Correspondence and Composition

Grant Schoenebeck

May 24, 2004

1 Introduction

In this paper we investigate Gaussian composition. Furthermore, we study the correspondence theorem of ideal classes and classes of binary quadratic forms. We also show a generalization of this correspondence and composition to higher dimensions recently discovered by Manual Bhargava. Along with this generalization, Gaussian composition is one of at least 14 such correspondences. Although, more is known about Gaussian composition than the higher dimensional models, such a correspondence makes particular questions more relevant than ever before.

Amazingly, although Gauss studied composition of quadric forms, he did so almost a century before ideas were studied. There are two ways to view these two phenomena: The first is to see the correspondence, which relates ideal classes and classes of binary quadratic forms, as the more important of the two. This correspondence allows us to relate the two objects and bring the tools used in one realm to bear on the problems in the other. For example, this correspondence defines a group on the classes of binary quadratic forms by simply looking the the ideal class corresponding to each form and pulling back the group structure. On the other hand, the composition can be viewed as more important. Then the correspondence simply gives us another language with which to see how composition works.

1.1 Outline

In section 2 we will lay out basic properties of quadratic forms that we will use, and in section 3 we'll lay out the properties of quadratic rings and their ideas that we will use. Section 4 shows the correspondence between these two objects, and how the properties about forms and rings previously described relate. In section 5 we show another type of correspondence and composition defined over cubes of integers.

1.2 Resources

Many of the proofs are left incomplete, and the reader may for other reason be interested in learning more about this topic.

Stein's notes are a good source for an overview the correspondence of ideals classes and classes binary quadratic forms in the case of ideals of maximal rings (rings of integers of a quadratic field). Sections 2 is taken mostly from these notes, as a good portion of section 3 and 4.

Cassel's text offers an exposition of Dirichlet's proof of the composition law on primitive binary quadratic forms. This reference is special in that it does not use ideals in any way. Section 2.2 is an quick glance of Cassel's exposition.

The article by Bhargava gives a very brief overview of new correspondence and composition laws discovered and discusses their future potential.

The lecture notes of Bhargava's class on quadratic forms at Harvard contain the proof of the higher composition law given in section 5 and also provided a clear but brief picture of Gauss composition.

The texts of Jones and Cohl both layout the composition law by first showing the correspondence between ideals classes and quadratic forms.

2 Quadratic Forms

We start off by defining quadratic forms and paying particular attention to facts that will play a role when we want to compose such forms.

Definition 1 *A* quadratic form $f(x_1, \ldots, x_n)$ *is a degree 2 homogeneous polynomial. That is to say that*

$$f(x_1, \ldots, x_n) = \sum_{i,j} a_{i,j} x_i x_j$$

In this paper we'll deal with only binary quadratic formulas, so $n = 2$. Forms of higher spaces are usually written out using a symmetric $n \times n$ matrix M so that

$$f(\mathbf{x}) = \mathbf{x}^T M \mathbf{x}$$

We instead write a binary quadratic form as

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

which we will often denote $[a, b, c]$ for notational convenience.

Definition 2 *We say that a form is* integral *if it can be expresses as* $\sum_{i,j} a_{i,j} x_i x_j$ *with* $a_{i,j} \in \mathbb{Z}$ *for all* i *and* j.

This definition is one of two that are commonly used. The other is to define a form as integral if

$$f(\mathbf{x}) = \mathbf{x}^T M \mathbf{x}$$

where the entries of M all lie in $\mathbb{Z}$. Under this definition $[a, b, c]$ can only be integral if b is even because the symmetric matrix associated with $[a, b, c]$ is $\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$. This is the definition that Gauss used, but in most modern texts, the more general definition, which we have adopted, is used.

Definition 3 *We say that a binary quadratic form* $f(x, y)$ represents *a number* $n \in \mathbb{Z}$ *if there exists* $x_0, y_0 \in Z$ *such that* $f(x_0, y_0) = n$.

Although we will not discuss it here, much work has been done to study what numbers a particular form represents. The work along these lines is amazingly rich and beautiful.

Definition 4 *We say that a binary quadratic form is* primitive *if* $gcd(a, b, c) = 1$.

