Appendix 12A. Composition rules: Gauss, Dirichlet, and Bhargava

We study generalizations of the identity (9.1.1), which leads to a notion of "multiplying" binary quadratic forms together, and hence to the group structure discovered by Gauss. We go on to study the reformulations of Dirichlet and Bhargava.

12.7. Composition and Gauss

In (9.1.1) we see that the product of any two integers represented by the binary quadratic form x^2+y^2 is also an integer represented by that binary quadratic form. We now look for further such identities. One easy generalization is given by

(12.7.1) $(u^2+Dv^2)(r^2+Ds^2) = x^2+Dy^2$ where $x = ur+Dvs$ and $y = us-vr$.

Therefore the product of any two integers represented by the binary quadratic form x^2+Dy^2 is also an integer represented by that binary quadratic form. For general *diagonal* binary quadratic forms (that is, having no "cross term" bxy) we have

(12.7.2) $(au^2+cv^2)(ar^2+cs^2) = x^2+acy^2$ where $x = aur+cvs$ and $y = us-vr$.

Notice here that the quadratic form on the right-hand side is different from those on the left; that is, the product of any two integers represented by the binary quadratic form ax^2+cy^2 is an integer represented by the binary quadratic form x^2+acy^2.

One can come up with a similar identity no matter what the quadratic form, though one proceeds slightly differently depending on whether the coefficient b is odd or even. The discriminant $d = b^2-4ac$ has the same parity as b. If d is even,

then

$$(au^2+buv+cv^2)(ar^2+brs+cs^2)=x^2-\frac{d}{4}y^2, \tag{12.7.3}$$

$$\text{where } x=aur+\tfrac{b}{2}(vr+us)+cvs \text{ and } y=rv-su.$$

If d is odd, then

$$(au^2+buv+cv^2)(ar^2+brs+cs^2)=x^2+xy-\frac{d-1}{4}y^2, \tag{12.7.4}$$

$$\text{where } x=aur+\tfrac{b-1}{2}vr+\tfrac{b+1}{2}us+cvs \text{ and } y=rv-su.$$

That is, the product of two integers represented by the same binary quadratic form can be represented by the principal binary quadratic form of the same discriminant.

Exercise 12.7.1. (a) Prove that if n is represented by $ax^2+bxy+cy^2$, then an is represented by the principal form of the same discriminant.

(b) Suppose that $d<0$. Deduce that if d is a square mod $4n$, then there is a multiple an of n which is represented by the principal form of discriminant d, with $1\le a\le\sqrt{|d|/3}$.

(c) We obtained the bound $1\le a\le\sqrt{|d|}$ when d is even in section 9.6. Use that method to find a bound in the case that d is odd.

What about the product of the values of two different binary quadratic forms? If d is even, we have

$$(au^2+buv+cv^2)(r^2-\tfrac{d}{4}s^2)=ax^2+bxy+cy^2, \tag{12.7.5}$$

$$\text{where } x=ur+\tfrac{b}{2}su+cvs \text{ and } y=vr-asu-\tfrac{b}{2}vs.$$

If d is odd, then

$$(au^2+buv+cv^2)(r^2+rs-\tfrac{d-1}{4}s^2)=ax^2+bxy+cy^2, \tag{12.7.6}$$

$$\text{where } x=ur+\tfrac{b+1}{2}su+cvs \text{ and } y=vr-asu-\tfrac{b-1}{2}vs.$$

That is, the product of an integer that can be represented by a binary quadratic form f and an integer that can be represented by the principal binary quadratic form of the same discriminant can be represented by f.

Exercise 12.7.2. Suppose that a is a prime and $d=b^2-4ac$ is even. Let $D=-d/4$.

(a) Show that if a divides r^2+Ds^2, then a divides either $r+(b/2)s$ or $r-(b/2)s$.

(b) Prove that if $r^2+Ds^2=an$, then there exist integers X,Y for which $n=aX^2+bXY+cY^2$.

If n is prime, then this result is true whether or not a is prime, but we will not prove that here. Assume though that is so.

