Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Imaginary Quadratic Fields
   - Units
   - Euclidean Imaginary Quadratic Fields
   - Quadratic Forms
   - Reduction Theory
   - Class Numbers and Quadratic Forms
   - Counting Quadratic Forms

The Objects of Study

- Throughout this set, we will be considering a field
$$K = \mathbb{Q}(\sqrt{d}),$$
where d is a negative, squarefree integer.
- That is, d is not divisible by the square of any prime.
- Every imaginary quadratic field can be written in this way for a unique choice of d.
- By a previous proposition, the ring of integers is:
  - $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, if $d \equiv 1 \pmod 4$;
  - $\mathbb{Z}[\sqrt{d}]$, otherwise.
- As d is squarefree, d is not divisible by the square of any prime.

  So the case $d \equiv 0 \pmod 4$ is not permitted.

  That is, the second case arises when $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$.

The Goals

- Our goal in this set is to:
  - Determine the fields with unique factorization;
  - Understand the failure of unique factorization in the other cases.
- We will see that there are very few imaginary quadratic fields with unique factorization.

Subsection 1

Units

Imaginary versus Real Quadratic Fields

- One difference between the case of imaginary quadratic fields and that of real quadratic fields concerns the group of units.
  - We will see that real quadratic fields have infinitely many units.
  - Imaginary quadratic fields will have only finitely many units.
    They are all roots of unity, and they are easy to determine.
- We shall see later that imaginary quadratic fields are the only fields other than $\mathbb{Q}$ for which the ring of integers has a finite group of units.
- By a previous lemma, $\alpha \in \mathbb{Z}_K$ is a unit precisely when $N(\alpha) = 1$.
- Since there are two possibilities for $\mathbb{Z}_K$, depending on $d \pmod 4$, we will divide the calculation into two cases.

$d \equiv 2,3 \pmod 4$

- In this case, we have

  $$\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}].$$

  Then a typical element is

  $$\alpha = a + b\sqrt{d},$$

  where a and b are in $\mathbb{Z}$.

  The norm of α is

  $$N_{K/\mathbb{Q}}(\alpha) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2.$$

  We need to solve the equation

  $$N_{K/\mathbb{Q}}(\alpha) = 1.$$

$d \equiv 2, 3 \pmod 4$ (Cont'd)

- Notice that:
  - a^2 is a non-negative integer;
  - $-db^2$ is also a non-negative integer (as $d < 0$).

  Since they add to 1, one of them is 0, and the other is 1.
  - Suppose $a^2 = 1$ and $-db^2 = 0$.
    Then $a = \pm 1$ and $b = 0$ (as $d \neq 0$).
    So ± 1 is always a unit (obviously invertible in $\mathbb{Z}_K$).
  - The other case is where $a^2 = 0$ and $-db^2 = 1$.
    If $d < -1$, then there is clearly no solution to $-db^2 = 1$.
    However, if $d = -1$, then $b = \pm 1$ is also possible.
    So in the field $\mathbb{Q}(\sqrt{-1})$, we also have units $0 \pm \sqrt{-1}$.
    In other words, $\pm i$ are units.

$d \equiv 1 \pmod 4$

- The ring of integers is now
$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$
A typical element is therefore
$$\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) = \frac{2a+b+b\sqrt{d}}{2}.$$
Again, we must compute the norm of α.
$$N(\alpha) = \alpha\overline{\alpha} = \frac{(2a+b+b\sqrt{d})(2a+b-b\sqrt{d})}{4} = \frac{(2a+b)^2-db^2}{4}.$$
Thus the equality $N(\alpha)=1$ is equivalent to finding integral solutions to
$$(2a+b)^2-db^2=4.$$

$d \equiv 1 \pmod 4$ ($d < -3$)

- We seek the integral solutions to $(2a+b)^2 - db^2 = 4$.
- Consider the case where $d < -3$.

  Then $d \leq -7$ (since $d \equiv 1 \pmod 4$).

  If $b \neq 0$, then $-db^2 \geq 7$.

  As $(2a+b)^2 \geq 0$, there are no solutions.

  So $b = 0$.

  In this case, our equation becomes $(2a+0)^2 = 4$.

  So $a = \pm 1$.

  So ± 1 are the only units in this case.

$d \equiv 1 \pmod 4$ ($d = -3$)

- Consider the case $d = -3$.

  Suppose $|b| \geq 2$. Then $-db^2 \geq 12$.

  So $(2a+b)^2 - db^2 = 4$ has no solutions.

  The only possible solutions occur when $b = -1, 0$ or 1.

  - Suppose $b = -1$. Then we must solve $(2a-1)^2 + 3 = 4$.
    This gives $2a - 1 = \pm 1$. So $a = 0$ or 1.
  - Suppose $b = 0$. Then we must solve $(2a)^2 = 4$.
    This gives $a = \pm 1$.
  - Suppose $b = 1$. Then we must solve $(2a+1)^2 + 3 = 4$.
    This gives $2a + 1 = \pm 1$. So $a = -1$ or 0.

  So $(a,b) = (0,-1)$, $(1,-1)$, $(-1,0)$, $(1,0)$, $(-1,1)$, $(0,1)$.

$d \equiv 1 \pmod 4$ ($d = -3$ Cont'd)

- We got $(a,b) = (0,-1)$, $(1,-1)$, $(-1,0)$, $(1,0)$, $(-1,1)$, $(0,1)$.

  The corresponding units $\alpha = a + b\frac{1+\sqrt{-3}}{2}$ are given by

  $$\frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -1, 1, \frac{-1+\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}.$$

  The numbers $\frac{\pm 1 \pm \sqrt{-3}}{2}$ and ± 1 are the sixth roots of unity.

  Denote

  $$\omega = \frac{-1+\sqrt{-3}}{2} = e^{2\pi i/3}.$$

  The ring of integers of $\mathbb{Q}(\sqrt{-3})$ is given by $\mathbb{Z}[\sqrt{-3}]$.

  We have $\omega^2 = e^{4\pi i/3} = \frac{-1-\sqrt{-3}}{2}$.

  So the units are given by $\{\pm 1, \pm\omega, \pm\omega^2\}$.

Summary

- We have shown that the only units in the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ are the elements of $\{\pm 1\}$, except in two cases.
  - The first is when $d = -1$.
    The units in the Gaussian integers $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.
  - The other exceptional case is when $d = -3$.
    The units in the ring of integers $\mathbb{Z}[\omega]$ of $\mathbb{Q}(\sqrt{-3})$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$.
- Notice that these units are all roots of unity, fourth roots, in the case of $\mathbb{Q}(i)$, and sixth roots in the case of $\mathbb{Q}(\sqrt{-3})$.

  So the units in every imaginary quadratic field are the roots of unity.
- Conversely, it is easy to see that every root of unity is a unit.

  Suppose λ is a root of unity in $\mathbb{Z}_K$.

  Then $\lambda^n = 1$ for some n. Then $\lambda \cdot \lambda^{n-1} = 1$.

  So λ is invertible, with inverse λ^{n-1} (which lies in $\mathbb{Z}_K$, as $\lambda \in \mathbb{Z}_K$ and $\mathbb{Z}_K$ is a ring).

Summarizing Theorem

- Write μ_k for the set of kth roots of unity in $\mathbb{C}$.
- We have proven the following result.

Theorem

Let $K = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z}_{<0}$ squarefree. Then λ is a unit in $\mathbb{Z}_K$ if and only if λ is a root of unity. Moreover, the units in $\mathbb{Z}_K$ are:

$$U(\mathbb{Z}_K) = \mathbb{Z}_K^\times = \begin{cases} \mu_4 = \{\pm 1, \pm i\}, & \text{if } d = -1, \\ \mu_6 = \{\pm 1, \pm \omega, \pm \omega^2\}, & \text{if } d = -3, \\ \mu_2 = \{\pm 1\}, & \text{otherwise.} \end{cases}$$

Subsection 2

Euclidean Imaginary Quadratic Fields

Unique Factorization and Euclidean Norms

- We have seen that the Gaussian integers $\mathbb{Z}[i]$ possess unique factorization.
- The proof involved showing that the norm function is Euclidean.
- Therefore, $\mathbb{Z}[i]$ is a Euclidean domain using this norm function.
- We now work out which imaginary quadratic fields can be shown to have unique factorization in the same way.
- That is, when the ring of integers is a Euclidean domain.
- We shall see later that there are imaginary quadratic fields with unique factorization which are not Euclidean in this sense.
- This provides examples of UFDs which are not Euclidean.

The Euclidean Condition

- Choose any α and β in $\mathbb{Z}_K$.
- For the norm function to be Euclidean, we must be able to find a quotient $\kappa \in \mathbb{Z}_K$ and a remainder $\rho \in \mathbb{Z}_K$, such that

$$\alpha = \kappa\beta + \rho, \quad N(\rho) < N(\beta).$$

- The method involves the following steps:
  - Consider the quotient $\frac{\alpha}{\beta}$;
  - Define κ to be the integer "closest" to it;
  - Define $\rho = \alpha - \kappa\beta$.

The Euclidean Condition (Cont'd)

- Then we have
$$\rho = \alpha - \kappa\beta = \beta\left(\frac{\alpha}{\beta} - \kappa\right).$$
- So we get
$$N(\rho) = N(\beta)N\left(\frac{\alpha}{\beta} - \kappa\right).$$
- So $N(\rho) < N(\beta)$ as long as $N(\frac{\alpha}{\beta} - \kappa) < 1$.
- In particular, $\mathbb{Z}_K$ is Euclidean if, for any $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{d})$, there is $\kappa \in \mathbb{Z}_K$, such that
$$N\left(\frac{\alpha}{\beta} - \kappa\right) < 1.$$
- The two different forms of $\mathbb{Z}_K$ impose studying two separate cases.

$d \equiv 2, 3 \pmod 4$

- We have
$$\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}].$$
Suppose that
$$\frac{\alpha}{\beta} = a + b\sqrt{d}, \quad a, b \in \mathbb{Q}.$$
We choose κ to be the "nearest" integer $m + n\sqrt{d} \in \mathbb{Z}_K$. This means choosing
$$|m - a| \le \frac{1}{2} \quad \text{and} \quad |n - b| \le \frac{1}{2}.$$
Then
$$\begin{array}{rcl} N(\frac{\alpha}{\beta} - \kappa) & = & N((a + b\sqrt{d}) - (m + n\sqrt{d})) \\ & = & N((a - m) + \sqrt{d}(b - n)) \\ & = & (a - m)^2 - d(b - n)^2 \\ & \le & (\frac{1}{2})^2 - d(\frac{1}{2})^2. \end{array}$$

$d \equiv 2,3 \pmod 4$ (Cont'd)

- We study two subcases regarding

$$N\left(\frac{\alpha}{\beta}-\kappa\right) \leq \left(\frac{1}{2}\right)^2 - d\left(\frac{1}{2}\right)^2.$$

  - Suppose $d=-1$ or -2.
    Then $N(\frac{\alpha}{\beta}-\kappa)<1$.
  - Suppose $d \leq -5$.
    Then there are quotients $\frac{\alpha}{\beta}$, with no integer κ satisfying

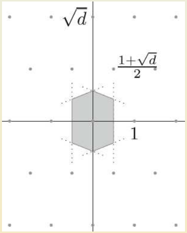
$$N\left(\frac{\alpha}{\beta}-\kappa\right)<1.$$

    E.g., just take $\alpha=1+\sqrt{d}$, $\beta=2$.

