April 24, 2014

THE IDEAL CLASS GROUP

AMREI OSWALD
ABSTRACT ALGEBRA, SPRING 2014

Abstract

When we form a finite algebraic extension of $\mathbb{Q}$, we are not guaranteed that the ring of integers, $\mathfrak{O}$, in our extension will be a unique factorization domain (UFD). We can obtain a measure of how far $\mathfrak{O}$ is from being a UFD by computing the class number which is defined as the order of the ideal class group. This paper describes the ideal class group and provides examples of how to compute this group. First, necessary terms are defined, such as norms of elements in a field extension and the ring of integers of a field. Then, we introduce the concept of fractional ideals and exploit the properties of Dedekind domains to show that the non-zero fractional ideals of a Dedekind domain form a group. This leads to a definition of the ideal class group and a proof of its finiteness. We then make these concepts more concrete by computing ideal class groups of quadratic field extensions. We finish by discussing the problem of computing discriminants given a class number.

1. Background

Algebraic number fields are finite extensions of $\mathbb{Q}$. In this paper, we will be dealing exclusively with algebraic number fields, and when we refer to a field, typically denoted k, it is assumed to be an algebraic number field.

Since k is a finite extension of $\mathbb{Q}$, there exists an $n \in \mathbb{Z}$ such that $[k : \mathbb{Q}] = n$. Say $B = \{1 = \alpha_1, \alpha_2, ..., \alpha_n\}$ where the α_i's for $i \neq 1$ are the elements adjoined to $\mathbb{Q}$ to form k. Then every element $a \in k$ can be written as a linear combination of elements in B. We can define a map $m_a : k \to k$ where for $b \in k$, $m_a(b) = a \cdot b$. Since $a \cdot b$ is some element in k, it can be written as a linear combination of α_i's.

We consider the action of m_a on the elements of B, specifically $m_a(\alpha_i) = c_{i,0}\alpha_1 + c_{i,1}\alpha_2, ..., c_{i,n}\alpha_n$. We can form the $n \times n$ matrix M_a where

$$M_a = \begin{bmatrix} c_{1,1} & c_{1,2} & ... & c_{1,n} \\ c_{2,1} & c_{2,2} & ... & c_{2,n} \\ \vdots & \vdots & & \vdots \\ c_{n,1} & c_{n,2} & ... & c_{n,n} \end{bmatrix}.$$

Definition Say $a \in k$ and M_a is defined as above. Then the norm of a is $\mathrm{N}(a) = \det(M_a)$, and the trace of a is $\mathrm{Tr}(a) = \mathrm{Tr}(M_a)$.

Note that both $\mathrm{N}(a)$ and $\mathrm{Tr}(a)$ are elements in $\mathbb{Q}$. The norm is multiplicative. In other words, if $a, b \in k$, then $\mathrm{N}(a) \cdot \mathrm{N}(b) = \mathrm{N}(ab)$. The trace is additive, $\mathrm{Tr}(a) + \mathrm{Tr}(b) = \mathrm{Tr}(a + b)$.

Every field has a ring of integers, typically denoted $\mathfrak{O}$.

Definition The ring of integers of a field k is the set

$$\mathfrak{O} = \{\alpha \in k \mid \mathrm{N}(\alpha) \in \mathbb{Z} \text{ and } \mathrm{Tr}(\alpha) \in \mathbb{Z}\}.$$

Much like $\mathbb{Z}$ forms a discrete lattice within $\mathbb{Q}$, the ring of integers of a field $\mathfrak{O}$ forms a discrete lattice in k. We will find it useful to think of $\mathfrak{O}$ this way.

Definition Let V be $\mathbb{R}^n$ or $\mathbb{Q}^n$ and let k be $\mathbb{R}$ or $\mathbb{Q}$ respectively. A lattice Λ in V is an additive subgroup of V with elements of the form $a_1v_1 + a_2v_2 + ... + a_nv_n$ where the a_i's $\in \mathbb{Z}$, the v_i's are linearly independent vectors in V, and Λ spans V as a k-vector space.

Intuitively, a lattice can be thought of as a collection of discrete, uniformly spaced points that cover the entire $\mathbb{Q}^n$ plane. For example, $\mathbb{Z}^2$ is a lattice in $\mathbb{Q}^2$. We can identify any k of degree n with $\mathbb{Q}^n$ since any element in k can be represented as a vector with coefficients in $\mathbb{Q}$. Then, the ring of integers of k, $\mathfrak{O}$, is a lattice in k. We would like to have some measure of the size of this lattice in k. This is called the volume of Λ, and we will define it below.

A field k has n embeddings into $\mathbb{C}$. Of these n embeddings, there are r_1 into $\mathbb{R}$ and there are r_2 complex conjugate pairs of embeddings into $\mathbb{C} \setminus \mathbb{R}$. Hence, $n = r_1 + 2r_2$. We denote the ith of the n embeddings by σ_i. The ring of integers $\mathfrak{O}$ of a field k can be finitely generated as linear combinations of a basis $\beta_1, \beta_2, ...\beta_n \in \mathfrak{O}$ with coefficients in $\mathbb{Q}$. We build the $n \times n$ matrix, M_k, as follows:

$$M_k = \begin{bmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & ... & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & ... & \sigma_2(\beta_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta_1) & \sigma_n(\beta_2) & ... & \sigma_n(\beta_n) \end{bmatrix}.$$

Definition The *volume* of $\mathfrak{O}$ in k is $\mathrm{Vol}(\mathfrak{O}/k) = 2^{-r_2}\det(M_k)$. The factor of 2^{-r_2} is to account for the double counting of complex conjugate embeddings.

Definition We denote the *discriminant* of the field k by Δ_k where $\Delta_k = \det(M_k)^2$.

However, while the above definition of the discriminant is very useful for more theoretical arguments that depend on r_1 and r_2, it does not allow for particularly straightforward computation. The matrix N_k given below is what is typically used to compute the discriminant of a field:

$$N_k = \begin{bmatrix} \mathrm{Tr}(\beta_1\beta_1) & \mathrm{Tr}(\beta_1\beta_2) & ... & \mathrm{Tr}(\beta_1\beta_n) \\ \mathrm{Tr}(\beta_2\beta_1) & \mathrm{Tr}(\beta_2\beta_n) & ... & \mathrm{Tr}(\beta_2\beta_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}(\beta_n\beta_1) & \mathrm{Tr}(\beta_n\beta_2) & ... & \mathrm{Tr}(\beta_n\beta_n) \end{bmatrix}.$$

Here, $\mathrm{Tr}(\beta_i\beta_j) = \mathrm{Tr}(M_{\beta_i\beta_j})$, $i, j = 1, ..., n$. Then, we have $\Delta_k = \det(N_k)$.