(c) Suppose that $(d/p)=1$ and that ap is the smallest multiple of p that is represented by the principal form. Prove that a here must take the same value as in exercise 12.6.9.

(d) Prove that $1\le a\le\sqrt{|d|/3}$ and then use exercises 12.4.4 and 12.6.1(b) to prove that if $p<\sqrt{|d|}/2$, then $a=p$.

What about two different binary quadratic forms with no particular structure? For example,

$$(4u^2+3uv+5v^2)(3r^2+rs+6s^2)=2x^2+xy+9y^2$$

by taking $x=ur-3us-2vr-3vs$ and $y=ur+us+vr-vs$. These are three inequivalent binary quadratic forms of discriminant -71. Gauss called this *composition*, that is, finding, for given binary quadratic forms f and g of the same

discriminant, a third binary quadratic form h of the same discriminant for which

$$f(u,v)g(r,s) = h(x,y),$$

where x and y are quadratic polynomials in u, v, r, and s.

These constructions suggest many questions. For example, are the identities that we found for two given quadratic forms the only possibility? Could the product of two sums of two squares always equal the value of some entirely different quadratic form? When we are given two quadratic forms of the same discriminant, is it true that there is always some third quadratic form of the same discriminant such that the product of the values of the first two always equals a value of the third? That is, is there always a composition of two given binary quadratic forms of the same discriminant? If so, can we determine the third quadratic form quickly?

Gauss proved that one *can always* find the composition of two binary quadratic forms of the same discriminant. The formulas above can mislead one into guessing that this is simply a question of finding the right generalization, but that is far from the truth. All of the examples, (12.7.1) through to (12.7.6), are so explicit only because they are very special cases in the theory. In Gauss's proof he had to prove that various other equations could be solved in integers in order to find h and the quadratic polynomials x and y (which are polynomials in u, v, r, and s). This was so complicated that some of the intermediate formulas took two pages to write down and are very difficult to make sense of.[4] We will prove Gauss's theorem though we will approach it in a somewhat different way.

Exercise 12.7.3. Given non-zero integers a, b, c, d prove that there exist integers m, n such that the set of integers that can be represented by $(ar+bs)(cu+dv)$ as r, s, u, v run over the integers is the same as the set of integers that can be represented by $mx+ny$ as x, y run over the integers.

We finish this section by presenting a fairly general composition.

Proposition 12.7.1. *Suppose that $a_ix^2+b_ixy+c_iy^2$ for $i=1,2$ are binary quadratic forms of discriminant d such that $q=(a_1,a_2)$ divides $\frac{b_1+b_2}{2}$. Then*

$$(12.7.7) \quad (a_1x_1^2+b_1x_1y_1+c_1y_1^2)(a_2x_2^2+b_2x_2y_2+c_2y_2^2) = a_3x_3^2+b_3x_3y_3+c_3y_3^2$$

where $a_3 = a_1a_2/q^2$ and b_3 is any integer simultaneously satisfying the following (solvable) set of congruences:

$$b_3^2 \equiv d \pmod{4a_1a_2/q^2},$$
$$b_3 \equiv b_1 \pmod{2a_1/q}, \qquad b_3 \equiv b_2 \pmod{2a_2/q},$$
$$b_3(b_1+b_2) \equiv b_1b_2+d \pmod{4a_1a_2/q},$$

and c_3 is chosen so that the discriminant of $a_3x_3^2+b_3x_3y_3+c_3y_3^2$ is d.

Exercise 12.7.4. Show that the above congruences for b_3 can be solved.

Proposition 12.7.1 implies that we can always compose two binary quadratic forms f and g of the same discriminant, whose leading coefficients are coprime.

[4] See article 234 and beyond in Gauss's book *Disquisitiones Arithmeticae* (1804).

