number field. We first develop some background to gain an understanding of what the class number is, then proceed to build tools to discuss computations of the class number, and, finally, we discuss work primarily done by Gauss on binary quadratic forms and the form class group to learn about the foundations of the class number.

1 Understanding What the Class Number Is

1.1 Background Technology

Definition 1.1.1. A *number field* (or *algebraic number field*) F is a finite field extension of $\mathbb{Q}$. As such, F may be viewed as a finite-dimensional vector space over $\mathbb{Q}$, with finite degree $[F:\mathbb{Q}]$ over $\mathbb{Q}$.

- If F has degree 2 over $\mathbb{Q}$, F is called a *quadratic field*. Examples of quadratic fields include $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$, where ω is a primitive cube root of unity, and $\mathbb{Q}(\sqrt{-5})$. Every quadratic field may be written in the form $\mathbb{Q}(\sqrt{d})$, where $d \neq 0, 1$ is a square-free integer. If $d < 0$, $\mathbb{Q}(\sqrt{d})$ is called an *imaginary quadratic field*, and if $d > 0$, $\mathbb{Q}(\sqrt{d})$ is called a *real quadratic field*.
- If F has degree 3 over $\mathbb{Q}$, F is called a *cubic field*. By the primitive element theorem, any cubic field may be written in the form $\mathbb{Q}(\alpha)$ for some $\alpha \in F$ such that the minimal polynomial of α over $\mathbb{Q}$ has degree 3. Examples of cubic fields include $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{5})$.
- If F is of the form $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity, F is called a *cyclotomic field*, and F has degree $\phi(n)$ over $\mathbb{Q}$.
- Most generally, if $f(x)$ is an irreducible polynomial of degree n over $\mathbb{Q}$, then $F = \mathbb{Q}[x]/(f(x))$ is a number field of degree n over $\mathbb{Q}$. By the primitive element theorem, F may be written in the form $\mathbb{Q}(\alpha)$ for some $\alpha \in F$ such that the minimal polynomial of α has degree n over $\mathbb{Q}$.

Our main focus will be on quadratic fields, but we will also include some results related to cubic and cyclotomic fields.

Definition 1.1.2. The *ring of integers* O_K of a number field K is the subring of K consisting of algebraic integers in K. That is, O_K is the set of elements $\alpha \in K$ such that α is a root of a monic polynomial in $\mathbb{Z}[x]$. As such, $\alpha \in K$ will belong to O_K if its minimal monic polynomial over $\mathbb{Q}$ is in $\mathbb{Z}[x]$. These elements are also called the *integral elements* of K over $\mathbb{Z}$, forming the *integral closure* of $\mathbb{Z}$ in K, which contains $\mathbb{Z}$ as a subring. O_K may be viewed as a finitely-generated $\mathbb{Z}$-module with an *integral basis* $b_1, b_2, ..., b_n \in O_K$ such that any element in O_K can be written as a linear combination of basis elements with coefficients in $\mathbb{Z}$.

When defining the class number of a number field, it will be necessary to think about certain ideals in this ring.

Proposition 1.1.3. The ring of integers of the quadratic field $K = \mathbb{Q}(\sqrt{d})$ is given by

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4 \end{cases}$$

, where $d \neq 0, 1$ is a square-free integer. (Theorem 3.4, [6])

We quickly note that it is not possible that $d \equiv 0 \pmod 4$, since this would violate d being square-free. Proving the above proposition amounts to first showing that O_K contains $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod 4$ (O_K contains $\mathbb{Z}$, contains $\frac{1+\sqrt{d}}{2}$ as it is a root of $f(x) = x^2 - x + \frac{1-d}{4}$, and O_K is a ring, so this follows), and contains $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod 4$ (which holds since O_K contains $\mathbb{Z}$, contains $\sqrt{d}$ as it is a root of $g(x) = x^2 - d$, and O_K is a ring). We simply show from here that there are no more integral elements of K over $\mathbb{Z}$, which uses no more technology than that of minimal polynomials and elementary modular arithmetic.

Remark 1.1.4. If ζ_n be a primitive n-th root of unity and $K = \mathbb{Q}(\zeta_n)$, $O_K = \mathbb{Z}[\zeta_n]$ [15]. One can also show that, if d is an integer that is not a perfect cube and K is the cubic field $\mathbb{Q}(\sqrt[3]{d})$, $O_K = \mathbb{Z}[\sqrt[3]{d}]$.

Definition 1.1.5. A *Dedekind domain* R is an integral domain such that R is Noetherian (that is, if we have ideals $I_1 \subseteq I_2 \subseteq \cdots I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$ of R, then there is some $n \in \mathbb{N}$ such that $I_n = I_{n+1}$), R is integrally closed in its field of fractions S (that is, R equals the integral closure of R in S), and every nonzero prime ideal of R is maximal.

- One can show that, if R is a Dedekind domain, then R is a unique factorization domain if and only if R is a principal ideal domain, because any UFD S is a PID if and only if every nonzero prime ideal of S is maximal [5].

The setting of Dedekind domains is of great importance for us, because if K is a number field, then O_K is a Dedekind domain (see Theorem 3.1.3 of [3]). Further, due to this, every ideal in O_K uniquely factors as a product of prime ideals (due to Theorems 12.2 and 12.3 of [12]).