Thus, the only imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$, with $d \equiv 2,3 \pmod 4$, which are Euclidean with respect to the norm function are $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$.

$d \equiv 1 \pmod{4}$

- Now we have
$$\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$
Suppose that
$$\frac{\alpha}{\beta} = a + b\sqrt{d}, \quad a, b \in \mathbb{Q}.$$



Choose κ to be the "nearest" integer $m + n\sqrt{d} \in \mathbb{Z}_K$.

However, $\mathbb{Z}_K$ now looks a little different.

It is the collection of points nearest to the origin lie in the shaded hexagon.

As in the first case, it will do to show that every point in $\mathbb{Q}(\sqrt{d})$ lies at a distance strictly less than 1 from some point in $\mathbb{Z}_K$.

The Vertices of the Hexagon

- That is, it would suffice that the hexagon above lie inside the unit circle.

  Since the edges are given by the bisectors of the lines joining the origin and the points ±1 and $\frac{\pm 1 \pm \sqrt{d}}{2}$, computing the vertices of the hexagon is elementary.

  View the hexagon above as plotted in the (x,y)-plane, and bounded by the bisectors of the lines joining $(0,0)$ to $(\pm 1,0)$ and to $(\pm\frac{1}{2}, \pm\frac{\sqrt{|d|}}{2})$, with $|d| > 1$.

  Then the vertices of the hexagon above are at

$$\left(0, \pm\frac{|d|+1}{4\sqrt{|d|}}\right) \quad \text{and} \quad \left(\pm\frac{1}{2}, \pm\frac{|d|-1}{4\sqrt{|d|}}\right).$$

$d \equiv 1 \pmod 4$ (Cont'd)

- It is now easy to check that if $d = -3$, $d = -7$ or $d = -11$, the hexagon lies entirely within the unit circle.

  The corresponding field then has a Euclidean algorithm.
- However, if $d \leq -19$, then $\sqrt{|d|} > 4$.

  The hexagon then contains points of $\mathbb{Q}(\sqrt{d})$ at a distance of more than 1 from any point of $\mathbb{Z}_K$ (e.g., $\frac{1}{4}\sqrt{d}$).

  So there can be no Euclidean algorithm using the norm function.
- We conclude that there are only five imaginary quadratic fields, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-11})$ which are Euclidean with respect to their norm function.
- It follows from a previous proposition and theorem that these five fields all have unique factorization.

Norms and Euclidean Functions

- We have now seen that there are exactly five imaginary quadratic fields whose rings of integers are Euclidean domains with respect to their norm function.
- Could there be other functions, different from the norm function, which make other rings of integers into Euclidean domains?
- It turns out that this is false.
- We give the complete argument below for the case $d \equiv 1 \pmod{4}$.
- The other case can be treated similarly.

Universal Side Divisor

Theorem

Suppose that R is a Euclidean domain with respect to a Euclidean function ϕ, but that R is not a field. Then there is a non-zero element u of R, which is not a unit, such that for all $x \in R$,

$$\text{either } u \mid x, \text{ or } u \mid x - v, \text{ for some unit } v \in R.$$

- Let S denote the set of non-zero elements of R which are not units.

  As R is not a field, S is not empty.

  Consider

  $$\phi(S) = \{\phi(s) : s \in S\}.$$

  $\phi(r)$ is a positive integer, for all $r \in R$.

  Choose $u \in S$, with $\phi(u)$ minimal amongst all the values in $\phi(S)$.

Universal Side Divisor (Cont'd)

- Let $x \in R$. By the Euclidean property
$$x = qu + r,$$
where either $r = 0$, or $\phi(r) < \phi(u)$.

  Suppose $r = 0$. Then $x = qu$. So $u \mid x$.

  Suppose $\phi(r) < \phi(u)$.

  $\phi(u)$ was the smallest value in $\phi(S)$.

  So we cannot have $r \in S$.

  Since $r \notin S$ and $r \neq 0$, we must have that r is a unit in R.

  Write v for this unit.

  Then $qu = x - v$ shows that $u \mid x - v$.
- The element u is often called a **universal side divisor**.

Criterion for Non-Euclidean Integral Domains

Corollary

Suppose that R is an integral domain that is not a field. If there are no elements u as in the theorem, then R is not Euclidean.

- Directly by the theorem.

Non-Euclidean Imaginary Quadratic Fields

Theorem

Suppose that $K = \mathbb{Q}(\sqrt{d})$ with d squarefree and negative. Suppose that $d \equiv 1 \pmod 4$, and that $d < -11$. Then $\mathbb{Z}_K$ is not Euclidean.

- By the corollary, we must show $\mathbb{Z}_K$ has no universal side divisor.

  Suppose to the contrary, such an element u exists.

  We know that $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

  By a previous theorem, the units in $\mathbb{Z}_K$ are simply $\{\pm 1\}$.

  By the property, for all $\alpha \in \mathbb{Z}_K$, we have $u \mid \alpha$, or $u \mid \alpha \pm 1$.

  We apply this with $\alpha = 2$. So we need $u \mid 2$, or $u \mid 2 \pm 1$.

  That is, u divides 1, 2 or 3.

  But u cannot divide 1, since u is not a unit.

  So u is a divisor of either 2 or 3.

Non-Euclidean Imaginary Quadratic Fields (Cont'd)

- We show that 2 and 3 are irreducible.

  If not, there would be some element β of norm 2 or 3.

  Suppose $\beta = a + b(\frac{1+\sqrt{d}}{2})$. Then

  $$N_{K/\mathbb{Q}}(\beta) = a^2 + ab + b^2\left(\frac{1-d}{4}\right).$$

  Now $d < -11$. So $k = \frac{1-d}{4} \geq 4$.

  We can see that

  $$a^2 + ab + kb^2 = 2 \quad \text{and} \quad a^2 + ab + kb^2 = 3$$

  have no solution for $k \geq 4$.

  Once $b \neq 0$, the left-hand side is too large.

  Then there is clearly no solution for a.

  So both 2 and 3 are irreducible.

Non-Euclidean Imaginary Quadratic Fields (Conclusion)

- Now u divides either 2 or 3.

  So we must have $u = 2, -2, 3$ or -3.

  Now take $\alpha = \frac{1+\sqrt{d}}{2}$ instead.

  Again, we should have $u \mid \alpha$ or $u \mid \alpha \pm 1$.

  However, none of these elements have ± 2 or ± 3 as divisors.

  So there can be no element u, and so $\mathbb{Z}_K$ is not Euclidean.
- A very similar argument applies in the remaining cases.

Theorem

Suppose that $K = \mathbb{Q}(\sqrt{d})$, with $d < 0$ squarefree.
Then $\mathbb{Z}_K$ is Euclidean if and only if $d = -1, -2, -3, -7$ or -11.

Subsection 3

Quadratic Forms

Significance of the Class Group

- As already remarked, the class group may be viewed as the obstruction to unique factorization.
  - If the class group is trivial, then the number field has unique factorization.
  - Otherwise unique factorization fails.
- We would like a way to calculate the class group to be able to ascertain whether or not the field has unique factorization.

Quadratic Forms

- We will show that the class number can be computed by counting a certain set of "binary quadratic forms".

Definition

A **quadratic form in n variables** is a homogeneous polynomial of degree 2, and is, therefore, of the form

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j.$$

- If we write $\boldsymbol{v}=(x_1\cdots x_n)^t$, and A for the matrix (a_{ij}), then we can write the form as

$$\boldsymbol{v}^tA\boldsymbol{v}.$$

- We will only consider the situation where $a_{ij}\in\mathbb{Z}$.

Binary Quadratic Forms and Discriminant

- We will focus on the case where $n=2$.

Definition

A **binary quadratic form** is a quadratic form in 2 variables, and is, therefore, of the form

$$f(x,y)=ax^2+bxy+cy^2,$$

for some $a,b,c\in\mathbb{Z}$. The **discriminant** of this form is b^2-4ac. We may abbreviate the form $ax^2+bxy+cy^2$ by (a,b,c).

Example: Consider the form x^2+y^2.

Its discriminant is -4.

The discriminant of $x^2+(-d)y^2$ is $4d$.

Positive Definite Quadratic Forms

Definition

Say that a quadratic form $f(x,y)$ is **positive definite** if:

1. $f(x,y) \geq 0$, for all $x, y \in \mathbb{R}$;
2. $f(x,y) = 0$ means that we must have $(x,y) = (0,0)$.

A quadratic form is **positive semi-definite** if $f(x,y) \geq 0$, for all $x, y \in \mathbb{R}$. Forms which take both positive and negative values are known as **indefinite**.

- There is a similar definition of **negative definite** and **negative semi-definite**, got by changing the sign in the inequality.

Positive Definite Forms and Discriminant

Corollary

The quadratic form $ax^2+bxy+cy^2$ is positive definite if and only if $a>0$ and the discriminant $b^2-4ac<0$.

- Suppose that $(a,b,c)=ax^2+bxy+cy^2$ is positive definite.

  If $a \not> 0$, substituting $(x,y)=(1,0)$ gives a negative value.

  If $c \not> 0$, $(x,y)=(0,1)$ would give something negative.

  Completing the square, we get:

  $$ax^2+bxy+cy^2=a\left(x+\frac{b}{2a}y\right)^2+\left(c-\frac{b^2}{4a}\right)y^2.$$

  Now $c>0$ may be refined into $c-\frac{b^2}{4a}>0$.

  Otherwise, $(x,y)=(-b,2a)$ would give a negative value to the form.

  As $a>0$, this is equivalent to $b^2-4ac<0$.

Imaginary Quadratic Fields and Quadratic Forms

- Recall that the norm of a complex number $x+iy$ is
$$N(x+iy)=(x+iy)(x-iy)=x^2+y^2.$$
- Notice that x^2+y^2 is a positive definite quadratic form.
- More generally, consider the complex number $x+y\sqrt{d}$ (where d is a negative, squarefree integer).
- Its norm is
$$x^2+(-d)y^2.$$
- We have started with a general element in an imaginary quadratic field and in both cases have recovered a positive definite binary quadratic form.

Introducing Equivalence of Quadratic Forms

- Two apparently different forms may really share many properties.
- I.e., they may, in some sense, be the same.

  Example: Consider the form
  $$x^2+2xy+2y^2.$$
  It can be rewritten
  $$(x+y)^2+y^2.$$
  A simple change of variable $X=x+y$, $Y=y$ allows us to write this as
  $$X^2+Y^2.$$
- For many applications, we may wish to regard the form $x^2+2xy+2y^2$ as equivalent to the form x^2+y^2.

Equivalent Quadratic Forms

Definition

Two quadratic forms $f(x,y)$ and $g(x,y)$ are **equivalent** if one can be transformed into the other by a substitution of the form

$$(x,y) \mapsto (px+qy, rx+sy),$$

where p,q,r,s are integers with $ps-qr=\pm 1$. That is, $f(x,y)$ and $g(x,y)$ are equivalent if $g(x,y)=f(px+qy,rx+sy)$, for some invertible matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$, the **general linear group** of 2×2 matrices with integer entries whose inverse also has integer entries.