Proof sketch. Computer software verifies that (12.7.7) holds taking $a_3 = a_1a_2/q^2$, for any integer q dividing (a_1, a_2), with

$$x_3 = qx_1x_2 + \frac{b_2 - b_3}{2a_2/q} \cdot x_1y_2 + \frac{b_1 - b_3}{2a_1/q} \cdot x_2y_1 + \frac{b_1b_2 + d - b_3b_1 - b_3b_2}{4a_1a_2/q} \cdot y_1y_2,$$

$$\text{and} \qquad y_3 = \frac{a_1}{q} \cdot x_1y_2 + \frac{a_2}{q} \cdot x_2y_1 + \frac{b_1 + b_2}{2q} \cdot y_1y_2.$$

To ensure that we are always working with integers, the coefficients of x_3 and y_3 must be integers. So this formula works if we can find integers q and b_3 for which q divides a_1, a_2, and $\frac{b_1+b_2}{2}$, and the above four congruences hold simultaneously for integer b_3. It is difficult to determine whether there is such a b_3 for an arbitrary q, but not so challenging if $q = (a_1, a_2)$ divides $\frac{b_1+b_2}{2}$. □

Corollary 12.7.1. *For any given integers a, b, c, h, k we have*

$$(ab, hk, ch) \cdot (ac, hk, bh) \sim (ah, hk, bc).$$

Proof. We multiply (ab, hk, ch) and $(ac, hk, bh) \sim (bh, -hk, ac)$ using the proof of Proposition 12.7.1. We take $q = b$ so that $a_3 = ah$ and $2q|b_1 + b_2 = 0$. Selecting $b_3 = hk$ we find that the congruences of Proposition 12.7.1 reduce to $d \equiv (hk)^2 \pmod{4abh}$, which follows from $d = (hk)^2 - 4abch$. Hence we have that $(ab, hk, ch) \cdot (ac, hk, bh) \sim (ab, hk, ch) \cdot (bh, -hk, ac) \sim (ah, hk, bc)$.

To get more symmetry in the statement of the result we note that $(ah, hk, bc) \cdot (bc, hk, ah) = 1$, and so

$$(ab, hk, ch) \cdot (ac, hk, bh) \cdot (bc, hk, ah) \sim 1. \qquad \square$$

12.8. Dirichlet composition

Dirichlet claimed that when he was a student, working with Gauss, he slept with a copy of *Disquisitiones* under his pillow every night for three years. It worked, as Dirichlet found a way to better understand Gauss's proof of composition, which amounts to a straightforward algorithm to determine the composition of two given binary quadratic forms f and g of the same discriminant.

Exercise 12.8.1. Given any primitive binary quadratic form $f(x, y) \in \mathbb{Z}[x, y]$ and non-zero integer A, prove that there exist integers r and s such that $f(r, s)$ is coprime to A. Deduce that there exists a binary quadratic form g, for which $f \sim g$, with $(g(1, 0), A) = 1$.

Exercise 12.8.2. Suppose that $f(x, y), F(X, Y)$ are two binary quadratic forms, with $\operatorname{disc}(f) \equiv \operatorname{disc}(F) \pmod 2$, for which $f(1, 0) = a$ is coprime to $F(1, 0) = A$. Prove that there exist quadratic forms $g = ax^2 + bxy + cy^2$ and $G = AX^2 + bXY + CY^2$ with the same middle coefficient, such that $f \sim g$ and $F \sim G$.

Now suppose we begin with two quadratic forms of the same discriminant. Let A be the leading coefficient of one of them. Then the other is equivalent to a quadratic form with leading coefficient a, for some integer a coprime to A, by exercise 12.8.1. Then these are equivalent to quadratic forms $g = ax^2 + bxy + cy^2$ and $G = AX^2 + bXY + CY^2$, respectively, by exercise 12.8.2. Since these have the

same discriminant we deduce that $ac = AC$ and so there exists an integer h for which

$$g(x,y) = ax^2 + bxy + Ahy^2 \quad \text{and} \quad G(x,y) = Ax^2 + bxy + ahy^2.$$

Then

$$H(m,n) = g(u,v)G(r,s) \text{ with } H(x,y) = aAx^2 + bxy + hy^2,$$
$$\text{where } m = ur - hvs \text{ and } n = aus + Avr + bvs.$$

