Composition and Bhargava's Cubes

Florian Bouyer

0807637

Contents

1 Introduction

In 1801, while studying binary quadratic forms, Gauss constructed a composition law in his Disquisitones Arithmeticae [Gauss(1986)]. This composition law gave a group structure to the set of equivalence classes of primitive binary quadratic forms of a given discriminant, which was remarkable as this was done before the notion of a group existed. A useful consequence of this group structure was discovered by Dirichlet around 1838, when he showed a bijection between this set and the set of ideal classes of quadratic orders. This had a twofold impact: in one direction it gave a simpler method of showing that composition did turn the aforementioned set into a group; while in the other direction it gave a tool to compute and understand the ideal classes, a tool which is still used today.

It seems natural to ask if we can find other sets of equivalent forms and equip them with a generalised composition law, which will not only turn the set into a group, but also give us a tool to explore different number fields or rings. In 2004 Bhargava started to answer this question in a series of four articles, where he finds fourteen composition laws which can be used to find information on number rings and their class groups. He finds these composition laws by considering different size cubes of integers and creating different forms from them. This idea was revolutionary as with this he managed to shed some light on quartic and quintic number fields. Due to the impact they had the cubes are now referred to as Bhargava's cubes.

This paper is divided in two main parts, in section 2 we will look at binary quadratic forms. We will spend some time on the reduction theory of positive definitive forms, look at Dirichlet's composition, before proving the correspondence between equivalence classes of primitive binary quadratic forms and ideal classes of oriented orders of quadratic fields. The aim of this section is to both show the depth of information we have from binary quadratic forms, we will only cover a minute fraction of it, and to introduce the main idea which links binary quadratic forms and ideal classes.

The second part, that is Section 3, will follow Bhargava's first, out of the four, papers. We will look at $2 \times 2 \times 2$ cubes of integers, and construct different objects which will be in correspondence with different modules of a quadratic ring. Since we will be exploring quadratic rings, among our constructions we will recover Gauss's composition law, but we shall look approach it from a different angle than in Section 2. The five objects we will be looking at are: binary quadratic forms; $2 \times 2 \times 2$ cubes of integers; binary cubic forms; pairs of binary quadratic forms and quaternary alternating 2-forms.

Notation. In this paper if $D < 0$ then $\sqrt{D}$ will be the notation for $i\sqrt{|D|}$.

2 A classical view on Gauss composition

2.1 Some definitions

To start this section we are going to follow [Cox(1989)] and [Lemmermeyer(2010)] to introduce the concept of quadratic forms and how this led Gauss to create a composition law. We start by defining our object of interest, namely:

Definition 2.1. A *binary quadratic form* is a polynomial in two variables of the form $f(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$.

Furthermore we say a binary quadratic form is *primitive* if $\gcd(a, b, c) = 1$.

Strictly speaking the above definition should be called "integral binary quadratic forms" but since in this paper we will only deal with integral forms, that is where the coefficients are over $\mathbb{Z}$, we will drop the adjective "integral". In this paper, to represent the binary quadratic form $ax^2 + bxy + cy^2$, we will alternate between the notation (a, b, c) (as used originally by Gauss [Gauss(1986), Section 153]) when we are not worried about the value of x and y, and the notation $f(x, y)$ (as used by Cox [Cox(1989)]). We note that any binary quadratic form is an integer multiple of a primitive binary quadratic form. An important number related to a binary quadratic form is the *discriminant*:

Definition 2.2. The *discriminant*, D, of a binary quadratic form (a, b, c) is the integer $D = b^2 - 4ac$.

If we consider the group $\mathrm{SL}_2(\mathbb{Z})$, that is the set of all two by two matrices with determinant 1 and integer entries equipped with the multiplication operation, we can define an action on the set of binary quadratic forms as follow. Let $f(x, y)$ be a binary quadratic form and

$$S = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Then we can define a new binary quadratic form $f^S(x, y) = f(rx + sy, tx + uy)$.

Definition 2.3. We say two binary quadratic forms $f(x, y)$ and $f'(x, y)$ are *equivalent* if there exists $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $f^S(x, y) = f'(x, y)$.

A number m is *represented* by a binary quadratic form $f(x, y)$ if there exists $(x_1, y_1) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ such that $f(x_1, y_1) = m$.

Next we note a few invariants of the action of $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 2.4. *Let $f(x, y)$ and $f'(x, y)$ be two equivalent binary quadratic forms then:*

1. *$f(x, y)$ and $f'(x, y)$ have the same discriminant,*

2. *$f(x, y)$ and $f'(x, y)$ represent the same numbers,*

3. let g and g' be the gcd of the coefficients of $f(x,y)$ and $f'(x,y)$ respectively. Then $g=g'$.

Proof. First we note that to every binary quadratic form corresponds a two-by-two matrix. Namely if $f(x,y)=ax^2+bxy+cy^2$, then the matrix

$$A=\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

is such that $f(x,y)=\underline{x}^TA\underline{x}$, where $\underline{x}=(x,y)$ is a column vector. We can see that $\det A=ac-\frac{b}{4}=-\frac{D}{4}$, where D is the discriminant of f. By definition $f'=f^S=(S\underline{x})^TA(S\underline{x})=\underline{x}^T(S^TAS)\underline{x}$ and since $\det S=1$ we have that $\det(S^TAS)=\det A$, i.e., the discriminant of f is the same as the discriminant of f'.

The binary quadratic form f can be considered as a map from $\mathbb{Z}^2\setminus\{(0,0)\}\to\mathbb{Z}$ mapping $(x,y)\mapsto f(x,y)$. Letting $f'=f^S$ we get the following commutative diagram:

$$\begin{tikzcd}
\mathbb{Z}^2\setminus\{(0,0)\} \arrow[r, "f"] & \mathbb{Z} \\
\mathbb{Z}^2\setminus\{(0,0)\} \arrow[u, "S", "\cong"'] \arrow[ur, "f'"'] &
\end{tikzcd}$$

Since $\mathrm{SL}_2(\mathbb{Z})$ is a group, every element $S\in\mathrm{SL}_2(\mathbb{Z})$ has an inverse, hence S really gives a bijection as showed in the diagram. So the image of f' is the same as the image of f, that is, they represent the same numbers.

Let g' the gcd of the coefficients of $f'(x,y)$. Then notice that the numbers that $f'(x,y)$ represents are all divisible by g'. Also note that $f(1,0)=a$, $f(0,1)=c$ and $f(1,1)=a+b+c$, so using the second statement of this theorem we know that $g'|a$, $g'|c$ and $g'|(a+b+c)$, hence $g'|b$. Hence $g'|g$, and a symmetrical argument gives $g|g'$, so we have $g=g'$ □

The last part of the theorem gives in particular that if $f(x,y)$ is primitive, then so is any binary quadratic form equivalent to $f(x,y)$. We note that $4af(x,y)=(2ax+by)^2-Dy^2$, using this identity we can see that if D is positive then $f(x,y)$ can represent both positive and negative integers. On the other hand if D is negative then $(2ax+by)^2-Dy^2$ is always positive so $f(x,y)$ can only represent positive integers if a is positive or only negative integers if a is negative. This leads to the following definition:

Definition 2.5. A binary quadratic form (a,b,c) is called:

- *positive definite* if $D<0$ and $a>0$,
- *negative definite* if $D<0$ and $a<0$,
- *indefinite* if $D>0$.

2.2 Reduction of positive definite forms

In this subsection we will only study definite binary quadratic forms. Since the study of negative definite binary quadratic form can be deduced from the study of positive definite quadratic forms, we will not worry about them. Furthermore we assume all binary quadratic forms are primitive. We will look at primitive indefinite binary quadratic forms in a later subsection.

The next question to arise is how to determine when two binary quadratic forms are equivalent? Lagrange came up with a reduction algorithm [Cox(1989), p35] which turns every binary quadratic form into a unique equivalent form with minimal coefficients.