If $ps-qr=+1$, we say that $f(x,y)$ and $g(x,y)$ are **properly equivalent** (and in this case the matrix above lies in $\mathrm{SL}_2(\mathbb{Z})$, the **special linear group** of 2×2 matrices with determinant 1).

Matrix Formulation of Equivalence

- Suppose
$$f(x,y)=\boldsymbol{v}^tA\boldsymbol{v}.$$
- Let
$$M=\begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$
- Then
$$M\boldsymbol{v}=\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} px+qy \\ rx+sy \end{pmatrix}.$$
- So we obtain
$$f(px+qy,rx+sy)=(M\boldsymbol{v})^tA(M\boldsymbol{v})=\boldsymbol{v}^t(M^tAM)\boldsymbol{v}.$$
- Thus, in terms of matrices, if f and g correspond to matrices A and B, respectively, then f and g are:
  - Equivalent if there exists $M\in \mathrm{GL}_2(\mathbb{Z})$, with $B=M^tAM$;
  - Properly equivalent if there exists $M\in \mathrm{SL}_2(\mathbb{Z})$, with $B=M^tAM$.

Subsection 4

Reduction Theory

Reduced Form of a Quadratic Form

- Reduction theory is an elegant theory which allows us to determine when two quadratic forms are properly equivalent.
  - If we are given a general (positive definite binary) quadratic form, then we can "reduce" it to a particular "reduced" form;
  - Two forms are properly equivalent precisely when they both reduce to the same form.

Definition

We say that a form

$$(a,b,c) = ax^2 + bxy + cy^2$$

is **reduced** if either $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

- The precise conditions in the definition are chosen so that:
  - Every form is properly equivalent to some reduced form;
  - No two different reduced forms are properly equivalent.

Basic Proper Equivalences

- We defined proper equivalence using matrices of determinant 1.
- We now isolate some special cases (seen later to generate $\mathrm{SL}_2(\mathbb{Z})$).
- Consider the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

- I.e., consider the transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix}.$$

- The form $ax^2+bxy+cy^2$ is then properly equivalent to

$$a(x+y)^2+b(x+y)y+cy^2.$$

- This expands to

$$ax^2+(2a+b)xy+(a+b+c)y^2.$$

- Thus, (a,b,c) is properly equivalent to $(a,b+2a,c+b+a)$.

Basic Proper Equivalences (Cont'd)

- The inverse transformation corresponds to the matrix

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

- Now we get

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x-y \\ y \end{pmatrix}.$$

- The form $ax^2+bxy+cy^2$ is then properly equivalent to

$$a(x-y)^2+b(x-y)y+cy^2 = ax^2+(-2a+b)xy+(a-b+c)y^2.$$

- So (a,b,c) is properly equivalent to $(a,b-2a,c-b+a)$.

Basic Proper Equivalences (Cont'd)

- We also use the transformation corresponding to

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

- We get

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ -x \end{pmatrix}.$$

- The form $ax^2 + bxy + cy^2$ is then properly equivalent to

$$ay^2 - bxy + c(-x)^2 = cx^2 - bxy + ay^2.$$

- So (a, b, c) is properly equivalent to $(c, -b, a)$.

Existence of a Reduced Form

- Using these three transformations only, any binary positive definite quadratic form can be seen to be equivalent to a reduced form.
- Take a positive definite binary quadratic form

$$(a,b,c) = ax^2 + bxy + cy^2, \quad a,c > 0.$$

- Apply the following rules repeatedly.
- Suppose $a > c$ or $a = c$ and $b < 0$.

  Apply the third rule and perform the transformation

$$(a,b,c) \mapsto (c,-b,a).$$

  In the first case, $c < a$.

  In the second case, $c = a$ and $0 < -b$.

Existence of a Reduced Form (Cont'd)

- Otherwise, we are in one of two situations:
- We could have $a < c$.

  If (a, b, c) is not reduced, it must be because $b \leq -a$ or $b > a$.

  If $b \leq -a$, apply the first rule, $(a, b, c) \mapsto (a, b + 2a, c + b + a)$.

  If $b > a$, apply the second rule $(a, b, c) \mapsto (a, b - 2a, c - b + a)$.

  The result should be a form for which the absolute value $|b|$ of the middle coefficient gets smaller (except in case $b = -a$, when $|b|$ may remain constant for a step).
- Alternatively, $a = c$ and $b \geq 0$.

  If (a, b, c) is not reduced, it must be because $b > a$.

  Then apply the second rule $(a, b, c) \mapsto (a, b - 2a, c - b + a)$.

  The result should again be a form for which the absolute value $|b|$ of the middle coefficient gets smaller.

Example

- Consider the form $7x^2 - 24xy + 21y^2$, or $(7, -24, 21)$ in shorthand.

  This is not reduced, as we do not have $-a < b \leq a$.

  But we do have $a < c$.
  - We apply the first rule, to get $(7, -24, 21) \mapsto (7, -10, 4)$.
    The new form is not reduced because $c < a$.
  - We apply the third rule $(7, -10, 4) \mapsto (4, 10, 7)$.
    The form $(4, 10, 7)$ is not reduced as $b > a$.
  - We apply the third rule to get $(4, 10, 7) \mapsto (4, 2, 1)$.
    We still do not have a reduced form, as $a > c$.
  - We apply the third rule to get $(4, 2, 1) \mapsto (1, -2, 4)$.
    The form $(1, -2, 4)$ is not reduced as $-a \geq b$.
  - The first rule finally gives $(1, -2, 4) \mapsto (1, 0, 3)$.
    This form is reduced.

Using Matrices: Transformation 1

- One way to follow the transformations is to keep track of the changes of variable required.
- Alternatively, we can think about the matrix transformations involved.
- The first time that we applied the rule $(a,b,c) \mapsto (a,b+2a,c+b+a)$, we essentially made the change of variable $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$.

  This means that we make the transformation $(x,y) \mapsto (x+y,y)$.

  We can check $7(x+y)^2 - 24(x+y)y + 21y^2 = 7x^2 - 10xy + 4y^2$.

  Let $f_0 = (7,-24,21)$, $f_1 = (7,-10,4)$ and $M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

  Then we have
  $$f_0\left(M_1 \begin{pmatrix} x \\ y \end{pmatrix}\right) = f_1\left(\begin{pmatrix} x \\ y \end{pmatrix}\right).$$

Using Matrices: Inverse of Transformation 1

- Write
$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = M_1 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix}.$$
Apply the inverse matrix to write (x,y) in terms of (x_1,y_1):
$$\begin{pmatrix} x \\ y \end{pmatrix} = M_1^{-1} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_1 - y_1 \\ y_1 \end{pmatrix}.$$
We therefore see
$$f_0\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = f_1\left(M_1^{-1}\begin{pmatrix} x \\ y \end{pmatrix}\right).$$
I.e., $7x_1^2 - 24x_1y_1 + 21y_1^2 = 7(x_1-y_1)^2 - 10(x_1-y_1)y_1 + 4y_1^2$.
So, if $\boldsymbol{v} = \begin{pmatrix} x \\ y \end{pmatrix}$, $f_0(M_1\boldsymbol{v}) = f_1(\boldsymbol{v})$ and $f_0(\boldsymbol{v}) = f_1(M_1^{-1}\boldsymbol{v})$.

Using Matrices: Transformation 2

- Next we applied the third rule $(a,b,c) \mapsto (c,-b,a)$ to f_1.

  We already noted that this corresponds to the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

  We can write f_2 for the form $(4,10,7)$.
  We should have $f_1(M_2\boldsymbol{v}) = f_2(\boldsymbol{v})$ and $f_1(\boldsymbol{v}) = f_2(M_2^{-1}\boldsymbol{v})$.
  We already know that $f_0(M_1\boldsymbol{v}) = f_1(\boldsymbol{v})$ and $f_0(\boldsymbol{v}) = f_1(M_1^{-1}\boldsymbol{v})$.
  Combining, we get $f_2(\boldsymbol{v}) = f_1(M_2\boldsymbol{v}) = f_0(M_1(M_2\boldsymbol{v}))$.
  Recall that $\boldsymbol{v} = \begin{pmatrix} x \\ y \end{pmatrix}$, $M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
  So we get

  $$f_2(x,y) = f_0\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) = f_0(-x+y,-x).$$

  This can easily be verified by a simple calculation.

Using Matrices: Transformation 3-5

- Continuing, we get $M_3 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $M_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $M_5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are the matrices for the remaining three steps.

  We also have, in the final step, $f_5 = (1,0,3) = x^2 + 3y^2$.

  It follows that
  $$f_5(x,y) = f_0(M_1 M_2 M_3 M_4 M_5 (x,y)^t).$$

  We calculate that $M = M_1 M_2 M_3 M_4 M_5 = \begin{pmatrix} -2 & -3 \\ -1 & -2 \end{pmatrix}$.

  Moreover, we verify

$$\begin{aligned} f_0\left(M\begin{pmatrix} x \\ y \end{pmatrix}\right) &= 7(-2x-3y)^2 - 24(-2x-3y)(-x-2y) + 21(-x-2y)^2 \\ &= x^2 + 3y^2. \end{aligned}$$

Reduced Forms and Values for Coprime x, y

Lemma

Suppose that

$$f(x,y) = ax^2 + bxy + cy^2$$

is in reduced form.

- If $a < c$, then the smallest non-zero values taken by $f(x,y)$, for x and y coprime, are a and c. Furthermore, the only values of (x,y) with $f(x,y) = a$ are $(\pm 1, 0)$.
- If $a = c$, then the smallest non-zero value of $f(x,y)$ is a. There are either 4 (if $0 \leq b < a = c$) or 6 (if $a = b = c$) pairs (x,y) with $f(x,y) = a$.

- Suppose, first, $y = 0$.

  As $(x,y) = 1$, $x = \pm 1$.

  Hence, $f(\pm 1, 0) = a$.

Reduced Forms and Values for Coprime x, y (Cont'd)

- Suppose, next, $|y| = 1$ and $|x| \geq 2$.

  Then
  $$|2ax + by| \geq |2ax| - |by| \geq 4a - |b| \overset{|b| \leq a}{\geq} 3a.$$

  So
  $$\begin{array}{rcl} 4af(x,y) & = & (2ax+by)^2 - dy^2 \\ & \geq & 9a^2 - d \\ & = & 4ac + (9a^2 - b^2) \\ & = & 4ac + 8a^2 + (a^2 - b^2) \\ & \overset{|b| \leq a}{\geq} & 4ac. \end{array}$$

  So $f(x, \pm 1) > c$, if $|x| \geq 2$.

Reduced Forms and Values for Coprime x, y (Cont'd)

- If $|y| \geq 2$, then

$$\begin{array}{rcl} 4af(x,y) & = & (2ax+by)^2 - dy^2 \\ & \geq & -dy^2 \\ & \geq & -4d \\ & = & 16ac - 4b^2 \\ & \geq & 12ac + 4(ac - b^2) \\ & \overset{|b| \leq a \leq c}{\geq} & 12ac \\ & \geq & 4ac. \end{array}$$

Again, $f(x,y) > c$, if $|y| \geq 2$.

In summary, $f(x,y) > c$, if $|x| \geq 2$ or $|y| \geq 2$.

Finally, $f(\pm 1, 0) = a$, $f(0, \pm 1) = c$, $f(\pm 1, \pm 1) = a + b + c > c$ and $f(\pm 1, \mp 1) = a - b + c \geq c$. The result follows easily in each case.