Unlike in $\mathbb{Z}$, we are not guaranteed unique factorization in $\mathfrak{O}$. However, we can make some statements about the behavior of ideals in $\mathfrak{O}$. We will do this in the next section. For now, we will introduce some necessary terms.

Definition Let $R_1 \subset R_2$ be commutative rings with identity and $\alpha \in R_2$. Then, R_1 is *integrally closed* in R_2 if the existence of an $f(x) \in R_1[x]$ such that $f(\alpha) = 0$ implies that $\alpha \in R_1$.

Factorization of elements in a ring is guaranteed by the *ascending chain condition* which states that every strictly ascending chain of ideals is finite. In other words, if we have ideals I_i such that $I_1 \subset I_2 \subset I_3 \subset ...$, where each inclusion is a proper inclusion, then there exists a finite m such that I_{m+1} cannot exist because it would simply be a repetition of I_m.

Definition A ring R is *Noetherian* if every ideal is finitely generated. Equivalently, R satisfies the ascending chain condition.

Definition An integral domain $\mathfrak{o}$ with identity is a *Dedekind domain* if it satisfies the following:

- $\mathfrak{o}$ is Noetherian.
- $\mathfrak{o}$ is integrally closed in its field of fractions.
- Eery non-zero prime ideal of $\mathfrak{o}$ is maximal.

The ring of integers $\mathfrak{O}$ of any algebraic number field k is a Dedekind domain. So, properties of Dedekind domains are very important for studying algebraic number fields.

2. Integral and Fractional Ideals

For the entirety of this section let $\mathfrak{o}$ be a Dedekind domain and k its field of fractions. If I and J are two ideals of $\mathfrak{o}$, their product is defined as follows

$$IJ = \left\{ \sum_{i,j} x_i y_j | x_i \in I, y_j \in J \right\}.$$

We know that this product is also an ideal. Since multiplication in $\mathfrak{o}$ is commutative, we can simply swap the order of multiplication of x_i and y_j in the sum above to give an equivalent JI. Therefore, ideal multiplication is commutative. Due to the absorption property of ideals, $\mathfrak{o}$ acts an identity element. Any element of an ideal I multiplied by anything in $\mathfrak{o}$ gives us another element of I.

We say that an ideal I divides another ideal J if $J \subset I$. An ideal P is prime if and only if $P|IJ$ implies that $P|I$ or $P|J$. Additionally, any element $p \in \mathfrak{o}$ is prime if and only if $p\mathfrak{o}$ is a prime ideal.

Definition The norm of an ideal I of $\mathfrak{o}$ is its index, $\mathrm{N}(I) = [\mathfrak{o} : I]$.

A *fractional ideal* $\mathfrak{I}$ has the form $\frac{\beta}{\gamma} I$ for some ideal $I \in \mathfrak{o}$ and $\frac{\beta}{\gamma} \in k$. Then, $\gamma\mathfrak{I} \subset \mathfrak{o}$ is an ideal. We refer to γ as the denominator of $\mathfrak{I}$. Note that fractional ideals are not necessarily ring ideals. In fact, $\mathfrak{I}$ is a ring ideal only if $\frac{\beta}{\gamma} \in \mathfrak{o}$. We will refer to ring ideals as integral ideals when it is necessary to distinguish between the two.

Definition Any fractional ideal $\mathfrak{I}$ can be written as αI for some $\alpha \in k$ and an integral ideal I of $\mathfrak{o}$. Then, the norm of $\mathfrak{I}$ is given by $\mathrm{N}(\mathfrak{I}) = \mathrm{N}(\alpha I) = \mathrm{N}(\alpha) \cdot \mathrm{N}(I)$.

If $\mathfrak{I}$ and $\mathfrak{J}$ are two fractional ideals with denominators γ_i and γ_j respectively, then we can define the product of $\mathfrak{I}$ and $\mathfrak{J}$ as follows

$$\mathfrak{I} \cdot \mathfrak{J} = \frac{1}{\gamma_i \gamma_j} (\gamma_i \mathfrak{I}) \cdot (\gamma_j \mathfrak{J}).$$

Note that both $\gamma_i\mathfrak{I}$ and $\gamma_j\mathfrak{J}$ are integral ideals, so they are multiplied as described at the beginning of this section.

The following lemmas will very useful in proving that the non-zero fractional ideals of a Dedekind domain form a multiplicative abelian group.

Lemma 2.1. *If I is a non-zero ideal of $\mathfrak{o}$, then $P_1P_2...P_m \subset I$ where the P_i's are prime ideals.*

Proof. We proceed by contradiction. Say the assertion is false. Then, there exist ideals in $\mathfrak{o}$ that do not contain a product of prime ideals. Because $\mathfrak{o}$ is Noetherian, we can choose a maximal I among the ideals that lack this property. Note that I cannot be prime because then it would satisfy the assertion. So, we can choose $\beta_1, \beta_2 \in \mathfrak{o}$ but not in I such that $\beta_1\beta_2 \in I$. Set $J_1 =< I, \beta_1 >$ and

$J_2 =< I, \beta_2 >$. Then, both J_1 and J_2 strictly contain I. By the maximality of I, J_1 and J_2 both contain a product of prime ideals. However, notice that elements in $J_1 \cdot J_2$ have the form

$$\sum_{i,j}(a_i + b_i\beta_1)(a_j + b_j\beta_2) = \sum_{i,j} a_i a_j + a_i b_j \beta_2 + a_j b_i \beta_1 + b_i b_j \beta_1 \beta_2,$$

where the a_i's and a_j's are in I and the b_i's and b_j's are in $\mathfrak{o}$. Note that each term above must be in I by the absorption property of ideals. Therefore, $J_1 \cdot J_2 \subset I$, which means that I contains the products of prime ideals contained in J_1 and J_2. This is a contradiction, and thus, every nonzero ideal in $\mathfrak{o}$ contains a product of prime ideals. □

Lemma 2.2. *Every non-zero prime ideal P of $\mathfrak{o}$ is invertible.*

Proof. Let $P^- = \{\alpha \in k | \alpha P \subset \mathfrak{o}\}$. Choose $\beta \neq 0 \in P$. Then, $\beta P^- \subset \mathfrak{o}$ is an integral ideal and therefore, P^- is a fractional ideal. Since $\mathfrak{o} \subset P^-$, we have that $P \subset P^- P \subset \mathfrak{o}$. Since $\mathfrak{o}$ is a Dedekind domain, P is maximal, and one of these inclusions must be an equality. Say that $\mathfrak{o} = P^- P$, then P^- is the inverse of P and we are done.

