9.2 Binary Quadratic Forms

9.2.1 Introduction

A *binary quadratic form* is a homogeneous polynomial

$$f = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y].$$

We say that n is *represented* by f if there are integers $x, y \in \mathbb{Z}$ such that $f(x, y) = n$. The representability problem will partially motivate our interest in quadratic forms.

Problem 9.2.1. Given a binary quadratic form f, give a good way to determine whether or not any given integer n is represented by f.

We gave a simple solution to this problem in Section 9.1 in the case when $f = x^2 + y^2$. The set of sums of two squares is the set of integers n such that any prime divisor p of n of the form $4m + 3$ exactly divides n to an even power (along with 0).

9.2.2 Equivalence

For simplicity below we will sometimes write $f\begin{pmatrix} x \\ y \end{pmatrix}$ for $f(x, y)$.

Definition 9.2.2. The modular group $\mathrm{SL}_2(\mathbb{Z})$ is the group of all 2×2 integer matrices with determinant $+1$.

If $\gamma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form, let

$$f|_\gamma(x, y) = f(px + qy, rx + sy) = f\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right).$$

Proposition 9.2.3. *The above formula defines a right action of the group* $\mathrm{SL}_2(\mathbb{Z})$ *on the set of binary quadratic forms, in the sense that*

$$f|_{\gamma\delta} = (f|_\gamma)|_\delta,$$

for any $\gamma, \delta \in \mathrm{SL}_2(\mathbb{Z})$.

Proof. Suppose $\gamma, \delta \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$f|_{\gamma\delta}\begin{pmatrix} x \\ y \end{pmatrix} = f\left(\gamma\delta\begin{pmatrix} x \\ y \end{pmatrix}\right) = f|_\gamma\left(h\begin{pmatrix} x \\ y \end{pmatrix}\right) = (f|_\gamma)|_\delta\begin{pmatrix} x \\ y \end{pmatrix}.$$

$\square$

Proposition 9.2.4. *Let* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ *and let* f *be a binary quadratic form. The set of integers represented by* f *is exactly the same as the set of integers represented by* $f|_\gamma$. *(The converse is not true; see Example 9.3.4.)*

Proof. If $f(x_0, y_0) = n$ then since $\gamma^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, we have $\gamma^{-1}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \in \mathbb{Z}^2$, so

$$f|_\gamma \left(\gamma^{-1}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}\right) = f\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = n.$$

Thus every integer represented by f is also represented by $f|_\gamma$. Conversely, if $f|_\gamma \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = n$, then $f\left(\gamma\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}\right) = n$, so f represents n. □

Define an equivalence relation $\sim$ on the set of all binary quadratic forms by $f \sim f'$ if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $f|_\gamma = f'$.

For simplicity, we will sometimes denote the quadratic form $ax^2 + bxy + cy^2$ by (a, b, c). Then, for example, since $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we see that $(a, b, c) \sim (c, -b, a)$, since if $f(x, y) = ax^2 + bxy + cy^2$, then $f(-y, x) = ay^2 - bxy + cx^2$.

Example 9.2.5. Consider the binary quadratic form

$$f(x, y) = 458x^2 + 214xy + 25y^2.$$

Solving the representation problem for f might, at first glance, look hopeless. We find $f(x, y)$ for a few values of x and y:

$$\begin{aligned} f(-1, -1) &= 17 \cdot 41 \\ f(-1, 0) &= 2 \cdot 229 \\ f(0, -1) &= 5^2 \\ f(1, 1) &= 269 \\ f(-1, 2) &= 2 \cdot 5 \cdot 13 \\ f(-1, 3) &= 41 \end{aligned}$$

Each number is a sum of two squares! Letting $\gamma = \left(\begin{smallmatrix} 4 & -3 \\ -17 & 13 \end{smallmatrix}\right)$, we have

$$\begin{aligned} f|_\gamma &= 458(4x - 3y)^2 + 214(4x - 3y)(-17x + 13y) + 25(-17x + 13y)^2 \\ &= \cdots = x^2 + y^2!! \end{aligned}$$

Thus by Proposition 9.2.4, f represents an integer n if and only if n is a sum of two squares.

9.2.3 Discriminants

Definition 9.2.6. The *discriminant* of $f(x, y) = ax^2 + bxy + cy^2$ is $b^2 - 4ac$.