Existence and Uniqueness of Reduced Forms (Existence)

Theorem

Every positive definite binary quadratic form is properly equivalent to a unique reduced form.

- Firstly, we verify that the algorithmic process for reducing quadratic forms terminates after a finite number of steps with a reduced form.

  At each step, none of the operations increase the coefficient of x^2.

  As this is a natural number, eventually it must become constant.

  At this point, the remaining operations do not increase $|b|$.

  Again eventually $|b|$ must become constant.

  Suppose that a rule maps (a,b,c) to a form with the same values of a and $|b|$. This is only possible if one of the following cases.
  - $a=b$ (and then c is also fixed, as the discriminant b^2-4ac is fixed);
  - if $a=-b$, and the first rule $(a,b,c)\mapsto(a,b+2a,c+b+a)$ is applied. Then $a=b\leq c$, and the form is now reduced.

  Thus, every form is equivalent to some reduced form.

Existence and Uniqueness of Reduced Forms (Uniqueness)

- If a form were equivalent to two different reduced forms, then these reduced forms would be equivalent to each other.

  So in the final step we show that two distinct reduced forms cannot be equivalent to each other.

  Suppose that

  $$\begin{array}{rcl} f(x,y) & = & ax^2+bxy+cy^2; \\ g(x,y) & = & Ax^2+Bxy+Cy^2. \end{array}$$

  are two reduced forms which are properly equivalent.

  Claim: $f=g$, using the preceding lemma repeatedly.

  The smallest positive number represented by $f(x,y)$ is a.

  The smallest positive number represented by $g(x,y)$ is A.

  On the other hand, equivalent forms represent the same numbers.

  So $a=A$.

Existence and Uniqueness of Reduced Forms (Cont'd))

- Suppose, first, $c > a$.
  Then there are precisely two pairs $(\pm 1, 0)$ with $f(x,y) = a$.
  As f and g are equivalent, the same will be true of g, so $C > A$.
  c is the second smallest positive number represented by $f(x,y)$.
  C is the second smallest positive number represented by $g(x,y)$.
  It follows that $c = C$.
  As f and g have the same discriminant, $b = \pm B$.
  We want to see that $b = B$.
  We have
  $$g(x,y) = f(px+qy, rx+sy), \text{ for } \begin{pmatrix} p & q \\ r & s \end{pmatrix} \text{ of determinant } 1.$$
  f and g both have the same coefficient of x^2.
  So $p = \pm 1$ and $r = 0$.
  We can assume $p = 1$ by multiplying all of p, q, r and s by -1 if needed.
  As $ps - qr = 1$, we see that $s = p = 1$.

Existence and Uniqueness of Reduced Forms (Cont'd))

- Then $g(x,y) = f(x+qy,y)$.

  If $f(x,y)$ is (a,b,c), then $f(x+qy,y)$ is $(a,b+2qa,c+qb+q^2a)$.

  Since both are reduced, $-a < b \leq a$ and $-a < b+2qa \leq a$.

  This is only possible with $q = 0$.

  So $B = b$ also.
- If $c = a$, then there are either 4 or 6 pairs (x,y) with $f(x,y) = a$.

  So the same is true of g.

  Thus $C = A$ also.

  By the definition of reduced form, $0 \leq b \leq a$ and $0 \leq B \leq A$.

  But the discriminants of f and g coincide.

  So $b = \pm B$.

  As both b and B are non-negative, $b = B$.

Automorphs

Definition

Let $f(x,y)$ be a binary quadratic form. We say that a matrix

$$M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

is an automorph of f if

$$f(x,y) = f(px+qy, rx+sy).$$

Automorphs of Quadratic Forms

Corollary

Suppose that $f(x,y)$ is a reduced binary quadratic form.

- If $f(x)=x^2+y^2$, there are 4 automorphs of f, given by
$$\left\{\pm I,\pm\begin{pmatrix} 0 & 1 \\ -1 & 0. \end{pmatrix}\right\};$$
- If $f(x)=x^2+xy+y^2$, there are 6 automorphs of f, given by
$$\left\{\pm I,\pm\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},\pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\right\}.$$
- In all other cases, there are just 2 automorphs, given by $\{\pm I\}$.

Proof of the Corollary (Case $a < c$)

- Suppose first that $a < c$.

  By the lemma, the only pairs (x, y) with $f(x, y) = a$ are given by $(\pm 1, 0)$.

  A matrix M which is an automorph must map $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ into $\begin{pmatrix} \pm 1 \\ 0 \end{pmatrix}$.

  So the first column of M must be $\begin{pmatrix} \pm 1 \\ 0 \end{pmatrix}$.

  As M has determinant 1, $M = \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, for some $m \in \mathbb{Z}$.

  However, $f(x + my, y)$ can only be the same as $f(x, y)$ if $m = 0$ (by looking at the coefficient of xy say).

  Thus, $M = \pm I$.

Proof of the Corollary (Case $a = c$)

- Next, consider the cases where $a = c$.

  Suppose, first, $0 \leq b < a = c$.

  The lemma gives 4 pairs (x, y) with $f(x, y) = a$: $(\pm 1, 0)$ and $(0, \pm 1)$.

  So two different cases emerge.

  In the first, $M = \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$.

  Then $m = 0$ for the same reasons as when $a < c$.

  In the second, $M = \pm \begin{pmatrix} 0 & -1 \\ 1 & m \end{pmatrix}$. Then $M\boldsymbol{v} = \begin{pmatrix} -y \\ x + my \end{pmatrix}$.

  If $f(x, y) = ax^2 + bxy + cy^2$, then

  $$f(-y, x + my) = cx^2 + (2mc - b)xy + (a - mb + m^2 c)y^2.$$

Proof of the Corollary (Case $a = c$ Cont'd)

- Comparing coefficients of xy gives $b = 2mc - b$.

  So $b = mc$.

  However, $0 \leq b < c$. So $b = 0$. This gives $m = 0$.

  Then there are 4 automorphs, as claimed.

  Suppose, next, that $b = a = c$.

  By the proof of the lemma, we get 6 pairs (x, y) with $f(x, y) = a$.

  They are $(\pm 1, 0)$, $(0, \pm 1)$ and $(\pm 1, \mp 1)$.

  These are the first columns of possible matrices M giving automorphs.

  A similar argument gives the 6 different matrices of the statement.

The Special Linear Group $\mathrm{SL}_2(\mathbb{Z})$

Corollary

$\mathrm{SL}_2(\mathbb{Z})$ is generated by the two matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

- Let $M \in \mathrm{SL}_2(\mathbb{Z})$.

  Consider any form with 2 automorphs, say $f(x,y) = x^2 + 2y^2$.

  Consider
  $$f'(x,y) = f(M(x,y)^t).$$

  This is another quadratic form which is properly equivalent to f.

  Reduce this form by the above method.

  We must end up with the reduced form in the same class as f'.

  This must be f itself, since it is a reduced form, properly equivalent to f', and there is a unique such form.

The Special Linear Group $\mathrm{SL}_2(\mathbb{Z})$ (Cont'd)

- The reduction steps correspond to application of the matrices

$$\left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right), \left(\begin{array}{cc} 1 & -1 \\ 0 & 1 \end{array}\right), \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right).$$

But we have

$$\left(\begin{array}{cc} 1 & -1 \\ 0 & 1 \end{array}\right) = \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right)^{-1}.$$

So all reductions are expressible in terms of

$$T = \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right) \quad \text{and} \quad S = \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right)$$

and their inverses (note that $S^{-1} = -S$).

The Special Linear Group $\mathrm{SL}_2(\mathbb{Z})$ (Cont'd)

- The reduction of f' to f involves writing
$$f'(M_1M_2\cdots M_t(x,y)^t)=f((x,y)^t),$$
where $M_1,\ldots,M_t$ are T,T^{-1} or S.
By definition of f', this means that
$$f(MM_1M_2\cdots M_t(x,y)^t)=f((x,y)^t).$$
This can only happen if
$$MM_1M_2\cdots M_t=\pm I.$$
But this means that
$$M=M_t^{-1}\cdots M_1^{-1}.$$
So we have written M as a product of matrices which are T,T^{-1} or $S^{-1}=-S=S^3$.

Subsection 5

Class Numbers and Quadratic Forms

Ideal Classes and Reduced Quadratic Forms

- Recall that d is a negative squarefree integer.

Theorem

The class number of $K = \mathbb{Q}(\sqrt{d})$ is equal to the number of reduced quadratic forms with discriminant D, where $D = D_K$ is given by

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

- We will show that there exists a bijection between the ideal classes of $\mathbb{Q}(\sqrt{d})$ and reduced quadratic forms with discriminant D.

Ideal Classes and Reduced Quadratic Forms (Strategy)

- We must give:
  - A mapping from ideals to quadratic forms;
  - An inverse mapping from quadratic forms to ideals.
- I.e., we must show that:
  - Every ideal generates a quadratic form;
  - Every quadratic form comes from an ideal.
  - Any ideals in the same ideal class generate properly equivalent quadratic forms;
  - Two properly equivalent quadratic forms come from ideals in the same ideal class.

Motivating Example

- Recall that $\mathbb{Q}(\sqrt{-5})$ does not have unique factorization, since the number 6 can be factorized as $2 \cdot 3$ and as $(1+\sqrt{-5})(1-\sqrt{-5})$.
- These were genuinely distinct factorizations.
- We could resolve the non-uniqueness of factorization by introducing ideals in the ring of integers $Z[\sqrt{-5}]$,

$$\begin{array}{ll} \mathfrak{a}_1 = \langle 2, 1+\sqrt{-5}\rangle; & \mathfrak{a}_2 = \langle 2, 1-\sqrt{-5}\rangle = \mathfrak{a}_1; \\ \mathfrak{a}_3 = \langle 3, 1+\sqrt{-5}\rangle; & \mathfrak{a}_4 = \langle 3, 1-\sqrt{-5}\rangle. \end{array}$$

- Then

$$\langle 2\rangle = \mathfrak{a}_1\mathfrak{a}_2;\ \langle 3\rangle = \mathfrak{a}_3\mathfrak{a}_4;\ \langle 1+\sqrt{-5}\rangle = \mathfrak{a}_1\mathfrak{a}_3;\ \langle 1-\sqrt{-5}\rangle = \mathfrak{a}_2\mathfrak{a}_4.$$

- The two distinct factorizations are resolved when we use non-principal ideals.

Motivating Example ($\mathfrak{a}_1$)

- Notice next that $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$.
- We can plot elements of ideals in the complex plane.

  Example: Consider $\mathfrak{a}_1 = \langle 2, 1 + \sqrt{-5} \rangle$.

  Its elements are

$$\begin{aligned} &\{2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5}) : a, b, c, d \in \mathbb{Z}\} \\ &= \{(2a + c - 5d) + (2b + c + d)\sqrt{-5} : a, b, c, d \in \mathbb{Z}\} \\ &= \{A + B\sqrt{-5} : A, B \in \mathbb{Z}, 2 \mid A - B\} \\ &= \{2x + (1 + \sqrt{-5})y : x, y \in \mathbb{Z}\}. \end{aligned}$$

  Not only are 2 and $1 + \sqrt{-5}$ generators for this ideal as a $\mathbb{Z}[\sqrt{-5}]$-module, but also as a $\mathbb{Z}$-module.