Say that $P^- P = P$. Choose the minimal m such that there exists a product

$$P_1 P_2 ... P_m \subset < \beta > \subset P$$

where β is as defined previously. One of the P_i's must be in P. Otherwise, we could choose an α_i for each P_i such that α_i is not in P, and then $\prod_i \alpha_i$ would not be in P. Say that P_1 is the prime ideal contained in P, then by the maximality of P_1, $P_1 = P$.

By the minimality of m, $P_2 P_3 ... P_m \not\subset < \beta >$, and there must be a $\gamma \in P_2 P_3 ... P_m$ that is not in $< \beta >$. Note that $\gamma P = \gamma P_1 \subset P_1 P_2 ... P_m \subset < \beta >$. Set $\delta = \frac{\gamma}{\beta}$. Then δ cannot be contained in $\mathfrak{o}$, because if $\beta | \gamma$ then γ would have to be contained in $< \beta >$ which contradicts its definition. However, it is true that

$$\delta P = \frac{\gamma}{\beta} P \subset \frac{\gamma}{\beta} < \beta >= \gamma \mathfrak{o},$$

which means that $\delta \in P^-$ and so $\delta P \subset P^- P = P$. Therefore, there exists elements $a, b \in P$ such that $\delta a = b$, and $\delta a - b = 0$. Since $a, b \in \mathfrak{o}$ and $\mathfrak{o}$ is Dedekind, and thus integrally closed in k, this implies that $\delta \in \mathfrak{o}$ which is a contradiction.

Hence, it cannot be true that $P^- P = P$, and $P^- P = \mathfrak{o}$ for every prime P. □

We would like to extend the existence of inverses from prime ideals to all non-zero integral ideals. We can do this using lemma 2.2.

Lemma 2.3. *Every non-zero integral ideal of $\mathfrak{o}$ is invertible.*

Proof. If the statement is not true, then there must be a maximal non-invertible ideal I. If we consider the set of ideals containing I, there must be a maximal ideal among them call it P. Since P is maximal, it must be a prime ideal. Thus, by lemma 2.2, there exists an inverse of P, denote it P^{-1}.

Notice that $IP \subset I \subset P$. Multiplying every term in this chain of inclusions by P^{-1} gives us $I \subset IP^{-1} \subset \mathfrak{o}$. Assume for the purpose of contradiction that the inclusion on the left were equality. In other words, $I = IP^{-1}$. This would imply that $IP^{-1} \subset \mathfrak{o}$, Then, for any $\beta \in P^{-1}$, there exists $\alpha \in I$ and $\gamma \in \mathfrak{o}$ such that $\alpha\beta = \gamma$. This implies that $\alpha\beta - \gamma = 0$, and because $\mathfrak{o}$ is integrally closed in k, this means $\beta \in \mathfrak{o}$. Therefore, $P^{-1} \subset \mathfrak{o}$ and multiplying by P on both sides of this inclusion gives us

$$P^{-1}P = \mathfrak{o} \subset \mathfrak{o}P = P,$$

which cannot be true since P is a maximal ideal in $\mathfrak{o}$. Thus, $I \neq P^{-1}I$.

Since the inclusion $I \subset IP^{-1}$ is proper, IP^{-1} must have an inverse by the maximality of I, denote it J. Then, $IP^{-1}J = \mathfrak{o}$ and $P^{-1}J$ is an inverse for I.

□

We will denote the inverse of any ideal I by I^{-1}. Now that we have inverses for any integral ideal, it is not too difficult to extend this to inverses of fractional ideals. This means we have all the tools necessary to prove that the fractional ideals of a Dedekind domain form a group.

Theorem 2.4. *The non-zero fractional ideals of a Dedekind domain form an abelian group under multiplication.*

Proof. Closure and commutativity come directly from the closure and commutativity of multiplication in a field and ideal multiplication. Note that if $\mathcal{I}$ and $\mathcal{J}$ are two fractional ideals with denominators γ_i and γ_j respectively, then

$$\mathcal{I} \cdot \mathcal{J} = \frac{1}{\gamma_i \gamma_j}(\gamma_i \mathcal{I}) \cdot (\gamma_j \mathcal{J}) = \frac{1}{\gamma_j \gamma_i}(\gamma_j \mathcal{J}) \cdot (\gamma_i \mathcal{I}) = \mathcal{J} \cdot \mathcal{I}$$

and so we have commutativity. Associativity can be shown in a similar manner.

Notice that

$$\gamma_i \gamma_j \frac{1}{\gamma_i \gamma_j}(\gamma_i \mathcal{I}) \cdot (\gamma_j \mathcal{J}) = (\gamma_i \mathcal{I}) \cdot (\gamma_j \mathcal{J}),$$

where $(\gamma_i \mathcal{I}) \cdot (\gamma_j \mathcal{J})$ is an integral ideal. Therefore, $\gamma_i \gamma_j$ is the denominator of $\mathcal{I} \cdot \mathcal{J}$ and $\mathcal{I} \cdot \mathcal{J}$ is also a fractional ideal, and we have closure. As in integral ideal multiplication, the identity element is $\mathfrak{o}$, since

$$\mathcal{I} \cdot \mathfrak{o} = \frac{1}{\gamma_i}(\gamma_i \mathcal{I}) \cdot \mathfrak{o} = \frac{1}{\gamma_i}(\gamma_i \mathcal{I}) = \mathcal{I}.$$

Set $I = \gamma_i \mathcal{I}$. Then, I is an integral ideal and has an inverse I^{-1}. Consider the element $\gamma_i I^{-1}$. Multiplication by $\mathcal{I}$ gives

$$\mathcal{I} \cdot \gamma_i I^{-1} = \frac{1}{\gamma_i} \cdot \gamma_i (\gamma_i \mathcal{I}) \cdot (I^{-1}) = I \cdot I^{-1} = \mathfrak{o},$$

and $\gamma_i I^{-1}$ is an inverse for $\mathcal{I}$. Therefore, the fractional ideals of $\mathfrak{o}$ form a multiplicative abelian group. □

From here, we can prove that in a Dedekind domain, integral ideals have unique factorization. Thus, while we have no guarantee of unique factorization of elements in the ring of integers, we do have unique factorization of integral ideals.

