IDEAL CLASS GROUPS

ARJUN VENKATRAMAN

1. Introduction

In class, we discussed the class group of quadratic forms of discriminant d, that is, the abelian group of all classes of quadratic forms of the given discrimanant (with order equal to its class number). There is a separate way to describe these groups in an algebraic fashion as being derived from ideals of the integer ring of number fields. This allows further examination of class groups from an algebraic perspective, and also allows extensions into other types of number fields (for instance, the class group of biquadratic fields can be derived from those of its quadratic subfields [Sim95]). In this paper, we establish the ideal class group, examine its relationship with the quadratic form class group, and prove that the group is finite.

2. Basic Definitions

To discuss ideal class groups, we must first define ideals.

Definition 2.1. An ideal I of a ring R is an additive subgroup of the ring in which for all $i \in I$ and $r \in R, ri \in I$.

There are also specific types of ideals that interest us.

Definition 2.2. A *prime ideal* is an ideal $I \neq R$ such that $\forall a, b \in R$ and $ab \in I$, either

$$a \in I \text{ or } b \in I.$$

As the name and definition suggest, prime ideals share a lot of properties with prime numbers. In fact, the prime ideals of the ring $\mathbb{Z}$ are exactly the ideals consisting of all multiples of some prime p plus the 0 ideal.

Definition 2.3. A *principal ideal* is an ideal which can be expressed as aR for some $a \in R$

Definition 2.4. An ideal I of a ring R is *maximal* if there are no ideals properly contained in R which properly contain I.

Definition 2.5. Given a ring R, an R-module is an abelian group M combined with a multiplication action by R: $R \times M \to M$ which satisfies the distributive and associative property, with the identity element of R also acting as the identity element within this action.

Date: December 9, 2018.

3. The Ring of Integers

In addition, we also need to generalize the concept of the ring of integers $\mathbb{Z}$ to all fields which are finite-degree extensions of $\mathbb{Q}$, which we call *number fields*.

Definition 3.1. An *algebraic integer* over a number field K is an element of K which is a root of some monic polynomial with integer coefficients.

The algebraic integers of $\mathbb{Q}$ are exactly the integers $\mathbb{Z}$, and the algebraic integers serve as the generalization for $\mathbb{Z}$ over all number fields.

To prove that the algebraic integers form a ring, we first prove the following:

Theorem 3.2. *The group $\mathbb{Z}[a]$ is finitely generated iff a is an algebraic integer.*

Proof. If a is algebraic, then we have some monic polynomial f of degree m with integer coefficients such that $f(a) = 0$. This means that all a^n can be generated by the set $1, a, a^2, a^3, ..., a^{m-1}$, as it can be written as $a^m a^{n-m}$ and simplified using the monic polynomial; this can be repeated until a polynomial of degree less than m is left. This makes that set a finite set of generators for $\mathbb{Z}[a]$.

If $\mathbb{Z}[a]$ is finitely generated by a set $a_1, a_2, a_3, \ldots, a_m$, then for each generator, find a function f_i such that $f_i(a) = a_i$. Then, pick some N larger than the highest degree of the f_is. a^N can be written as some linear combination of the generators $k_1a_1+k_2a_2+k_3a_3+\ldots+k_ma_m$. Thus, we have $x^N - (k_1f_1(x) + k_2f_2(x) + k_3f_3(x) + \ldots + k_mf_m(x)) = 0$, which is a monic degree-N polynomial with integer coefficients for which a is a solution. ■

From this, we can now show that the set of all algebraic integers forms a ring $\mathcal{O}$.

Theorem 3.3. *The set of all algebraic integers of a number field K forms a ring.*

Proof. If α and β are algebraic integers, then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated, and $\mathbb{Z}[\alpha, \beta]$ is also finitely generated. Since $\mathbb{Z}[\alpha, \beta]$ is a ring, $\mathbb{Z}[\alpha + \beta]$ and $\mathbb{Z}[\alpha\beta]$ are subrings of $\mathbb{Z}[\alpha, \beta]$ and are thus also finitely generated, meaning that $\alpha + \beta$ and $\alpha\beta$ are also algebraic integers. Thus, the set $\mathcal{O}_K$ of all algebraic integers of a number field K is a ring which we call the *ring of integers* of K. ■

Before we continue, we establish the concept of the *norm* of elements of K and ideals of $\mathcal{O}$.

Definition 3.4. The norm of an element a of K is the product of the images of a in each of the embeddings from K to $\mathbb{C}$.

Definition 3.5. The norm of an ideal I of $\mathcal{O}$ is defined as the order of $\mathcal{O}/I$.