Definition 1.1.6. If K is a number field, and $J \subseteq K$, J is a *fractional ideal* of O_K if $aJ = \{aj : j \in J\}$ is an ideal of O_K for some $a \in O_K$ such that $a \neq 0$. If aJ is a principal ideal of O_K, then J is *principal fractional ideal* of O_K. ([12], Definition 12.4)

We will see that it is these ideals of O_K that drive the definition of the class number of K.

If J is a (principal) fractional ideal of O_K, some authors may simply write that J is a (principal) fractional ideal of K. Further, any ideal of O_K is a fractional ideal.

1.2 The Class Number

With all of the machinery in Section 1.1, we are now ready to introduce the notion of the class group and corresponding class number.

Definition 1.2.1. The *class group* (often called the *ideal class group* to distinguish from the *form class group*, which we discuss in Section 3) of a number field K (or of O_K) is the quotient group Cl_K (or Cl_{O_K} or $Cl(K)$) given by $Cl_K = (\text{fractional ideals of } O_K)/(\text{principal fractional ideals of } O_K)$. The order of the class group is called the *class number* of K. ([12], Definition 12.9)

It is important to note that the class number of a number field K is always finite. Class numbers are typically studied in the context of a number field, which is our primary focus. However, one may consider the class number of a general Dedekind domain, and I'm told by Andrew Salch that there are a relatively small subset of mathematicians such as Frank Okoh that also study the class number of non-Dedekind domains.

Example 1.2.2. Suppose that the class number of a number field K is 1. Then, every fractional ideal of O_K is a principal fractional ideal of O_K. Since any ideal of O_K is a fractional ideal, it follows that every ideal of O_K is a principal ideal of O_K, and O_K is a principal ideal domain. This implies O_K is actually a unique factorization domain, since O_K is a Dedekind domain. This leads to an important statement : a number field K has class number 1 $\iff$ O_K is a PID $\iff$ O_K is a UFD.

Continuing with this train of thought, it turns out that the larger the class number of a number field K, the greater the failure of O_K to be a principal ideal domain, or, equivalently, a unique factorization domain. In this way, the importance of the class number of K lies in its ability to measure the failure of O_K to be a unique factorization domain.

Computations of the class group and class number for a number field K are frequently done using algebraic tools such as the Minkowski bound, the trace and norm of elements $\alpha \in K$, and the discriminant of K. In the next section, we introduce these tools and use them to handle some of these computations.

2 Calculating the Class Number

2.1 Computational Tools

A nice general reference for these computational tools is contained in Sections 3 and 4 of [10].

Proposition 2.1.1. If K is a number field with $[K : \mathbb{Q}] = n$, there are exactly n embeddings of K into $\mathbb{C}$.

Let's convince ourselves of this. By the primitive element theorem, $K = \mathbb{Q}[x]/(f) = \mathbb{Q}(\gamma)$ for some $\gamma \in K$ such that the minimal polynomial f of γ over $\mathbb{Q}$ has degree n. As an irreducible polynomial over $\mathbb{C}$, this minimal polynomial has n distinct roots in $\mathbb{C}$. Letting $\beta_1, \beta_2, ..., \beta_n$ be the roots of these roots, the n unique embeddings from K into $\mathbb{C}$ are given by $\sigma_i : \mathbb{Q}[x]/(f) \hookrightarrow \mathbb{C} : x \longmapsto \beta_i$, where $1 \leq i \leq n$. There are no more distinct embeddings than these n, since the image of x must be one of the β_i.
We will continue to denote the n distinct embeddings of a number field of degree n over $\mathbb{Q}$ into $\mathbb{C}$ by $\sigma_1, \sigma_2, ..., \sigma_n$. If $\alpha \in K$, $\sigma_1(\alpha), \sigma_2(\alpha), ..., \sigma_n(\alpha)$ are called the *conjugates* of α. σ is *real* if $\sigma(K) \subset \mathbb{R}$ and *complex* if $\sigma(K) \subset \mathbb{C}$.

If K is a number field with $[K : \mathbb{Q}] = n$, and $\alpha, \beta \in K$, one can consider the multiplication map $\alpha : K \longrightarrow K : \beta \longmapsto \alpha\beta$. The characteristic polynomial of this map is given by $P_\alpha(x) = \Pi_{i=1}^n (x - \sigma_i(\alpha))$, and it has coefficients lying in $\mathbb{Q}$. Recalling that the trace of a linear operator is the sum of its eigenvalues and the determinant of the operator is the product of the eigenvalues, this polynomial is precisely what gives rise to the following definition.

Definition 2.1.2. Let K be a number field, and let $\alpha \in K$. The *norm* of α is given by $N(\alpha) = N_{K/\mathbb{Q}}(\alpha) = \Pi_{i=1}^n \sigma_i(\alpha) \in \mathbb{Q}$, and the *trace* of α is given by $Tr(\alpha) = Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \in \mathbb{Q}$.

In particular, the trace is additive and the norm is multiplicative – that is, for $\alpha, \beta \in K$, $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$ and $N(\alpha\beta) = N(\alpha)N(\beta)$. The trace is also $\mathbb{Q}$-linear.