Theorem 2.5. *Any non-zero integral ideal I in $\mathfrak{o}$ can be written as a product $I = P_1 P_2 ... P_m$ where the P_i's are prime ideals. Furthermore, this expression is unique up to the order of the factors.*

Proof. If there are integral ideals of $\mathfrak{o}$ with no factorization into prime ideals, we assume that I is maximal among them. Then, there exists a maximal ideal P such that $I \subset P$. Then, we have the chain of inclusions $IP \subset I \subset P$ and multiplying by P^{-1} gives $I \subset IP^{-1} \subset \mathfrak{o}$. If it were the case that $I = IP^{-1}$, then multiplying by I^{-1} on both sides gives $\mathfrak{o} = P^{-1}$, which is a contradiction. Therefore, I is properly contained in IP^{-1}, and by the maximality of I, IP^{-1} factors into prime ideals, say $IP^{-1} = P_1 P_2 ... P_{m-1}$. Then, if we multiply by P on either side and set $P = P_m$, we get

$$I = P_1 P_2 ... P_m,$$

and we have a prime factorization for I.

Now, say that I has two factorizations, where m is the minimal number of prime factors of I. Then, we have

$$I = P_1 P_2 ... P_m = Q_1 Q_2 ... Q_n,$$

where both $n, m > 0$. If P_1 were not one of the Q_i's where $i = 1, .., n$, then for every i we could find an α_i in Q_i such that $\alpha_i \notin P_1$. Then, $\prod_i \alpha_i \notin P_1$. However, it must be true that $\prod_i \alpha_i = \gamma_1 \gamma_2 .... \gamma_m$ for $\gamma_j \in P_j$ where $j = 1, ..., m$, and $\gamma_2 \gamma_3 ... \gamma_m \in \mathfrak{o}$, so the product $\gamma_1 \gamma_2 .... \gamma_m$ must be in P_1 by the absorption property of ideals. This is a contradiction.

So, we can remove a P_1 in both expressions for I, since $P_1 = Q_k$ for some $1 \leq k \leq n$. This contradicts the minimality of m. Thus, the decomposition of I is unique up to the order of the factors. □

3. The Ideal Class Group, C_k

We denote the group of non-zero fractional ideals of k by J_k. J_k has a subgroup consisting of all the principal fractional ideals of $\mathfrak{o}$. A principal fractional ideal is analogous to a principal integral ideal in that it has a single generator. We denote the group of non-zero principal fractional ideals I_k.

Definition If $\mathfrak{o}$ is a Dedekind domain with quotient field k. Then the ideal class group of k is $C_k = \frac{J_k}{I_k}$.

An element in C_k is a class of fractional ideals, $[\mathcal{I}]$. More precisely, it is a coset of the form $\mathcal{I}J_k = [\mathcal{I}]$. Two cosets $[\mathcal{I}]$ and $[\mathcal{J}]$ are equal when $\mathcal{I}$ and $\mathcal{J}$ differ by a constant. In other words, $[\mathcal{I}] = [\mathcal{J}]$ if and only if $\mathcal{I} = \alpha\mathcal{J}$ for some $\alpha \in k$. We know that $\mathcal{I}$ has a denominator $\gamma_i \in k$, and from the previous statement we get $[\mathcal{I}] = [\gamma_i\mathcal{I}]$. Since $\gamma_1\mathcal{I}$ is an integral ideal, every ideal class can be represented by an integral ideal.

Note that C_k is trivial if every ideal of k is a principal ideal. Hence, the class group gives us a measure of how close $\mathfrak{o}$ is to being a principal ideal domain. To make this notion more precise, we define the the class number.

Definition Set $h(k) = |C_k|$. Then $h(k)$ is the class number of k.

Since every principal ideal domain is a unique factorization domain, the class number can also be thought of as a measure of how close a field k is to being a unique factorization domain. The next theorem will show that $h(k)$ is always finite for any algebraic number field. This is not too surprising, since algebraic number fields are finite extensions of $\mathbb{Q}$, a unique factorization domain.

Theorem 3.1. *Let $\mathfrak{M}_k$ denote a positive constant. Then each of the following statements implies the next:*

(a) Each fractional ideal $\mathcal{I}$ contains an $\alpha \neq 0$ for which $|N(\alpha)| \leq \mathfrak{M}_k \cdot N(\mathcal{I})$.
(b) Each ideal class in C_k contains an integral ideal I of norm $N(I) \leq \mathfrak{M}_k$.
(c) C_k is finite.

Proof. Say that (a) holds. Then, for some fractional ideal $\mathcal{I} \in J_k$ there exists an inverse, $\mathcal{I}^{-1}$. By hypothesis, we know that there exists an $\alpha \in \mathcal{I}^{-1}$ such that

$$|\mathrm{N}(\alpha)| \leq \mathfrak{M}_k \cdot \mathrm{N}(\mathcal{I}^{-1}).$$

We can multiply by $\mathrm{N}(\mathcal{I})$ on either side to obtain the following:

$$|\mathrm{N}(\alpha)|\,\mathrm{N}(\mathcal{I}) \leq \mathfrak{M}_k \cdot \mathrm{N}(\mathcal{I}^{-1})\mathrm{N}(\mathcal{I})$$

We know that every ideal norm is a positive number, allowing us to pull it inside absolute values. Therefore, the expression above simplifies as follows:

$$|\mathrm{N}(\alpha\mathcal{I})| \leq \mathfrak{M}_K \cdot \mathrm{N}(\mathcal{I}^{-1}\mathcal{I}) = \mathfrak{M}_K \cdot \mathrm{N}(\mathfrak{O}).$$

Since $\mathcal{I}^{-1} = \{\alpha \in k : \alpha\mathcal{I} \in \mathfrak{O}\}$, we set $I = \alpha\mathcal{I}$ and I is an integral ideal. Also, note that $\mathrm{N}(\mathfrak{O}) = [\mathfrak{O} : \mathfrak{O}] = 1$. Therefore, we can simplify the above even further to obtain

$$\mathrm{N}(I) \leq \mathfrak{M}_k,$$

and (a) implies (b).

To prove that (b) implies (c), we just need to show that there are only finitely many integral ideals of norm less than $\mathfrak{M}_k$. Consider the lattice formed by the ring of integers $\mathfrak{O}$. All integral ideals are finitely generated by elements of this lattice, and the norm of these generators determines the norm of the ideal. Thus, if we bound the norm of integral ideals, we are bounding the norm of their generators. Given a bounded subset of the lattice formed by $\mathfrak{O}$, there are only finitely many points within this bound. Thus, there are only finitely many integral ideals with norm less than a certain bound. □

Given the above theorem, all we need to show the finiteness of C_k is an element of sufficiently small norm in any fractional ideal. To do this, we need to think of fractional ideals as lattices in $\mathbb{R}^n$.