Theorem 2.6 (Definition). *Every (primitive positive definite) binary quadratic form is equivalent to a unique binary quadratic form $Q=(a,b,c)$ where Q has the property that*

$$\begin{cases} |b|\leq a\leq c & \text{in all cases,} \\ b\geq 0 & \text{if } |b|=a \text{ or } a=c. \end{cases}$$

The form Q is said to be (Lagrange) reduced.

Remark. While there is a notion of reduced form in the indefinite case, the reduced form is not unique. That is, an indefinite binary quadratic form can be equivalent to several reduced forms. For this reason the theory of indefinite binary quadratic form is quite interesting, but it would take us too far afield to what we want to do.

Proof. For the proof of existence of such a quadratic form we will follow the constructive proof in [Lemmermeyer(2010), p9] while for the uniqueness part we will have a close look at [Cox(1989), p27].

Existence: Let

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

and let our binary quadratic form be (a, b, c). Note that T^{-n} turns (a, b, c) into $(a, b-2an, an^2-bn+c)$ and U turns (a, b, c) into $(c, -b, a)$. We are going to apply the following algorithm:

1. If $|b| > a$, then apply T^{-n}, with an appropriate n, to (a, b, c) to reduce b mod $2a$ so that $|b| \leq a$.

2. If $a > c$, then apply U to (a, b, c).

3. If $|b| \leq a \leq c$, then stop; else go to 1.

This algorithm terminates when $|b| \leq a$ and $a \leq c$, i.e., when the first two required conditions are met. This algorithm has to terminate, because at every loop of the algorithm we are making $|b|$ smaller and since $|b| \in \mathbb{N}$ we can not keep reducing $|b|$ indefinitely. We now need to consider the two cases: if $|b| = a$, or $a = c$ with $b < 0$. In the first case the transformation T^{-1} takes $(a, -a, c)$ to (a, a, c) which is of the required form, while in the second case we use the matrix U to change $(a, -b, a)$ into (a, b, a). This proves the existence of reduced binary quadratic forms.

Uniqueness: Before we proceed we show that if $f(x, y) = (a, b, c)$ is reduced, then the smallest number it represent is a. Let $f(x, y)$ be reduced. Notice that $f(\pm1, 0) = a$ and $f(0, \pm1) = c$. Suppose that $x^2 \leq y^2$. Then $|x| \leq |y|$ so $f(x, y) \geq ax^2+bxy+cx^2 \geq ax^2-|bxy|+cy^2 \geq x^2(a-|b|+c)$. Similarly if $y^2 \leq x^2$ then $f(x, y) \geq y^2(a-|b|+c)$, so putting these together we get $f(x, y) \geq \min\{x^2, y^2\}(a-|b|+c)$. Hence if $xy \neq 0$ then $f(x, y) \geq a - |b| + c$, and since $f(x, y)$ is reduced $a - |b| + c \geq c > a$. So a is the smallest number represented by $f(x, y)$. If furthermore we say a number is ***properly*** represented if $\gcd(x, y) = 1$, then, when $a \neq c$, we see that c is the next smallest properly represented number of $f(x, y)$.

Let $f(x, y) = (a, b, c)$ be reduced with $a < c < a - |b| + c$, we deal with the case $|b| = a$ or $a = c$ in the next paragraph. Suppose that $g(x, y) = (a', b', c')$ is an other reduced binary quadratic form which is equivalent to $f(x, y)$, then since the represent the same numbers (Proposition 2.4) they must have the same first coefficient, i.e., $a = a'$. We know $a \leq c'$, (as $g(x, y)$ is reduced) so suppose $a = c'$ then $g(\pm1, 0) = g(0, \pm1) = a$. In that case, since $g(x, y)$ is equivalent to $f(x, y)$, $f(x, y)$ must also have four different solutions to $f(x, y) = a$. This is a contradiction as we know: if $xy \neq 0$ then $f(x, y) \geq a - |b| + c > a$; and $f(0, y) = cy^2 > a$; so $(\pm1, 0)$ are the only two solutions to $f(x, y) = a$. Hence $a < c'$ which, since c' is the next smallest number properly represented by $g(x, y)$, means that $c = c'$. Since $f(x, y)$ and $g(x, y)$ are equivalent they have the same discriminant hence, since $a = a', c = c'$, we have $b' = \pm b$. By assumption $g(x, y) = f(rx + sy, tx + uy)$ with $ru - st = 1$, so $a = g(1, 0) = f(r, t)$ and $c = g(0, 1) = f(s, u)$. This implies that $(r, t) = (\pm1, 0)$ and $(s, u) = (0, \pm1)$. So $f = g^{\mathrm{id}}$ or $f = g^{-\mathrm{id}}$ where id is the identity 2×2 matrix and $-$id the 2×2 diagonal matrix with -1 as entries. In either case, this implies that $b' = b$, i.e., $f(x, y) = g(x, y)$.

If $|b| = a$ or $a = c$ then we no longer have the inequality $a < c < a - |b| + c$. In both cases we still have that a is the smallest number represented by $f(x, y)$, hence $a = a'$. We show that in both cases $c = c'$. If $a = c$ and $a < c'$ then $g(x, y) = a$ means $(x, y) = (\pm1, 0)$ but $f(x, y) = a$ has at least four different solutions which is a contradiction so we must have that $a = c$ implies $a = c'$, i.e., $c = c'$. If $|b| = a$ and $a < c$ then since we still have the inequality $a < a - |b| + c$, we can use the same argument as before to show that $a < c'$ and conclude that $c = c'$, as c' is still the next smallest number properly represented by $g(x, y)$. So in all cases we have $a = a', c = c'$ which means $b' = \pm b$ as $f(x, y), g(x, y)$ have the same discriminant. Since either $|b| = a$ or $a = c$ we have $b \geq 0$ and either $|b'| = |b| = a$ or $c' = c = a = a'$. Hence $b' \geq 0$ and $b' = b$, i.e., $f(x, y) = g(x, y)$. □

This theorem is useful in the study of equivalence classes of binary quadratic forms as it gives a natural representative of such class. If we fix a discriminant $D < 0$ and denote by $[f(x, y)]$ (or $[(a, b, c)]$)

the equivalence class of $f(x,y)$, which we can represent by its reduced binary quadratic form, we can look at the set of all equivalence classes of binary quadratic forms with discriminant D. We will let $h(D)$ denote the number of equivalent classes.

Theorem 2.7. *Let $D < 0$ be fixed, then $h(D)$ is equal to the number of reduced forms of discriminant D. Furthermore $h(D)$ is finite.*

Proof. The first part follows from the previous theorem. For the second part fix $D < 0$ and let $f(x,y) = (a,b,c)$ be a reduced binary quadratic form of discriminant D. Then $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$, hence $a \leq \sqrt{-D/3}$. Since $|b| \leq a$ and $a, b \in \mathbb{Z}$ there are only a finite number of possibilities for a and b. Furthermore since $c = \frac{D-b^2}{-4a}$ we have that c is determined once a and b are known. So for a fixed $D < 0$ there are only a finite number of reduced binary quadratic forms with discriminant D. □

2.3 Dirichlet composition

Stepping back to include indefinite binary quadratic forms, we use the same notation $[f(x,y)]$ to denote the equivalence class of $f(x,y)$. We have a set of equivalence classes of primitive binary quadratic forms, so one might ask is can we find a binary operation to turn this set into a group? Gauss answered this question by defining how to compose two binary quadratic forms of a given discriminant D [Gauss(1986), section 235]. Unfortunately it is regarded by many mathematicians to be “difficult, sometimes even very difficult” to understand and work with [Shanks(1989)]. It is often easier to follow Dirichlet’s basic idea (first appearing in [Dirichlet(1871), 10th Supplement]), which originally was somewhat more restrictive as it imposes some conditions to the two forms to be composed, but does have the advantage of having an explicit formula. We can slightly modify Dirichlet composition to overcome the restriction imposed.