Motivating Example ($\mathfrak{a}_1$ Cont'd)

- Thus, any element of the ideal can be written as

$$2x + (1+\sqrt{-5})y, \quad x, y \in \mathbb{Z}.$$

So the general element of this ideal is

$$(2x+y) + y\sqrt{-5}, \quad x, y \in \mathbb{Z}.$$

The norm of this element is

$$\begin{array}{rcl} (2x+y)^2 + 5y^2 & = & 4x^2 + 4xy + 6y^2 \\ & = & 2(2x^2 + 2xy + 3y^2). \end{array}$$

We take out the common factor of 2.

We obtain the quadratic form $(2,2,3)$.

It is positive definite of discriminant -20.

Motivating Example ($\mathfrak{a}_3$)

- We next try $\mathfrak{a}_3 = \langle 1+\sqrt{-5}\rangle$.
- We try to give a set of 2 generators for $\mathfrak{a}_3$ over $\mathbb{Z}$.
- Then we consider the norm of a general element of the ideal.

  Elements of $\mathfrak{a}_3$ are given by:

$$\begin{aligned}&\{3(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5}) : a,b,c,d\in\mathbb{Z}\}\\ =&\{(3a+c-5d)+(3b+c+d)\sqrt{-5} : a,b,c,d\in\mathbb{Z}\}\\ =&\{A+B\sqrt{-5} : A,B\in\mathbb{Z}, 3\mid A-B\}\\ =&\{3x+(1+\sqrt{-5})y : x,y\in\mathbb{Z}\}.\end{aligned}$$

  Generators for this ideal as a $\mathbb{Z}$-module are given by 3 and by $1+\sqrt{-5}$.

Motivating Example ($\mathfrak{a}_3$ Cont'd)

- So a general element of the ideal is
$$3x+(1+\sqrt{-5})y, \quad x,y\in\mathbb{Z}.$$
The norm is
$$\begin{array}{rcl}(3x+y)^2+5y^2 & = & 9x^2+6xy+6y^2\\ & = & 3(3x^2+2xy+2y^2).\end{array}$$
It is 3 times the non-reduced form $(3,2,2)$.
We can reduce $(3,2,2)$ in the usual way:
$$\begin{array}{rcll}(3,2,2) & \mapsto & (2,-2,3) & [(a,b,c)\mapsto(c,-b,a)]\\ & \mapsto & (2,2,3). & [(a,b,c)\mapsto(a,b+2a,c+b+a)]\end{array}$$

Motivating Example (Summary)

- Consider a nonprincipal ideal $\mathfrak{a}$ in $\mathbb{Z}[\sqrt{-5}]$.
- Start with any pairs of generators α and β for $\mathfrak{a}$.
- Write a general element in the form

$$\alpha x + \beta y.$$

- Take the norm.
- The result is always (a multiple of) a form properly equivalent to $(2,2,3)$.

Motivating Example (Principal Ideals)

- Now consider a principal ideal.

  Example: The easiest is the whole ring of integers $\langle 1\rangle$.

  The general element is
  $$1\cdot(x+y\sqrt{-5}),\quad x,y\in\mathbb{Z}.$$
  The norm of $x+y\sqrt{-5}$ is x^2+5y^2.

  Example: Consider the principal ideal $\langle 1+\sqrt{-5}\rangle$.

  The general element of this ideal is
  $$(1+\sqrt{-5})(x+y\sqrt{-5})=(x-5y)+(x+y)\sqrt{-5}.$$
  It has norm
  $$\begin{array}{rcl}(x-5y)^2+5(x+y)^2 & = & 6x^2+30y^2\\ & = & 6(x^2+5y^2).\end{array}$$
  Again, we see the quadratic form $(1,0,5)$ appearing.

Motivating Example (Principal Ideals Summary)

- Let $\mathfrak{a}$ be a principal ideal of norm N.
- Write a general element in the form

$$\alpha x + \beta y,$$

  for generators α and β.
- Then take the norm of this general element.
- We obtain something of the form

$$N \cdot f(x,y),$$

  where $f(x,y)$ is a quadratic form which reduces to $(1,0,5)$.

Ordering the Generators

- In the two examples, the order of the generators did not matter.
- In general, switching the generators α and β, interchanges x and y.
- Now (c, b, a) is not, in general, properly equivalent to (a, b, c).
- In the case of $\mathbb{Q}(\sqrt{-5})$, and quadratic forms of discriminant -20:
  - $(5,0,1)$ is properly equivalent to $(1,0,5)$;
  - $(3,2,2)$ is properly equivalent to $(2,2,3)$.
- We need to make a choice regarding the order of our generators.
- We will always pick α and β so that the angle of clockwise rotation from β to α is greater than from α to β.
- Equivalently, $\frac{\beta}{\alpha}$ should lie in the upper-half complex plane, i.e., should have positive imaginary part.

Outline of the Desired Bijection

Definition

A pair (α,β) of complex numbers is **ordered** if $\mathrm{im}\left(\frac{\beta}{\alpha}\right) > 0$.

- Let $\mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field.
- Consider any ideal in the ring of integers of $\mathbb{Q}(\sqrt{d})$.
  - We can find an ordered pair of generators, (α,β), for the ideal as a $\mathbb{Z}$-module, so that every element of the ideal is written as $\alpha x+\beta y$, for $x,y \in \mathbb{Z}$;
  - The norm of this general element turns out to be the norm of the ideal multiplied by a quadratic form in x and y, and this quadratic form has discriminant D;
  - Different choices of ordered generators give properly equivalent quadratic forms.
- This gives a map from ideals to proper equivalence classes of quadratic forms.

Outline of the Desired Bijection (Cont'd)

- Two ideals which are in the same ideal class will map to two properly equivalent forms.
- This will give a map from the class group to the set of proper equivalence classes of positive definite binary quadratic forms of discriminant D.
- We will see that this is a bijection.
- We work in $K = \mathbb{Q}(\sqrt{d})$, with d squarefree and negative.
- We write D for d or $4d$.
- We five a complete proof for $d \equiv 2,3 \pmod 4$, where $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$.
- The arguments for $d \equiv 1 \mod 4$ are very similar, but almost all the details need minor amendment.

The Case $d \equiv 2, 3 \pmod 4$ Strategy

- Fix $d \equiv 2, 3 \pmod 4$.
- Write $D = 4d$ for the discriminant of $\mathbb{Q}(\sqrt{d})$.
- We will show that there is a bijection between classes of ideals in $\mathbb{Z}[\sqrt{d}]$ and proper equivalence classes of (positive definite) quadratic forms of discriminant $D = 4d$.

  This will involve several steps.

  1. Given an ideal $\mathfrak{a}$ in $\mathbb{Z}_K$, we start by choosing a particular ordered basis. We observe that this basis gives a quadratic form of discriminant D.
  2. Changing the ordered basis produces a properly equivalent form. So our map can be viewed as a map from ideals to proper equivalence classes of quadratic forms of discriminant D.
  3. Two ideals in the same equivalence class map to the same proper equivalence class of quadratic forms. So we get a map Φ from ideal classes to proper equivalence classes of quadratic forms.
  4. Finally, we define a map Ψ from proper equivalence classes of quadratic forms of discriminant D to ideal classes, and check $\Psi = \Phi^{-1}$.

Stage 1: Ordered Bases of Ideals (Lemma 1)

Lemma

Let $\mathfrak{a}$ be an ideal in the ring of integers $\mathbb{Z}_K$. Then there are positive integers $a, b, c \in \mathbb{Z}$, with $c \mid a$ and $c \mid b$, such that

$$\mathfrak{a} = a\mathbb{Z} + (b + c\sqrt{d})\mathbb{Z}.$$

- Let a be the smallest positive integer in $\mathfrak{a}$.

  Let $b + c\sqrt{d}$ be any element in $\mathfrak{a}$ with $c > 0$ as small as possible.

Stage 1: Ordered Bases of Ideals (Lemma 1 Cont'd)

Claim: $\mathfrak{a} = a\mathbb{Z} + (b + c\sqrt{d})\mathbb{Z}$.

We must show that the only elements in $\mathfrak{a}$ are of this form.

Suppose $m + n\sqrt{d} \in \mathfrak{a}$.

Choose $s \in \mathbb{Z}$ so that the coefficient of $\sqrt{d}$ in

$$(m + n\sqrt{d}) - s(b + c\sqrt{d})$$

satisfies $0 \le n - sc < c$.

By our choice of $b + c\sqrt{d}$, we have $n - sc = 0$. So $n = sc$.

It follows that $(m + n\sqrt{d}) - s(b + c\sqrt{d}) = m - sb$.

This is a non-negative integer in $\mathfrak{a}$.

We now subtract a multiple of a so that $0 \le (m - sb) - ta < a$.

By minimality of a, we have $(m - sb) - ta = 0$.

Combining these gives

$$(m + n\sqrt{d}) - s(b + c\sqrt{d}) - ta = 0.$$

So $m + n\sqrt{d} \in a\mathbb{Z} + (b + c\sqrt{d})\mathbb{Z}$.

Stage 1: Ordered Bases of Ideals (Lemma 1 Cont'd)

Claim: $c \mid a$.

Suppose, to the contrary, that $c \nmid a$.

We have $a \in \mathfrak{a}$.

By the multiplicative property of ideals, $a\sqrt{d} \in \mathfrak{a}$.

We also have $b + c\sqrt{d} \in \mathfrak{a}$.

If $c \nmid a$, then we can subtract some multiple of $b + c\sqrt{d}$ from $a\sqrt{d}$ to get

$$a\sqrt{d} - t(b + c\sqrt{d}) = -b + (a - tc)\sqrt{d} \in \mathfrak{a}.$$

We can choose t so that $0 < a - tc < c$.

This contradicts the minimality of c.

So $c \mid a$.

Stage 1: Ordered Bases of Ideals (Lemma 1 Cont'd)

Claim: $c \mid b$.

Suppose, to the contrary that $c \nmid b$.

As $b + c\sqrt{d} \in \mathfrak{a}$, we also have

$$(b + c\sqrt{d})\sqrt{d} = b\sqrt{d} + dc \in \mathfrak{a}.$$

Then, as $c \nmid b$, we can subtract some multiple of $b + c\sqrt{d}$ to get

$$b\sqrt{d} + dc - t(b + c\sqrt{d}) = (dc - tb) + \sqrt{d}(b - tc) \in \mathfrak{a}.$$

If $c \nmid b$, we can choose t so that $0 < b - tc < c$.

This contradicts the minimality of c.

So $c \mid b$ in this case.

This completes the proof of the lemma.

- If $\sqrt{d}$ is chosen as the square root of d lying in the upper-half complex plane, the pair $(a, b + c\sqrt{d})$ of the lemma is ordered.

Stage 1: Ordered Bases of Ideals (Lemma 2)

Lemma

Suppose that the ideal $\mathfrak{a}$ of $\mathbb{Z}_K$ is written

$$\mathfrak{a} = a\mathbb{Z} + (b + c\sqrt{d})\mathbb{Z},$$

as in the preceding lemma. Then $N_{K/\mathbb{Q}}(\mathfrak{a}) = ac$.

- $N_{K/\mathbb{Q}}(\mathfrak{a})$ is the index of $\mathfrak{a}$ in $\mathbb{Z}[\sqrt{d}]$.