An integral ideal is simply a subset of $\mathfrak{O}$. So, it can be isomorphically identified with a subset of the lattice formed by $\mathfrak{O}$ and can be thought of as a lattice in its own right. Since fractional ideals are simply a scaling of an integral ideal, the same is true for fractional ideals. Thus, if we can bound the points in a lattice, we can extend this bound to elements of fractional ideals. The following proposition gives us this bound.

Note that a *convex set* S is a set such that any two points, $x, y \in S$ can be joined by a line segment entirely contained in S. A *closed set* is a set that contains its own boundary.

Theorem 3.2 (**Minkowski's Theorem**). *Let Λ be a lattice in $\mathbb{R}^n$ and let S be a bounded, closed, convex subset of $\mathbb{R}^n$ that is symmetric about the origin. Then S contains a point of Λ other than the origin, provided 2^n Vol$(\mathbb{R}^n/\Lambda) \leq$ Vol(S).*

The volume of S is in terms of something called a Haar measure which is far too involved to describe here. Essentially $\mathrm{Vol}(S)$ is a generalization of the notion of volume from $\mathbb{R}^3$ to higher dimensions.

Say that S is any closed, bounded, convex subset of $\mathbb{R}^n$ symmetric with respect to the origin and denote its volume v. Denote by M

$$\max(\left|x_1x_2...x_{r_1}(x_{r_1+1}^2 + x_{r_1+r_2+1}^2)...(x_{r_1+r_2}^2 + x_n^2)\right|) \tag{1}$$

for all points $x_i \in S$. Here, r_1 and r_2 are defined as in section 1. Let $\mathcal{I}$ be any fractional ideal in k. The volume of $\mathcal{I}^{-1}$ is some fraction of the volume of $\mathfrak{O}$. More specifically, $\mathrm{Vol}(k/\mathcal{I}^{-1}) = \frac{2^{-r_2}\sqrt{|\Delta_k|}}{\mathrm{N}(\mathcal{I})}$, and we will denote this quantity c. We set $\lambda = 2(\frac{c}{v})^{1/n}$ and consider the volume of λS. Calculating this volume involves n multiplications of λ since the dimension of S is n. We end up with

$$\mathrm{Vol}(\lambda S) = \lambda^n \mathrm{Vol}(S) = 2^n \frac{c}{v} v = 2^n c.$$

Thus, we have a set λS such that $\mathrm{Vol}(\lambda S) = 2^n \mathrm{Vol}(k/\mathcal{I}^{-1})$ and we can apply theorem 3.2. This theorem tells us there exists an $\alpha \in \mathcal{I}^{-1} \cap \lambda S$ such that $|\mathrm{N}(\alpha)| \leq \lambda^n M$. Since $\mathcal{I}^{-1}$ was simply an arbitrary fractional ideal, we have found a bounded element in any fractional ideal.

Now, we would like to use our bound on elements in fractional ideals to get an explicit bound on the norm of ideals. Note that since $\alpha \in \mathcal{I}^{-1}$, $\alpha\mathcal{I}$ is an integral ideal, and we denote it I. Multiplying the above inequality on both sides by $\mathrm{N}(\mathcal{I})$ gives us

$$\mathrm{N}(I) \leq \lambda^n M \mathrm{N}(\mathcal{I}) = \left(2\left(\frac{c}{v}\right)^{1/n}\right)^n M\mathrm{N}(\mathcal{I}) = 2^n \left(\frac{2^{-r_2}\sqrt{|\Delta_k|}}{v\mathrm{N}(\mathcal{I})}\right) M\mathrm{N}(\mathcal{I}) = 2^{r_1+r_2} M \frac{\sqrt{|\Delta_k|}}{v}.$$

At this point, all we need to bound C_k is a set S as above. One such set is the following:

$$S = \left\{ x_i \in \mathbb{R}^n \mid \sum_{i=1}^{r_1} |x_i| + \sum_{i=r_1+1}^{r_1+r_2} \sqrt{x_i + x_{i+r_2}} \leq 1 \right\}.$$

This set is convex. The volume is as follows:

$$\mathrm{Vol}(S) = \frac{2^{r_1+r_2}(\pi)^{r_2}}{4^{r_2}n!},$$

and computing M as defined in eq. (1) gives us $M = n^{-n}$. Thus, every class group of k contains an ideal I such that

$$\mathrm{N}(I) \leq \sqrt{\Delta_k}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

The above is known as Minkowski's bound.

4. Computations of C_k for Quadratic Field Extensions

Computations of the class group are particularly straightforward in quadratic fields. These are fields of the form $\mathbb{Q}[\sqrt{D}]$ for some $D \in \mathbb{Z}$. Quadratic fields have a basis $\{1, \sqrt{D}\}$. Therefore, for some $\alpha = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$, the matrix M_α is as follows:

$$M_\alpha = \begin{bmatrix} a & b \\ bD & a \end{bmatrix}.$$

So, $\mathrm{Tr}(\alpha) = 2a$ and $\mathrm{N}(\alpha) = a^2 - Db^2$.

To compute class groups, we also need the discriminant of $\mathbb{Q}[\sqrt{D}]$. So, we need to compute a basis for the ring of integers of $\mathbb{Q}[\sqrt{D}]$ denoted $\mathfrak{O}$.

Proposition 4.1. *Say that D is a square-free integer. Then the ring of integers of $\mathbb{Q}[\sqrt{D}]$ is given by $\mathfrak{O} = \mathbb{Z}[\delta]$, where*

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

Proof. Notice that in either case, δ is in $\mathfrak{O}$ since it either satisfies the equation $x^2 - D = 0$ or $x^2 - x + \frac{1-D}{4} = 0$. Both of these equations have coefficients in $\mathbb{Z}$, and since $\mathfrak{O}$ is integrally closed and contains $\mathbb{Z}$, this means that $\delta \in \mathfrak{O}$. Thus, $\delta\mathbb{Z}$ is an integral ideal, and so $\mathbb{Z} + \delta\mathbb{Z} \subset \mathfrak{O}$.