Dirichlet went on to interpret this in terms of what we would today call *ideals*; and this in turn led to the birth of modern algebra by Dedekind. In this theory one is typically not so much interested in the identity, writing H as a product of g and G (which is typically very complicated and none too enlightening), but rather in how to determine H from g and G. Dirichlet's proof goes as follows:

The ideal $I\left(\frac{-b+\sqrt{d}}{2}, a\right)$ is associated to a given binary quadratic form $ax^2 + bxy + cy^2$ (see section 12.10 of appendix 12B). Therefore when we multiply together g and G, we multiply together their associated ideals to obtain

$$J := I\left(\frac{-b+\sqrt{d}}{2}, a\right) \cdot I\left(\frac{-b+\sqrt{d}}{2}, A\right),$$

which contains aA as well as both $a \cdot \frac{-b+\sqrt{d}}{2}$ and $A \cdot \frac{-b+\sqrt{d}}{2}$. Since $(a, A) = 1$ there exist integers r, s for which $ar + As = 1$ and so our new ideal contains

$$r \cdot a \cdot \frac{-b+\sqrt{d}}{2} + s \cdot A \cdot \frac{-b+\sqrt{d}}{2} = \frac{-b+\sqrt{d}}{2}.$$

Therefore

$$J = I\left(\frac{-b+\sqrt{d}}{2}, aA\right)$$

which is the ideal associated with the binary quadratic form H.

Defining the class group. We now know that we can multiply together the values of any two quadratic forms of the same discriminant and get another. Since there are only finitely many equivalence classes of binary quadratic forms of a given discriminant this might seem to lead to a group structure, under multiplication. To prove this we will need to know that the usual group properties hold (most importantly, associativity), and also that the values of a binary quadratic form classifies the form. Unfortunately this is not quite true. In exercise 12.6.2 we saw that the only issue in distinguishing between the values taken by forms is perhaps the values taken by $ax^2 + bxy + cy^2$ and $au^2 - buv + cv^2$. However there is an automorphism $u = x, v = -y$ between their sets of values so they cannot be distinguished in this way. On the other hand, the ideals

$$I\left(\frac{-b+\sqrt{d}}{2}, a\right) \quad \text{and} \quad I\left(\frac{b+\sqrt{d}}{2}, a\right)$$

are quite distinct, and so multiplying ideals (and therefore forms) using Dirichlet's technique leads one immediately to being able to determine a group structure. This is called the *class group*, since the group acts on equivalence classes of ideals (and

so of forms). In this approach, associativity follows easily, as multiplication of the numbers in the ideals multiply associatively, and it is similarly evident that the class group is commutative. Therefore the class group is a commutative group, acting on the ideal classes of a given discriminant, with identity element given by the class of principal ideals (which correspond to the principal form).

We will now give a useful criterion to determine how to take square roots inside the class group.

Proposition 12.8.1. *If f is a binary quadratic form of fundamental discriminant d which represents the square of an odd integer, then there exists a binary quadratic form g of discriminant d for which $g \cdot g \sim f$.*

Proof. We begin by squaring the primitive form $ax^2 + bxy + acy^2$. Then

$$J := I\left(\frac{-b+\sqrt{d}}{2}, a\right)^2$$

contains $a^2, a \cdot \frac{-b+\sqrt{d}}{2}$, and $(\frac{-b+\sqrt{d}}{2})^2 = -a^2c - b(\frac{-b+\sqrt{d}}{2})$. Therefore J contains $a \cdot \frac{-b+\sqrt{d}}{2}$ and $b \cdot \frac{-b+\sqrt{d}}{2}$. Now $(a, b) = 1$ or else our original form was not primitive, and so J contains $\frac{-b+\sqrt{d}}{2}$. Therefore

$$J = I\left(\frac{-b+\sqrt{d}}{2}, a^2\right)$$

and the corresponding binary quadratic form is $a^2x^2 + bxy + cy^2$.

One can justify this by finding a suitable multiplication of forms, namely,

$$(ar^2 + brs + acs^2)(au^2 + buv + acv^2) = a^2x^2 + bxy + cy^2,$$

where $x = ru - csv$ and $y = asu + arv + bsv$.