Definition 2.1.3. Let K be a number field such that $[K : \mathbb{Q}] = n$, with $b_1, b_2, ..., b_n$ an integral basis for O_K. Then the *discriminant* of K is given by

$$\Delta_K = \begin{vmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdot & \cdot & \cdot & \sigma_1(b_n) \\ \sigma_2(b_1) & \sigma_2(b_2) & \cdot & \cdot & \cdot & \sigma_2(b_n) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \sigma_n(b_1) & \sigma_n(b_2) & \cdot & \cdot & \cdot & \sigma_n(b_n) \end{vmatrix}^2 = \begin{vmatrix} Tr(b_1b_1) & Tr(b_1b_2) & \cdot & \cdot & \cdot & Tr(b_1b_n) \\ Tr(b_2b_1) & Tr(b_2b_2) & \cdot & \cdot & \cdot & Tr(b_2b_n) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ Tr(b_nb_1) & Tr(b_nb_2) & \cdot & \cdot & \cdot & Tr(b_nb_n) \end{vmatrix} \in \mathbb{Q}$$

Example 2.1.4.
(a) Let K be a quadratic field $\mathbb{Q}(\sqrt{d})$, and consider $\alpha = a+b\sqrt{d} \in K$. There are 2 distinct embeddings of K into $\mathbb{C}$, given by $\sigma_1(\alpha) = a+b\sqrt{d}$ and $\sigma_2(\alpha) = a-b\sqrt{d}$ (and, note that, if K is imaginary, both embeddings are complex, while if K is real, neither are complex). This gives $Tr(\alpha) = (a+b\sqrt{d}) + (a-b\sqrt{d}) = 2a$ and $N(a+b\sqrt{d}) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2$. If $d \equiv 1 \bmod 4$, an integral basis for O_K is given by $b_1 = 1, b_2 = \frac{1+\sqrt{d}}{2}$, and we get $\Delta_K = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d$. If $d \equiv 2,3 \pmod 4$, an integral basis for O_K is given by $b_1 = 1, b_2 = \sqrt{d}$, and we get $\Delta_K = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d$. Thus, we get a useful formula for the discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$, given by $\Delta_K = \begin{cases} 4d & d \equiv 2,3 \,(\mathrm{mod}\, 4) \\ d & d \equiv 1 \,(\mathrm{mod}\, 4) \end{cases}$.

(b) Let $K = \mathbb{Q}(\sqrt[3]{d}) = \mathbb{Q}(\theta)$ be a cubic field, where d is not a perfect cube, and consider $\alpha = a+b\theta+c\theta^2 \in K$. There are 3 distinct embeddings of K into $\mathbb{C}$, given by $\sigma_1(\alpha) = \alpha, \sigma_2(\alpha) = a+b\zeta_3\theta+c\zeta_3^2\theta^2$ and $\sigma_3(\alpha) = a+b\zeta_3^2\theta+c\zeta_3\theta^2$, where ζ_3 is a cube root of unity $\Rightarrow Tr(\alpha) = \sigma_1(\alpha)+\sigma_2(\alpha)+\sigma_3(\alpha) = 3a+b\theta(1+\zeta_3+\zeta_3^2)+c\theta^2(1+\zeta_3+\zeta_3^2) = 3a$, and $N(\alpha) = \sigma_1(\alpha)\cdot\sigma_2(\alpha)\cdot\sigma_3(\alpha) = a^3+2b^2+4c^3+6abc$. An integral basis for O_K is given by $b_1 = 1, b_2 = \sqrt[3]{d}$ and $b_3 = \sqrt[3]{d^2}$. Thus, we get $\Delta_K = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 3d \\ 0 & 3d & 0 \end{vmatrix} = -27d^2$.

(c) Let $K = \mathbb{Q}(\omega)$, where ω is a primitive 5-th root of unity. Since $[K:\mathbb{Q}] = \phi(5) = 4$, there are 4 distinct embeddings of K into $\mathbb{C}$, given by $\sigma_1 : \omega \longmapsto \omega$, $\sigma_2 : \omega \longmapsto \omega^2$, $\sigma_3 : \omega \longmapsto \omega^3$, and $\sigma_4 : \omega \longmapsto \omega^4$. Let $\alpha = a+b\omega+c\omega^2+d\omega^3+e\omega^4 \in K$. Then, $Tr(\alpha) = (a+b\omega+c\omega^2+d\omega^3+e\omega^4)+(a+b\omega^2+c\omega^4+d\omega+e\omega^3)+(a+b\omega^3+c\omega+d\omega^4+e\omega^2)+(a+b\omega^4+c\omega^3+d\omega^2+e\omega^1) = 4a+(b+c+d+e)(\omega+\omega^2+\omega^3+\omega^4) = 4a-(b+c+d+e)$. Calculating $N(\alpha) = \sigma_1(\alpha)\cdot\sigma_2(\alpha)\cdot\sigma_3(\alpha)\cdot\sigma_4(\alpha)$ is algebraically much more complicated. An integral basis for O_K is given by $b_1 = 1$, $b_2 = \omega$, $b_3 = \omega^2$, and $b_4 = \omega^3$. Thus, we get $\Delta_K = \begin{vmatrix} 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega \\ 1 & \omega^3 & \omega & \omega^4 \\ 1 & \omega^4 & \omega^3 & \omega^2 \end{vmatrix}^2 = 125$. In fact, if K is the number field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity ($n \geq 3$), this agrees with the formula for the discriminant of K, given by $\Delta_K = (-1)^{\phi(n)/2}\frac{n^{\phi(n)}}{\Pi_{p|n}p^{\phi(n)/(p-1)}}$.