Dirichlet then found a group isomorphism between the set of equivalence classes of primitive binary quadratic forms of a fixed discriminant and equivalence classes of proper ideals of fixed orders of a quadratic field, hence easily establishing that the equivalence class of binary quadratic forms form an abelian group. Intuitively, since binary quadratic forms represent an infinite sets of numbers, given two binary quadratic forms we want to find a third one that represents the pairwise products of the numbers the two binary quadratic forms represent. For a historical point of view we are going to give Gauss’ definition of composition first.

Note. For this subsection we assume that $D \neq 0$ and that our binary quadratic forms are primitive.

Definition 2.8. Let $f(x,y)$ and $g(x,y)$ be two binary quadratic form. Define a *direct composition* to be a form $F(x,y) = ax^2 + bxy + cy^2$ such that

$$\begin{cases} f(x,y)g(z,w) = F\left(B_1(x,y;z,w), B_2(x,y;z,w)\right), \\ a_1b_2 - a_2b_1 = f(1,0), \\ a_1c_2 - a_2c_1 = g(1,0), \end{cases}$$

where $B_i(x,y;z,w) = a_i xz + b_i xw + c_i yz + d_i yw$, with $a_i, b_i, c_i, d_i \in \mathbb{Z}$, are bilinear forms.

As we can see, this definition is not very easy to work with as it does not give a way of automatically creating a direct composition. For this end, Dirichlet’s composition is much easier to use and is often regarded as the way to do composition nowadays. To define Dirichlet’s composition we need the following lemma.

Lemma 2.9. *Let $f(x,y) = (a,b,c)$ and $g(x,y) = (a',b',c')$ be two binary quadratic form of discriminant D and let $gcd(a, a', \frac{b+b'}{2}) = e$. (Note that b and b' must have the same parity since $f(x,y)$, $g(x,y)$ have the same discriminant). Then there is a unique integer B modulo $\frac{2aa'}{e^2}$ such that:*

$$\begin{aligned} B &\equiv b \; mod \; \frac{2a}{e}, \\ B &\equiv b' \; mod \; \frac{2a'}{e}, \\ B^2 &\equiv D \; mod \; \frac{4aa'}{e^2}. \end{aligned}$$

Proof. This proof loosely follows [Cox(1989), p 48]. First we are going to show that the three given condition can be rearranged to give three equivalent conditions. If an integer B satisfies the first two congruences then $B^2-(b+b')B+bb' \equiv (B-b)(B-b') \equiv 0 \bmod \frac{4aa'}{e}$. Hence rearranging and dividing by $2e$, which we can, since $2e|(b+b')$ and $2e|\,(b(b+b')-4ac)=(bb'+D)$, we get that $\frac{b+b'}{2e}B \equiv \frac{bb'+D}{2e} \bmod \frac{2aa'}{e^2}$. Multiplying the first two congruences by $\frac{a'}{e}$ and $\frac{a}{e}$ respectively we have that out initial conditions become:

$$\begin{aligned} \frac{a'}{e}B &\equiv \frac{a'}{e}b \bmod \frac{2aa'}{e^2}, \\ \frac{a}{e}B &\equiv \frac{a}{e}b' \bmod \frac{2aa'}{e^2}, \\ \frac{b+b'}{2e}B &\equiv \frac{bb'+D}{2e} \bmod \frac{2aa'}{e^2}. \end{aligned} \tag{2.1}$$

We can just work backward to see the implication the other-way, as the first two congruence are equivalent to $B \equiv b \mod \frac{2a}{e}$ and $B \equiv b' \mod \frac{2a'}{e}$. Then the argument works in reverse.

So we need to find B which satisfy the latter three conditions, which is easier to find as the equations are all modulo $\frac{2aa'}{e^2}$ and all linear (we removed the B^2 term). Since $\gcd(\frac{a}{e}, \frac{a'}{e}, \frac{b+b'}{2e}) = 1$ by Euclid's algorithm we know there exists $n_1, n_2, n_3 \in \mathbb{Z}$ such that $n_1\frac{a}{e} + n_2\frac{a'}{e} + n_3\frac{b+b'}{2e} = 1$. Fix such n_1, n_2, n_3 and let B be the unique number between 0 and $2aa'$ such that $B \equiv n_1\frac{ab'}{e} + n_2\frac{a'b}{e} + n_3\frac{bb'+D}{2e} \bmod \frac{2aa'}{e^2}$. Note that since $D = b'^2 - 4a'c' = b^2 - 4ac$ then $a'D \equiv a'b^2 \bmod \frac{2aa'}{e^2}$ and $aD \equiv ab'^2 \bmod \frac{2aa'}{e^2}$, furthermore since $b \equiv b' \bmod 2$ we have $aa'b \equiv aa'b' \bmod \frac{2aa'}{e^2}$. Now we can see that

$$\frac{a'}{e}B \equiv n_1\frac{a'ab'}{e^2} + n_2\frac{a'a'b}{e^2} + n_3\frac{a'bb'+a'D}{2e^2} \equiv \left(n_1\frac{a}{e} + n_2\frac{a'}{e} + n_3\frac{b+b'}{2e}\right)\frac{a'}{e}b \equiv \frac{a'}{e}b \bmod \frac{2aa'}{e^2}$$

$$\frac{a}{e}B \equiv n_1\frac{aab'}{e^2} + n_2\frac{aa'b}{e^2} + n_3\frac{abb'+a'D}{2e^2} \equiv \left(n_1\frac{a}{e} + n_2\frac{a'}{e} + n_3\frac{b+b'}{2e}\right)\frac{a}{e}b' \equiv \frac{a'}{e}b' \bmod \frac{2aa'}{e^2}$$

$$\frac{b+b'}{2e}B \equiv n_1\frac{abb'+ab'^2}{2e^2} + n_2\frac{a'b^2+a'b'b}{2e^2} + n_3\frac{bb'+D}{2e}\frac{b+b'}{2e} \equiv \frac{bb'+D}{2e} \bmod \frac{2aa'}{e^2}$$

Hence we have constructed a B which satisfies the congruences (2.1). Suppose that there is a second B' which satisfies the three relations, then after some rearrangement we have $\frac{a'}{e}(B-B') \equiv \frac{a}{e}(B-B') \equiv \frac{b+b'}{2e}(B-B') \equiv 0 \mod \frac{2aa'}{e^2}$. Hence we have $\frac{2aa'}{e^2}|\frac{a}{e}(B-B')$, $\frac{2aa'}{e^2}|\frac{a'}{e}(B-B')$ and $\frac{2aa'}{e^2}|\frac{b+b'}{2e}(B-B')$, this implies that $\frac{2a}{e}, \frac{2a'}{e}|(B-B')$. Using the fact that $\gcd(\frac{a}{e}, \frac{a'}{e}, \frac{b+b'}{2e}) = 1$ and the last divisibility condition we see that $\frac{2aa'}{e^2}|(B-B')$, i.e., $B \equiv B' \mod \frac{2aa'}{e^2}$. Hence we have found a unique (modulo $\frac{2aa'}{e^2}$) B which satisfies the conditions. □

Definition 2.10. Let $f(x,y) = (a,b,c), g(x,y) = (a',b',c')$ be two binary quadratic forms of discriminant D. Then the *Dirichlet composition* of $f(x,y)$ and $g(x,y)$ is the form

$$F(x,y) = \frac{aa'}{e^2}x + Bxy + \frac{e^2(B^2-D)}{4aa'}y^2$$

where B is the (unique up to modulo $\frac{2aa'}{e^2}$) integer B of Lemma 2.9.

Remark. The proof of 2.9 gave us an explicit formula to calculate the integer B that we can use for Dirichlet composition, namely $B = n_1\frac{ab'}{e} + n_2\frac{a'b}{e} + n_3\frac{bb'+D}{2e}$ where n_1, n_2, n_3 are such that $n_1a + n_2a' + n_3\frac{b+b'}{2} = e$. At this point the reader might wonder why we went to prove a non-trivial lemma instead of defining B for Dirichlet composition as in the previous sentence, which is a nicer and more straightforward definition. One of the reasons is that way we established some of the congruences that B satisfy, which we will use in other proofs of this paper, and, in a few cases, the congruence gives an easier B to work with than the explicit formula, which still involve running Euclid's algorithm.