Now if f represents a^2 with $(a, d) = 1$, then there exist integers b, c such that the quadratic form $F := a^2x^2 + bxy + cy^2$ is equivalent to f. Note that $(a, b)^2$ divides $d = b^2 - 4a^2c$, which is a fundamental discriminant and so squarefree except perhaps a power of 2. However a is odd and so $(a, b) = 1$. Therefore we let $g = ax^2 + bxy + acy^2$ so that, as in the previous paragraph $g \cdot g \sim F \sim f$. □

12.9. Bhargava composition[6]

Let us begin with one further explicit composition, a tiny variant on (12.7.3) (letting $s \to -s$ there):

$$(au^2 + 2Buv + cv^2)(ar^2 - 2Brs + cs^2) = x^2 + (ac - B^2)y^2$$
$$\text{where } x = aur + B(vr - us) - cvs \text{ and } y = us + vr.$$

Combining this with the results of the previous section suggests that if the discriminant d is divisible by 4 (which is equivalent to b being even), then

$$F(u, v)G(r, s)H(m, -n) = P(x, y) \tag{12.9.1}$$

[6]Although there is no Nobel Prize in mathematics, there is the *Fields Medal*, awarded every four years, only to people 40 years of age or younger. In 2014, in Korea, one of the laureates was Manjul Bhargava for a body of work that begins with his version of composition, as discussed here, and allows us to much better understand many classes of equations, especially cubic.

where $P(x,y) = x^2 - \frac{d}{4}y^2$ is the principal form and x and y are cubic polynomials in m, n, r, s, u, v. Analogous remarks can be made if the discriminant is odd.

In 2004 Bhargava came up with an entirely new way to find all of the triples F, G, H of binary quadratic forms of the same discriminant for which (12.9.1) holds: We begin with a 2-by-2-by-2 cube, the corners of which are labeled with the integers a, b, c, d, e, f, g, h.

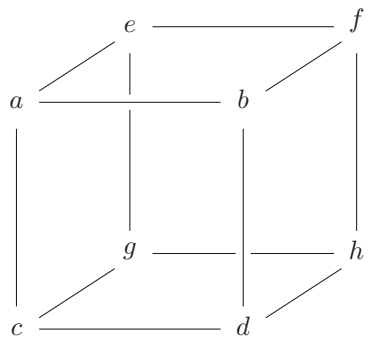

Figure 12.2. Bhargava's Rubik-type cube.

There are six faces of a cube, and these can be split into three parallel pairs. To each such parallel pair consider the pair of 2-by-2 matrices given by taking the entries in each face, those entries corresponding to opposite corners of the cube, always starting with a. Hence we get the pairs

$$M_1(x,y) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} x + \begin{pmatrix} e & f \\ g & h \end{pmatrix} y = \begin{pmatrix} ax+ey & bx+fy \\ cx+gy & dx+hy \end{pmatrix},$$
$$M_2(x,y) := \begin{pmatrix} a & c \\ e & g \end{pmatrix} x + \begin{pmatrix} b & d \\ f & h \end{pmatrix} y = \begin{pmatrix} ax+by & cx+dy \\ ex+fy & gx+hy \end{pmatrix},$$
$$M_3(x,y) := \begin{pmatrix} a & b \\ e & f \end{pmatrix} x + \begin{pmatrix} c & d \\ g & h \end{pmatrix} y = \begin{pmatrix} ax+cy & bx+dy \\ ex+gy & fx+hy \end{pmatrix},$$

where we have, in each, appended the variables, x, y, to create matrix functions of x and y. The determinant, $-Q_j(x,y)$, of each $M_j(x,y)$ is a quadratic form in x and y. Incredibly Q_1, Q_2, and Q_3 all have the same discriminant and their composition equals P, the principal form, just as in (12.9.1). We present two proofs. First, by substitution, one can exhibit that

$$Q_1(x,-y) = Q_2(x_2,y_2)Q_3(x_3,y_3)$$

where

$$y = \begin{pmatrix} x_3 & y_3 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \quad \text{and} \quad x = \begin{pmatrix} x_3 & y_3 \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Let's work though an example: Plot the cube in three dimensions, take the Cartesian coordinates of every corner (each 0 or 1), and then label the corner

(x, y, z), with $2^2x + 2y + z$, squared. Hence

$$a, b, c, d, e, f, g, h = 2^2, 6^2, 0^2, 4^2, 3^2, 7^2, 1^2, 5^2,$$

yielding the cube in Figure 12.3.