Let $\alpha = a + b\sqrt{D} \in \mathfrak{O}$. Then, $\mathrm{Tr}(\alpha) = 2a$ and $\mathrm{N}(\alpha) = a^2 - Db^2$ as above. Both the trace and norm must be in $\mathbb{Z}$ by the definition of being in $\mathfrak{O}$. Set $a = \frac{r}{2}$ and $b = \frac{m}{n}$ for some $r, m, n \in \mathbb{Z}$ such that $\gcd(m, n) = 1$. Plugging this into the expression for the norm of α gives us

$$\mathrm{N}(\alpha) = \frac{r^2}{4} - D\frac{m^2}{n^2},$$

and we can rearrange this to obtain $4m^2D = n^2(r^2 - 4\mathrm{N}(\alpha))$. Thus, $n^2|4m^2D$, and since $\gcd(m, n) = 1$, this reduces to $n^2|4D$. Say p is an odd prime factor of n. Then $p^2|D$, which contradicts the square-freeness of D. So, n must be a power of 2 which means that D must also be a power of 2. Since D is square-free, $4 \nmid D$. This means that D cannot contain a power of 2 greater than 2, and thus, it must be true that $n^2|8$ which implies $n = 1$ or 2. This means we can write $b = \frac{s}{2} \in \mathbb{Z}$ since if $n = 1$, we can simply make s even.

Since $a^2 - Db^2 \in \mathbb{Z}$, $\frac{r^2}{4} - D\frac{s^2}{4} = c$ for some $c \in \mathbb{Z}$. Thus, $r^2 = s^2D + 4c$, which implies that $r^2 \equiv s^2D \pmod 4$. There are two cases to consider.

The first case is $D \not\equiv 1 \pmod 4$. Note that the only squares in $\mathbb{Z}_4$ are 0 and 1. Since $s^2D \equiv r^2 \pmod 4$, D must be a square, and must therefore be 0 (mod 4). Thus, $r \equiv s \equiv 0$ and hence, r and s are even integers. This means that a and b are in $\mathbb{Z}$ and $\mathfrak{O} \subset \mathbb{Z} + \mathbb{Z}\sqrt{D}$.

The second case is $D \equiv 1 \pmod 4$. In this case, $r^2 \equiv s^2 \pmod 4$ and this means that $r \equiv s \equiv 0 \pmod 2$. Thus, $r = s + 2c$ for some $c \in \mathbb{Z}$ and we have

$$\alpha = \frac{r + s\sqrt{D}}{2} = \frac{s + 2c + s\sqrt{D}}{2} = c + s\frac{1 + \sqrt{D}}{2},$$

which means that $\mathfrak{O} \subset \mathbb{Z} + \frac{1+\sqrt{D}}{2}\mathbb{Z}$. □

Note that δ is the solution to an irreducible polynomial in $\mathbb{Z}[x]$. We will refer to the coefficients of this polynomial in computations, and so we denote this polynomial by $x^2 - tx + n$, where $\delta^2 - t\delta + n = 0$.

We can now compute the discriminant of $\mathbb{Q}[\sqrt{D}]$ using the basis $\{1, \delta_0\}$ for $\mathfrak{O}$. We build the matrix M_D which has two different forms based on δ,

$$M_D = \begin{bmatrix} 2 & 0 \\ 0 & 2D \end{bmatrix} \text{ or } \begin{bmatrix} 2 & 1 \\ 1 & \frac{1+D}{2} \end{bmatrix},$$

and thus $\Delta_D = 4D$ or $\Delta_D = D$. Notice that $\mathrm{Tr}(\delta) = 0$ or 1, and $\mathrm{N}(\delta) = -D$ or $\frac{1-D}{4}$. In either case, $\Delta_D = (\mathrm{Tr}(\delta))^2 - 4\mathrm{N}(\delta)$.

In quadratic fields, we can express ideals in a standard form

$$I = d(a\mathbb{Z} + (-b + \delta)\mathbb{Z})$$

where $a, b, d \in \mathbb{Z}$ and $b^2 - tb + n \equiv 0 \pmod{a}$.

Proposition 4.2. *If we set*

$$\bar{I} = d(a\mathbb{Z} + (-b + t - \delta)\mathbb{Z}),$$

then $I\bar{I} = \mathfrak{O} \cdot N(I)$*, or* $I\bar{I} =< N(I) >$.

Primes in $\mathbb{Z}$ are not necessarily primes in extensions of $\mathbb{Z}$. We need to have some idea of how primes behave in extensions to effectively compute the class number.

Definition Let $p \in \mathbb{N}$ be a prime. Then, the prime factorization of $< p >$ in $\mathfrak{O}$ has can have the following forms.

(a) $< p >= P$ where $\mathrm{N}(P) = p^2$. This means that the principal ideal generated by p is prime. In this case, we say that p is *inert*.
(b) $< p >= P^2$ with $\mathrm{N}(P) = p$. Then, we say that p is *ramified*.
(c) $< p >= P\bar{P}$ with $\mathrm{N}(P) = p$ and $P \neq \bar{P}$. Then, we say p is *split*.

Determining which of these forms $< p >$ takes on is actually not too difficult. The following proposition makes it relatively simple. We will state it without proof.

Proposition 4.3. *Let $p \in \mathbb{N}$ be a prime.*

(a) If $\Delta_k \pmod p$ is a not a perfect square, then p is inert.
(b) If $\Delta_k \pmod p$ is a non-zero perfect square or 0, pick an element $b \in \mathbb{Z}$ so that $b^2 - tb + n \equiv 0 \pmod p$. Put $P = p\mathbb{Z} + (-b + \delta)\mathbb{Z}$. Then, the following hold:
- *P is a prime ideal of $\mathfrak{O}$.*
- *$\bar{P} = p\mathbb{Z} + (-(t - b) + \delta)\mathbb{Z}$.*
- *$\Delta_k \pmod p$ is 0 if and only if $P = \bar{P}$ and p is ramified.*
- *$\Delta_k \pmod p$ is a non-zero perfect square if and only if $P \neq \bar{P}$ and p is split.*

The above proposition tells us that the only primes p that ramify in a quadratic extension k are those that satisfy $p|\Delta_k$.

Example Say $k = \mathbb{Q}[\sqrt{-14}]$, then $\mathfrak{O} = \mathbb{Z}[\sqrt{-14}]$. The only prime factors of $\Delta_k = -56$ are 2 and 7, so 2 and 7 are the only ramified primes. We have $\delta = \sqrt{-14}$, which is the root of $x^2 + 14 = 0$, which reduces to $x^2 = 0$ modulo both 2 and 7. So, we set $b = t - b = 0$ in proposition 4.3 part (b). This gives us that

$$< 2 >= P_2^2 = (2\mathbb{Z} + \sqrt{-14})^2$$

and

$$< 7 >= P_7^2 = (7\mathbb{Z} + \sqrt{-14}\mathbb{Z})^2.$$

The ideals P_2 and P_7 are prime ideals of $\mathfrak{O}$.

