Quadratic Forms and Class Groups

Oliver Cai

July 13, 2024

The Object of Interest

Definition

An integral **binary quadratic form** (abbreviated to just "form") is a function of the form $f(x, y) = ax^2 + bxy + cy^2$, for integers a,b,c.

The Object of Interest

Definition

An integral **binary quadratic form** (abbreviated to just "form") is a function of the form $f(x, y) = ax^2 + bxy + cy^2$, for integers a,b,c.

Definition

The **discriminant** of a binary quadratic form $ax^2 + bxy + cy^2$ is $b^2 - 4ac$.

Simplifications

Eventually, we will place these forms into equivalence classes, so we'll begin picking the nice ones.

Definition

A binary quadratic form is **reduced** if $|b| \leq a \leq c$, and $a = c$ or $a = |b|$ implies $b \geq 0$.

Simplifications

Eventually, we will place these forms into equivalence classes, so we'll begin picking the nice ones.

Definition

A binary quadratic form is **reduced** if $|b| \leq a \leq c$, and $a = c$ or $a = |b|$ implies $b \geq 0$.

Definition

A binary quadratic form is **primitive** if $\gcd(a, b, c) = 1$, and is **positive definite** if it only outputs nonnegative numbers, $a > 0$, and $f(x, y) = 0 \iff x = y = 0$.

It turns out that these two are equivalent.

Saving Words

Definition

A form $f(x, y)$ is **properly equivalent** to a form g if we have $f(x, y) = g(px + qy, rx + sy)$ and $ps - qr = 1$ (as opposed to ± 1 for just "equivalent") for $p, q, r, s \in \mathbb{Z}$.

Saving Words

Definition

A form $f(x, y)$ is **properly equivalent** to a form g if we have $f(x, y) = g(px + qy, rx + sy)$ and $ps - qr = 1$ (as opposed to ± 1 for just "equivalent") for $p, q, r, s \in \mathbb{Z}$.

Theorem

Primitive positive definite forms are properly equivalent to a unique reduced form.

Classes...

Proposition

Properly equivalent forms have equal discriminant.

Classes...

Proposition

Properly equivalent forms have equal discriminant.

Definition

The **class number** of D, denoted $h(D)$, is the number of primitive positive definite, binary quadratic forms with discriminant D.

Classes...

Proposition

Properly equivalent forms have equal discriminant.

Definition

The **class number** of D, denoted $h(D)$, is the number of primitive positive definite, binary quadratic forms with discriminant D.

Example

We have $h(-4) = 1$ since the only reduced, positive definite form with discriminant -4 is $x^2 + y^2$.

Classes...

Proposition

Properly equivalent forms have equal discriminant.

Definition

The **class number** of D, denoted $h(D)$, is the number of primitive positive definite, binary quadratic forms with discriminant D.

Example

We have $h(-4) = 1$ since the only reduced, positive definite form with discriminant -4 is $x^2 + y^2$.
On the other hand, $h(-20) = 2$; we have $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ with discriminant -20.

...and Groups

Theorem

Let the set of reduced forms with discriminant D be $C(D)$ with $D \equiv 0, 1 \pmod 4$ negative. Then $C(D)$ forms an abelian group of order $h(D)$ under composition, known as the **class group** *for binary quadratic forms with discriminant D.*

Composition is very complicated; we can restrict the notion of composition to obtain a formula. One restriction, **Dirichlet composition**, has the following requirements: to compose two forms $ax^2 + bxy + cy^2$ and $a'x^2 + b'xy + c'y^2$,

- The forms should have negative discriminant, and
- $\gcd\left(a, a', \frac{b+b'}{2}\right) = 1$.

A Useful Notion

We need a notion of "representing" an integer.

Definition

A binary quadratic form **represents** an integer n if we have $f(x, y) = n$ for some integral x, y. $f(x, y)$ **properly represents** n if we have $f(x, y) = n$ for relatively prime x, y.

For example, the form $f(x, y) = 2x^2 + 3xy + y^2$ properly represents 35 since $f(2, 3) = 35$.

Useful Lemmas

We will use these two lemmas:

Lemma

Given a reduced form $f(x, y)$ and $M \in \mathbb{Z}$, $f(x, y)$ can properly represent at least one integer relatively prime to M.

Lemma

A form $f(x, y)$ properly represents $m \in \mathbb{Z}$ if and only if we have $f(x, y)$ properly equivalent to $mx^2 + bxy + cy^2$ for some integer b, c.

Using Useful Lemmas

Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y)$ representatives of classes in $C(D)$.

By our first lemma, $g(x, y)$ represents a number a' that is relatively prime to a, and by our second lemma, $g(x, y)$ is properly equivalent to $g'(x, y) = a'x^2 + b'xy + c'y^2$ for integral a', b', c'.

Using Useful Lemmas

Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y)$ representatives of classes in $C(D)$.

By our first lemma, $g(x, y)$ represents a number a' that is relatively prime to a, and by our second lemma, $g(x, y)$ is properly equivalent to $g'(x, y) = a'x^2 + b'xy + c'y^2$ for integral a', b', c'.

So Dirichlet composition applies on $f(x, y)$ and $g'(x, y)$, so it is defined for any two pairs of classes in $C(D)$.

Using Useful Lemmas

Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y)$ representatives of classes in $C(D)$.

By our first lemma, $g(x, y)$ represents a number a' that is relatively prime to a, and by our second lemma, $g(x, y)$ is properly equivalent to $g'(x, y) = a'x^2 + b'xy + c'y^2$ for integral a', b', c'.

So Dirichlet composition applies on $f(x, y)$ and $g'(x, y)$, so it is defined for any two pairs of classes in $C(D)$.