Definition 5 *We define the* determinant *of a quadratic form* $[a, b, c]$ *to be* $b^2 - 4ac$.

Now we want to set up a notion of equivalence on forms.

Definition 6 *We say that two binary quadratic forms* f *and* g *are* improperly equivalent *if there exists a matrix* $A \in GL_2(\mathbb{Z})$ *such that*

$$f(A\begin{pmatrix} x \\ y \end{pmatrix}) = g(x, y)$$

First note that equivalence is an equivalence relation. The reason is that we define equivalence in this way is explained by the following proposition.

Proposition 7 *If f and g are improperly equivalent binary quadratic forms, then they represent the same numbers.*

Proof: If f represents n than there exists $x_0, y_0 \in \mathbb{Z}$ such that $f(x_0, y_0) = n$, but there exists $A \in GL_2(\mathbb{Z})$ such that $f(x, y) = g(A\binom{x}{y})$ so g represents n also. ■

Proposition 8 *If f and g are improperly equivalent binary quadratic forms, then they have the same discriminant.*

This follows from that fact that

$$disc\left(g(A\begin{pmatrix} x \\ y \end{pmatrix})\right) = disc\,(g(x, y)) \cdot disc\,(A)^2$$

which can be verified by arithmetic, so we will not show the computation here. See [Ste03] for the details. □

At first "improperly equivalent" seems like it should be the correct definition. However, later on we will see that even a stricter notion of equivalence works, and so we will want to use that. It turns out that this stricter definition is vital to understanding forms, but we will not see any applications in this paper. One example is studying the genera of forms.

Definition 9 *We say that two binary quadratic forms f and g are* properly equivalent *if there exists a matrix $A \in SL_2(\mathbb{Z})$ such that*

$$f(A\begin{pmatrix} x \\ y \end{pmatrix}) = g(x, y)$$

We want that the forms are equivalent in this higher sense, and we note that the discriminant cannot tell if two forms are improperly, or properly equivalent. Also, note here that $f(x, y)$ is always improperly equivalent to $f(y, x)$, but not necessarily properly equivalent. So the proper part of equivalence is an ordering condition on the variables.

Example 10 $f = [1, 0, 3]$ is properly equivalent to $g = [31, -40, 13]$ because

$$g\left(\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}\mathbf{x}\right) = \left(\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}\mathbf{x}\right)^T \begin{bmatrix} 31 & -20 \\ -20 & 13 \end{bmatrix} \left(\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}\mathbf{x}\right) =$$

$$\mathbf{x}^T \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 31 & -20 \\ -20 & 13 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \mathbf{x} = \mathbf{x}^T \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \mathbf{x}$$

Example 11 $f = [3, 0, 1]$ is improperly, but not properly equivalent to $g = [31, -40, 13]$. The previous example shows that $[1, 0, 3]$ and g are improperly equivalent. We know that f and $[1, 0, 3]$ are improperly equivalent, so it follows that f and g are improperly equivalent.

However, supposed that they are properly equivalent. Then by transitivity $[1, 0, 3]$ and f are also properly equivalent. However

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\mathbf{x}\right) = \mathbf{x}^T \begin{bmatrix} a & b \\ c & d \end{bmatrix}^T \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathbf{x} =$$

$$\mathbf{x}^T \begin{bmatrix} a^2 + 3c^2 & ab + 3cd \\ ab + 3cd & b^2 + 3d^2 \end{bmatrix} \mathbf{x}$$

for this to be the form $[3, 0, 1]$ it must be that $a^2 + 3c^2 = 3 \Rightarrow a = 0, c = 1$, and $b^2 + 3d^2 = 1 \Rightarrow b = 1, d = 0$. But $\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = -1$. So f and $[1, 0, 3]$ are not properly equivalent.

2.1 Addition Properties of the Discriminant

The discriminant will be central to our treatment of binary quadratic forms. The sign of the discriminant is very important.

