Quadratic forms and quadratic extensions

Bill Casselman
University of British Columbia
cass@math.ubc.ca

In this essay I’ll say something about the relationship between non-degenerate integral quadratic forms and lattices in quadratic field extensions. The main result will be a bijection between strict equivalence classes of lattices and proper equivalence of integral binary quadratic forms.

I’ll illustrate this by looking at quadratic imaginary extensions. Real quadratic fields is much more complicated, and I’ll deal with these fields in another essay.

Main results are perhaps essentially due to Gauss, but I follow primarily [Davenport:1992].

Contents

1. Lattices .................................................. 1
2. ... in dimension two .................................. 3
3. Positive definite quadratic forms ..................... 7
4. Euclidean domains ..................................... 8
5. References ............................................. 12

1. Lattices ...

In this section I’ll discuss briefly integral quadratic forms in arbitrary dimensions.

Suppose $V$ to be a vector space of dimension $n$ over $\mathbb{Q}$. I’ll write vectors as column matrices. A basis of $V$ is thus a horizontal array of vectors. If a coordinate system is in place, it may also be considered a matrix of size $n \times n$, whose columns are the vectors in the basis. The coordinate matrix $x$ of a vector $v$ with respect to the basis $\lambda$ is defined by the condition that

$$v = \lambda x.$$

A lattice in $V$ is an embedded copy of $\mathbb{Z}^n$.

1.1. Lemma. An additive subgroup of $V$ is a lattice if and only if (i) it is a finitely generated and (ii) for every $v$ in $V$ some $nv$ with $n > 0$ lies in $L$.

A quadratic function on $V$ is a function $Q$ with values in $\mathbb{Q}$ such that

$$B_Q(x, y) = Q(x + y) - Q(x) - Q(y)$$

is bilinear. It is called non-degenerate if the bilinear form $B$ is non-degenerate. If $(\lambda_i)$ is a basis of $V$ then $Q$ determines the quadratic form

$$Q(u) = \sum_{i,j} m_{i,j}x_i x_j \quad (m_{i,j} = B(\lambda_i, \lambda_j)/2)$$

for $u = \sum x_i \lambda_i$. This can also be written as

(1.2) $$Q(u) = \sum_i m_{i,i} x_i^2 + \sum_{i<j} 2m_{i,j} x_i x_j .$$

It can also be expressed in matrix form:

$$Q(u) = \trans x M x.$$ 

Suppose we change the basis to $\mu = \lambda X$, with $X$ an invertible matrix in $\text{GL}_n(\mathbb{Q})$. It $u$ is a vector in $V$ then its coordinate arrays $x, y$ are determined by the equation $u = \lambda x = \mu y$, which gives the coordinate
transformation $x = XY$. This leads directly to a formula for a transformed quadratic function. It is most simply given as a matrix equation:

$$t^* M \lambda x = t^* X M \lambda X y = t^* M \mu y .$$

The matrix of $Q$ with respect to the basis $\mu$ is hence

$$M_\mu = t^* X M \lambda X .$$

The bilinear form $B_Q$ may also be expressed as a matrix product:

$$B(u, v) = 2 t^* X M \lambda y .$$

The matrix $M_\lambda$ is non-singular if and only if the quadratic form is non-degenerate.

If $L$ is a lattice in $V$, a choice of basis will determine a quadratic form. A change of basis will change the form by a matrix $X$ in $GL_n(\mathbb{Z})$, according to (1.3). The two forms will be called properly equivalent if $\det(X) = 1$.

Given $Q$, the lattice $L$ is called integral if $Q$ takes integral values on it. Equivalent is the condition that the coefficients in (1.2), determined by a basis of $L$, be integral. I should point out that this convention as to what constitutes an integral lattice is not universal. Some authors, including Gauss, require that the matrix $M_\lambda$ have integral entries.