The discriminant of a number field K is necessary to use a primary tool for computing the class number of K, the Minkowski bound.

Definition 2.1.5. Let K be a number field of degree n over $\mathbb{Q}$. Then, every ideal class in Cl_K contains an integral ideal in O_K of norm less than or equal to *Minkowski's constant* $M_K = \sqrt{|\Delta_K|}(\frac{4}{\pi})^{r_2}\frac{n!}{n^n}$, where r_2 is half of the number of complex field embeddings of K into $\mathbb{C}$. This is known as *Minkowski's bound*. As a consequence, Cl_K is generated by prime ideals of norm at most M_K.

The *norm* of an ideal $I \subseteq O_K$ above refers to its *absolute norm*, $N(I) = |O_K/I|$.

An important consequence of Minkowski's bound (which we mentioned earlier in this paper) is that, if K is a number field, as the number of integral ideals in O_K of a specified norm is finite, the class group of K must have finite order (see 5.3.6 of [3]).

We briefly note that the *Hurwitz constant* of a number field K serves as another upper bound to help compute the class number of K, and can be computed from an integral basis of K. However, the bound one achieves from Minkowski's constant is more accurate. Ireland-Rosen's bound is another less robust bound to assist with class number calculations.

Remark 2.1.6. Recall that if $K = \mathbb{Q}(\alpha)$ is a number field, K contains $\mathbb{Q}$ and O_K contains $\mathbb{Z}$. For a prime ideal $\mathfrak{p}$ of O_K, $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. That is, $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime number p, and we say that the prime $\mathfrak{p}$ of O_K *lies over* (p). More generally, prime ideals of an extension field lie over prime ideals of

the ground field. Thus, since prime ideals in $\mathbb{Q}$ are generated by prime numbers, to help determine prime ideals of O_K, we look to determine prime ideal factorizations in K.

For a given (p), we can often find the primes $\mathfrak{p}$ in O_K lying over (p) by factoring the minimal polynomial f of α over $\mathbb{Q}$ into irreducible factors mod p. The ideal $\mathfrak{p} =< p, h(\alpha) >$ in O_K lies over (p), then, if h is one of these irreducible factors. This correspondence between primes in O_K lying over (p) and irreducible factors of f modulo p is one consequence of theory developed by Dedekind. Even when this does not suffice, we may still find primes $\mathfrak{p}$ of O_K lying over (p) by finding prime ideals of O_K/pO_K and pulling these back to O_K [13].

Remark 2.1.7. If $\mathfrak{p}$ is prime in O_K, its *norm* $N(P)$ is $|O_K/\mathfrak{p}|$. The ideal $\mathfrak{p}O_K$ is the product of prime ideals with norm a power of p, and each power is determined by the ramification index of the corresponding prime ideal. Further, since every nonzero prime ideal of O_K factors as a product of prime ideals of O_K, one can show that the ideal $\mathfrak{p}$ in O_K is prime if it has norm p. Essentially, one can learn about the factorization of the ideal xO_K in the ring of integers of a number field K by looking at the factorization of the norm of x as an element of $\mathbb{Z}$.

A helpful consequence of this theory is that if a prime p *ramifies* in K (that is, $(p) = pO_K$ factors as a product of powers of prime ideals, and one of these powers is greater than 1), there is only one ideal of norm p in O_K. Dedekind's Theorem states that a rational prime number is ramified in K if and only if $p|\Delta_K$. If a prime p *splits* as a product of two distinct prime ideals, then there are exactly 2 ideals of norm p in O_K [13].

2.2 Examples

Example 2.2.1.
(a) Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. $n = 2$ and $r_2 = 2$, so Minkowski's bound gives $M_K = (2/\pi)\sqrt{|4d|}$ if $d \equiv 2, 3 \pmod 4$ and $M_K = (2/\pi)\sqrt{|d|}$ if $d \equiv 1 \pmod 4$. We now use this to compute the class number of K when $d = -1, -2, -3$ and -7. For $d = -1$ and $d = -2$, we have $M_K = 4/\pi \approx 1.27$ and $M_K = 4\sqrt{2}/\pi \approx 1.80$, respectively. For $d = -3$ and $d = -7$, we have $M_K = 2\sqrt{3}/\pi \approx 1.10$ and $M_K = 2\sqrt{7}/\pi \approx 1.68$, respectively. In all four cases, the Minkowski bound is less than 2 $\Rightarrow$ every ideal class in Cl_K must contain the trivial ideal (1), as this is the only ideal of norm 1 in O_K. Thus, there can only be one ideal class, and the class number of K is exactly 1. That is, Cl_K is trivial, and O_K is a UFD.

(b) Now, let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. $n = 2$ and $r_2 = 0$, so Minkowski's bound gives $M_K = \frac{\sqrt{|4d|}}{2}$ if $d \equiv 2, 3 \pmod 4$ and $M_K = \frac{\sqrt{|d|}}{2}$ if $d \equiv 1 \pmod 4$. We now use this to compute the class number of K when $d = 2, 3, 5$ and 13. For $d = 2$ and $d = 3$, we have $M_K = \sqrt{2}$ and $M_K = \sqrt{3}$, respectively. For $d = 5$ and $d = 13$, we have $M_K = \sqrt{5}/2 \approx 1.12$ and $M_K = \sqrt{13}/2 \approx 1.80$, respectively. Since the Minkowski bound is less than 2 for all four cases, we use the same argument as (a) to conclude that in every case, the class number of K is 1.