  Coset representatives for the quotient $\mathbb{Z}[\sqrt{d}]/\mathfrak{a}$ are given by

  $$\{x + y\sqrt{d} : 0 \leq x < a,\ 0 \leq y < c\}.$$

  This set has cardinality ac.

Stage 1: Ordered Bases of Ideals (Lemma 3)

Lemma

Let a, b and c be in $\mathbb{Z}$. Then the $\mathbb{Z}$-module $\mathfrak{a} = a\mathbb{Z} + (b + c\sqrt{d})\mathbb{Z}$ is an ideal in $\mathbb{Z}_K$ if and only if $c \mid a, c \mid b$ and $ac \mid c^2 d - b^2$.

- The difference between a $\mathbb{Z}$-module and a $\mathbb{Z}_K$-ideal is the following:
  - To be a $\mathbb{Z}$-module, we need to be able to multiply members of the set by elements of $\mathbb{Z}$ and remain in the set;
  - To be an ideal of $\mathbb{Z}_K$, we need to be able to multiply members of the set by elements of $\mathbb{Z}_K$ and remain in the set.

  The condition reflects the requirement that if $\alpha \in \mathfrak{a}$, then $\alpha\sqrt{d} \in \mathfrak{a}$.

  Suppose $\alpha = ax + (b + c\sqrt{d})y = (ax + by) + c\sqrt{d}y$.

  Then $\alpha\sqrt{d} = cdy + (ax + by)\sqrt{d}$.

  For all choices of $x, y \in \mathbb{Z}$, we need that this is in $\mathfrak{a}$.

  I.e., for all $x, y \in \mathbb{Z}$, $\alpha\sqrt{d} = as + (b + c\sqrt{d})t$, for some $s, t \in \mathbb{Z}$.

Stage 1: Ordered Bases of Ideals (Lemma 3 Cont'd)

- For all $x, y \in \mathbb{Z}$, we need $\alpha\sqrt{d} = as + (b + c\sqrt{d})t$, for some $s, t \in \mathbb{Z}$. Comparing coefficients of 1 and $\sqrt{d}$, we need that the equations $as + bt = cdy$, $ct = ax + by$ have solutions with $s, t \in \mathbb{Z}$, for all $x, y \in \mathbb{Z}$. We can read off the value of t from the second equation. We have $t = \frac{ax+by}{c}$ and $t \in \mathbb{Z}$, for all $x, y \in \mathbb{Z}$ if $c \mid a$ and $c \mid b$. Conversely, suppose $t \in \mathbb{Z}$, for all $x, y \in \mathbb{Z}$. Then $c \mid a$ (choose $x = 1$, $y = 0$) and $c \mid b$ (choose $x = 0$, $y = 1$). So the condition that $t \in \mathbb{Z}$ is equivalent to $c \mid a$ and $c \mid b$. Having solved for t, we can read off

$$s = \frac{cdy - bt}{a} = \frac{cdy - b(\frac{ax+by}{c})}{a} = \frac{-abx + (c^2d - b^2)y}{ac}.$$

  This is an integer for all $x, y \in \mathbb{Z}$ if and only if:
  - $ac \mid ab$ (which follows if $c \mid b$);
  - $ac \mid c^2d - b^2$.

Stage 1: Ideals to Forms (Proposition)

Proposition

Let $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}(b + c\sqrt{d})$ be an ideal of $\mathbb{Z}_K$. Then

$$\frac{N_{K/\mathbb{Q}}(ax + (b + c\sqrt{d})y)}{N_{K/\mathbb{Q}}(\mathfrak{a})}$$

is a quadratic form with integer coefficients of discriminant D.

- Notice that

$$\begin{aligned} N_{K/\mathbb{Q}}(ax + by + c\sqrt{d}y) &= (ax + by)^2 - dc^2y^2 \\ &= a^2x^2 + 2ab \cdot xy + (b^2 - c^2d)y^2. \end{aligned}$$

This gives the form $(a^2, 2ab, b^2 - c^2d)$ of discriminant $4a^2c^2d$.

Stage 1: Ideals to Forms (Cont'd)

- We got the form $(a^2, 2ab, b^2 - c^2 d)$ of discriminant $4a^2c^2d$.

  By the lemma, each of a^2, $2ab$ and $b^2 - c^2 d$ is divisible by ac.

  So the quadratic form can be written

  $$ac\left(\frac{a}{c}x^2 + 2\frac{b}{c}xy + \left(\frac{b^2 - c^2 d}{ac}\right)y^2\right) = N_{K/\mathbb{Q}}(\mathfrak{a})\Phi(\mathfrak{a}).$$

  Now

  $$\frac{a}{c}x^2 + 2\frac{b}{c}xy + \left(\frac{b^2 - c^2 d}{ac}\right)y^2$$

  has integer coefficients.

  Moreover, its discriminant is indeed $D = 4d$.

Stage 1: Ideals to Forms (Positivity)

- Let $\mathfrak{a}$ be an ideal of $\mathbb{Z}[\sqrt{d}]$.
  Let (α,β) be an ordered basis for $\mathfrak{a}$.
  If $(x,y)\neq(0,0)$, we see
  $$N_{K/\mathbb{Q}}(\alpha x+\beta y)>0$$
  is the square of the modulus of a non-zero complex number.
  Thus $N_{K/\mathbb{Q}}(\alpha x+\beta y)$ is positive definite.
  Further, in this situation, the same method as above shows that
  $$\begin{aligned} N_{K/\mathbb{Q}}(\alpha x+\beta y) &= (\alpha x+\beta y)(\overline{\alpha}x+\overline{\beta}y) \\ &= (\alpha\overline{\alpha})x^2+(\alpha\overline{\beta}+\overline{\alpha}\beta)xy+(\beta\overline{\beta})y^2 \\ &= N_{K/\mathbb{Q}}(\alpha)x^2+T_{K/\mathbb{Q}}(\alpha\overline{\beta})xy+N_{K/\mathbb{Q}}(\beta)y^2. \end{aligned}$$
  This is clearly a quadratic form.
  As $\alpha,\beta\in\mathbb{Z}[\sqrt{d}]$, by a previous corollary, the coefficients are all in $\mathbb{Z}$.

Stage 2: Changing Ordered Generators

- We see how the quadratic form changes when we change the ordered generating set.

  Suppose that (α, β) is one ordered generating set for $\mathfrak{a}$.

  We could choose this to be of the form $(a, b + c\sqrt{d})$.

  Suppose that $\gamma, \delta \in \mathbb{Z}[\sqrt{d}]$ is another basis for $\mathfrak{a}$ as a free abelian group, and that (γ, δ) is ordered.

  Then
  $$\left(\begin{array}{c}\alpha\\ \beta\end{array}\right) = M\left(\begin{array}{c}\gamma\\ \delta\end{array}\right),$$
  for some matrix $M = \left(\begin{array}{cc}p & r\\ q & s\end{array}\right)$, with entries in $\mathbb{Z}$ of determinant ±1.

Stage 2: Changing Ordered Generators (Lemma)

Lemma

Suppose z is in the upper-half complex plane, and $M = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Then $\frac{q+sz}{p+rz}$ is in the upper-half complex plane if and only if $M \in \mathrm{SL}_2(\mathbb{Z})$.

- An easy calculation gives the imaginary part of $\frac{q+sz}{p+rz}$,

$$\frac{q+sz}{p+rz} = \frac{(q+sz)(p+r\overline{z})}{(p+rz)(p+r\overline{z})} = \frac{(pq+rsz\overline{z})+(psz+qr\overline{z})}{|p+rz|^2}.$$

So the imaginary part is

$$\frac{\mathrm{im}(z)(ps-qr)}{|p+rz|^2}.$$

This is positive if and only if $ps-qr = \det M > 0$.

Stage 2: Changing Ordered Generators (Cont'd)

- Recall the ordered bases (α,β) and (γ,δ).

  We have

  $$\frac{\beta}{\alpha}=\frac{q\gamma+s\delta}{p\gamma+r\delta}=\frac{q+s\frac{\delta}{\gamma}}{p+r\frac{\delta}{\gamma}}.$$

  Now (α,β) and (γ,δ) are both ordered.

  Hence, both $\frac{\beta}{\alpha}$ and $\frac{\delta}{\gamma}$ lie in the upper-half complex plane.

  By the lemma, $\det M=1$. We conclude $M\in\mathrm{SL}_2(\mathbb{Z})$.

  From (α,β), we get a quadratic form

  $$f_{\alpha,\beta}=\frac{N_{K/\mathbb{Q}}(\alpha x+\beta y)}{N_{K/\mathbb{Q}}(\mathfrak{a})}.$$

  We have already seen that this is integral and positive definite in the particular case $(\alpha,\beta)=(a,b+c\sqrt{d})$ above.

Stage 2: Changing Ordered Generators (Cont'd)

- In the same way, from (γ,δ) we get a positive definite quadratic form
$$f_{\gamma,\delta}(x,y)=\frac{N_{K/\mathbb{Q}}(\gamma x+\delta y)}{N_{K/\mathbb{Q}}(\mathfrak{a})}$$
We have
$$\begin{array}{rcl}N_{K/\mathbb{Q}}(\mathfrak{a})\cdot f_{\alpha,\beta}(x,y) & = & (\alpha x+\beta y)(\overline{\alpha}x+\overline{\beta}y)\\ & = & (x\ \ y)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}(\overline{\alpha}\ \overline{\beta})\begin{pmatrix}x\\ y\end{pmatrix}\\ & = & (x\ \ y)\begin{pmatrix}p & r\\ q & s\end{pmatrix}\begin{pmatrix}\gamma\\ \delta\end{pmatrix}(\overline{\gamma}\ \overline{\delta})\begin{pmatrix}p & r\\ q & s\end{pmatrix}^T\begin{pmatrix}x\\ y\end{pmatrix}\\ & = & (px+qy\ \ rx+sy)\begin{pmatrix}\gamma\\ \delta\end{pmatrix}(\overline{\gamma}\ \overline{\delta})\begin{pmatrix}px+qy\\ rx+sy\end{pmatrix}\\ & = & N_{K/\mathbb{Q}}(\mathfrak{a})\cdot f_{\gamma,\delta}(px+qy,rx+sy).\end{array}$$

Stage 2: Changing Ordered Generators (Cont'd)

- Since $\det M = 1$, the two quadratic forms are properly equivalent.

  In the particular case $(\alpha, \beta) = (a, b + c\sqrt{d})$, $f_{\alpha,\beta}(x, y)$ is integral and positive definite of discriminant D.

  So $f_{\gamma,\delta}(x, y)$ is integral and positive definite of discriminant D for any ordered basis for $\mathfrak{a}$.

  Suppose $\mathfrak{a}$ is an ideal of $\mathbb{Z}_K$.

  We know that:

  - We can write it in the form $\mathbb{Z}a + \mathbb{Z}(b + c\sqrt{d})$;
  - Its norm is ac.

Stage 2: Changing Ordered Generators (Cont'd)

- We send $\mathfrak{a}$ to a proper equivalence class of quadratic forms via

$$\Phi(\mathfrak{a}) = \left[\frac{N_{K/\mathbb{Q}}(ax + (b + c\sqrt{d})y)}{N_{K/\mathbb{Q}}(\mathfrak{a})} \right].$$

  Note that the square brackets indicate that the image is the proper equivalence class of forms.

  We saw we could use any ordered basis for $\mathfrak{a}$, and still get the same proper equivalence class.