4. Fractional Ideals

Now that we have established that the algebraic integers form a ring, we can use this ring to create a group structure on generalized versions of its ideals—this group has the ideal class group as a quotient group.

This group structure is defined through the *fractional ideal*, which is defined as follows:

Definition 4.1. A nonzero $\mathcal{O}$-submodule I of K is a fractional ideal of $\mathcal{O}$ if $\exists a \in \mathcal{O}, a \neq 0$ such that aI is an ideal of $\mathcal{O}$.

To prove that the fractional ideals do indeed form a group, we must show that each fractional ideal has an inverse. We first do this solely for the prime (integral) ideals:

Given a prime ideal $\mathfrak{p}$, define $\mathfrak{p}^{-1}$ as the set of all $x \in K$ such that $x\mathfrak{p} \subset \mathcal{O}$.

Theorem 4.2. *$\mathfrak{p}^{-1}$ is a fractional ideal.*

Proof. Take some nonzero $a \in \mathfrak{p}$. Then, by the definition above, $a\mathfrak{p}^{-1} \subset \mathcal{O}$, and furthermore is an (integral) ideal of $\mathcal{O}$, so $\mathfrak{p}^{-1}$ is a fractional ideal. ■

Given that it is a fractional ideal, we must now prove that it is indeed an inverse of $\mathfrak{p}$ (meaning that $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$). Before we can do this, we need an identity element. In this case, that element is the ring itself, $\mathcal{O}$. Because fractional ideals are $\mathcal{O}$-modules, $I\mathcal{O} = I$ for all fractional ideals I. Next, we also need the following theorems and lemmas, which will not be proven here.

Theorem 4.3. *All prime ideals of $\mathcal{O}$ are maximal.*

Lemma 4.4. *Every nonzero ideal I of $\mathcal{O}$ contains a product of prime ideals. [Lap06]*

Now, we can prove that $\mathfrak{p}^{-1}$ is a correctly defined inverse, starting with the following lemma:

Lemma 4.5. $\mathcal{O} \subsetneq \mathfrak{p}^{-1}$.

Proof. By their definitions, all elements of $\mathcal{O}$ must be in $\mathfrak{p}^{-1}$; we therefore must find some element of $\mathfrak{p}^{-1}$ that is not in $\mathcal{O}$. To do this, we take some nonzero $a \in \mathfrak{p}$, and find a product of prime ideals $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_k \subset a\mathcal{O}$ with minimal k. We know that $a\mathcal{O} \subset \mathfrak{p}$; therefore, by the definition of prime ideals and because all prime ideals are maximal, $\mathfrak{p} = \mathfrak{p}_i$ for some i. Because k is minimal, the product of the remaining prime ideals is not contained in $a\mathcal{O}$. This means we can find some element b that is not in $a\mathcal{O}$ but is contained in the product of the remaining prime ideals, meaning that $b\mathfrak{p} \subset a\mathcal{O}$. This means that $ba^{-1}\mathfrak{p} \subset \mathcal{O}$, so $ba^{-1} \in \mathfrak{p}^{-1}$, but $ba^{-1} \notin \mathcal{O}$. ■

Theorem 4.6. $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$.

Proof. By the definition of $\mathfrak{p}^{-1}$, we have $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}$. Since $\mathfrak{p}$ is a prime ideal and thus a maximal ideal, there can be no ideal properly between $\mathfrak{p}$ and $\mathcal{O}$, meaning that $\mathfrak{p}\mathfrak{p}^{-1}$ is equal to one of these ideals.

First, assume $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Then we take a generating set $\beta_1, \beta_2, \beta_3, ..., \beta_k$ of $\mathfrak{p}$. Also, from the previous lemma, there is at least one $a \in \mathfrak{p}^{-1}$ such that $a \notin \mathcal{O}$. We then have that $a\mathfrak{p} \subset \mathfrak{p}$, so for each β_i, $a\beta_i$ can be written as a linear combination of $beta_i$s (with coefficients in $\mathcal{O}$ as follows:

$$a\beta_i = \sum_{j=1}^{k} c_{i,j}\beta_j$$

for all β_i.

Rearranging terms gives us

$$\sum_{j=1}^{k} c_{i,j}\beta_j - a\beta_i = 0$$

.