Definition 12 *We say that a binary quadric form f is* definite *if disc$(f) < 0$.*

Proposition 13 *Definite forms either represent only positive numbers, or only negative numbers, but never both.*

Proof: Let $f(x,y) = ax^2 + bxy + cy^2$. Then

$$\begin{aligned} 4a(f(x,y)) &= 4a(ax^2 + bxy + cy^2) = 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 + (4ac - b^2)y^2 \geq 0 \end{aligned}$$

■

Another relevant fact is that the discriminant is always $\equiv 0, 1 \mod 4$. This follows easily from that fact that the only quadratic residues mod 4 are 0 and 1, and the discriminant $= b^2 - 4ac \equiv b^2 \mod 4$. Moreover, for any possible discriminant, a number $\equiv 0, 1 \mod 4$, we can find a form with that discriminant.

In fact, there are a special set of forms, called the principal forms, which correspond to each possible discriminant.

Definition 14 *The* principal form *of discriminant d is* $[1, 0, -d/4]$ *if* $d \equiv 0 \mod 4$*, and* $[1, 1, -(d-1)/4]$ *if* $d \equiv 1 \mod 4$.

A quick calculation shows that the primitive form of discriminant d, indeed has discriminant d. This gives us an explicit bijection between possible discriminants and a particular set of binary quadratic forms. These forms will play a special role in the correspondence between binary quadratic forms and ideals later.

2.2 A Look Toward Composition

Gauss proved that that proper equivalence classes of primitive binary quadratic forms with the same determinant have a group structure.

The basic idea is that any two forms of the same determinant are properly equivalent to two forms with the same middle coefficient and with leading coefficients that are relatively prime. So given two primitive binary quadratic forms $f_1(x,y) = a_1x^2 + b_1xy + c_1y^2$ and $f_2(x,y) = a_2x^2 + b_2xy + c_2y^2$ such that $disc(f_1) = disc(f_2)$, we can find properly equivalent forms $f_1'(x,y) = a_1'x^2 + bxy + c_1'y^2$ and $f_2'(x,y) = a_2'x^2 + bxy + c_2'y^2$ of f_1 and f_2 respectively, where a_1' and a_2' are relatively prime. Note that the middle coefficients are the same, and also that if $a \neq 0$, then c is completely determined by a, b, and the determinant.

The composition of the class of f_1 and the class of f_2 is the same as the composition of the class of f_1' and f_2'. And we define class of the composition of these forms to be the class of $f_3' = a_1'a_2'x^2 + bxy + c_3y^2$ where c_3 is what it needs to be to make f_3 have the same determinant as f_1 and f_2. Notice we multiply the leading coefficients, and leave the middle one the same.

This gives intuition that the "principal" forms are the identity elements of the group. Say that $[1, b, c]$ is a principal form. Then $b = 0$ or $b = 1$. Because the leading coefficient of the principal form is 1, we find a properly equivalent form $[1, b+2k, c]$ for any $k \in \mathbb{Z}$ by applying the matrix $\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ to the form. Now any form $[a', b', c']$ of the same discriminant must have $b' \equiv b \mod 2$.

So given any form $[a', b', c']$ of the same discriminant as the principal form $[1, b, c]$, there is a form $[1, b', c'']$ properly equivalent to $[1, b, c]$. Then the composition of $[a', b', c']$ and $[1, b', c'']$ is $[a', b', c']$ (because $1 \cdot a' = a'$ and $b' = b'$), thus showing the the principal from is the identity.

Although, this is the original way that Gauss proceeded, we will take a different route. We will create a bijection between classes of quadratic forms of discriminant d, and ideal classes of quadratic rings with discriminant d. Then, the group structure of the ideal classes of the rings will endow the proper equivalence classes of binary quadratic forms of determinant d with a group structure.

3 Ideals of Quadric Rings

In this section we describe the properties of quadratic rings and their ideals that are necessary to understand the composition. Many texts only describe the correspondence for maximal rings (rings which are the ring of integers for some quadratic field), but this leaves a ting of desire. Gauss's original worked for any primitive forms, not simply forms with discriminant's corresponding to discriminants of quadratic fields. Moreover this limitation is not inherent to the problem, and we can avoid it by looking at quadratic rings more generally.