Suppose $S$ to be any set of rational numbers with the property that $n|S|$ is contained in the positive integers for some $n > 0$. Since every set of positive integers has a minimum element, the set $n|S|$ possesses a greatest common divisor, say $g$. Then $g/n$ is the greatest common divisor of $S$. In particular, if $L$ is a lattice in $V$ the image $Q(L)$ has a greatest common divisor, which I’ll call $\Gamma(L)$. It is often called the norm of $L$.

1.4. Lemma. Suppose $L$ to be a lattice in $V$. If

$$Q(u) = \sum_{i \leq j} m_{i,j} x_i x_j$$

is the quadratic form corresponding to some basis of $L$, then $\Gamma(L)$ is the greatest common divisor of the $m_{i,j}$.

The group $GO_Q$ is made up of all the linear transformations $T$ if $V$ such that $Q(T(u)) = c Q(u)$ for every $u$ in $V$ and some scalar $c$, which I define to be $NM(T)$. The map taking $T$ to $NM(T)$ is a homomorphism. The following is elementary:

1.5. Lemma. For $T$ in $GO_Q$ we have $\Gamma(T L) = |NM(T)| \cdot \Gamma(L)$.

An integral form is called primitive if $\Gamma(L) = 1$. Thus a lattice $L$ is always primitive with respect to $Q/\Gamma(L)$.

The discriminant $D_L$ of the lattice is

$$|\det(2M_\lambda)| = 2^n |\det(M_\lambda)| .$$

Because of (1.3), this is independent of the choice of basis.

Define

$$L^\perp = \{ v \in \mathbb{R}^n | B(v, L) \subseteq \mathbb{Z} \} .$$

It is a lattice if and only if $Q$ is non-degenerate, and then has as basis the dual $(\lambda^\vee_i)$ of the basis $(\lambda_i)$ with respect to $B$, which is

$$\lambda^\vee = \lambda(2M_\lambda)^{-1} .$$

Hence:

1.6. Proposition. If the restriction of $Q$ to the lattice $L$ is integral, then $L$ is contained in $L^\perp$, and its index in $L^\perp$ is equal to the discriminant.

The real point of the discriminant, which I shall not pursue here, is that it tells you about the quadratic forms induced on the finite groups $L/NL$. The radical of $Q$ on $L/NL$ is the subspace of all $u$ in $V$ such that $B_Q(u, L) \equiv_N 0$. This is the same as $NL^\perp \cap L$. It is trivial if and only if $N$ is relatively prime to the discriminant. The best measure of how bad things are is the set of principal divisors of $L^\perp/L$. 

Quadratic forms and quadratic extensions
2. ... in dimension two

Suppose now that \( F = \mathbb{Q}(\sqrt{N}) \) is a quadratic field extension of \( \mathbb{Q} \), with \( N \) square-free.

**ARITHMETIC IN THE FIELD.** Of course there are two square roots of \( N \), but I fix one and express it as \( \sqrt{N} \).

The map
\[
\sigma: x + y\sqrt{N} \mapsto x + y\sqrt{N} = x - y\sqrt{N}
\]
is the unique non-trivial automorphism of \( F \). Let
\[
\text{IM}(x + y\sqrt{N}) = y.
\]

Multiplication by \( \gamma \in F \) is a \( \mathbb{Q} \)-linear transformation. If a basis of \( F \) is chosen, it will be associated to a matrix \( \pi_{\gamma} \). For example, if the basis is \( (1, \sqrt{N}) \) and \( \gamma = x + y\sqrt{N} \), then
\[
\pi_{\gamma} = \begin{bmatrix} x & Ny \\ y & x \end{bmatrix}.
\]

The trace of \( \pi_{\gamma} \) is \( \text{TR}_{F/\mathbb{Q}}(\gamma) = \gamma + \overline{\gamma} \), and \( \det(\pi_{\gamma}) = \text{NM}_{F/\mathbb{Q}}(\gamma) = \gamma\overline{\gamma} \).