Naturally we need to check a few properties of Dirichlet composition to see that they it is useful when considering equivalence classes of binary quadratic forms, especially the implied claim that the Dirichlet composition of two binary form is unique, in fact one can easily see that it is not. The following theorem will clarify these issues.

Theorem 2.11. *Let $f(x,y) = (a,b,c)$ and $g(x,y) = (a',b',c')$ be two binary quadratic forms of discriminant D that are both positive definite or both indefinite and $F(x,y), F'(x,y)$ be two Dirichlet compositions . Then*

- *$F(x,y)$ is a primitive binary quadratic form with discriminant D. If $D < 0$ then $F(x,y)$ is positive definite.*
- *$[F(x,y)] = [F'(x,y)]$.*

Proof. For ease of notation we will assume $\gcd(a, a', \frac{b+b'}{2}) = 1$ (one can check that replacing $a, a', \frac{b+b'}{2}$ by $\frac{a}{e}, \frac{a'}{e}, \frac{b+b'}{2e}$ respectively in the right places will still make the argument hold). We prove that F is primitive. Let $C = \frac{B^2-D}{4aa'}$ so that $F(x,y) = aa'x^2 + Bxy + Cy^2$. Recall that (a,b,c) is equivalent to $(a, b+2an, an^2+bn+c)$ (see proof of 2.6) and by definition $B = b+2an$ for some $n \in \mathbb{Z}$. Notice that $a'C = \frac{B^2-D}{4a} = \frac{4a^2n^2+4ban+b^2-b^2+4ac}{4a} = an^2+bn+c$, hence (a,b,c) is equivalent to $(a, B, a'C)$ similarly (a',b',c') is equivalent to (a', B, aC). Notice that if we let $X = xz - Cyw$ and $Y = axw + a'yz + Byw$ then we can see that

$$\begin{aligned} F(X,Y) &= aa'x^2z^2 + aBx^2zw + a^2Cx^2w^2 + aa'C^2y^2w^2 \\ &\quad + a'^2Cy^2z^2 + a'BCy^2zw + B^2xyzw + aBCxyw^2 \\ &= (ax^2 + Bxy + a'Cy^2)(a'z^2 + Bzw + aCw^2) \end{aligned}$$

Since $(a, B, a'C)$ and (a', B, aC) represent the same numbers as (a,b,c) and (a',b',c') respectively we see that $F(x,y)$ represents all the numbers of the form $f(x_1,y_1)g(z_1,w_1)$. Suppose that $F(x,y)$ is not primitive, that is, there is a prime p that divides the coefficients of $F(x,y)$, then p divides all the numbers $F(x,y)$ represents. Hence we have that p divides all the numbers of the form $f(x_1,y_1)g(z_1,w_1)$, so $p|aa'$. Suppose that $p \nmid a$, then $p|a'$. But $p|ac'$ implies $p|c'$ and $p|a(a'+b'+c')$ hence $p|b'$ contradicting the primitivity of $g(x,y)$. So we have that $p|a$ and $p|a'$, but the same argument can be repeated on $p|cc'$ implying that p divides c and c'. Furthermore $p|(a+b+c)(a'+b'+c')$ implies $p|bb'$ so either all the coefficients of $f(x,y)$ or all the coefficients of $g(x,y)$ are divisible by p again, contradicting primitivity of $f(x,y)$ or $g(x,y)$. Hence there is no prime p that divides the coefficients of $F(x,y)$. The discriminant of $F(x,y)$ is $B^2 - 4(aa')\frac{B^2-D}{4aa'} = D$. If $D < 0$ then both $a, a' > 0$, hence so is aa', so $F(x,y)$ is positive definite.

Let $F(x,y) = (aa', B, C)$ and $F'(x,y) = (aa', B', C')$ where $B' = B + 2aa'n$ for some $n \in \mathbb{Z}$ and $C' = \frac{B'^2-D}{4aa'}$. Then applying T^{-n} to (aa', B, C) we get (aa', B', C'). Hence $[F(x,y)] = [F'(x,y)]$ □

2.4 The group of positive definite binary quadratic forms.

We are now on our way to show that the set of (primitive) binary quadratic forms of discriminant D, which for this section we will denote $C(D)$, is a finite abelian group. We will split the proof in two cases: when $D < 0$ and when $D > 0$ and square-free. The second case is a slight generalisation of the first case and the proof is fairly similar, in fact it covers the first case. We split it into two cases so to introduce new concepts slowly.

We are going to look at quadratic fields, let us denote such a field as $\mathbb{Q}(\sqrt{N})$ where N is a square-free integer. So if $\alpha \in K = \mathbb{Q}(\sqrt{N})$ then $\alpha = a + b\sqrt{N}$ for some $a, b \in \mathbb{Q}$, we denote the conjugate of α, i.e., the non-trivial automorphism acting on α, by $\overline{\alpha} = a - b\sqrt{N}$. Also in this paper by *minimal polynomial* of an element α we will mean the least degree polynomial $f \in \mathbb{Z}[x]$ with coprime coefficients such that $f(\alpha) = 0$ and the leading coefficient of f is positive, not the least degree monic polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.

Definition 2.12. Let $K = \mathbb{Q}(\sqrt{N})$ be a quadratic field. We defined an *order* $\mathcal{O}$ in K to be a subset of K such that

1. $\mathcal{O}$ is a subring of K,
2. $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module,
3. $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

We note that $\mathcal{O}$ has rank two over $\mathbb{Z}$ and hence we can define it by its basis α, β. We use the notation $[\alpha, \beta]$ to mean the $\mathbb{Z}$-module with α, β as its basis.

Let $\mathcal{O}_K$ denote the *maximal order* and define the *discriminant* of K to be as follow:

$$d_K = \begin{cases} N & \text{if } N \equiv 1 \bmod 4, \\ 4N & \text{otherwise.} \end{cases}$$

The *conductor* of $\mathcal{O}$ is the index $[\mathcal{O}_K : \mathcal{O}] = f$ and define the *discriminant* of the order $\mathcal{O} = [\alpha, \beta]$ to be

$$D = \left(\det \begin{pmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{pmatrix}\right)^2 .$$

One can show that $\mathcal{O}_K = [1, \omega_K]$ where $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$ (a fact from MA3A6 Algebraic Number Theory) and if f is the conductor of $\mathcal{O}$ then $\mathcal{O} = [1, f\omega_K]$. Since the discriminant does not depend on the choice of basis we can see that $D = f^2 d_K$ using the previous basis. We can see from the this that if D is the discriminant of $\mathcal{O}$ the quadratic field, K, which $\mathcal{O}$ is an order of is $K = \mathbb{Q}(\sqrt{D})$, furthermore D satisfies $D \equiv 1, 0 \bmod 4$.

Definition 2.13. Let K be a quadratic field and let I be an ideal of an order $\mathcal{O}$. We say that I is a *proper ideal* if $\mathcal{O} = \{\beta \in K : \beta I \subset I\}$.

A *fractional ideal* I of $\mathcal{O}$ is a $\mathcal{O}$-module such that $\omega I \subseteq \mathcal{O}$ for some $\omega \in \mathcal{O}$. Given a fractional ideal I, we say that it is *invertible* if there exists a fractional ideal J such that $IJ = \mathcal{O}$.

Note that the definition of proper extends to fractional ideals, also by the definition of proper ideal, every ideal I is a proper ideal of a unique order $\mathcal{O}$. Recall that the norm of an element $\alpha \in K$ is $N(\alpha) = \alpha\overline{\alpha}$, while the norm of an fractional ideal $I = [\alpha, \beta] \lhd \mathcal{O} = [1, \tau]$, is

$$N(I) = \text{abs}\left(\begin{vmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{vmatrix} \frac{1}{\sqrt{|D|}}\right),$$

where D is the discriminant of $\mathcal{O}$ (or K), or equivalently if $\alpha = a_1 + a_2\tau, \beta = b_1 + b_2\tau$, then

$$N(I) = \text{abs}\left(\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}\right).$$

This is often thought as the index of I in $\mathcal{O}$, that is, $N(I) = \frac{[L:I]}{[L:\mathcal{O}]}$ where L is lattice containing both $\mathcal{O}$ and I, that is, L is a $\mathbb{Z}$-module of rank 2 which contains both $\mathcal{O}$ and I. Note that we have to take the absolute value so that the definition is independent of the choice of the basis for I. We will use Tr to denote the trace functions which maps α to $\alpha + \overline{\alpha}$.