Example 9.2.7. Notice that $\mathrm{disc}(x^2 + y^2) = -4$ and

$$\mathrm{disc}(458, 214, 25) = 214^2 - 4 \cdot 25 \cdot 458 = -4.$$

That the discriminants are the same indicates that $(1, 0, 1)$ and $(458, 214, 25)$ are closely related.

Proposition 9.2.8. *If $f \sim f'$, then* $\mathrm{disc}(f) = \mathrm{disc}(f')$.

Proof. By elementary algebra, one sees that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\mathrm{disc}(f|_\gamma) = \mathrm{disc}(f) \cdot \det(\gamma)^2 = \mathrm{disc}(f).$$

Since $f' = f|_\gamma$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the proposition follows. □

The converse of the proposition is false. Forms with the same discriminant need not be equivalent. For example, the forms $(1,0,6)$ and $(2,0,3)$ have discriminant -24, but are not equivalent. To see this, observe that $(1,0,6)$ represents 1, but $2x^2 + 3y^2$ can not represent 1.

Proposition 9.2.9. *The set of all discriminants of forms is exactly the set of integers d such that $d \equiv 0$ or $1 \pmod 4$.*

Proof. First note that $b^2 - 4ac$ is a square modulo 4, so it must equal 0 or 1 modulo 4. Next suppose d is an integer such that $d \equiv 0$ or $1 \pmod 4$. If we set

$$c = \begin{cases} -d/4, & \text{if } d \equiv 0 \pmod 4 \\ -(d-1)/4 & \text{if } d \equiv 1 \pmod 4, \end{cases}$$

then $\mathrm{disc}(1,0,c) = d$ in the first case and $\mathrm{disc}(1,1,c) = d$ in the second. □

Definition 9.2.10. The form $(1,0,-d/4)$ or $(1,1,-(d-1)/4)$ of discriminant d that appears in the proof of the previous proposition is called the *principal form* of discriminant d.

d	principal form	
-4	(1,0,1)	$x^2 + y^2$
5	(1,1,-1)	$x^2 + xy - y^2$
-7	(1,1,2)	$x^2 + xy + 2y^2$
8	(1,0,-2)	$x^2 - 2y^2$
-23	(1,1,6)	$x^2 + xy + 6y^2$
389	(1,1,-97)	$x^2 + xy - 97y^2$

9.2.4 Definite and Indefinite Forms

Definition 9.2.11. A quadratic form with negative discriminant is called *definite.* A form with positive discriminant is called *indefinite.*

This definition is motivated by the fact that the nonzero integers represented by a definite form are all either positive or negative. To see this, let (a,b,c) be a quadratic form, multiply by $4a$ and complete the square:

$$\begin{aligned} 4a(ax^2 + bxy + cy^2) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 + (4ac - b^2)y^2 \end{aligned}$$

If $\operatorname{disc}(a, b, c) < 0$ then $4ac - b^2 = -\operatorname{disc}(a, b, c) > 0$, so the nonzero values taken on by $ax^2 + bxy + cy^2$ are only positive or only negative, depending on the sign of a. On the other hand, if $\operatorname{disc}(a, b, c) > 0$, then $(2ax+by)^2+(4ac-b^2)y^2$ takes both positive and negative values, so (a, b, c) does also.

9.2.5 Rings of Integers in Quadratic Fields

We have seen quadratic number fields several times before. We now make the theory more precise, in order to see how the arithmetic of quadratic number fields is closely linked to the theory of quadratic forms.

Let $D \neq 0, 1$ be a square-free integer. The quadratic field obtained by adjoining $\sqrt{D}$ to $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

Definition 9.2.12 (Integral). An element $x \in K$ is *integral over* $\mathbb{Z}$ if it is the root of a quadratic polynomial of the form $x^2 + ax + b$ with $a, b \in \mathbb{Z}$.

The integral elements of K form an important subring of K.

Definition 9.2.13 (Ring of Integers). The *ring of integers* in K is

$$\mathcal{O}_K = \{x \in K \mid x \text{ is integral over } \mathbb{Z}\}.$$

It's not at all clear from the definition just what $\mathcal{O}_K$ is, or even that it's a ring. Proposition 9.2.16 below will give a more explicit description of $\mathcal{O}_K$.

Lemma 9.2.14. *The map $K \to K$ given by*

$$a + b\sqrt{D} \mapsto \overline{a + b\sqrt{D}} = a - b\sqrt{D}$$

is an isomorphism of fields.