Every element \( \gamma \) of \( F \) will be the root of a unique polynomial (2.1)
\[
a x^2 + bx + c
\]
with \( a, b, c \) relatively prime integers and \( a > 0 \). I’ll call it the **characteristic polynomial** of \( \gamma \).

**2.2. Lemma.** The group \( \text{GO}_{\text{NM}} \) is the semi-direct product of \( F^\times \) and \( \{1, \sigma\} \).

**Proof.** This reduces to the claim that if \( g \neq 1 \) lies in \( \text{GO}_{\text{NM}} \) and \( g(1) = 1 \) then \( g = \sigma \).

**BINARY FORMS.** I’ll say that a pair \((\lambda, \mu)\) in \( F \) is **positively oriented** if
\[
\text{IM} \det \begin{bmatrix} \lambda & \mu \\ \overline{\lambda} & \overline{\mu} \end{bmatrix} = \frac{\lambda\overline{\mu} - \overline{\lambda}\mu}{2\sqrt{N}} > 0.
\]

Thus in \( \mathbb{Z}[i] \) the basis \((i, 1)\) is positively oriented. If \((\lambda, \mu)\) is not positively oriented, then \((\lambda, \mu)\) is, so that every lattice in \( F \) possesses a positively oriented basis, which will be unique to up transformations \( \mu = \lambda X \) with \( X \) in \( \text{SL}_2(\mathbb{Z}) \). Conjugation swaps the rows of this matrix, and hence reverses parity of every pair.

Suppose \( L \) to be a lattice in \( F \) with positively oriented basis \( \Lambda = (\lambda, \mu) \). To these is associated the quadratic form \( Q_\Lambda(x, y) = (x\lambda + y\mu)(x\overline{\lambda} + y\overline{\mu}) = Ax^2 + Bxy + Cy^2 \)

with
\[
A = \text{NM}(\lambda) \\
B = \text{TR}(\lambda\overline{\mu}) \\
C = \text{NM}(\mu)
\]

To this is turn is associated the primitive form
\[
q_\Lambda(x, y) = \frac{Q_\Lambda}{\text{IM}(L)} = ax^2 + bxy + cy^2,
\]
with the coefficients integral and relatively prime. If a different oriented basis of \( L \) is chosen, then \( q_L \) is transformed by some matrix in \( \text{SL}_2(\mathbb{Z}) \), hence to a properly equivalent form.

The map \( L \mapsto q_L \) therefore induces a well defined map from lattices in \( F \) to proper equivalence classes of quadratic forms. **When do two lattices give rise to the same class? What is the image of this map?**
The answer to the first question is not difficult.

2.3. Proposition. Two lattices $L_1$ and $L_2$ in $F$ give rise to the same proper equivalence class of binary quadratic forms if and only if $L_2 = \gamma L_1$ for some $\gamma \in F^\times$ with $NM(\gamma) > 0$.

In this case, the two lattices are said to be strictly equivalent. For $F$ quadratic imaginary, this is no constraint since norms are always non-negative.

Proof. Suppose $NM(\gamma) > 0$ and $\Lambda = (\lambda, \mu)$ an oriented basis then

$$\det \begin{bmatrix} \gamma \lambda & \gamma \mu \\ \lambda & \mu \end{bmatrix} = NM(\gamma) \det \begin{bmatrix} \lambda & \mu \\ \lambda & \mu \end{bmatrix}$$

so that multiplication by $\gamma$ takes a positively oriented pair to a positively oriented pair. The quadratic form $Q_{\gamma} = NM(\gamma) Q_{L_1}$, and since $\Gamma(\gamma L) = |NM(\gamma)| |\Gamma(L)|$, the form $q_{\gamma L}$ is exactly the same as $q_L$.