Theorem 2.14. *Let $K = \mathbb{Q}(\tau)$ be a quadratic field and $ax^2 + bx + c$ the minimal polynomial of τ. Then $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$ of K.*

Proof. We can easily see that $[1, \tau]$ is an $[1, a\tau]$-module as $1, \tau, a\tau$ and $a\tau^2 = -b\tau - c$ are all in $[1, \tau]$, furthermore $a[1, \tau] \subset [1, a\tau]$, hence $[1, \tau]$ is a fractional ideal of $[1, a\tau]$. From this it follows that $[1, a\tau] \subset \{\beta \in K : \beta[1, \tau] \subset [1, \tau]\}$.

The condition {let $\beta \in K$ be such that $\beta[1, \tau] \subset [1, \tau]$} is equivalent to the condition {let $\beta \in K$ be such that $\beta \in [1, \tau]$ and $\beta\tau \in [1, \tau]$}. Now $\beta \in [1, \tau]$ means that there exists $m, n \in \mathbb{Z}$ such that $\beta = m + n\tau$. Hence $\beta\tau = m\tau + n\tau^2 = m\tau + \frac{n}{a}(-b\tau - c) = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau$. So $\beta\tau \in [1, \tau]$ if and only if $a|n$ (since $\gcd(a, b, c) = 1$ as they are the coefficients of the minimal polynomial). Hence $\beta = m + an'\tau$, implying that $\{\beta \in L : \beta[1, \tau] \subset [1, \tau]\} \subseteq [1, a\tau]$. So $\{\beta \in K : \beta[1, \tau] \subset [1, \tau]\} = [1, a\tau]$ □

In particular the previous theorem states that $[1, \tau]$ is a proper ideal of only $[1, a\tau]$. The next theorem shows us a property of quadratic fields, which in general does not hold for higher degree number fields.

Theorem 2.15. *Let $\mathcal{O}$ be an order in a quadratic field K and let I be a fractional $\mathcal{O}$-ideal. Then I is proper if and only if I is invertible.*

Proof. Suppose I is invertible, that is, there is another fractional ideal J such that $IJ = \mathcal{O}$. If $\beta \in K$ and $\beta I \subset I$ then $\beta\mathcal{O} = \beta IJ \subset IJ = \mathcal{O}$. Since $\beta\mathcal{O} \subset \mathcal{O}$ we have $\beta \in \mathcal{O}$, hence I is proper.

Suppose $I = [\alpha, \beta]$ ($\alpha, \beta \in K$) is a proper fractional ideal. Letting $\tau = \frac{\beta}{\alpha}$ we have $I = \alpha[1, \tau]$. Let $ax^2 + bx + c$ be the minimal polynomial of τ. Then by Theorem 2.14, we know that $\mathcal{O} = [1, a\tau]$. Since $\overline{\tau}$ is also a root of the minimal polynomial of τ we know that $[1, a\overline{\tau}] = [1, a\tau] = \mathcal{O}$ and by Theorem 2.14 $\overline{I} = \overline{\alpha}[1, \overline{\tau}]$ is proper fractional ideal of $\mathcal{O}$. Next consider $aI\overline{I} = a\alpha\overline{\alpha}[1, \tau][1, \overline{\tau}] = N(\alpha)[a, a\tau, a\overline{\tau}, a\tau\overline{\tau}]$. Furthermore since we have an explicit quadratic polynomial which has τ and $\overline{\tau}$ as its only roots we know $\tau + \overline{\tau} = -\frac{b}{a}$ and $\tau\overline{\tau} = \frac{c}{a}$, so $aI\overline{I} = N(\alpha)[a, a\tau, -b, c] = N(\alpha)[1, a\tau] = N(\alpha)\mathcal{O}$ (where the second to last equality follows from the fact $\gcd(a, b, c) = 1$). Hence there exists a fractional ideal, namely $J = \frac{a}{N(\alpha)}\overline{I}$, such that $IJ = \mathcal{O}$ □

Definition 2.16. Let $\mathcal{O}$ be an order of a quadratic field K. Let $I(\mathcal{O})$ denote the *set of invertible fractional ideals* of $\mathcal{O}$, and $P(\mathcal{O})$ be the *set of non-zero principal ideals* of $\mathcal{O}$.

It is quite clear, since every invertible ideal has an inverse and the multiplication of any two invertible ideal is an invertible ideal, that $I(\mathcal{O})$ forms an abelian group under multiplication. Notice also that $P(\mathcal{O}) \subset I(\mathcal{O})$, which allows us to define our object of interest.

Definition 2.17. Let $\mathcal{O}$ be an order of a quadratic field K. We define the *ideal class group* of $\mathcal{O}$ to be $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$.

We can finally prove our claim of $C(D)$, with $D < 0$, forming a group by relating $C(\mathcal{O})$ to $C(D)$.

Theorem 2.18. *Let $D < 0$ and $\mathcal{O} = [1, f\omega_K]$ an order with discriminant D of the quadratic field $K = \mathbb{Q}(\sqrt{D})$, where f is the conductor of $\mathcal{O}$ and $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$ with d_K the discriminant of K.*

1. *If $f(x, y) = (a, b, c)$ is a binary quadratic form with discriminant D then $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ is a proper ideal of $\mathcal{O}$,*
2. *$C(D)$ is a group and the map sending $f(x, y)$ to $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ induces an isomorphism between $C(D)$ and $C(\mathcal{O})$. Hence the order of $C(\mathcal{O})$ is the class number $h(D)$.*

Proof. This proof follows [Cox(1989), p 137]. Let $f(x, y) = (a, b, c)$ be a binary quadratic form with discriminant $D < 0$. Since $D < 0$, the complex roots of $f(x, 1) = ax^2 + bx + c$ are not real, so let τ be the unique root with positive imaginary part, we say τ is <u>the</u> root of $f(x, y)$. Since $a > 0$, it follows that $\tau = \frac{-b+\sqrt{D}}{2a}$, hence $\left[a, \frac{-b+\sqrt{D}}{2}\right] = [a, a\tau] = a[1, \tau]$. Recall that if D is the discriminant of $\mathcal{O}$ then $K = \mathbb{Q}(\sqrt{D})$ hence $\tau \in K$. Now by Lemma 2.14 we know that $a[1, \tau]$ is a proper ideal of the order $[1, a\tau]$ so we want to prove that $\mathcal{O} = [1, a\tau]$. First recall that $f^2 d_K = D = b^2 - 4ac$ hence fd_K and b have the same parity, so $\frac{b+fd_k}{2} \in \mathbb{Z}$. We use this fact to show:

$$\begin{aligned} a\tau &= \frac{-b + \sqrt{D}}{2} \\ &= \frac{-b + f\sqrt{d_K}}{2} \\ &= -\frac{b + fd_K}{2} + f\left(\frac{d_K + \sqrt{d_K}}{2}\right) \\ &= -\frac{b + fd_K}{2} + fw_K \end{aligned}$$

Hence $[1, a\tau] = [1, f\omega_K]$, so we have finished proving the first part.