Proof. We have

$$\begin{aligned}
\overline{(a + b\sqrt{D})(c + d\sqrt{D})} &= \overline{(ac + bd) + (ad + bc)\sqrt{D}} \\
&= (ac + bd) - (ad + bc)\sqrt{D} \\
&= (a - b\sqrt{D})(c - d\sqrt{D}) \\
&= \overline{a + b\sqrt{D}c + d\sqrt{D}}.
\end{aligned}$$

□

Lemma 9.2.15. *Let $\alpha \in K$. The determinant of left multiplication by α on the 2-dimensional $\mathbb{Q}$-vector space K is $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$. The trace of left multiplication is $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$. The characteristic polynomial of left multiplication by α is $x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha)$.*

Proof. A basis for K as a $\mathbb{Q}$-vector space is $1, \sqrt{D}$. The matrix of left multiplication by $\alpha = a + b\sqrt{D}$ on this basis is $\begin{pmatrix} a & Db \\ b & a \end{pmatrix}$. Since $T(\alpha) = 2a$ and $N(\alpha) = a^2 - Db^2$, the lemma follows. □

Proposition 9.2.16. *If* $D \equiv 1 \pmod 4$ *let* $\alpha = (1+\sqrt{D})/2$, *and otherwise let* $\alpha = \sqrt{D}$. *Then*

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \{a\alpha + b : a, b \in \mathbb{Z}\}.$$

Proof. First we prove that if $x = a + b\alpha \in \mathbb{Z}[\alpha]$, then $x \in \mathcal{O}_K$. By Lemma 9.2.15 it suffices to show that $\mathrm{Tr}(x)$ and $\mathrm{N}(x)$ lie in $\mathbb{Z}$. First we verify this for $x = \alpha$ by noting that $\mathrm{Tr}(\alpha) = 1$ and

$$N(\alpha) = \begin{cases} (1-D)/4 & \text{if } D \equiv 1 \pmod 4 \\ D & \text{otherwise.} \end{cases}$$

More generally, if $x = a + b\alpha$ with $a, b \in \mathbb{Z}$, then

$$\mathrm{Tr}(x) = \mathrm{Tr}(a + b\alpha) = 2a + b\,\mathrm{Tr}(\alpha) = 2a + b \in \mathbb{Z},$$

and

$$\begin{aligned} \mathrm{N}(x) &= (a + b\alpha)(a + b\overline{\alpha}) \\ &= a^2 + ab(\alpha + \overline{\alpha}) + b^2\alpha\overline{\alpha} \\ &= a^2 + ab\,\mathrm{Tr}(\alpha) + b^2\,\mathrm{N}(\alpha) \in \mathbb{Z}. \end{aligned}$$

For the other inclusion, suppose $x = a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ is integral over $\mathbb{Z}$. Then $\mathrm{Tr}(x) = 2a \in \mathbb{Z}$ and $\mathrm{N}(x) = a^2 - b^2D \in \mathbb{Z}$. Thus $a = a'/2$ for some $a' \in \mathbb{Z}$ and $(a')^2/4 - b^2D \in \mathbb{Z}$. Thus $(2b)^2D \in \mathbb{Z}$, so since D is square free the denominator of b is either 1 or 2. The denominator of b is 2 if and only if the denominator of a is 2 since $a^2 - b^2D \in \mathbb{Z}$. If the denominator of b is 1, then $a, b \in \mathbb{Z}$ and we are done, and if the denominator of b is 2, then $2b \in \mathbb{Z}$ and $(a')^2 \equiv (2b)^2D \pmod 4$, so D is a perfect square modulo 4 and hence $D \equiv 1 \pmod 4$ (since D is square free) and $x \in \mathbb{Z}[\alpha]$. □

Let $K = \mathbb{Q}\sqrt{D}$. Let $d = D$ if $D \equiv 1 \pmod 4$ and $d = 4D$ otherwise. We will see later that there is a natural bijection between ideals in $\mathcal{O}_K$ and binary quadratic forms of discriminant d. Moreover, $\mathrm{SL}_2(\mathbb{Z})$ equivalence of quadratic forms will correspond to a natural equivalence relation on ideals. Finally, the set of equivalence classes of ideals in $\mathcal{O}_K$ will have the structure of finite abelian group induced by multiplication of ideals. Understanding whether or not numbers are represented by certain quadratic forms, will correspond to deciding whether or not certain ideals are principal in $\mathcal{O}_K$, and this in turn leads to class field theory, which is one of the major accomplishments of 20th century number theory.