Conversely, suppose $L_1$ and $L_2$ are associated to the equivalent primitive forms. Changing a basis if necessary, we may assume that the primitive forms associated to the lattices are actually the same. This means that if $(\lambda_i, \mu_i)$ are the relevant bases,

$$A_2 x^2 + B_2 xy + C_2 y^2 = \rho (A_1 x^2 + B_1 xy + C_1 y^2)$$

for some $\rho > 0$. The linear transformation taking $\lambda_1$ to $\lambda_2$ and $\mu_1$ to $\mu_2$ is therefore in $GO$. Since they are both positively oriented, Lemma 2.2 implies that it amounts to multiplication by an element of $F^\times$. Since $\rho > 0$, its norm is positive.

Finding an answer to the second question will take a bit longer.

ORDERS. An order in $F$ is a subring (containing 1) that is also a lattice. There is a simple classification.

An integer in $F$ is an element $\gamma$ whose characteristic polynomial is monic. Equivalently

$$TR(\gamma) \text{ and } NM(\gamma)$$

are both in $\mathbb{Z}$.

2.4. Lemma. The element $\gamma$ is an integer of $F$ if and only if multiplication by $\gamma$ takes some lattice in $F$ into itself.

Proof. One way because given a basis of the lattice, multiplication by $\gamma$ is expressed as multiplication by a matrix in $M_2(\mathbb{Z})$.

The other because if the characteristic polynomial of $\gamma$ is monic, the lattice spanned by 1 and $\gamma$ is stable under multiplication by $\gamma$:

$$\gamma \cdot 1 = \gamma$$

$$\gamma \cdot \gamma = -b\gamma - c.$$
2.6. Proposition. If $F = \mathbb{Q}(\sqrt{N})$ with $N$ square-free, its ring of integers $\mathfrak{o}$ has as basis $1$ and $\omega_N$, where

$$\omega_N = \begin{cases} \frac{1 + \sqrt{N}}{2} & \text{if } N \equiv 1 \pmod{4} \\ \sqrt{N} & \text{otherwise.} \end{cases}$$

For example, the integers in $\mathbb{Q}(\sqrt{-1})$ are generated over $\mathbb{Z}$ by $\sqrt{-1}$, while those in $\mathbb{Q}(\sqrt{-3})$ are generated by $(1 + \sqrt{-3})/2$.

2.7. Corollary. If $F = \mathbb{Q}(\sqrt{N})$, the norm form on $\mathfrak{o}_F$ is

$$\begin{cases} m^2 + mn + \left(\frac{1 - N}{4}\right) n^2 & \text{if } N \equiv 1 \pmod{4} \\ m^2 + Nn^2 & \text{otherwise.} \end{cases}$$

Let $D_N = D_F$ be the corresponding discriminant. It is $N$ in the first case, $4N$ in the second.

I’ll call the discriminant of the integer lattice of a quadratic extension a **minimal** discriminant. These are precisely the integers $D$ with either (i) $D \equiv 4 \pmod{4}$ and square-free or (ii) $D \equiv 0$, $D/4 \equiv 1 \pmod{2}$ and square-free.

2.8. Lemma. If $\gamma$ is an integer in $F$ but not in $\mathbb{Q}$, then the lattice with basis $(1, \gamma)$ is an order. Conversely, every order in $F$ has a basis $(1, \gamma)$ with $\gamma$ in $\mathfrak{o}$.

Proof. One way is an immediate consequence of Lemma 2.4.

For the other, suppose $\tau$ to be an order in $F$, say with basis $\lambda, \mu$. By Lemma 2.4, they are all integers.

Since 1 is in $\tau$, we may write $$1 = a\lambda + b\mu.$$ The greatest common divisor of $a$ and $b$ is certainly 1, so we can find $\ell, m$ such that $am + \ell b = 1$. But then

$$\begin{bmatrix} \lambda & \mu \\ a & b \end{bmatrix} \begin{bmatrix} \ell \\ m \end{bmatrix} = \begin{bmatrix} 1 - \ell \lambda + m\mu \end{bmatrix} = \begin{bmatrix} 1 & \gamma \end{bmatrix}$$

is also a basis of $\tau$.