Lets look at some primes and see what happens to them in $\mathbb{Z}[\sqrt{-14}]$. Consider 11, where $56 \equiv 10 \pmod{11}$. Since 10 is not a perfect square in $\mathbb{Z}_{11}$, 11 is inert. Consider 23, where $-56 \equiv 13 \pmod{23}$. Note that $6^2 = 36 \equiv 13 \pmod{23}$. Thus, $\Delta_k \pmod{23}$ is a perfect square and splits. Note that $3^2 + 14 \equiv 0 \pmod{23}$, so we set $b = 3$ and apply proposition 4.3 part (b) to factor $< 23 >$ as follows:

$$< 23 >= (23\mathbb{Z} + (-3 + \sqrt{-14}\mathbb{Z})(23\mathbb{Z} + (3 + \sqrt{-14})\mathbb{Z}).$$

We will now give several examples of how to compute the class group of a quadratic extension using the tools presented above. We will start with a relatively simple example.

Example Let $k = \mathbb{Q}[i]$, then $\mathfrak{O} = \mathbb{Z}[i]$. The formula above gives us $\Delta_k = -4$. Thus, we can use Minkowski's bound to represent any ideal class by an integral ideal I such that

$$\mathrm{N(I)} \leq \frac{2}{\pi}\sqrt{4} \approx 1.27.$$

Since $\mathrm{N}(I)$ must be an integer, this means $\mathrm{N}(I) = 1$. Thus, $I = \mathfrak{O}$, which implies that $C_k = \mathfrak{O}$, and we have a trivial class group. Hence, $\mathbb{Z}[i]$ is a principal ideal domain.

The above example simply confirms that the Gaussian integers are a unique factorization domain, and we were able to prove this without using the division algorithm.

Example Let $k = \mathbb{Q}[\sqrt{-19}]$, which has $\mathfrak{O} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ and $\Delta_k = 19$. From Minkowski's bound we get that

$$\mathrm{N}(I) \leq \frac{2}{\pi}\sqrt{19} \approx 2.7,$$

and thus $\mathrm{N}(I) \leq 2$. If $\mathrm{N}(I) = 2$, then by proposition 4.2 $I\bar{I} =< 2 >$ and I must be a prime factor of $< 2 >$. However, this is impossible, since 2 does not split in $\mathbb{Q}[\sqrt{-19}]$. Thus, the only possible value for $\mathrm{N}(I)$ is 1. As such, we have $h(k) = 1$ and k is a principal ideal domain.

It can be shown that $\mathbb{Q}[\sqrt{-19}]$ is not a Euclid domain. It is difficult to show this is a UFD because we lack a division algorithm. Using the class number circumvents this problem.

Example In general, we have a PID when Minkowski's boud is less than 2. For a real quadratic extension, this means that $\Delta_k \leq 16$, and for an imaginary quadratic extension we have $\Delta_k \leq \pi^2$. Thus, we have that $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{4}], \mathbb{Q}[\sqrt{13}], \mathbb{Q}[\sqrt{i}], \mathbb{Q}[\sqrt{-2}], \mathbb{Q}[\sqrt{-3}]$, and $\mathbb{Q}[\sqrt{-7}]$ all have class number 1 and are UFD's.

Note that the above is not a complete list of fields with class number 1. The immediately preceding example shows that it is certainly possible to have $h(k) = 1$ with a Minkowski bound greater than 2.

The following proposition will allow us to do a more complicated example.

Proposition 4.4. *The ideal class group of $\mathbb{Q}[\sqrt{D}]$ is generated by finitely many class $[P]$, where P ranges over ideals of prime norm bounded by $N(P) \leq \mathfrak{M}_k$. In other words, $[\mathfrak{O}] = [P_1]^{e_1}[P_2]^{e_2}...[P_m]^{e_m}$ where the P_i's are prime ideals and e_i's are positive integers.*

Example Let $k = \mathbb{Q}[\sqrt{-47}]$, giving us $\mathfrak{O} = \mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$ or $\delta = \frac{1+\sqrt{-47}}{2}$. We have that δ satisfies $\delta^2 - \delta + 12 = 0$ giving us $t = 1$. The Minkowski bound gives us that C_k is generated by ideals P with prime norm bounded by

$$\mathrm{N}(P) \leq \frac{2}{\pi}\sqrt{47} \approx 4.36,$$

thus, the two possible values of $\mathrm{N}(P)$ are 2 and 3. Then, since $12 \equiv 0$ modulo both 2 and 3, we set $b = 0$. The possible factorizations of $< \mathrm{N}(P) >$ are

$$< 2 >= P_2\bar{P}_2 = (2\mathbb{Z} + \frac{1+\sqrt{-47}}{2}\mathbb{Z}) \cdot (2\mathbb{Z} + \frac{12\sqrt{-47}}{2}\mathbb{Z})$$

or

$$< 3 >= P_3\bar{P}_3 = (3\mathbb{Z} + (-1 + \frac{1+\sqrt{-47}}{2}\mathbb{Z})) \cdot (3\mathbb{Z} - \frac{1+\sqrt{-47}}{2}\mathbb{Z}).$$

Therefore, $[\mathfrak{O}]$ factors as some product of the form $[P_2]^a[P_3]^b$ and $[P_2]^a[P_3]^b =< \alpha >$ for some $\alpha \in \mathfrak{O}$ of norm 2^a3^b. Note that $\mathrm{N}(\delta) = \frac{1}{4} + \frac{47}{4} = 12 = 2^2 \cdot 3$. We find that

$$< \delta >= P_2^2\bar{P}_3,$$

and thus by proposition 4.2, $\mathrm{N}(P_2^2) = \delta$ and $[P_3] = P_2^2$. So, we can replace every power of $[P_3]$ with a power of $[P_2]$ and $C_k =< [P_2] >$.

Now we just need to find the order of $[P_2]$. This is the smallest positive integer r such that $[P_2]^r =< \beta >$ for some $\beta \in \mathfrak{O}$. Set $\beta = x + y\delta$. Taking the norm gives us

$$2^r = \mathrm{N}\,(x + y\delta) = x^2 + xy + 12y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{47}{4}y^2.$$

If $y = 0$, then we have $\beta = 2^{r/2}$, which would mean that $< 2^{r/2} >= P_2^{r/2}\bar{P}^{r/2}$ by proposition 4.2. This contradicts our hypothesis that $< \beta >= P_2^r$.