Definition 15 *A* quadratic ring *is a commutative and associative ring with identity of free rank 2 as a $\mathbb{Z}$-module.*

If S is a quadratic rings, then $S = \langle 1, \tau \rangle$ where $1 \cdot 1 = 1$, $1 \cdot \tau = \tau$, and $\tau^2 = a + b\tau$. Now because adding $k \in \mathbb{Z}$ to τ adds $2k$ to b we can always make it so that $b = 0$ or $b = 1$. For if $\tau^2 = a + b\tau$, then $(\tau + k)^2 = (a + k^2) + (2k + b)\tau$.

Definition 16 *The* discriminant *of $S = \langle 1, \tau \rangle$ is $b^2 + 4a$, the discriminant of the characteristic polynomial of τ, $\tau^2 - b\tau - a = 0$.*

We can embed any quadratic ring into $\mathcal{C}$ in exactly two ways by letting τ be the two solution to the characteristic polynomial (unless $a = b = 0$). We will implicitly ignore this special case for the rest of the paper.

Note again here that the discriminant is always $0, 1 \mod 4$. And that we can get any discriminant by setting $b = 0$, $a = d/4$ if $d \equiv 0 \mod 4$ and $b = 1$, $a = (d-1)/4$ if $d \equiv 1 \mod 4$.

This gives us a bijective function $S : \tilde{\mathbb{Z}} \leftrightarrow$ quadratic rings, where $\tilde{\mathbb{Z}} = \{x \in \mathbb{Z} : x \equiv 0, 1 \mod 4\}$.

Let R be a quadratic ring, and I an idea of R.

Definition 17 *We define the norm of I to be $|R/I|$ when considering the additive group structure of R and I.*

Proposition 18 *If $I \subseteq R$ is an ideal with basis $[\alpha, \beta]$ and d is the discriminant of R then*

$$\begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix} = d \cdot N(I)^2$$

Proof: There exists a 2×2 integer matrix A such that

$$A \binom{a_1}{a_2} = \binom{\alpha}{\beta}$$

where (a_1, a_2) is a basis for R as a $\mathbb{Z}$ module. But then

$$\begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix} = det\left(A \begin{bmatrix} a_1 & a_1' \\ a_2 & a_2' \end{bmatrix}\right)^2 = det(A)^2 d = N(I)^2 d$$

■

Definition 19 *We define the norm of an element $\alpha \in \mathbb{R}$ to be $\alpha \cdot \alpha' \in \mathbb{Z}$ where α and α' are the two embeddings of α in to $\mathcal{C}$.*

Two ideals I and J of a quadratic ring R are considered equivalent if there exist elements $\alpha, \beta \in R$ so that $\alpha I = \beta J$ and $N(\alpha\beta) > 0$

Furthermore, because any quadratic ring R is isomorphic to a free $\mathbb{Z}$-module: $\mathbb{Z} \oplus \mathbb{Z}$, we know that any ideal of R can generated by two elements.

So we can write any ideal I as $I = [\alpha, \beta]$ so that $I = \{x\alpha + y\beta : x, y \in \mathbb{Z}\}$. Now in setting up the equivalence, it will be important that we not arbitrarily order the basis of an ideal. This corresponds to quadratic forms being "properly" equivalent. In our correspondence, we will set up something like $N(\alpha x + \beta y)$. If we did not order α and β, then $N(\alpha x + \beta y)$ would be equivalent to $N(\beta x + \alpha y)$, which would mean in our correspondence that $f(x, y)$ is always properly equivalent to $f(y, x)$. The point here is that well ordering on bases, and proper equivalence will end up being the same thing, but one deals with forms, and the other with ideals.

Definition 20 *A basis $[\alpha, \beta]$ of an $I \subseteq R$ is* correctly ordered *if*

$$\frac{\alpha\beta' - \beta\alpha'}{d} > 0$$

where d is the discriminant and α', and β' are the other embedding into the complex numbers of α and β.

Similarly to with the case of quadratic forms we have the following proposition.