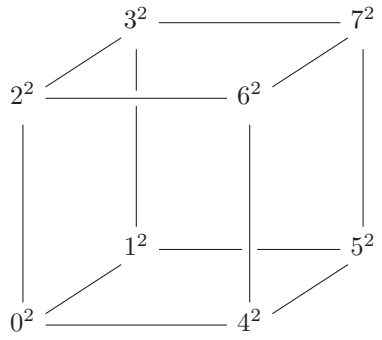

Figure 12.3. The construction of three binary quadratic forms using Bhargava's cube.

This cube leads to three binary quadratic forms of discriminant $-7 \cdot 4^4$:
$Q_1 = -4^2(4x^2+13xy+11y^2)$, $Q_2 = -2^2(x^2-2xy+29y^2)$, and $Q_3 = 4^2(8x^2+5xy+y^2)$.
After some work one can verify that

$$Q_1(m, n)Q_2(r, s)Q_3(u, v) = 4(x^2 + 4^3 \cdot 7y^2),$$

where x and y are the following cubic polynomials in m, n, r, s, u, v:

$$x = 8(-11mru - 3mrv + 25msu + 17msv - 17nru - 4nrv + 59nsu + 32nsv)$$

and $y = mru + mrv + 21msu + 5msv + 3nru + 2nrv + 31nsu + 6nsv$.

Bhargava proves his theorem, inspired by a 2-by-2-by-2 Rubik's cube. His idea is to apply one invertible linear transformation at a time, simultaneously to a pair of opposite sides, and to slowly "reduce" the numbers involved, while retaining the equivalence classes of Q_1, Q_2, and Q_3, until one reduces to a cube and a triple of binary quadratic forms with coefficients having a convenient structure.

Lemma 12.9.1. *If one applies an invertible linear transformation to a pair of opposite sides, then the associated binary quadratic form is transformed in the usual way, whereas the other two quadratic forms remain the same.*

Therefore we can act on our cube by such $\mathrm{SL}(2, \mathbb{Z})$-transformations, in each direction, and the three binary quadratic forms each remain in the same equivalence class.

Proof. If $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$, then we replace the face

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ by } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \beta; \text{ and } \begin{pmatrix} e & f \\ g & h \end{pmatrix} \text{ by } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \delta.$$

Then $M_1(x,y)$ gets mapped to

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\alpha + \begin{pmatrix} e & f \\ g & h \end{pmatrix}\beta\right\}x + \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\gamma + \begin{pmatrix} e & f \\ g & h \end{pmatrix}\delta\right\}y,$$

that is, $M_1(\alpha x+\gamma y, \beta x+\delta y)$. Therefore the quadratic form $Q_1(x,y)$ gets mapped to $Q_1(\alpha x+\gamma y, \beta x+\delta y)$ which is equivalent to $Q_1(x,y)$. Now $M_2(x,y)$ gets mapped to

$$\begin{pmatrix} a\alpha+e\beta & c\alpha+g\beta \\ a\gamma+e\delta & c\gamma+g\delta \end{pmatrix}x + \begin{pmatrix} b\alpha+f\beta & d\alpha+h\beta \\ b\gamma+f\delta & d\gamma+h\delta \end{pmatrix}y = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}M_2(x,y);$$

hence the determinant, $-Q_2(x,y)$, is unchanged. An analogous calculation reveals that $M_3(x,y)$ gets mapped to $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}M_3(x,y)$ and the determinant, $-Q_3(x,y)$, is also unchanged. □

The previous lemma allows one to proceed in "reducing" the three binary quadratic forms to equivalent forms that are easy to work with (rather as in Dirichlet's proof).