If $y \neq 0$, then because y must be an integer, $\mathrm{N}(\beta) \geq [47/4] = 12$, so $\mathrm{N}(\beta)$ cannot be 2, 4, or 8.

If $\mathrm{N}(\beta) = 16$, then $y = \pm 1$ otherwise our value would get too big. However, $x^2 + x + 12 = 16$ has no solutions in $\mathbb{Z}$.

So, we consider $\mathrm{N}(\beta) = 32$. Then we have $32 = x^2 + xy + 12y^2$. Once again, $y = \pm 1$, which gives us the solution $x = 4$ and $y = 1$. Thus, we have $< 4 + \delta >= P_2^5$ and $C_k = \mathbb{Z}_5$.

5. Characterizing Fields with Given $h(k)$ and Gauss' Class Number Problem

An active area of research in algebraic number theory is how to determine the fields of a given class number. In other words, if we are given a class number, can we find all the fields with that class number? This is by no means a trivial problem. The following proposition shows how we can determine characteristics of a field with a certain class number.

Proposition 5.1. *For a field k, $h(k) \leq 2$ if and only if for every nonzero integer $\alpha \in \mathfrak{O}$, the number of primes, p_i, in any factorization $\alpha = p_1p_2...p_n$ depends only on α. In other words, any factorization of α into primes has n terms.*

Proof. If $h(k) = 1$, we have a unique factorization domain, and we are done. Say that $h(k) = 2$ and consider the factorization of $< \alpha >$ into prime ideals

$$< \alpha >= P_1P_2...P_sQ_1Q_2...Q_t, \tag{2}$$

where the P_i's are principal ideals and the Q_j's are not. Then, we can say that $P_i =< p_i >$ for $i = 1, ..., s$. Since $h(k) = 2$, any product of 2 nonprincipal ideals must be a principal ideal. This is because $C_k \cong \mathbb{Z}_2$ where 0 indicates a principal ideal and 1 is a non-principal ideal. Since $1 + 1 \equiv 0 \pmod 2$, the multiplication of any non-principal ideals gives a principal ideal. Therefore, we have that $Q_jQ_k =< q_{j,k} >$ for $j, k = 1, ...t$, where $< q_{j,k} >$ is a prime ideal. Furthermore, t must be

even because the product on the left of eq. (2) must be a principal ideal and the product of an odd number of non-principal ideals gives a principal ideal. Set $t = 2u$.

By unique factorization of ideals, the numbers s and t are fixed. If there were prime factors of α other than the generator p_i and q_j, then they would generate another prime ideal which cannot happen since factorization into prime ideals is unique. Thus, α factors as follows

$$\alpha = rp_1p_2...p_{1,2}...p_{t-1,t},$$

where r is a unit. This factorization has exactly $s + u$ primes.

It remains to show that when $h > 2$, there are factorizations with different values of n. We assume the existence of a class $[I]$ with order $m > 2$. Let P be a prime ideal in $[I]$ and P' a prime ideal in $[I]^{-1}$. Then, it must be true that $P^m =< p >$, $(P')^m =< p' >$ for some primes $p, p' \in \mathfrak{O}$. Additionally, since P' is in the inverse ideal class of P, the multiplication of these two elements results in an element in the identity ideal class, which is the class of principal ideals. Thus, $PP' =< p_1 >$ for some prime $p_1 \in \mathfrak{O}$. This gives us

$$p_1^m = rpp',$$

where r is a unit, and we have two prime factorizations with a different number of primes.

Now, we assume the existence of two classes $[I]_1$ and $[I]_2$ of order 2 such that $[I]_3 = [I]_1[I]_2$ is not principal. Choose three prime ideals $P_j \in [I]_j$. Then,

$$P_j^2 =< p_j > \text{ for } j = 1, 2, 3 \text{ and } P_1P_2P_3 =< p >,$$

where p_1, p_2, p_3, and p must all be primes. Then, we have that $p^2 = p_1p_2p_3$ which is two prime factorizations with different numbers of elements. □

While computing the class number of a given field is relatively doable, characterizing fields given a class number is a very challenging problem. Carl Friedrich Gauss made several famous conjectures about the discriminants of quadratic fields with certain class numbers. His first conjecture was that as $h(k) \to \infty$, $\Delta_k \to -\infty$. Gauss also conjectured that the number of negative discriminants with a given class number is finite. Both of these conjectures have since been proven, though it took quite a long time. In 1983, more than a hundred years later, it was found that there exists a bound $B(n)$ such that if $H(k) = n$, then $|\Delta_k| \leq B(n)$ when $\Delta_k < 0$. Gauss' challenge to find an effective algorithm to compute the discriminants with a given class number has not been answered.

6. Conclusion

Although we can lose unique factorization of integers when finitely extending number fields, we do have some structure that allows us to get a grasp on how integers factor. The ring of integers of a field is a Dedekind domain, and the properties of Dedekind domains can be exploited to form a group from the fractional ideals of our field. This group allows us to form the ideal class group which in turn helps us determine how elements factor in our field extension. The lattice structure of the ring of integers guarantees us a bound on the size of the ideal class group. Minkowski's bound gives us an explicit number to compute. These computations are particularly tractable in quadratic field extensions. Starting with a class number and determining the fields with that particular class number is much more difficult and remains an unsolved problem.

References

[1] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, 50, Cambridge Univ. Press, Cambridge, 2001. MR1826558 (2002a:11117)
[2] M. Trifkovic. *Algebraic theory of quadratic numbers*, Springer, New York, 2013.
[3] K. Conrad. Class Group Calculations. http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/classgpex.pdf (accessed March 6, 2014).
[4] Carlitz, L. A characterization of algebraic number fields with class number two. Proc. Amer. Math. Soc. 11 1960 391–392. MR0111741 (22 #2603)
[5] D. Goldfeld, Gauss's class number problem for imaginary quadratic fields, Bull. Amer. Math. Soc. (N.S.) **13** (1985), no. 1, 23–37. MR0788386 (86k:11065))
[6] P. Ribenboim, *My numbers, my friends*, Springer, New York, 2000. MR1761897 (2002d:11001)
[7] K. Conrad. Trace and Norm. http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/tracenorm.pdf (accessed April 14, 2014).