Before we prove the second part, we claim that if $\tau \in \mathbb{C}$ and $r, s, t, u \in \mathbb{Z}$ then

$$\Im\left(\frac{r\tau + s}{t\tau + u}\right) = \det\begin{pmatrix} r & s \\ t & u \end{pmatrix} \frac{\Im(\tau)}{|t\tau + u|^2} \tag{2.2}$$

To prove this, let $\tau = x + iy$ then

$$\begin{aligned} \Im\left(\frac{r\tau+s}{t\tau+u}\right) &= \Im\left(\frac{(rx+riy+s)(tx-tiy+u)}{(u+tx)^2+t^2y^2}\right) \\ &= \frac{1}{|t\tau+u|^2}\Im(rtixy+ruiy-rtixy-stiy) \\ &= \frac{1}{|t\tau+u|^2}\det\begin{pmatrix} r & s \\ t & u\end{pmatrix}\Im(iy) \end{aligned}$$

We are going to show the map is well-defined. Let $f(x, y)$ and $f'(x, y)$ be binary quadratic forms of discriminant D and τ, τ' be their respective root. Suppose that they are equivalent, i.e., let $f(x, y) = f'(rx + sy, tx + uy)$ with $ru - st = 1$. Then

$$0 = f(\tau, 1) = f'(r\tau + s, t\tau + u) = (t\tau + u)^2 f'\left(\frac{r\tau+s}{t\tau+u}, 1\right), \tag{2.3}$$

but using equation (2.2) we have that $\frac{r\tau+s}{t\tau+u}$ has positive imaginary part, hence by uniqueness of τ' we have $\tau' = \frac{r\tau+s}{t\tau+u}$. Let $\lambda = t\tau + u \in K^*$ then $\lambda[1, \tau'] = (t\tau + u)[1, \frac{r\tau+s}{t\tau+u}] = [t\tau + u, r\tau + s] = [1, \tau]$.

To show that the map is injective we work backward. Conversely suppose $[1, \tau] = \lambda[1, \tau']$ for some $\lambda \in K^*$ then $[1, \tau] = [\lambda, \lambda\tau']$, in other words $\lambda\tau' = r\tau + s$ and $\lambda = t\tau + u$ for some $r, s, t, u \in \mathbb{Z}$, such that the matrix

$$S = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

is invertible. Rearranging we get $\tau' = \frac{r\tau+s}{t\tau+u}$, but since τ and τ' both have positive imaginary parts by equation (2.2), we have that the determinant of S is positive, i.e., $ru - st = 1$. Then by equation (2.3) we have that $f'(rx + sy, tx + uy)$ and $f(x, y)$ have the same roots, so it follows that they are equal hence $f(x, y)$ is equivalent to $f'(x, y)$. We have just shown that two binary quadratic forms are equivalent if and only if $[1, \tau] = \lambda[1, \tau']$, but the last equality is the same as saying that $[1, \tau]$ and $[1, \tau']$ are in the same quotient. So we have proved that the map sending $f(x, y)$ to $a[1, \tau]$ induces an injection $C(D) \to C(\mathcal{O})$

Now we show the map is surjective. Let I be a fractional ideal of $\mathcal{O}$ and let $I = [\alpha, \beta]$ for some $\alpha, \beta \in K$. Switching α and β if necessary we can assume that $\tau = \frac{\beta}{\alpha}$ has a positive imaginary part and let $ax^2 + bx + c$ be the minimal polynomial of τ with $a > 0$. Let $f(x, y) = ax^2 + bxy + cy^2$, note that since τ is a root and is not a real number the form $f(x, y)$ must have a negative discriminant and hence is positive definite. Furthermore since the discriminant of $\mathcal{O} = [1, a\tau]$ is $D = (a\tau - a\overline{\tau})^2 = b^2 - 4ac$ we have that the discriminant of $f(x, y)$ is D. So $f(x, y)$ is a binary quadratic form (it is primitive as it $ax^2 + bx + c$ is a minimal polynomial) that maps to $a[1, \tau]$. But $a[1, \tau]$ lies in the class of $I = [\alpha, \beta] = \alpha[1, \tau]$ in $C(\mathcal{O})$ so the map is surjective. We have a bijection between the sets $C(D) \to C(\mathcal{O})$.

Let $f(x, y) = (a, b, c)$ and $g(x, y) = (a', b', c')$ be two binary quadratic forms of discriminant D and $F(x, y)$ their Dirichlet composition, then their images are $[a, \frac{-b+\sqrt{D}}{2}]$, $[a', \frac{-b'+\sqrt{D}}{2}]$, $[\frac{aa'}{e^2}, \frac{-B+\sqrt{D}}{2}]$ respectively where $e = \gcd(a, a', \frac{b+b'}{2})$ and $B = \frac{1}{e}(n_1ab' + n_2a'b + n_3\frac{bb'+D}{2})$ for some $n_1, n_2, n_3 \in \mathbb{Z}$ such that $n_1a + n_2a' + n_3\frac{b+b'}{2} = e$. To prove our claim that Dirichlet composition corresponds to multiplication of ideals (up to equivalence classes in both cases) we need to show that $[a, \frac{-b+\sqrt{D}}{2}][a', \frac{-b'+\sqrt{D}}{2}] = [aa', a\frac{-b'+\sqrt{D}}{2}, a'\frac{-b+\sqrt{D}}{2}, \frac{\frac{1}{2}(bb'+D)-\frac{1}{2}(b+b')\sqrt{D}}{2}]$ is equivalent to $[\frac{aa'}{e^2}, \frac{-B+\sqrt{D}}{2}]$. We claim that in fact the product is equal to $[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e]$. To see this, if we recall that the norm is multiplicative, we see that the $N([aa', a\frac{-b'+\sqrt{D}}{2}, a'\frac{-b+\sqrt{D}}{2}, \frac{\frac{1}{2}(bb'+D)-\frac{1}{2}(b+b')\sqrt{D}}{2}]) = aa' = N([\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e])$, furthermore we we can use our congruences (2.1) and the fact $e|a$, $e|a'$, $e|\frac{b+b'}{2}$ to show that $[a, \frac{-b+\sqrt{D}}{2}][a', \frac{-b'+\sqrt{D}}{2}] \subseteq [\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e]$ (for example $a\frac{-b'+\sqrt{D}}{2} = n\frac{aa'}{e} + me\frac{-B+\sqrt{D}}{2}$, where $m = \frac{a}{e}$ and n is such that $\frac{a}{e}B = \frac{a}{e}b' + 2n\frac{aa'}{2^2}$). Putting these two facts together together we have $[a, \frac{-b+\sqrt{D}}{2}][a', \frac{-b'+\sqrt{D}}{2}] = [\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e]$, but $[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e] = \frac{1}{e}[\frac{aa'}{e^2}, \frac{-B+\sqrt{D}}{2}]$, hence they are in the same ideal class, completing the proof. □

Remark. We make a remark about the map we described when proving surjectivity of the bijection. Note that if τ has for minimal polynomial $ax^2 + bx + c$ then $N(\tau) = \frac{c}{a}$ and $\mathrm{Tr}(\tau) = \frac{b}{a}$. Furthermore, we have that $N([1, \tau]) = \frac{1}{a}$, so the binary quadratic form associated to $[1, \tau]$ was $\frac{x^2+\mathrm{Tr}(\tau)xy+N(\tau)y^2}{N([1,\tau])}$.

Now if $\tau = \frac{\beta}{\alpha}$, notice that $N([1,\tau]) = \frac{\overline{\beta}}{\overline{\alpha}} - \frac{\beta}{\alpha} = \frac{\overline{\beta}\alpha - \overline{\alpha}\beta}{\alpha\overline{\alpha}} = \frac{N([\alpha,\beta])}{N(\alpha)}$ and $\mathrm{Tr}(\frac{\beta}{\alpha}) = \mathrm{Tr}(\frac{\beta\overline{\alpha}}{N(\alpha)}) = \frac{\mathrm{Tr}(\alpha\overline{\beta})}{N(\alpha)}$. So we have that the binary quadratic form associated to $I = [\alpha, \beta]$ is

$$\frac{x^2 + \frac{\mathrm{Tr}(\alpha\overline{\beta})}{N(\alpha)}xy + \frac{N(\beta)}{N(\alpha)}y^2}{\frac{N(I)}{N(\alpha)}} = \frac{N(\alpha)x^2 + \mathrm{Tr}(\alpha\overline{\beta})xy + N(\beta)y^2}{N(I)} = \frac{N(\alpha x + \beta y)}{N(I)}.$$

2.5 General case

We are now going to consider the equivalence classes of primitive indefinite binary quadratic forms. The reason the previous proof would fail if $D > 0$ is that the roots of $f(x,1)$ are real, and hence our inverse map is not unique as it depends on the choice of $\sqrt{D}$. This can be rectified by considering the *narrow class group* instead of the class group. Before we can define this we need a few definitions.