Example 2.2.2. Let $K = \mathbb{Q}(\zeta_5)$. Then $n = 4$, $r_2 = 2$ and $\Delta_K = 125$, so Minkowski's bound gives $M_K \approx 1.7$. Thus, by the same arguments in (a), K has class number 1.

An important takeaway from the last two examples is, if we get $M_K < 2$ for a number field K, we can conclude immediately that K has class number 1.

Example 2.2.3.
(a) Let $K = \mathbb{Q}(\sqrt{-5})$. $n = 2$, $r_2 = 2$, and $\Delta_K = -20$, so Minkowski's bound gives $M_K = (2/\pi)\sqrt{20} \approx 2.85$. By Dedekind's Theorem, 2 ramifies in K (which we can verify by observing that x^2+5 factors as $(x+1)^2$ mod 2, so that $(2) = 2O_K = (2, 1+\sqrt{-5})^2) \Rightarrow$ there is only one ideal of norm 2 in O_K, and the class number is at most 2. However, $O_K = \mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain, since $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, and the only units in O_K are 1 and -1 (that is, none of those 4 factors are *associates*). Thus, the class number of K cannot be 1 $\Rightarrow$ the class number of K is 2.

(b) Let $K = \mathbb{Q}(\sqrt{6})$. $n = 2$, $r_2 = 0$, and $\Delta_K = 24$, so Minkowski's bound gives $M_K = \sqrt{6} \approx 2.45$. By Dedekind's Theorem, 2 ramifies in K, and the rest of the argument proceeds as in (a), where $O_K = \mathbb{Z}[\sqrt{6}]$

is not a unique factorization domain since $-2 = (2+\sqrt{6})(2-\sqrt{6})$, and both factors are associates, because $(2+\sqrt{6})/(2-\sqrt{6}) = -5-2\sqrt{6}$, which is a unit. Thus, the class number of K here is also 2.

Example 2.2.4.
(a) Let $K = \mathbb{Q}(\sqrt{17})$. $n = 2$, $r_2 = 0$ and $\Delta_K = 17$, so Minkowski's bound gives $M_K = \frac{\sqrt{17}}{2} \approx 2.06$. By Dedekind's Theorem, 2 does not ramify in K – in fact, 2 splits as a product of two distinct prime ideals, and there are 2 ideals of norm 2 in O_K. However, these ideals are principal, since $-2 = [(3+\sqrt{17})/2][(3-\sqrt{17})/2]$. Thus, every ideal class contains a principal ideal, and the class number of K is 1.

(b) Let $K = \mathbb{Q}(\sqrt{14})$. $n = 2$, $r_2 = 0$ and $\Delta_K = 56$, so Minkowski's bound gives $M_K = \sqrt{14} \approx 3.74$. 3 remains prime, so there are no ideals of norm 3. 2 ramifies by Dedekind's Theorem, so there is only one ideal of norm 2 in O_K. But, this ideal is principal, since $2 = (4+\sqrt{14})(4-\sqrt{14})$. Thus, similar to (a), we get trivial class group, and the class number of K is 1.

Section 4.3.2 in [3] is helpful in addressing the different cases considered when factoring the ideal (p) in O_K for a quadratic field K. In the last example, case $c2$ was used for part (a), while cases $a2$ and b were used for part (b).

Example 2.2.5. Let $K = \mathbb{Q}(2^{1/3})$. $n = 3$, $r_2 = 1$ and $\Delta_K = -108$, so Minkowski's bound gives $M_K \approx 2.94$. Thus, every ideal in O_K is equivalent to one whose norm is at most 2 – that is, we only need to check the prime ideals of norm at most 2 in O_K, as each ideal class group contains such an ideal. The only ideal of norm 1 in O_K is the full ring of integers. Consider a prime ideal $\mathfrak{p}$ in O_K of norm 2, lying over an ideal (p) of $\mathbb{Z}$. In O_K, we have the factorization $2O_K = (2, 2^{1/3})^2 = (2^{1/3})^3$. Thus, the ideal class group of O_K is generated by (1) and $(2^{1/3})$, both principal. Therefore, the class number of K is 1.

Completing computations to find the class number of an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ partially addresses problems posed by Gauss in his work *Disquisitiones Arithmeticae* (1801). Gauss conjectured the following [1] :

- As d approaches $-\infty$, the class number of $\mathbb{Q}(\sqrt{d})$ tends to ∞.

  This was later proved by Heilbronn in 1934. In fact, it turns out that for a given class number, there are finitely many imaginary quadratic fields with that class number.

- For low class numbers, Gauss gave different lists of which imaginary quadratic fields have that class number, and conjectured this list to be complete.

  For class numbers $1, 2$ and 3, work of Baker, Stark, Heegner, and Oesterlé proved Gauss' lists to indeed be complete. Watkins solved the problem for class number up to 100 in 2004. For class number 1, Gauss' list was $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$, now known as the *Heegner numbers*. Providing such lists became known as the *class number problem*.

- There are infinitely many quadratic fields with class number 1.

  This is still an open problem. A list of real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ known to have class number 1 is complete up to $d = 100$, and [2] contains that list. The article contains similar results for cubic and cyclotomic fields. Further, [17] discusses a complicated formula, the *class number formula*, to compute the class number of a quadratic field along with related results.