2.9. Proposition. Every order in $F$ is contained in the ring $\mathfrak{o}_F$.

Proof. Choose a basis of the order $\tau$, and $\gamma$ in $\tau$. Then multiplication by $\gamma$ amounts to matrix multiplication by an integral matrix, so its characteristic polynomial is monic and integral.

2.10. Lemma. The orders in $F_N$ are the lattices with basis 1, $f\omega_N$ for some $f > 0$.

Proof. Suppose $\tau$ to be an order in $F_N$. It certainly contains 1 as part of a basis. Suppose $a + b\omega_N$ lie in $\tau$ with $f > 0$ smallest. Then $f\omega_N$ is also in $\tau$, and any other element of $\tau$ will be of the form $a + b f\omega_N$.

2.11. Lemma. The discriminant of the order $\mathbb{Z}[f\omega_N]$ is

$$\begin{cases} f^2 N & \text{if } N \equiv 1 \pmod{4} \\ 4f^2 N & \text{otherwise.} \end{cases}$$

In particular, the orders are distinguished by their discriminants. The possible discriminants are all those $D \equiv 0$ or 1. Every possible discriminant has a unique factorization as $f^2 D_F$ for some quadratic extension $F = F_N$.

Let $\tau_D$ be the unique order with discriminant $D$. 
ENDOMORPHISMS. If \( L \) is a lattice in \( F \), its endomorphism ring \( \text{End}(L) \) is that of all \( \alpha \) in \( F \) such that \( \alpha L \subseteq L \). If \( L \) has basis \( (\lambda, \mu) \), what is \( \text{End}(L) \)?

2.12. Proposition. Let
\[ ax^2 + bxy + cy^2 \]
be the characteristic form associated to the positively oriented basis \( (\lambda, \mu) \) of the lattice \( L \). Then \( \gamma = -\mu/\lambda \) satisfies the quadratic equation
\[ a\gamma^2 + b\gamma + c = 0 \]
and \( \text{End}(L) \) is the ring \( \mathbb{Z}[a\gamma] \).

Note that \( a\gamma \) is an integer.

Proof. For the first assertion:
\[
Ax^2 + Bx + C = (x\lambda + \mu)(x\bar{\lambda} + \bar{\mu})
= |\lambda|^2(x + \mu/\lambda)(x - \bar{\mu}/\bar{\lambda})
= |\lambda|^2(x - \gamma)(x - \bar{\gamma}).
\]

For the second, let \( \lambda = x + y\gamma \). The lattice \( (\lambda, \mu) \) is similar to \( ((1, \gamma)) \), and the endomorphism rings of similar lattices are the same. Since
\[
\lambda \cdot 1 = x + y\gamma,
\lambda \cdot \gamma = -\left(\frac{cy}{a}\right) + \left(x - \frac{by}{a}\right)\gamma,
\]
\( \lambda \) lies in \( \text{End}(L) \) if and only if \( x, y, cy/a, by/a \) are all integers. But \( a, b, c \) have greatest common divisor equal to 1. Therefore it is required that \( x, y, and y/a \) all be integers.

2.13. Corollary. Suppose \( L \) to be a lattice in \( F \) with characteristic form \( ax^2 + bxy + cy^2 \). The ring \( \text{End}(L) \) is the unique order of \( F \) whose discriminant is \( b^2 - 4ac \).

In other words, a primitive form associated to \( L \) has the same discriminant as \( \text{End}(L) \).

MODULES. What remains to be shown:

2.14. Proposition. If \( Q \) is a rational binary quadratic form, then there exists a unique quadratic extension \( F \), \( \lambda \) in \( F \) with \( \text{IM}(\lambda) > 0 \)
(\( \lambda, \mu \)) in \( F \), and a rational constant \( \rho \neq 0 \) such that \( Q = \rho Q_{\lambda, \mu} \).