Definition 2.19. An order $\mathcal{O}$ of discriminant D is said to be *oriented* once a choice of $\sqrt{D}$ has been made.

Once this choice has been made we can define a map $\pi : \mathcal{O} \to \mathbb{Z}$ by $\pi(\tau) = \frac{\tau - \overline{\tau}}{\sqrt{D}}$, which has the particularity that $\pi(x + y\sqrt{D}) = 2y$ With the idea of oriented order comes the idea of orientating fractional ideal.

Definition 2.20. An *oriented fractional ideal* of an oriented order $\mathcal{O}$ is a pair (I, ϵ), where I is a fractional ideal of $\mathcal{O}$ and $\epsilon \in \{\pm 1\}$ is the orientation. We say (I, ϵ) is *positively oriented* if $\epsilon = 1$, otherwise it is *negatively oriented.*

A basis α, β of an oriented fractional ideal (I, ϵ) is said to be *correctly oriented* if $\pi(\overline{\alpha}\beta) = \frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\sqrt{D}}$ has the same sign as ϵ.

We define the product of two oriented fractional ideal (I, ϵ) and (I', ϵ'), of an order $\mathcal{O}$ of discriminant D, to be $(II', \epsilon\epsilon')$. This can easily be extended to the product of an oriented fractional ideal and an element of $\mathbb{Q}(\sqrt{D})$ to be $\alpha(I, \epsilon) = (\alpha I, \mathrm{sgn}(N(\alpha))\epsilon)$, where $\mathrm{sgn}(\alpha)$ is the usual sign function. We will from now on assume that all fractional ideals of an oriented order are themselves oriented, hence we will write I to mean the pair (I, ϵ). Furthermore, when talking about a basis of an oriented ideal, we will amuse that the basis is correctly oriented. We just need one more definition, a refinement of equivalent ideals for our new setting, and then we can define the *narrow class group.*

Definition 2.21. Two oriented fractional ideals, I, J of an order $\mathcal{O}$ of a discriminant D, are *equivalent* if there exists $\alpha \in \mathbb{Q}(\sqrt{D})$ such that $\alpha I = J$.

We defined *the narrow class group, $C^+(\mathcal{O})$,* of an oriented order $\mathcal{O}$, to be the set of equivalence classes of oriented fractional invertible ideals.

Remark. In many literature, the narrow class group is defined differently as follows: Let $P^+(\mathcal{O})$ be the set of principal fractional ideal of $\mathcal{O}$ with a generator of positive norm. The *narrow class group* is $C^+(\mathcal{O}) = I(\mathcal{O})/P^+(\mathcal{O})$. While the usual narrow class groups has the property that $C^+(\mathcal{O}) = C(\mathcal{O})$ when $D < 0$, it has the problem that you need to deal with positive definite binary quadratic forms separately from negative definite binary quadratic forms. Our definition has the advantage that it gives the correct notion when $D < 0$ as it does not distinguish between positive definite and negative definite, a distinction that we can not make in section 3.

Another side remark is that we can relate $C^+(\mathcal{O})$ to $C(\mathcal{O})$ by considering the following short exact sequence:

$$\begin{tikzcd}
1 \arrow[r] & \{\pm 1\}/N(\mathcal{O}^*) \arrow[r] & C^+(\mathcal{O}) \arrow[r] & C(\mathcal{O}) \arrow[r] & 1 \\
\epsilon \arrow[r, mapsto] & (\mathcal{O}, \epsilon) & (I, \epsilon) \arrow[r, mapsto] & I
\end{tikzcd}$$

If the discriminant D of $\mathcal{O}$ is negative, then every element of $\mathcal{O}$, including units, have a positive norm, hence $\{\pm 1\}/N(\mathcal{O}^*\} = \{\pm 1\}$. Furthermore the short exact sequence split, since the map defined by $I \mapsto (I, 1)$ is a section of the map $(I, \epsilon) \mapsto I$, it is only well defined since ideals are only equivalent to ideals with the same orientation. Since the short exact sequence split, we have by the splitting lemma $C^+(\mathcal{O}) \cong \{\pm 1\} \times C(\mathcal{O})$. If $D > 0$ and $\mathcal{O}$ has a unit with negative norm, then $\{\pm 1\}/N(\mathcal{O}^*) = 1$, so $C^+(\mathcal{O}) \cong C(\mathcal{O})$. Finally if $D > 0$ and $\mathcal{O}$ does not have any unit with negative norm, then all we can say is that $C^+(\mathcal{O}) \twoheadrightarrow C(\mathcal{O})$.

With the above remark we redefine $C(D)$ to be the set of equivalence classes of primitive binary quadratic forms of discriminant D. In particular when $D < 0$ then $C(D)$ includes both positive definite and negative definite form, hence it is twice the size of our previous $C(D)$. With oriented fractional ideals, we need to make a slight modification to the definition of the norm of an ideal. Recall that when we defined it, it was pointed out that we had to take the absolute value so that the definition is independent of the choice of basis. It turns out that with oriented fractional we do not need to take the absolute value anymore, or equivalently the norm of an oriented ideal is $\epsilon N(I)$. Tha is if α, β is a correctly oriented basis of I, then

$$N(I) = \begin{pmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{pmatrix} \frac{1}{\sqrt{D}}$$

Theorem 2.22. *Let D be a non-square integer and $\mathcal{O}$ an oriented order with discriminant D of the quadratic field $K = \mathbb{Q}(\sqrt{D})$. Then there is a bijection between the $C(D)$ and $C^+(\mathcal{O})$ defined by $[(a, b, c)]$ maps to the equivalence class of $[a, \frac{-b+\sqrt{D}}{2}]$. This bijection is an isomorphism of groups.*

Proof. This proof will follow the same structure as the proof of Theorem 2.18 with a few slight alteration. We first show that $[a, \frac{-b+\sqrt{D}}{2}]$ is a proper ideal of $\mathcal{O}$. Let $f(x, y) = (a, b, c)$ be a binary quadratic form. Let τ be the root of $f(x, 1) = ax^2 + bx + c$ such that $\pi(\tau)$ has the same sign as a. Explicitly, using the quadratic formula, we have $\tau = \frac{-b+\sqrt{D}}{2a}$. Since $N(a) > 0$, we have $[a, \frac{-b+\sqrt{D}}{2}] = a[1, \tau]$ is equivalent to $[1, \tau]$ in $C^+(\mathcal{O})$. By Theorem 2.14 we know $[1, \tau]$ is a proper ideal.

We now check the map is well defined. Suppose that $f(x, y) = (a, b, c)$ and $f'(x, y) = (a', b', c')$ such that $f(x, y) = f'(rx + sy, tx + uy)$ with $ru - st = 1$, this means that $a' = au^2 - but + ct^2$. Let τ be the root of $f(x, 1)$ with $\pi(\tau)$ having the same sign as a, and τ' the root of $f'(x, 1)$ with $\pi(\tau')$ having the same sign as a', we show how to relate τ and τ'. Consider

$$0 = f(\tau, 1) = f'(r\tau + s, t\tau + u) = (t\tau + u)^2 f'\left(\frac{r\tau + s}{t\tau + u}, 1\right) \tag{2.4}$$

and we calculate that

$$\begin{aligned} \pi\left(\frac{r\tau + s}{t\tau + u}\right) &= \pi\left(\frac{(r\tau + s)(t\overline{\tau} + u)}{N(t\tau + u)}\right) \\ &= \pi\left(\frac{rt\tau\overline{\tau} + su + ru\tau + st\overline{\tau}}{N(t\tau + u)}\right) \\ &= \frac{(ru - st)(\tau - \bar{\tau})}{N(t\tau + u)\sqrt{D}} \\ &= \frac{\pi(\tau)}{N(t\tau + u)} \end{aligned} \tag{2.5}$$

But we have that $N(t\tau + u) = (t\tau + u)(t\overline{\tau} + u) = u^2 + \mathrm{Tr}(\tau)tu + N(\tau)t^2 = u^2 - \frac{b}{a}tu + \frac{c}{a}t^2 = \frac{a'}{a}$. So we have two cases:

Case 1. $N(t\tau + u) > 0$: in which case a and a' have both the same sign and $\tau' = \frac{r\tau+s}{t\tau+u}$. Then if we let $\lambda = t\tau + u \in \mathbb{Q}(\sqrt{D})^*$, we have $N(\lambda) > 0$ and $\lambda[1, \tau'] = [1, \tau]$. Hence our two ideals are equivalent, as both $[1, \tau']$ and $[1, \tau]$ have the same orientation.