Gauss formulated his work on the class number of quadratic fields in terms of binary quadratic forms, and defined a product for them. His work, largely included in *Disquisitiones Arithmeticae*, was clarified and successfully translated to have consequences related to ideal class groups of quadratic fields only later, after, for example, Kummer and Dedekind put in work to define ideals (see page 74 of [14], and the brief discussion on the next few pages as a supplement for what we study in Section 3). In fact, Gauss' work with binary quadratic forms motivated Kummer and Kronecker, inspired by Gauss' composition of classes of quadratic forms, to define number fields and ideal class groups in general. In the next section, we will take a closer look at the foundational work of Gauss and others on the class number in terms of the theory on these forms that they developed, and show its connection to the modern study of the class number of quadratic fields. A general reference for what we discuss in Section 3 is [7] (Sections 2A, 3A, 3D, and 7D, in particular).

3 Foundational Theory Using Quadratic Forms & Its Connection to the Class Group of Quadratic Fields

3.1 Relevant Theory of Quadratic Forms

The theory of quadratic forms we discuss was first introduced and studied by Gauss, but built upon by others such as Lagrange, Dedekind and Dirichlet.

Definition 3.1.1. A *binary quadratic form* is a polynomial $q(x,y) = ax^2 + bxy + cy^2$ in two variables x and y, with coefficients a, b and c and *discriminant* $\Delta = b^2 - 4ac$ (and, it follows that $\Delta \equiv 0 \pmod 4$ or $\Delta \equiv 1 \pmod 4$). When $a, b, c \in \mathbb{Z}$, $q(x,y)$ is known as an *integral binary quadratic form* (often simply called a binary quadratic form, which is the convention we will use). We denote the space of binary quadratic forms of discriminant Δ by F_Δ.

If $\Delta \neq 0$, $q(x,y)$ is called *nondegenerate*; otherwise, $q(x,y)$ is *degenerate*. $q(x,y)$ is *primitive* if $gcd(a,b,c)$, also known as the *content* of the form, is equal to 1. A binary quadratic form is *definite* if $\Delta < 0$, *positive definite* if $\Delta < 0$ and $a > 0$, and *indefinite* if $\Delta > 0$. When $\Delta < 0$, we may call $q(x,y)$ an imaginary quadratic form, and if $\Delta > 0$, $q(x,y)$ is called a *real quadratic form*. If $q(x,y)$ is a (positive) definite binary quadratic form, we say it is *reduced* if $|b| \leq a \leq c$ and $b \geq 0$ if $a = c$ or $a = |b|$. If $q(x,y)$ is an indefinite form, it is reduced if $|\sqrt{\Delta} - 2|c|| < b < \sqrt{\Delta}$.

Two binary quadratic forms $q(x,y)$ and $q'(x,y)$ are *equivalent*, or *properly equivalent* (and, we may write $q(x,y) \sim q'(x,y)$) , if $q'(x,y) = q(\alpha x + \beta y, \gamma x + \delta y)$ and the integer matrix $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ has determinant 1 (i.e., $A \in SL_2(\mathbb{Z})$). $q(x,y)$ and $q'(x,y)$ are *improperly equivalent* if $q'(x,y) = q(\alpha x + \beta y, \gamma x + \delta y)$ and A has determinant ± 1 (as was considered by Lagrange). If $q(x,y)$ and $q'(x,y)$ are equivalent, they have the same discriminant Δ; however, there are inequivalent forms that have equal discriminants (a brief discussion of much of this is covered in [11]).

In their treatment of the theory of binary quadratic forms that leads to the ideal class group of quadratic fields, many authors restrict their attention to positive definite forms, for simplicity. Further, when working with binary quadratic forms, attention is often restricted to primitive forms, because every form is a multiple of a primitive one. Lastly, there is a notion of equivalence of binary quadratic forms under an action of $GL_2(\mathbb{Z})$, and since $SL_2(\mathbb{Z})$ is a subgroup of $GL_2(\mathbb{Z})$, this action restricts to the action of $SL_2(\mathbb{Z})$ on binary quadratic forms described above (see Section 1.2 of [16]).

The proper equivalence $\sim$ defined in the above definition indeed defines an equivalence relation on the set of binary quadratic forms :
(i) $q(x,y) = q(1x + 0y, 0x + 1y) \Rightarrow q(x,y) \sim q(x,y)$,
(ii) $q(x,y) \sim q'(x,y) \Rightarrow q'(x,y) = q(\alpha x + \beta y, \gamma x + \delta y)$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1 \Rightarrow$ $q(x,y) = q'(\delta x - \beta y, -\gamma x + \alpha y) \Rightarrow q'(x,y) \sim q(x,y)$, and
(iii) $q(x,y) \sim q'(x,y)$, $q'(x,y) \sim q''(x,y)$ for binary quadratic forms $q(x,y), q'(x,y), q''(x,y) \Rightarrow$ $q'(x,y) = q(\alpha_1 x + \beta_1 y, \gamma_1 x + \delta_1 y)$ and $q''(x,y) = q'(\alpha_2 x + \beta_2 y, \gamma_2 x + \delta_2 y)$ for some $\alpha_i, \gamma_i, \beta_i, \delta_i \in \mathbb{Z}$ $(i = 1, 2)$ such that $\alpha_1\delta_1 - \beta_1\gamma_1 = \alpha_2\delta_2 - \beta_2\gamma_2 = 1 \Rightarrow$
$q''(x,y) = q((\alpha_1\alpha_2 + \beta_1\gamma_2)x + (\alpha_1\beta_2 + \beta_1\gamma_2)y, (\gamma_1\alpha_2 + \delta_1\gamma_2)x + (\gamma_1\beta_2 + \delta_1\delta_2)y) \Rightarrow q(x,y) \sim q''(x,y)$.