  So Φ really only depends on $\mathfrak{a}$ and not on the basis.

  So Φ maps an ideal $\mathfrak{a}$ to the proper equivalence class of quadratic forms $[f_{\alpha,\beta}(x,y)]$ of discriminant D, where $\mathfrak{a}$ has ordered basis (α, β).

Stage 3: Ideal Classes to Classes of Forms

Proposition

If $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same ideal class, then $\Phi(\mathfrak{a})$ and $\Phi(\mathfrak{b})$ are properly equivalent.

- Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in the same ideal class.

  Then there exists $\theta \in K$, such that $\mathfrak{b} = \theta\mathfrak{a}$.

  Write $\theta = \frac{\gamma}{\delta}$, for $\gamma, \delta \in \mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$.

  Then this is equivalent to $\delta\mathfrak{b} = \gamma\mathfrak{a}$.

  Suppose that $\mathfrak{a}$ can be written $\mathbb{Z}\alpha + \mathbb{Z}\beta$.

  Then $\gamma\mathfrak{a}$ can be written $\mathbb{Z}(\gamma\alpha) + \mathbb{Z}(\gamma\beta)$.

  By the multiplicativity of the norm,

$$N_{K/\mathbb{Q}}(\alpha\gamma x + \beta\gamma y) = N_{K/\mathbb{Q}}(\gamma) N_{K/\mathbb{Q}}(\alpha x + \beta y).$$

Stage 3: Ideal Classes to Classes of Forms

- Further, the multiplicativity of the norm of ideals gives

$$N_{K/\mathbb{Q}}(\langle\gamma\rangle\mathfrak{a}) = N_{K/\mathbb{Q}}(\langle\gamma\rangle)N_{K/\mathbb{Q}}(\mathfrak{a}) = \left|N_{K/\mathbb{Q}}(\gamma)\right| N_{K/\mathbb{Q}}(\mathfrak{a}).$$

  Since K is imaginary quadratic, $N_{K/\mathbb{Q}}(\gamma) > 0$.

  Consequently we have an equality

$$f_{\gamma\alpha,\gamma\beta}(x,y) = f_{\alpha,\beta}(x,y).$$

  So $\Phi(\gamma\mathfrak{a}) = \Phi(\mathfrak{a})$.

  Similarly, $\Phi(\delta\mathfrak{b}) = \Phi(\mathfrak{b})$.

  But γ and δ were chosen so that $\delta\mathfrak{b} = \gamma\mathfrak{a}$.

  Therefore, $\Phi(\mathfrak{a}) = \Phi(\mathfrak{b})$.

- It follows that Φ can be viewed as a map from the set of equivalence classes of ideals of $\mathbb{Z}_K$ to the set of proper equivalence classes of positive definite quadratic forms of discriminant D_K.

Stage 4: Classes of Forms to Ideal Classes

- Conversely, we can associate an ideal to a quadratic form of discriminant $D = 4d$ by the map

$$\Psi((a,b,c)) = \mathbb{Z}a + \mathbb{Z}\left(\frac{b}{2} + \sqrt{d}\right).$$

Since $D = b^2 - 4ac$ is even, so is b.

We can check that this is an ideal using a previous lemma.

As $c = 1$, only the final condition requires checking.

But this is just $a \mid \frac{b^2}{4} - d$.

As $D = b^2 - 4ac = 4d$, this is immediate.

Stage 4: Classes of Forms to Ideal Classes (Cont'd)

Proposition

If (a,b,c) and (a',b',c') are properly equivalent, then the ideals $\Psi((a,b,c))$ and $\Psi((a',b',c'))$ lie in the same ideal class.

- Proper equivalences are built up from the basic equivalences

$$\begin{array}{lcl}(a,b,c) & \sim & (a,b\pm 2a,c\pm b+a);\\ (a,b,c) & \sim & (c,-b,a).\end{array}$$

We have:

$$\begin{array}{lcl}\Psi((a,b\pm 2a,c\pm b+a)) & = & \mathbb{Z}a+\mathbb{Z}(\frac{b\pm 2a}{2}+\sqrt{d})\\ & = & \mathbb{Z}a+\mathbb{Z}(\frac{b}{2}+\sqrt{d})\\ & = & \Psi((a,b,c)).\end{array}$$

Stage 4: Classes of Forms to Ideal Classes (Cont'd)

- On the other hand,

$$\Psi((c,-b,a)) = \mathbb{Z}c + \mathbb{Z}(-\frac{b}{2} + \sqrt{d}).$$

We show this is an ideal in the same ideal class as $\Psi((a,b,c))$. We have

$$\begin{array}{rcl}
\left(\frac{b+2\sqrt{d}}{2c}\right)\Psi((c,-b,a)) & = & \left(\frac{b+2\sqrt{d}}{2c}\right)\left[\mathbb{Z}c + \mathbb{Z}\left(-\frac{b}{2} + \sqrt{d}\right)\right] \\
 & = & \left[\mathbb{Z}\left(\frac{b+2\sqrt{d}}{2}\right) + \mathbb{Z}\left(\frac{d-\frac{b^2}{4}}{c}\right)\right] \\
 & & (\text{scaling by } \frac{b+2\sqrt{d}}{2c} \in \mathbb{Z}[\sqrt{d}]) \\
 & = & \mathbb{Z}(\frac{b}{2} + \sqrt{d}) + \mathbb{Z}(-a) \\
 & & (b^2 - 4ac = 4d \text{ and } \mathbb{Z}a = \mathbb{Z}(-a)) \\
 & = & \Psi((a,b,c)).
\end{array}$$

Stage 4: Classes of Forms to Ideal Classes (Cont'd)

- We showed
$$\left(\frac{b+2\sqrt{d}}{2c}\right)\Psi((c,-b,a))=\Psi((a,b,c)).$$
Thus the ideal $\Psi((c,-b,a))$ is just a multiple of the ideal $\Psi((a,b,c))$ by some constant.

  They therefore lie in the same ideal class.
- Thus Ψ gives a map from proper equivalence classes of quadratic forms of discriminant $D_K=4d$ to ideal classes in $\mathbb{Z}_K=\mathbb{Z}[\sqrt{d}]$.

Stage 4: Classes of Forms to Ideal Classes (Theorem)

Theorem

The maps Φ and Ψ give inverse bijections between the set of proper equivalence classes of quadratic forms of discriminant $4d$ and the set of ideal classes in $\mathbb{Z}[\sqrt{d}]$.

- We need to prove that the maps are two-sided inverses.

  In other words, it must be shown that:

  - If (a, b, c) is a quadratic form of discriminant $4d$, then $\Phi(\Psi((a, b, c)))$ is a quadratic form properly equivalent to (a, b, c);
  - If $\mathfrak{a}$ is an ideal in $\mathbb{Z}[\sqrt{d}]$, then $\Psi(\Phi(\mathfrak{a}))$ is an ideal which is in the same ideal class as $\mathfrak{a}$.

Stage 4: Classes of Forms to Ideal Classes (Theorem Cont'd)

- Suppose that (a, b, c) is a quadratic form of discriminant $4d$.

  Then
  $$\Psi((a,b,c)) = \mathbb{Z}a + \mathbb{Z}\left(\frac{b}{2} + \sqrt{d}\right)$$
  is an ideal of norm a.

  Moreover,
  $$\begin{array}{rcl} \frac{N_{K/\mathbb{Q}}(ax+(\frac{b}{2}+\sqrt{d})y)}{a} & = & \frac{1}{a}(a^2x^2+abxy+(\frac{b^2}{4}-d)y^2) \\ & = & ax^2+bxy+(\frac{b^2-4d}{4a})y^2 \\ & = & ax^2+bxy+cy^2 \quad (4d = b^2-4ac). \end{array}$$

  So $\Phi(\Psi((a,b,c)))$ is equal to (a,b,c).

Stage 4: Classes of Forms to Ideal Classes (Theorem Cont'd)

- Finally, let $\mathfrak{a}$ denote an ideal in $\mathbb{Z}[\sqrt{d}]$.

  Write it

  $$\mathbb{Z}a+\mathbb{Z}\left(b+c\sqrt{d}\right),$$

  with $c \mid a$ and $c \mid b$.

  Then $N_{K/\mathbb{Q}}(\mathfrak{a})=ac$.

  We have

  $$\Phi(\mathfrak{a})=\frac{N_{K/\mathbb{Q}}(ax+(b+c\sqrt{d})y)}{N_{K/\mathbb{Q}}(\mathfrak{a})}=\frac{a}{c}x^2+2\frac{b}{c}xy+\frac{b^2-c^2d}{ac}y^2.$$

  Moreover,

  $$\Psi(\Phi(\mathfrak{a}))=\mathbb{Z}\frac{a}{c}+\mathbb{Z}\left(\frac{b}{c}+\sqrt{d}\right)=\frac{1}{c}(\mathbb{Z}a+\mathbb{Z}(b+c\sqrt{d})).$$

  Therefore, $\Psi(\Phi(\mathfrak{a}))$ is in the same ideal class as $\mathfrak{a}$.

$d \equiv 1 \pmod 4$: Stage 1 (Sketch)

- The arguments for the case where $d \equiv 1 \pmod 4$ are identical to the case where $d \equiv 2, 3 \pmod 4$.
- The minor changes needed to almost all the details arise from the differences in the rings of integers.
- Fix $d \equiv 1 \pmod 4$.
- Write $D = d$ for the discriminant of $K = \mathbb{Q}(\sqrt{d})$.
- At Stage 1, there are several adjustments to make to the structure theory of ideals.

$d \equiv 1 \pmod 4$: Stage 1 (Sketch Cont'd)

- The statement of the first lemma will be the same, except to replace $\sqrt{d}$ by
$$\rho_d = \frac{1+\sqrt{d}}{2}.$$

Lemma

Let a be an ideal in the ring of integers $\mathbb{Z}_K$. Then there are integers $a, b, c \in \mathbb{Z}$ with $c \mid a$ and $c \mid b$, such that
$$\mathfrak{a} = a\mathbb{Z} + (b + c\rho_d)\mathbb{Z}.$$

- The proof is very similar to that of the first lemma in the previous case.
- The norm of the ideal $\mathfrak{a} = a\mathbb{Z} + (b + c\rho_d)$ is ac, as in the second lemma.

$d \equiv 1 \pmod 4$: Stage 1 (Sketch Cont'd)

Lemma

Suppose that $d \equiv 1 \pmod 4$. Let a, b and c be in $\mathbb{Z}$. Then the $\mathbb{Z}$-module

$$\mathfrak{a} = a\mathbb{Z} + (b + c\rho_d)\mathbb{Z}$$

is an ideal in $\mathbb{Z}_K$ if and only if $c \mid a$, $c \mid b$ and $ac \mid c^2(\frac{d-1}{4}) - b^2 - bc$.

- Consider an ideal

$$\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}(b + c\rho_d).$$

We show that

$$\Phi(\mathfrak{a}) = \frac{N_{K/\mathbb{Q}}(ax + (b + c\rho_d)y)}{N_{K/\mathbb{Q}}(\mathfrak{a})}$$

is a quadratic form with integer coefficients of discriminant $D = d$.