Proposition 21 *Any two correctly ordered bases of an ideal $I \subseteq R$ are equivalent by an element of $SL_2(\mathbb{Z})$ and conversely, any basis that are equivalent by an element of $SL_2(\mathbb{Z})$ to an correctly ordered basis, is well ordered.*

The proof is easy enough, so we omit it. See [Ste03] for the details. □

4 Correspondence

We are now ready to show the correspondence between ideals and binary quadratic forms. First we explicitly state the correspondence.

Definition 22 *Given an ideal I, with an ordered basis $[\alpha, \beta]$ we define*

$$Q(I) = \frac{N(\alpha x + by)}{N(I)}$$

Definition 23 *Given a binary quadratic form $Q = ax^2 + bxy + cy^2$ we define*

$$I(Q) = [a, \frac{b - \sqrt{d}}{2}]$$

where $d = b^2 - 4ac$, the discriminant.

Note that the ideal we obtain does not depend on c. The agrees with how we composed forms before.

Proposition 24 *If $[\alpha, \beta]$ is an ideal $I \subseteq R$, then $Q(I)$ is a integral quadratic form with the same discriminant as R.*

Proof: $Q(I) = N(\alpha x + by)/N(I) = [a, b, c]$, and $N(\alpha x + by) = (\alpha x + \beta y)(\alpha' + \beta' y) = \alpha\alpha' x^2 + (\alpha\beta' + \alpha'\beta)xy + \beta\beta' y^2 = Ax^2 + Bxy + Cy^2$. Now A, B, and C are in $\mathbb{Z}$ because they are norms and traces. Also they are each elements of $II' = N(I)$ and so [a, b, c] is an integral form.

We also want to show that the discriminant of this form is that of R. But $disc([a, b, c]) = b^2 - 4ac = (B^2 - 4AC)/N(I)^2 = (\alpha\beta' - \beta\alpha)^2/N(I)^2 = d$. The last step follows from Proposition 18. ■

This shows that at least we don't land too far from our goal. We show that the same is true for the mapping in the opposite direction.

Proposition 25 *Let $Q = [a, b, c]$ be a quadratic form of discriminant d (if $d < 0$ assume that Q is positive definite), then $I(Q)$ is an ideal of a quadratic ring of discriminant d.*

Proof: It is easy to see that $I(Q)$ is an ideal of $S(d)$ because $\frac{b-\sqrt{d}}{2}$ is the root of the characteristic polynomial of the quadratic ring $S(d)$. ■

Before proceeding further, we explicitly state the goal.

Theorem 26 *There is a bijection between classes of properly equivalent binary quadratic forms of discriminant d and ideal classes of $S(d)$, (where we take the positive definite forms if $d < 0$).*

The proof consists of showing that $I(Q(I))$ is equivilent (in the same ideal class as) I, and that $Q(I(Q))$ is properly equivalent to Q. The proof is long and not very enlightening, so we omit it here, but refer the reader to [Jon67]. □

This correspondence works pretty well flawlessly. But, composition on binary quadratic forms was studied before this correspondence was known. In a sense, the correspondence is just an easy way of seeing the composition, and Gauss discovered the more fundamental results when he found the composition law on binary quadratic forms. However, it is the correspondence that gives many applications for the composition.

5 The Cube Law

What we are really seeing here is that modulo $SL_2(\mathbb{Z})$ the binary quadratic forms have a group structure when the discriminant is fixed. Also, the discriminant is an invariant of the action of $SL_2(\mathbb{Z})$.

We now extend these properties to an larger object than binary quadratic forms. Again we will find a group structure on the forms with the same discriminant, and again we will define the discriminant to be an invariant of an action on the objection.

The objects that we will look at are elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. These can be thought of as cubes of integers. That is, $a, b, c, d, e, f, g \in \mathbb{Z}$ looking like

```
  e-----f
 /|    /|
a-|---b |
| g---|-h
|/    |/
c-----d
```

We again set up an equivalence using $SL_2(\mathbb{Z})$, but this time $SL_2(\mathbb{Z})$ can act on it in three different ways, so we define an action of $SL_2(\mathbb{Z})^3$ on $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. To show how this works, we define the following matrices, which are just the faces of the cube.