We can check that Dirichlet composition is both well-defined for classes and that it induces a group directly from the definition. Proof: lots of algebra.

Cool, it's Finite

Theorem

$h(D)$ is finite for $D < 0$.

Recall that a form is reduced if $|b| \leq a \leq c$, and $a = c$ or $a = |b|$ implies $b \geq 0$.

Proof.

Use the conditions for a reduced form to bound a, b, c relative to each other. $\square$

This is a surprise tool that will help us later.

The Object of Interest

Definition

A complex number is an **algebraic integer** if it is the root of a monic polynomial with integral coefficients.

Definition

A **number field** is a subfield of $\mathbb{C}$ with finite degree as an extension of $\mathbb{Q}$.

Definition

The **ring of integers** or **number ring** $\mathcal{O}_K$ of a number field K is the set of algebraic integers in K. Equivalently, letting $\mathbb{A}$ be the set of algebraic integers in $\mathbb{C}$, we have $\mathcal{O}_K = K \cap \mathbb{A}$.

As an example, consider the number field $\mathbb{Q}(\sqrt{-1}) = \{\alpha + \beta i : \alpha, \beta \in \mathbb{Q}\}$. Then, its ring of integers is simply $\mathbb{Z}[i]$, also known as the Gaussian Integers.

More specifically...

Proposition

Let m be a squarefree (not divisible by the square of a prime) integer. Then, the set of algebraic integers in $\mathbb{Q}(\sqrt{m})$ is:

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}, m \equiv 2, 3 \pmod 4,$$

$$\left\{ \frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\}, m \equiv 1 \pmod 4.$$

Proof.

Write $\alpha = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, and note that $x^2 - 2rx + r^2 - ms^2$ is its corresponding polynomial. Check when the coefficients are integers. $\square$

The Ideal Class Group

Definition

Define an equivalence relation $\sim$ on the set of ideals of $\mathcal{O}$ by $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}$. The number of equivalence classes of ideals under $\sim$ is the **class number** of $\mathcal{O}$, denoted h. These equivalence classes also form a group under multiplication of ideals, which is known as the **ideal class group**.

Elements of the ideal class group are also known as **ideal classes**. For instance, consider the two principal ideals $(2i)$ and (3) in $\mathbb{Z}[i]$. These are equivalent since $3(2i) = 2i(3)$.

The Ideal Class Group

Definition

Define an equivalence relation $\sim$ on the set of ideals of $\mathcal{O}$ by $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}$. The number of equivalence classes of ideals under $\sim$ is the **class number** of $\mathcal{O}$, denoted h. These equivalence classes also form a group under multiplication of ideals, which is known as the **ideal class group**.

Elements of the ideal class group are also known as **ideal classes**.
For instance, consider the two principal ideals $(2i)$ and (3) in $\mathbb{Z}[i]$. These are equivalent since $3(2i) = 2i(3)$.

"Class group" and "class number" do sound familiar. I wonder why.

Why do we Care?

One reason is that the ideal class group can tell us if a number ring has unique factorization!

Theorem

If a number ring R has a trivial ideal class group, then it has unique factorization.

Proof.

Recall that a trivial group consists of the identity and nothing else.

Why do we Care?

One reason is that the ideal class group can tell us if a number ring has unique factorization!

Theorem

If a number ring R has a trivial ideal class group, then it has unique factorization.

Proof.

Recall that a trivial group consists of the identity and nothing else. The principal ideals form the identity for the ideal class group.

Why do we Care?

One reason is that the ideal class group can tell us if a number ring has unique factorization!

Theorem

If a number ring R has a trivial ideal class group, then it has unique factorization.

Proof.

Recall that a trivial group consists of the identity and nothing else.
The principal ideals form the identity for the ideal class group.
Thus, a trivial ideal class group implies that all ideals are principal, so R is a principal ideal domain, and thus has unique factorization. $\square$

Also a Group

Proposition

For every ideal $\mathfrak{a}$ of a number ring R, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal.

Also a Group

Proposition

For every ideal $\mathfrak{a}$ of a number ring R, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal.

This lets us take inverses in the set of ideal classes, rounding out this corollary:

Corollary

The ideal classes in a number ring form a group under multiplication of ideals.

The Main Point

Theorem

The ideal class group of any number ring is finite.

The proof involves thinking of the number ring as a lattice, then thinking about volumes in that lattice.

The Main Point

Theorem

The ideal class group of any number ring is finite.

The proof involves thinking of the number ring as a lattice, then thinking about volumes in that lattice.

We are more interested in the case of quadratic number rings, so let's set that up.

Mostly the Main Point

The **discriminant** of a number field $Q(\sqrt{D})$ is an invariant of the number field. For the quadratic case, one can show that it's equal to

$$\begin{cases} d, & d \equiv 1 \pmod 4, \\ 4d, & d \equiv 2,3 \pmod 4. \end{cases}$$

Theorem

The class group for quadratic forms with discriminant D is isomorphic to the ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$ for $D < 0$.
In particular, the isomorphism takes the primitive positive definite binary quadratic form $ax^2 + bxy + cy^2$ to the ideal generated by the set $\left\{a, \frac{-b+\sqrt{D}}{2}\right\}$.

In Particular,

Corollary

The ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$ *is finite for* $D < 0$.

In Particular,

Corollary

The ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$ is finite for $D < 0$.

Recall:

Theorem

$h(D)$ is finite for $D < 0$.

In Particular,

Corollary

The ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$ is finite for $D < 0$.

Recall:

Theorem

$h(D)$ is finite for $D < 0$.

Proof.

Let the ring of integers of $\mathbb{Q}(\sqrt{D})$ be $\mathcal{O}$. Then $\mathcal{O}$ has the same cardinality as the class group of quadratic forms with discriminant D, which we know to be finite. □