Proof. Suppose given the form
\[ ax^2 + bxy + cy^2, \]
and let \( d = b^2 - 4ac \). However, the right hand side is
\[ a(x^2 + (b/a)xy + (c/a)y^2) \]
which can be factored as
\[ a(x - \gamma y)(x - \bar{\gamma} y) \]
if
\[ \gamma^2 - (b/a)\gamma + (c/a) = 0. \]
But this has roots
\[ \frac{b/a \pm \sqrt{(b/a)^2 - 4c/a}}{2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{d}}{2a}. \]
If necessary, we can replace \( \gamma \) by its conjugate to make the pair \( 1, \gamma \) oriented. The field \( F \) is determined by \( Q \), since it is generated by \( \sqrt{D_L} \).
Thus, the map from lattices to primitive forms induces a bijection between strict equivalence classes of integral lattices whose endomorphism ring is $\mathbb{Z}_D$ in $F$ and proper equivalence classes of primitive quadratic forms whose discriminant is $D$.

It remains to describe the classification of reduced non-degenerate forms. I’ll do this for positive definite ones in the rest of this essay.

3. Positive definite quadratic forms

In considering positive definite forms, it is useful to consider lattices in $\mathbb{C}$. A basis $(\lambda, \mu)$ of the lattice $L$ determines by restriction of the usual norm $|z|^2$ the positive definite quadratic form

$$ax^2 + bxy + cy^2.$$ 

It is called reduced if either $a \leq c$ and $|b| \leq |a|$, 

3.1. Proposition. Every positive definite quadratic form in two dimensions with real coefficients is equivalent to a reduced form.

One might then wonder, when are reduced forms unique? Or, when are two reduced forms equivalent? A form is called strictly reduced if either $c > a$ and $|b| \leq |a|$ or $c = a$ and $0 \leq b \leq a$.

3.2. Corollary. Every form is equivalent to a unique strictly reduced form.

Proof. Suppose $(u, v)$ to be a basis defining the form. The condition $|b| \leq |a|$ means geometrically that the projection of $v$ onto the line through $u$ lies in the interval $(-u/2, u/2]$, or in other words that $-1/2 < \frac{u \cdot v}{u \cdot u} < 1/2$.

The other condition means $|u| \leq |v|$. Choose $u$ to have the smallest length in the lattice determining the form. One can find $n$ such that $v - nu$ has the proper projection.

I leave the rest as exercise.

The reduced form can also be found by a simple algorithm, perhaps due to Gauss. Start with $ax^2 + bxy + cy^2$. If $a > c$, swap $u$ and $v$. Change $v$ to some $v + nu$ to impose the projection condition. Repeat until both conditions are satisfied.

**How to classify reduced forms of a given discriminant $D$?** Because $D = b^2 - 4ac$ and $D < 0$ while $0 < a \leq c$, one can deduce that

$$b^2 \leq 4ac \leq D/3.$$ 

Also, $b$ must be even if $D \equiv 4 \pmod{4}$ and odd if $D \equiv 2 \pmod{4}$. So we should scan through all $b$ of suitable parity from $0$ to $\lfloor \sqrt{D/3} \rfloor$, and for each factor, if possible, $ac = (D + b^2)/4$. Reject all for which $|b| \leq |a| \leq |c|$ does not hold.

**Examples.**

1) Take $D = -3$. Then $N = 3$, and the unique reduced form is $m^2 + mn + n^2$.

2) Take $D = -4$. Then $N = 1$, and the only reduced form is $m^2 + n^2$.

3) Take $D = -12$. Then $N = 3$, and the reduced forms are $m^2 + 3n^2$ and $2m^2 + 2mn + 2n^2$. The last is not primitive.

4) Take $D = -20$. Then $N = 5$, and the two reduced forms are $m^2 + 5m^2$ and $2m^2 + 2mn + 3n^2$. 

4. Euclidean domains

In this last section I’ll interpret some features of positive definite binary forms geometrically.

If all lattices stable under \( r \) are generated by a single element, \( r \) is said to be a principal ideal domain. There is one simple sufficient condition for this to happen, when \( r \) has a division algorithm. In this section I’ll use visual techniques in several cases to see that this is true.