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$
$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix} \qquad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}$$
$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix} \qquad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}$$

Then the first component of $SL_2(\mathbb{Z})^3$ acts on M_1 and N_1 adding linear combinations of them. The second component of $SL_2(\mathbb{Z})^3$ acts on M_2 and N_2, and the third on M_3 and N_3.

We can also define three quadratic forms from this cube.

$$Q_i(x, y) = -Det(M_i x - N_i y)$$

Proposition 27 *Q_1, Q_2, and Q_3 all have the same discriminant.*

The proof only involves arithmetic, and so we omit it. □

Proposition 28 *Q_1 an invariant of the action $\{e\} \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$*

Proof: By looking at the cube, we can see that actions of the form $\{e\} \times SL_2(\mathbb{Z}) \times \{e\}$ act on M_2 and N_2, or the right at left sides of the cube. The corresponds to acting on the column of M_1 and N_1 by the same action of $SL_2(\mathbb{Z})$. Similarly actions of the form $\{e\} \times \{e\} \times SL_2(\mathbb{Z})$ action on the rows of M_1 and N_1. We know that operations of $SL_2(\mathbb{Z})$ on the rows or columns of a matrix do not change the determinant. ■

A similar fact holds for Q_2 and Q_3.

Proposition 29 *$disc(-Det(M_1x-N_1y))$ is an invariant of the action $SL_2(\mathbb{Z})^3$*

Proof: This follows from the previous proposition and that fact that when $SL_2(\mathbb{Z})$ acts on M_1 and N_1, we will get a different Q_1 which is properly equivalent to previous one. And they therefore have the same discriminant. ■

To show the laws of composition, we first create a correspondence, and then gives the cubes the same composition as the obvious composition on the equivalent algebraic objects.

5.1 The Correspondence

We first need another definitions.

Definition 30 *Fractional ideals I_1, I_2, $I_3 \subseteq R$ are* collinear ideas *if $I_1 \cdot I_2 \cdot I_3 \subseteq S$ and $N(I_1)N(I_2)N(I_3) = 1$.*

Now we state the goal:

Theorem 31 *There is a bijection natural*

$$\frac{\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2}{SL_2(\mathbb{Z})^3} \leftrightarrow (S, (I_1, I_2, I_3))$$

where S is a quadratic ring and I_1, I_2, $I, 3$ are a triple of collinear ideals.

Proof: Suppose we have $(S,(I_1,I_2,I_3))$ as described above. Then $s =< 1,\tau >$ where $\tau^2 = D/4$ if $D = disc(S) \equiv 0 \mod 4$, and $\tau^2 = \tau + (D-1)/4$ if $D = disc(S) \equiv 1 \mod 4$. Then let $I_1 =< \alpha_1, \alpha_2 >$, $I_2 =< \beta_1, \beta_2 >$, and $I_3 =< \gamma_1, \gamma_2 >$.

$$\alpha_i \beta_j \gamma_k = c_{i,j} + a_{i,j}\tau \qquad (1 \le i,j,k \le 2) \tag{1}$$

where the a's and the c's are all integers because the ideals are collinear.

Now we let the a's define a cube in the obvious way. (It will turn out that the c's just depend on how we choose τ). With a little work we can see that applying an element of $M \in SL_2(\mathbb{Z})$ to the basis of I_1 is like applying $M \times \{e\} \times \{e\}$ to A.

Conversely, suppose we have a cube A, we go backward in the same manner. We have to show that the c's are really already determined, and that the inverse map is the same as the forward one. We do so in two steps.

Step 1: We can write:

$$\begin{aligned} \alpha_i &= r_i + s_i\tau \\ \beta_i &= t_i + u_i\tau \\ \gamma_i &= v_i + w\tau \end{aligned}$$

for $r_i, s_i, t_i, u_i, v_i \in \mathbb{Q}$ because $I_i \subset S \otimes \mathbb{Q}$.

By some arithmetic, we see from the the forward map that $disc(A) = N(I_1)^2 N(I_2)^2 N(I_3)^2 D$ where D is the discriminant of the quadratic ring that we are in. (To see this note that $N(I_1) = \begin{vmatrix} r_1 & s_1 \\ r_2 & s_2 \end{vmatrix}$. Because I_1, I_2, and I_3 are collinear we get that $disc(A) = D$. So we already know the discriminant of the ring that we are dealing with, and we get a monic quadratic equation for τ. We multiply out the left side of the equations 1, write it so that the power of τ is always < 2, and equate the coefficients of τ in order to get the values of the a's in terms of these indeterminants.