We may form a factor set of the relation $\sim$ consisting of the collection of proper equivalence classes of binary quadratic forms defined by $\sim$. In particular, as was considered by Gauss, we may study the set of proper equivalence classes of binary quadratic forms under $\sim$ with a fixed discriminant, $Cl(\Delta) = F_\Delta / \sim$.

Brahmagupta's composition law states that, given two numbers $a^2 + nb^2$ and $c^2 + nd^2$, we have $(a^2 + nb^2)(c^2 + nd^2) = (ac - nbd)^2 + n(ad + bc)^2 = X^2 + nY^2$ (where $X = ac - nbd, Y = ad + bc$), i.e., that the set of numbers of the form $a^2 + nb^2$ are closed under multiplication. Gauss, restricting his attention to primitive binary quadratic forms, took inspiration from this in defining a composition $q_1(x_1, y_1) \circ q_2(x_2, y_2)$ of two binary quadratic forms q_1 and q_2 of discriminant Δ to produce a form $q_3(x,y)$ with the same discriminant, where x, y are quadratic expressions in x_1, y_1, x_2, y_2. The especially remarkable property of this composition is that it gives $Cl(\Delta)$ the structure of a finite abelian group. With this, we may now formally define the form class group (see Sections 4.2 and 4.3 of [11]).

Definition 3.1.2. The set of proper equivalence classes of binary quadratic forms with discriminant Δ under composition of forms $Cl(\Delta) = F_\Delta/\sim$ is called the *form class group* of discriminant Δ. The form class group is a finite abelian group, with order the *class number* $|Cl(\Delta)| = h(\Delta)$ of discriminant Δ.

It is worth briefly commenting on the group structure of $Cl(\Delta)$. Gauss provided a simple *reduction algorithm* that, given a binary quadratic form $q(x, y)$, produced a properly equivalent reduced binary quadratic form $q'(x, y)$ in a finite number of steps. Using Gauss' algorithm, one can show that, if $q(x, y)$ has negative discriminant, $q(x, y)$ is properly equivalent to a unique reduced binary quadratic form (and, with this, we can construct a canonical representative of each equivalence class of $Cl(\Delta)$), and there is a *cycle* of reduced binary quadratic forms such that each element of a proper equivalence class of binary quadratic forms of positive discriminant is equivalent to one of the forms in this cycle [9]. Further, the identity element of $Cl(\Delta)$ is the *principal class* of discriminant Δ, the proper equivalence class of the *principal form*. If $\Delta \equiv 0 \pmod 4$, the principal form is given by $x^2 - \frac{\Delta}{4}y^2$, and if $\Delta \equiv 1 \pmod 4$, the principal form is given by $x^2 - xy + \frac{1-\Delta}{4}$ (see Definition 2.7 of [8]). The inverse of the binary quadratic form $q_1(x, y) = ax^2 + bxy + cy^2$ is given by $q_2(x, y) = ax^2 - bxy + cy^2$. Finiteness of $|Cl(\Delta)| = h(\Delta)$ was due to a result of Lagrange, although Gauss' work sufficed to see this.

Example 3.1.3.
(i) There is only 1 proper equivalence class in $Cl(-8)$, with the reduced binary quadratic form representative $x^2 + 2y^2$. Thus, $h(-8) = 1$.

(ii) Consider the form class group of discriminant -20. There are 2 distinct proper equivalence classes in $Cl(-20)$ with reduced binary quadratic form representatives $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. Thus, $h(-20) = 2$.

(iii) Consider the form class group of discriminant -56. There are 4 distinct proper equivalence classes in $Cl(-56)$ with reduced binary quadratic form representatives $q_1 = x^2 + 14y^2$, $q_2 = 2x^2 + 7y^2$, $q_3 = 3x^2 + 2xy + 5y^2$, and $q_4 = 3x^2 - 2xy + 5y^2$. Thus, $h(-56) = 4$. Further, using Gauss' method for composing quadratic forms, one can verify the identities $q_3 \circ q_3 \sim q_4 \circ q_4 \sim q_2$, and conclude that $Cl(-56)$ is isomorphic to the cyclic group of order 4 (Example 4.4.6 and Exercise 4.15 of [11]).

In light of the above example, let us revisit the ideal class group of a quadratic field $\mathbb{Q}(\sqrt{d})$ from the first two sections of this paper for a moment. $\mathbb{Q}(\sqrt{-8}) = \mathbb{Q}(\sqrt{-2})$ has class number 1, as shown in example 2.2.1. $\mathbb{Q}(\sqrt{-20}) = \mathbb{Q}(\sqrt{-5})$ has class number 2, as shown in Example 2.2.3. One can also show that $\mathbb{Q}(\sqrt{-56}) = \mathbb{Q}(\sqrt{-14})$ has class group isomorphic to C_4, and thus, has class number 4. It is no coincidence that, in all of these cases, the class number of $K = \mathbb{Q}(\sqrt{d})$ occurring as the order of the ideal class group of K agrees with the class number $h(\Delta)$ of the form class group of discriminant Δ, the discriminant of K, as we will see in Section 3.2.