$d \equiv 1 \pmod 4$: Stage 1 (Sketch Cont'd)

- Indeed,

$$\begin{aligned} & N_{K/\mathbb{Q}}(ax+by+c\rho_d y) \\ & = (ax+by+\tfrac{c}{2}y)^2 - \tfrac{c^2}{4}dy^2 \\ & = a^2x^2+(2ab+ac)xy+\left(b^2+bc+c^2(\tfrac{1-d}{4})\right)y^2. \end{aligned}$$

This gives the quadratic form

$$\left(a^2, 2ab+ac, b^2+bc+\frac{(1-d)c^2}{4}\right)$$

of discriminant a^2c^2d.

We again extract the common factor ac from each coefficient.

We, thus, obtain

$$\Phi(\mathfrak{a}) = \frac{a}{c}x^2 + \left(\frac{2b}{c}+1\right)xy + \left(\frac{b^2+bc+c^2(\frac{1-d}{4})}{ac}\right)y^2.$$

$\Phi(\mathfrak{a})$ has integer coefficients and discriminant $D = d$.

$d \equiv 1 \pmod 4$ (Sketch Conclusion)

- The rest of Stage 1 is unchanged, as this just depends on the definition of the quadratic form as associated to an ordered pair of generators for an ideal.
- Stage 2 is unchanged, as this is essentially just a result in linear algebra.
- Stage 3 is also unchanged.
- In Stage 4, the inverse map Ψ is defined by

  $$\Psi((a,b,c)) = \mathbb{Z}a + \mathbb{Z}\left(\frac{b-1}{2} + \rho_d\right) = \mathbb{Z}a + \mathbb{Z}\left(\frac{b+\sqrt{d}}{2}\right).$$

  Recall that b is odd, as $d = b^2 - 4ac \equiv 1 \pmod 4$.
- The proof of the last proposition is unchanged, except that, with the amended definition of Ψ, $(\frac{b+\sqrt{d}}{2c})\Psi((c,-b,a)) = \Psi((a,b,c))$.

Subsection 6

Counting Quadratic Forms

Review

- We now know:
  - There is a bijection from the class group in an imaginary quadratic number field to the collection of positive definite binary quadratic forms with the appropriate discriminant;
  - Every positive definite binary quadratic form is equivalent to a unique reduced form with the same discriminant.
- This means that the size of the class group of $K = \mathbb{Q}(\sqrt{d})$ is the same as the number of reduced quadratic forms of discriminant D_K.
- Thus, to calculate the class number of $\mathbb{Q}(\sqrt{d})$, it suffices to count the number of reduced quadratic forms of discriminant $D = D_K$.

Finiteness of the Class Group

Theorem

There are only finitely many reduced quadratic forms of discriminant D.

- If (a,b,c) is reduced, we have $0 \leq |b| \leq a \leq c$.

  So certainly $0 \leq b^2 \leq ac$.

  Then
  $$-4ac \leq b^2 - 4ac \leq ac - 4ac = -3ac.$$

  So $-4ac \leq D \leq -3ac$.

  This gives a finite range for ac,
  $$-\frac{D}{4} \leq ac \leq -\frac{D}{3}.$$

Finiteness of the Class Group (Cont'd)

- There are finitely many possibilities for a, since $a^2 \le ac$ (as $a \le c$).

  In particular, $a^2 \le ac \le -\frac{D}{3}$.

  So a is bounded.

  As $|b| \le a$, so is b.

  For each choice of a and b, there is at most one value of c, with

  $$b^2 - 4ac = D.$$

- We have a bijection between this set and the class group.

Theorem

The class group of an imaginary quadratic field is finite.

Example

- We compute the class number of $\mathbb{Q}(\sqrt{-13})$.

  First, we have $-13 \equiv 3 \pmod 4$.

  Therefore, $D = 4d = -52$.

  It follows that the class group of $\mathbb{Q}(\sqrt{-13})$ is in bijection with the collection of reduced quadratic forms of discriminant -52.

  We are looking for triples (a, b, c), such that:

  - $b^2 - 4ac = -52$;
  - $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

  We noted that we must have $\frac{52}{4} \leq ac \leq \frac{52}{3}$. So $13 \leq ac \leq 17$.

  We try each possibility.

  - Suppose $ac = 13$.
    Since $b^2 - 4ac = -52$, $b = 0$.
    We have $ac = 13$, and $0 \leq a \leq c$.
    So the only possibility is $a = 1, c = 13$.
    We get the triple $(1, 0, 13)$.

Example (Cont'd)

- Suppose $ac = 14$.
  Since $b^2 - 4ac = -52$, $b^2 = 4$. So $b = \pm 2$.
  We have $ac = 14$, and $0 < a \leq c$.
  So the possibilities for (a, c) are $(a, c) = (1, 14)$ and $(2, 7)$.
  This gives 4 possible triples:
  - $(a, b, c) = (1, 2, 14)$. Not reduced, as $|b| > a$. Applying $(a, b, c) \mapsto (a, b - 2a, c - b + a)$ gives $(1, 2, 14) \mapsto (1, 0, 13)$.
  - $(a, b, c) = (1, -2, 14)$. Not reduced, as $|b| > a$. Applying $(a, b, c) \mapsto (a, b + 2a, c + b + a)$ gives $(1, -2, 14) \mapsto (1, 0, 13)$.
  - $(a, b, c) = (2, 2, 7)$. This is reduced.
  - $(a, b, c) = (2, -2, 7)$. Not reduced, as $b = -a$. Applying $(a, b, c) \mapsto (a, b + 2a, c + b + a)$ gives $(2, -2, 7) \mapsto (2, 2, 7)$.

Example (Cont'd)

- Suppose $ac = 15$.
  Then b^2 must be 8.
  But this is not a square.
- Suppose $ac = 16$.
  Then b^2 must be 12.
  This is not a square.
- Suppose $ac = 17$.
  Then b^2 must be 16.
  So $b = \pm 4$.
  Now there are no solutions to $ac = 17$ satisfying $4 = |b| \leq a \leq c$.

We conclude that there are two reduced forms of discriminant -52, namely $(1,0,13)$ and $(2,2,7)$.

The class number of $\mathbb{Q}(\sqrt{-13})$ is therefore 2.

A Non-Euclidean Field with Unique Factorization

- We compute the class number of $\mathbb{Q}(\sqrt{-19})$.

  This time, $-19 \equiv 1 \pmod 4$.

  So $D = d = -19$.

  We count the number of reduced forms with discriminant -19.

  Now $-\frac{D}{4} \leq ac \leq -\frac{D}{3}$ yields $\frac{19}{4} \leq ac \leq \frac{19}{3}$.
  So $ac = 5$ or $ac = 6$.

  - Suppose $ac = 5$.
    Since $b^2 - 4ac = -19$, we need $b^2 = 1$.
    We get $(1,1,5)$ and $(1,-1,5)$ as the only possibilities.
    The first is reduced.
    The second is not.
    Applying $(a,b,c) \mapsto (a, b+2a, c+b+a)$, we get $(1,1,5)$.

A Non-Euclidean Field with Unique Factorization

- Suppose $ac = 6$.
  Since $b^2 - 4ac = -19$, we need $b^2 = 5$.
  This is not a square.
  So there are no reduced forms with $ac = 6$.

Thus, the only reduced form of discriminant -19 is $(1,1,5)$.

Because of the bijection with the class group, we see that the class number of $\mathbb{Q}(\sqrt{-19})$ is 1.

We have found a quadratic field with class number 1.

So it has unique factorization!

Now we have found an example of a field with unique factorization which is not Euclidean.

The Class Number One Problem

- Consider the imaginary quadratic fields

  $$\mathbb{Q}(\sqrt{-1}),\quad \mathbb{Q}(\sqrt{-2}),\quad \mathbb{Q}(\sqrt{-3}),\quad \mathbb{Q}(\sqrt{-7}),\quad \mathbb{Q}(\sqrt{-11}),$$
  $$\mathbb{Q}(\sqrt{-19}),\quad \mathbb{Q}(\sqrt{-43}),\quad \mathbb{Q}(\sqrt{-67}),\quad \mathbb{Q}(\sqrt{-67}).$$

  The class groups of these fields are trivial.

  So these fields have unique factorization.
- Gauss predicted that these were the only such fields.
- This central problem in algebraic number theory was known as the "Class Number One Problem".
  - It was not until the 1960s that a proof was given, by Alan Baker and Harold Stark independently.
  - Subsequently, it was observed that an earlier, rather obscurely written, attempt by Kurt Heegner (dating from the early 1950s) was also valid.
- Baker won the Fields Medal for the techniques he introduced in his solution of the problem.

A Partial Result on the Class Number One Problem

- We prove only the following partial result.

Theorem

Suppose that $d \equiv 2,3 \pmod 4$ is a negative squarefree integer.
Then $\mathbb{Q}(\sqrt{d})$ has unique factorization if and only if $d = -1$ or $d = -2$.

- In view of the bijection between class numbers and quadratic forms, we can restate our result in terms of quadratic forms.

Theorem

Suppose that $d \equiv 2,3 \pmod 4$ is negative and squarefree, and $D = 4d$.
The only cases where there is only one reduced quadratic form of discriminant D is when $d = -1$ or $d = -2$.

- Actually, we shall prove a result which applies to more general values of d (note that -4 is divisible by 4, and that -3 and -7 are both congruent to $1 \pmod 4$).

Unique Reduced Form of Discriminant $D = 4d$

Theorem

Suppose that d is negative, and write $D = 4d$. The only cases where there is only one reduced quadratic form of discriminant D is when $d = -1, -2, -3, -4, -7$.

- In each case, $(1, 0, -d)$ is a reduced quadratic form of discriminant D.

  For all values of d, except those listed in the theorem, we will simply write down another one, thus proving the theorem.

  - If $-d$ is not a prime power, then we can write $-d = ac$ with $(a, c) = 1$, and $1 < a < c$ (for example, if $-d = 45$, we can choose $a = 5$, $c = 9$). Then $(a, 0, c)$ is reduced of discriminant D different from $(1, 0, -d)$.
  - If $-d = 2r$, then if $r \geq 4$, we can use $(4, 4, 2^{r-2} + 1)$.
    This is easily checked to be reduced, as $4 < 2^{r-2} + 1$.
    For $r = 3$, when $d = -8$, we also have $(3, 2, 3)$.
    This just leaves $-d = 1, 2, 4$, which are in the statement.

Unique Reduced Form of Discriminant $D = 4d$ (Cont'd)

- If $-d = p^r$, where p is an odd prime and $r \geq 1$, then consider $p^r + 1$, which will be even.
  - If $p^r + 1 = ac$, with $2 \leq a < c$ and $(a, c) = 1$, we can use $(a, 2, c)$.
    This can be done whenever $p^r + 1$ is not a power of 2.
    E.g., if $-d = 27$, then use $28 = 4 \times 7$, and use $(4, 2, 7)$.
  - If $p^r + 1 = 2s$ with $s \geq 6$, use $(8, 6, 2^{s-3} + 1)$.
    This is again reduced.
  - If $p^r + 1 = 32$ (so that $p = 31$, $r = 1$), use $(5, 4, 7)$ or $(5, -4, 7)$.
  - The equation $p^r + 1 = 16$ has no solutions, since 15 is not a prime power.
  - The possibilities $p^r + 1 = 8$ (so $p = 7$, $r = 1$ giving $d = -7$), $p^r + 1 = 4$ (giving $d = -3$), $p^r + 1 = 2$ (so $d = -1$) are given in the statement.