Step 2: We show that the c's are determined using the associative law.

$$\begin{aligned} & (\alpha_i\beta_j\gamma_k)(\alpha_{i'}\beta_{j'}\gamma_{k'}) = (\alpha_{i'}\beta_j\gamma_k)(\alpha_i\beta_{j'}\gamma_{k'}) \\ \Rightarrow \quad & (c_{ijk} + a_{ijk}\tau)(c_{i'j'k'} + a_{i'j'k'}\tau) = (c_{i'jk} + a_{i'jk}\tau)(c_{ij'k'} + a_{ij'k'}\tau) \end{aligned}$$

If we write out these equations for all $1 \le i,j,k \le 2$ and $i \ne i'$, $j \ne j'$, $k \ne k'$ we get eight equations. Then equating the coefficients of 1 and τ gives equations for the c's in terms of the a's.

The ideal classes of I_1, I_2, and I_3 are also determined because $I_1 = [\alpha_1, \alpha_2]$ where $\alpha_1 = c_{1jk} + a_{1jk}\tau$ and $\alpha_2 = c_{2jk} + a_{2jk}\tau$. ■

The correspondence then defines a group action on cubes of the same determinant, because there is a natural group structure on triples of collinear ideas of a particular quadratic ring, namely multiplying element wise. So $(I_1, I_2, I_3), (J_1, J_2, J_3) \rightsquigarrow (I_1J_1, I_2J_2, I_3J_3)$

We now note that this composition is only one of at least 14, which include Gaussian composition. For a full list of the 14 correspondences, see [Bha].

There is also a neat corollary. For any cube $A \rightsquigarrow Q_1, Q_2, Q_3$ we can define the "sum" of Q_1, Q_2, and Q_3 is zero.

Corollary 32 *This is Gaussian composition!*

This is because under the correspondence of quadratic forms and ideals, Q_1, Q_2, Q_3 correspond to (I_1, I_2, I_3), the collinear triple of ideals. Therefore, in a maximal ring, $I_1 \cdot I_2 \cdot I_3 = 1$.

5.2 Application

In this section we briefly describe one application of correspondence. It is easier to enumerate the proper equivalence classes of quadratic forms, than it is do directly compute the ideal class of a quadratic ring. Of course, using correspondence, we see that each of these problems is actually the same.

Reduction theory has been used to compute the equivalence classes of quadratic forms of a certain discriminant.

Definition 33 *A positive definite quadratic form $[a, b, c]$ is reduced if $|b| \leq a \leq c$ and at least on of the two inequalities is an equality.*

The use of this definition is that there is only one reduced quadratic form an any equivalence class. So searching for all equivalence classes of a particular discriminant is as easy as finding all the reduced forms of a certain discriminant.

These new correspondences includes cubic rings with ideals. If such a notion of reduction could be found on the forms which correspond to cubic rings and an ideal, then it would be likely yield a fast algorithm for finding the ideal classes of cubic rings.

References

[Bha] Manjul Bhargava. Math 251: Arithematic theory of quadratic forms. Course notes, taken by me from Math 251, taught at Harvard in the spring of 2003.

[Bha02] Manjul Bhargava. Gauss composition and generalizations. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 1–8. Springer, Berlin, 2002.

[Cas78] J. W. S. Cassals. *Rational Quadratic Forms.* Academic Press, 1978.

[Coh62] Harvey Cohn. *Advanced Number Theory.* Dover, 1962.

[Jon67] Burton W. Jones. *The Arithmetic Theory of Quadratic Forms*, volume 10 of *The Carus Mathematical Monographs.* The Mathematical Association of America, 1967.

[Ste03] William Stein. Elementary number theory and elliptic curves. Course notes from Math 124: Elementrary Number Theory, taught at Harvard in the fall of 2002. http://modular.fas.harvard.edu/edu/Fall2002/124/stein/, MAY 2003.