Taking these equations for each i gives us a system of k equations in the β_is, which can be expressed as a matrix equation:

$$\begin{pmatrix} c_{1,1}-a & c_{1,2} & \dots & c_{1,k} \\ c_{2,1} & c_{2,2}-a & \dots & c_{2,k} \\ \dots & \dots & & \dots \\ c_{k,1} & c_{k,2} & \dots & c_{k,k}-a \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \dots \\ \beta_k \end{pmatrix} = 0$$

Thus, the matrix on the left must have determinant 0. The determinant here, however, is a monic polynomial in a with integer coefficients. Thus, a is the zero of some such monic polynomial, making it an algebraic integer; therefore, $a \in \mathcal{O}$. However, we defined $a \notin \mathcal{O}$, giving us a contradiction. Thus,

$$\mathfrak{p}^{-1}\mathfrak{p} \neq \mathfrak{p}$$

so

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

■

We can now use this definition of the inverse of a prime ideal to define inverses for all (integral) ideals.

Theorem 4.7. *All integral ideals are invertible in the fractional ideals.*

Proof. Assume there is some integral ideal I which is not invertible; furthermore, assume that it is a largest such ideal and is not strictly contained in any other non-invertible ideal.

We know that I is not prime—and, by extension, not maximal—so I must be contained in some maximal, prime $\mathfrak{p}$. Since $\mathcal{O} \subset \mathfrak{p}^{-1}$, $I \subset \mathfrak{p}^{-1}I$.

By the same logic as in the proof of the previous theorem, if $I = \mathfrak{p}^{-1}I$, then composing $a\beta i$ for all generators β_i yields that $a \in \mathcal{O}$ for any $a \in \mathfrak{p}^{-1}$, a contradiction. Therefore $I \subsetneq \mathfrak{p}^{-1}I$. Since I is not strictly contained by any non-invertible ideals, $\mathfrak{p}^{-1}I$ must be invertible. Call its inverse J; we have that $J\mathfrak{p}^{-1}I = \mathcal{O}$. Thus, $J\mathfrak{p}^{-1}$ is the inverse of I, and I is in fact invertible. ■

This can now be easily extended to fractional ideals.

Corollary 4.8. *Every fractional ideal I is invertible.*

Proof. I can be written as $\frac{J}{a}$, where J is an integral ideal. We have

$$aJ^{-1}\frac{J}{a} = J^{-1}a\frac{J}{a} = J^{-1}J = \mathcal{O}$$

Therefore, aJ^{-1} is the inverse of I. ■

Therefore, all fractional and integral ideals have inverses within the fractional ideals. Therefore we have proven:

Theorem 4.9. *The fractional ideals over a number field K form a group I_K under multiplication.*

5. The Ideal Class Group

We can also extend the concept of principal ideals to the fractional ideals, forming a subgroup of I_K.

Definition 5.1. A *principal fractional ideal* is a fractional ideal which can be expressed as aR for some $a \in K$. The group of these ideals is denoted $P(k)$ and is a subgroup of I_K.

Definition 5.2. The *ideal class group* $\mathrm{Cl}(K)$ of a number field K is defined as the quotient I_K/P_K, where P_K is the subgroup of principal ideals.

The ideal class group of $\mathbb{Q}[\sqrt{d}]$ can in fact be isomorphic to the class group based off of quadratic forms with discriminant d for d negative in certain cases. In particular, when d is negative and a discriminant for some positive definite quadratic form, then there is a bijection between the class group of quadratic forms with discriminant d and the ideal class group of $\mathbb{Q}[\sqrt{d}]$, created by mapping $ax^2 + bxy + cy^2$ to the ideal $[a, \frac{-b+\sqrt{d}}{2}]$. [Cox11]

6. The Ideal Class Group and Lattices

To show that the ideal class group is finite, we must first establish the following theorem about lattices, which is an extension of Minkowski's lemma:

Theorem 6.1. *Given a lattice Λ in $\mathbb{R}^n$, if X is a compact and convex set which is symmetric about 0 with volume greater than or equal to $2^n \operatorname{Vol}(\mathbb{R}^n/\Lambda)$, then there is at least one nonzero point in both Λ and X.*

Proof. We will take this proof in two cases, strict inequality and equality.

If $\operatorname{Vol}(X) > 2^n \operatorname{Vol}(\mathbb{R}^n/\Lambda)$, then the map ψ from $\mathbb{R}^n \to \mathbb{R}^n/\Lambda$ cannot be injective over $X/2$; therefore, there must be some x_1 and $x_2 \in X/2$ such that $\psi(x_1) = \psi(x_2)$. Since X, and thus also $X/2$, is symmetric and convex, $\frac{x_1-x_2}{2}$ is also in $X/2$. Thus, $x_1 - x_2$ is in X. Since $x_1 - x_2 = 0 \pmod{\mathbb{R}^n/\Lambda}$, $x_1 - x_2$ must also be in Λ, completing the proof.