Proof of the Bhargava composition. We will simplify the entries in the cube by the following reduction algorithm:

• We select the corner that is to be a so that $a \neq 0$.

• We will transform the cube to ensure that a divides b, c, and e. If not, say a does not divide e, then select integers α, β so that $a\alpha + e\beta = (a,e)$, and then let $\gamma = -e/(a,e),\ \delta = a/(a,e)$. In the transformed matrix we have $a' = (a,e),\ e' = 0$, and $1 \leq a' \leq a-1$. It may well now be that a' does not divide b' or c', so we repeat the process. Each time we do this we reduce the value of a by at least 1; and since it remains positive this can only happen a finite number of times. At the end of the process a divides b, c, and e.

• We will transform the cube to ensure that $b = c = e = 0$. We already have that $a|b,c,e$. Now select $\alpha = 1,\ \beta = 0, \gamma = -e/a,\ \delta = 1$, so that $e' = 0, b' = b, c' = c$. We repeat this in each of the three directions to ensure that $b = c = e = 0$.

Replacing a by $-a$, we have that the three matrices are

$$M_1(x,y) := \begin{pmatrix} -a & 0 \\ 0 & d \end{pmatrix}x + \begin{pmatrix} 0 & f \\ g & h \end{pmatrix}y, \quad \text{so that } Q_1(x,y) = adx^2 + ahxy + fgy^2,$$

$$M_2(x,y) := \begin{pmatrix} -a & 0 \\ 0 & g \end{pmatrix}x + \begin{pmatrix} 0 & d \\ f & h \end{pmatrix}y, \quad \text{so that } Q_2(x,y) = agx^2 + ahxy + dfy^2,$$

$$M_3(x,y) := \begin{pmatrix} -a & 0 \\ 0 & f \end{pmatrix}x + \begin{pmatrix} 0 & d \\ g & h \end{pmatrix}y, \quad \text{so that } Q_3(x,y) = afx^2 + ahxy + dgy^2.$$

All three Q_j have discriminant $(ah)^2 - 4adfg$, and we observe that

$$Q_1(fy_2x_3 + gx_2y_3 + hy_2y_3, ax_2x_3 - dy_2y_3) = Q_2(x_2,y_2)Q_3(x_3,y_3)$$

where $x_1 = fy_2x_3 + gx_2y_3 + hy_2y_3$ and $y_1 = ax_2x_3 - dy_2y_3$. □

This brings to mind the twists of the Rubik's cube, though in that case one has only finitely many possible transformations, whereas here there are infinitely many possibilities, as there are infinitely many invertible linear transformations over $\mathbb{Z}$.

Appendices. The extended version of chapter 12 has the following additional appendices:

Appendix 12B. *The class group* is a group whose elements are the equivalence classes of quadratic forms with multiplication defined by composition as in appendix 12A. We will focus on classifying the all-important elements of order two.

Appendix 12C. *Binary quadratic forms of positive discriminant.* We have already explored at length the theory of binary quadratic forms of negative discriminant. Positive quadratic forms are quite a bit trickier, largely because there are infinitely many automorphisms of the solutions of a quadratic equation of this discriminant, corresponding to the solutions to Pell's equation, whereas for negative discriminants there is usually just the one non-trivial automorphism $(x, y) \to (-x, -y)$. Here we present some of that theory.

Appendix 12D. *Sums of three squares.* We discover here the connection between sums of three squares and class numbers and then develop Dirichlet's class number formula.

Appendix 12E. *Sums of four squares.* We give two proofs that every positive integer is the sum of four squares, including one via the theory of quaternions, and then discuss how many representations each integer has as the sum of four squares.

Appendix 12F. *Universality.* A quadratic form is universal if it takes all positive integer values. Although these were classified long ago by Ramanujan it was only recently that researchers found a much neater classification: simply verifying that the quadratic form represents every integer up to 290.

Appendix 12G. *Integers represented in Apollonian circle packings.* In appendix 9C we developed some of the mathematics of the curvatures inside a circle tiled by smaller circles. Now we show how some subset of the integers represented can be found by reducing the question to values of binary quadratic forms.