I’ll recall first how to prove that \( \mathbb{Z} \) is a principal ideal domain. This means that any ideal is made up of multiples of a single element. Suppose \( I \) to be an ideal in \( \mathbb{Z} \), and suppose \( n \) to be a positive element in \( I \) of least magnitude. This implies that if \( m \) is any integer in \( I \) with \( |m| < |n| \) then \( m = 0 \)—or, equivalently, that if \( |m - ni| < n \) then \( m = ni \). But the division algorithm implies that the open intervals \((ni - n, ni + n)\) cover \( \mathbb{Z} \), so that indeed every element of \( I \) is a multiple of \( n \).

Of course, what the picture really illustrates is the division algorithm in \( \mathbb{Z} \), which when applied in Euclid’s algorithm leads to an explicit generator of any ideal in \( \mathbb{Z} \).

Something similar happens for the Gaussian integers \( \mathcal{O} = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i \). Here, the open unit discs around each of the \( z \) in \( \mathcal{O} \) cover all of \( \mathbb{C} \):

This is also true for the integral rings \( \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\omega_3], \mathbb{Z}[\omega_7] \), and \( \mathbb{Z}[\omega_{11}] \) (where \( \omega_N = (1 + \sqrt{-N})/2 \)), as the following picture suggests:
4.1. Proposition. Let $\mathfrak{o}$ be the ring of integers in a quadratic imaginary extension of $\mathbb{Q}$, embedded in $\mathbb{C}$. If the open unit disks around integers in $\mathfrak{o}$ cover $\mathbb{C}$, then every ideal $I$ in $\mathfrak{o}$ is principal.

Proof. Let $\alpha \neq 0$ an element of $I$ of smallest magnitude. Scaling the diagram by $\alpha$, we deduce that open discs of radius $|\alpha|$ cover $\mathbb{C}$. If $\beta$ is any of $I$, it will therefore lie within distance $|\alpha|$ of some element $\gamma$ of $\mathfrak{o} \cdot \alpha$. But because $|\alpha|$ is minimum, $\beta$ must in fact be $\gamma$.

This argument fails, however, for $\mathbb{Z}[\sqrt{-5}]$:
Interestingly, though, the same picture tells us more precisely how far this ring is from being a principal ideal domain.

Suppose $I$ to be an ideal in $\mathbb{Z}[\sqrt{-5}]$, and suppose $w$ to be of least magnitude in $I$. Building the lattice $L = \mathbb{Z}[\sqrt{-5}] \cdot w$ we get this picture:

Since $w$ is of least magnitude, there are no elements of $I$ within unit distance of any element of $L$. If $I$ is not identical with the principal ideal $L$ it must contain a point in the dark area in the following figure:
If it lies at \((x, y)\) there must also be elements of \(I\) of the form \((x + w, y)\), and by symmetry \(-x + w, \sqrt{-5} - y\). This will contradict the assumption on \(w\) unless \(x = 0\) or \(x = 1/2\), and \(y = \sqrt{-5}/2\), as indicated in this picture:

Since \(\sqrt{-5} \alpha = (5/2)w\), the ideal \(I\) cannot contain \(\alpha\). But it can very well contain \(\beta\), and the points in \(I\) then look like this:

The class number of \(\mathbb{Z}[\sqrt{-5}]\) is hence 2.
In the case of the ring $\mathbb{Z}[\sqrt{-19}]$, unit circles around its elements do not cover $\mathbb{C}$, but an argument similar to that we have just seen will show that it is nonetheless a principal ideal domain.

The other complex imaginary quadratic fields with class number 1 are $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, and $\mathbb{Q}(\sqrt{-163})$. I have not tried looking at those cases. That these have class number one is an elementary application of Gauss’ algorithm, but that these are all the ones with this property was only a conjecture of Gauss up until the mid-twentieth century.

5. References