3.2 Connection to Class Groups of Quadratic Fields

Definition 3.2.1. Let K be a number field. An element a of K is *totally positive* if $\sigma(a) > 0$ for any real embedding σ of K into $\mathbb{R}$. A *totally positive principal fractional ideal* of O_K, then, is an ideal in O_K of the form $(a) = aO_K$. The *narrow class group* of K is the quotient group $C_K^+ = I_K/P_K^+$, where I_K is the group of fractional ideals of O_K and P_K^+ is the group of totally positive principal fractional ideals of O_K. $|C_K^+|$ is the *narrow class number* of K.

Let K be a quadratic number field $\mathbb{Q}(\sqrt{d})$. We note that if $d < 0$, there are no real embeddings σ of K into $\mathbb{R}$, so every element of K is totally positive (that is, totally positive principal fractional ideals of O_K coincide with principal fractional ideals of O_K, and we see that C_K^+ is just the ideal class group of K), and if $d > 0$, we need $\sigma_1(\lambda), \sigma_2(\lambda) > 0$ in order for $\lambda = a + b\sqrt{d} \in K$ to be totally positive, where $\sigma_1 : K \longrightarrow \mathbb{R} : a + b\sqrt{d} \longmapsto a + b\sqrt{d}$ and $\sigma_2 : K \longrightarrow \mathbb{R} : a + b\sqrt{d} \longmapsto a - b\sqrt{d}$ [4].

Theorem 3.2.2. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with discriminant Δ. Then $Cl(\Delta)$ is isomorphic to the narrow class group of K.

We note that, if $d < 0$, one can simply say that $Cl(\Delta)$ is isomorphic to the ideal class group of K, following our note of the fact that the ideal class group of K is equal to the narrow class group of K in this case. Thus, the narrow class number of K coincides with the class number of K if $d < 0$. However, if $d > 0$, the ideal class group of K may be half the size of the narrow class group of K (as is the case with $\mathbb{Q}(\sqrt{3})$, which has class number 1 but narrow class number 2).

The above Theorem is at the heart of the connection between the form class group that we've discussed in this section and the ideal class group of a quadratic number field K discussed in Sections 1 and 2. It is significant in translating Gauss' work on binary quadratic forms and his construction of the form class group of a specified discriminant to the more modern notions of the ideal class group and class number of a quadratic field K that measures the failure of O_K to be a unique factorization domain.

Amazingly, Gauss' work went far beyond defining a proper equivalence of binary quadratic forms to construct the form class group. He also built a looser notion of equivalence on forms to construct a *genus* of forms [11]. This concept is out of the scope of this paper, but I'm certainly interested in continuing to read up on this idea.

References

[1] *Class Number Problem*. https://en.wikipedia.org/wiki/Class_number_problem.

[2] *List of Number Fields with Class Number One*. https://en.wikipedia.org/wiki/List_of_number_fields_with_class_number_one.

[3] Robert Ash. *A Course in Algebraic Number Theory*. Dover Publications, 2010.

[4] Steven Charlton. *Quadratic Forms and Quadratic Number Fields*. http://guests.mpim-bonn.mpg.de/spc/teaching/primes_17/handout2_quadratic_field.pdf.

[5] Brian Conrad. *Dedekind Domains*. http://math.stanford.edu/~conrad/210BPage/handouts/math210b-dedekind-domains.pdf.

[6] Keith Conrad. *Factoring in Quadratic Fields*. https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf.

[7] David Cox. *Primes of the Form $x^2 + ny^2$*. Wiley-Interscience, 1989.

[8] Daniel E. Flath. *Introduction to Number Theory*. Wiley, 1989.

[9] Andrew Granville. *Binary Quadratic Forms*. https://dms.umontreal.ca/~andrew/Courses/Chapter4.pdf.

[10] Minhyong Kim. *Math 3704 Lecture Notes*. https://www.ucl.ac.uk/~ucahmki/ant/3704notes.pdf.

[11] Kimball Martin. *Binary Quadratic Forms*. http://www2.math.ou.edu/~kmartin/ntii/chap4.pdf.

[12] Kimball Martin. *Prime Ideals*. http://www2.math.ou.edu/~kmartin/nti/chap12.pdf.

[13] Kimball Martin. *Primes in Extensions*. http://www2.math.ou.edu/~kmartin/ntii/chap2.pdf.

[14] James S. Milne. Algebraic number theory (v3.01), 2008. Available at www.jmilne.org/math/.

[15] Nicholas Phat Nguyen. *A Note on Cyclotomic Integers*. https://arxiv.org/ftp/arxiv/papers/1706/1706.05390.pdf.

[16] Corentin Perret-Gentil. *The Correspondence Between Binary Quadratic Forms and Quadratic Fields*. Master's thesis, 2012. https://corentinperretgentil.gitlab.io/static/documents/correspondence-bqf-qf.pdf.

[17] Roy Zhao. *The Class Number Formula for Quadratic Fields and Related Results*, 2016. https://people.math.ethz.ch/~pink/Theses/2016-Junior-Paper-Roy-Zhao.pdf.