In the case of equality, we know from the previous case that any set which is symmetric, compact, and convex and has a larger volume than X does include at least one point in Λ. Assume that X does not include any lattice points. Starting with the set $2X$ (which must have at least one lattice point per the previous case, which we shall call z_0). Then, another symmetric, compact, and convex set can be drawn within $2X$ which is larger than X but does not include z_0. This set then must include some other point in Λ, which we call z_1. Doing this repeatedly gives us an infinite sequence of distinct lattice points which all lie inside $2X$. However, $2X$ only contains a finite number of lattice points, leading to a contradiction. Therefore there must be some point in X which is also in Λ. ■

We can now relate the ring of integers to lattices through their embeddings, which allows us to use the previous result to prove that the ideal class group is finite.

Definition 6.2. The canonical embedding of the ring of integers $\mathcal{O}$ of a number field K, which has m_r real embeddings and m_c conjugate pairs of complex embeddings, is the embedding into $\mathbb{R}^n$, where n is the degree of the extension K as follows:

$$\sigma(a) = (r_1(a), r_2(a), r_3(a), ..., r_{m_r}(a), c_1(a), c_2(a), c_3(a), ..., c_{m_c}(a))$$

where $r_1, r_2, ..., r_{m_r}$ are the real embeddings of K and $c_1, c_2, ..., c_{m_c}$ are one of the two complex embeddings from each conjugate pair. Transposing $\mathbb{C}$ to $\mathbb{R}^2$ gives us a map to R^n.

Under this embedding, $\mathcal{O}(K)$ goes to a lattice in $\mathbb{R}^n$. We have that $\text{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}(K)))$ is equal to the determinant of the generator matrix of $\sigma(\mathcal{O}(K))$, which in turn is equal to $\frac{\sqrt{D}}{2^{m_c}}$, where D is the discriminant of the extension K.

7. Proof that the ideal class group is finite

We can now begin the proof.

Theorem 7.1. $\text{Cl}(K)$ *is a finite group.*

Proof. Because all fractional ideals are $\mathcal{O}$-modules, each of them also maps to a lattice in $\mathbb{R}^n$. Thus, we take a (nonzero) fractional ideal I, and find the lattice $\sigma(I^{-1})$. This lattice has fundamental parallelogram volume

$$\begin{aligned}\text{Vol}(\sigma(I^{-1})/\mathbb{R}^n) &= \text{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}(K)))N(I^{-1}) \\ &= \frac{\text{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}(K)))}{N(I)}\end{aligned}$$

Now, take some symmetric, convex, compact set X and scale it by

$$\lambda = 2\sqrt[n]{\frac{\text{Vol}(\mathbb{R}^n/\sigma(I^{-1})))}{\text{Vol}(X)}}$$

This gives

$$\text{Vol}(\lambda X) = 2^n \,\text{Vol}(\mathbb{R}^n/\sigma(I^{-1}))$$

which means we can now use our extension of Minkowski's theorem and find some a in λX which is also in $\sigma(\mathcal{O}(K))$. We can then take the ideal aI, which, since $a \in I^{-1}$, is an integral ideal in the same class as I.

We then have $N(aI) = N(I)n(a)$. Recalling the definition of the norm of an element in a number field, there must be a maximum element norm within the compact and convex X - we call that maximum norm M. The maximum norm over λX is likewise $\lambda^n M$ Thus, we have

$$\begin{aligned}N(aI) &\leq N(I)\lambda^n M \\ &\leq N(I)2^n \frac{\text{Vol}(\mathbb{R}^n/\sigma(I^{-1}))}{\text{Vol}(X)} \\ &\leq N(I)2^n \frac{\text{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}(K))}{\text{Vol}(X)N(I)} \\ &\leq 2^n \frac{\text{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}(K))}{\text{Vol}(X)}\end{aligned}$$

As the set X was chosen without regards to the ideal I, this last quantity is completely independent of I and applies to all fractional ideals I of K. Thus, we have shown that given a fractional ideal I, one can construct an integral ideal of the same class aI with a norm less than or equal to the finite bound $2^n \frac{\text{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}(K))}{\text{Vol}(X)}$.

This, in turn, means that every ideal class must have at least one ideal with norm less than or equal to $2^n \frac{\text{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}(K))}{\text{Vol}(X)}$. However, since there can only be a finite number of ideals

with norm less than or equal to any given value (and, of course, each such ideal belongs to exactly one class), there must be a finite number of ideal classes. ■

References

[Cox11] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[Lap06] Andrei Lapets. The ideal class group. 2006.

[Sim95] Patrick J Sime. On the ideal class group of real biquadratic fields. *Transactions of the American Mathematical Society*, 347(12):4855–4876, 1995.

Euler Circle, Palo Alto, CA 94306
E-mail address: arjun.b.venkatraman@gmail.com