Case 2. $N(t\tau + u) < 0$: in which case a and a' have different sign and $\tau' = \frac{r\tau+s}{t\tau+u}$. Then if we let $\lambda = t\tau + u \in \mathbb{Q}(\sqrt{D})^*$, we have $N(\lambda) < 0$ and $\lambda[1, \tau'] = [1, \tau]$. But since $[1, \tau']$ and $[1, \tau]$ have different orientation, we have that they are in fact equivalent.

Conversely, to show injectivity, suppose that $[1, \tau] = \lambda[1, \tau']$ for some $\lambda = t\tau + u \in \mathbb{Q}(\sqrt{D})$. Then we have $\lambda\tau' = r\tau + s$ and $\lambda = t\tau + u$ for some $r, s, t, u \in \mathbb{Z}$ such that the matrix

$$S = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

is invertible. Rearranging we get $\tau' = \frac{r\tau+s}{t\tau+u}$, and by equation (2.5), we have

$$\frac{\pi(\tau')}{\pi(\tau)} N(\lambda) = ru - st.$$

But since if $N(\lambda) > 0$ then $\pi(\tau)$ and $\pi(\tau')$ have the same sign, while if $N(\lambda) < 0$ then $\pi(\tau)$ and $\pi(\tau')$ have different sign, we have that $ru - st = 1$. So S is in $\mathrm{SL}_2(\mathbb{Z})$ and $f(x,1)$ and $f'(x,1)$ have the same roots, hence they are equivalent. We have shown that two binary quadratic forms are equivalent if and only if $[1,\tau] = \lambda[1,\tau']$ for some λ. Hence we have proved the map is injective.

We finally show the map is surjective. Let I be a fractional ideal of $\mathcal{O}$ and let $I = [\alpha, \beta]$ for some $\alpha, \beta \in K$. Without loss of generality we can assume $N(\alpha) > 0$, as every ideal has a basis with $N(\alpha) > 0$ which can be achieved by taking the smallest $\alpha \in \mathbb{Q}_{\geq 0} \cap I$. Let $\tau = \frac{\beta}{\alpha}$, so $I = \alpha[1,\tau]$. Consider the quadratic form

$$f(x,y) = \frac{N(x+\tau y)}{N([1,\tau])} = \frac{x^2 + \mathrm{Tr}(\tau)xy + N(\tau)y^2}{N([1,\tau])}.$$

Let $ax^2 + bxy + cy^2$ be the minimal polynomial of τ with $\mathrm{sgn}(a) = \mathrm{sgn}(\pi(\tau))$, hence $\gcd(a,b,c) = 1$. Then by Theorem 2.14 we see that that $[1,\tau]$ is a proper fractional ideal for the order $\mathcal{O}$, with $N([1,\tau]) = \frac{1}{a}$. Therefore $f(x,y) = ax^2 a\,\mathrm{Tr}(\tau)xy + N(\tau)y^2 = ax^2 + bxy + cy^2$. This shows that the map is surjective since $f(x,y) \mapsto [a, \frac{-b+\sqrt{D}}{2}]$ and $I = \alpha[1,\tau] = \alpha[1, \frac{-b+\sqrt{D}}{2a}]$ are both in the same ideal class as $N(\alpha) > 0$

Now that we have shown the bijection between $C(D)$ and $C^+(\mathcal{O})$, we claim that the work we have done in Theorem 2.18 shows how the bijection induces the isomorphism. □

We know that, for $D < 0$, $C(D)$ is finite and since Dirichlet composition is symmetric we have that $C(D)$ is a finite abelian group, we can prove the same results for $D > 0$, but this requires more background in the reduction theory of indefinite forms. We note that the inverse of the bijection is given in the above theorem, that is $I = [\alpha, \beta] \mapsto \frac{N(\alpha x + \beta y)}{N(I)}$.

We finish this section by finding the identity and the inverse of every element in $C(D)$, as this is often essential to group calculations.

Theorem 2.23. *Let $D \equiv 0, 1$ mod 4. The identity element of $C(D)$ is the class containing the principal form*

$$\begin{cases} x^2 - \frac{D}{4}y^2 & \text{if } D \equiv 0 \mod 4, \\ x^2 - xy + \frac{1-D}{4}y^2 & \text{if } D \equiv 1 \mod 4. \end{cases}$$

The inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.

Proof. Let $f(x,y) = (a,b,c)$ and $I(x,y)$ be the principal form. Let $\epsilon \in \{0,1\}$ be such that $\epsilon \equiv D$ mod 4. First we note that $\gcd(a, 1, \frac{b+\epsilon}{2}) = 1$. We show that in this case $B = b$, where B is the integer needed in Dirichlet composition. Since $D = b^2 - 4ac$ we easily see that $b^2 \equiv D$ mod $4a$, furthermore $b \equiv b$ mod $2a$. So if $4|D$ then $2|b$ so $b \equiv 0$ mod 2. If on the other hand $4 \nmid D$ then $2 \nmid b$ so $b \equiv 1$ mod 2. Hence b satisfy the three congruence relation needed to find B in the Dirichlet composition. Hence the Dirichlet composition of $f(x,y)$ and $I(x,y)$ is $ax^2 + bxy + \frac{b^2-(b^2-4ac)}{4a}y^2 = f(x,y)$ as required.

Let $f(x,y) = (a,b,c)$ and $\overline{f}(x,y) = (a,-b,c)$. Recall that $(a,-b,c)$ is equivalent to $(c,b,a) = g(x,y)$ and $\gcd(a,b,c) = 1$. It is easy to see that b satisfies the three congruence relations needed to find B, hence the Dirichlet composition of $f(x,y)$ and $g(x,y)$ is $acx^2 + bxy + \frac{b^2-D}{4ac}y^2 = acx^2 + bxy + y^2 = (ac, b, 1)$. While this is not the principal form, recall that (a,b,c) is equivalent to $(a, b+2an, an^2+bn+c)$ for any $n \in \mathbb{Z}$. If $D \equiv 0$ mod 4 then $2|b$ so let $n = \frac{b}{2}$ then, if we let $\sim$ denote equivalence, notice that

$$\begin{aligned} (ac,b,1) &\sim (1,-b,ac) \\ &\sim (1, -b+2n, n^2 - bn + ac) \\ &\sim (1, 0, \frac{b^2 - 2b^2 + 4ac}{4}) \\ &\sim (1, 0, -\frac{D}{4}) \end{aligned}$$

which is the principal form when $D \equiv 0$ mod 4. Similarly if $D \equiv 1$ mod 4 we can show that $(ac,b,1)$ is equivalent to the principal form by noticing that $2 \nmid b$ so if we let $n = \frac{b-1}{2}$ then $(ac,b,1) \sim (1, -b+2n, n^2-bn+ac) \sim (1, -1, \frac{b^2+2b+1-2b^2-2b+4ac}{4}) = (1, -1, \frac{1-D}{4})$. Hence in both cases the Dirichlet composition is in the class of the principal form, proving that the inverse of (a,b,c) is $(a,-b,c)$. □

3 Bhargava's cubes

3.1 A new look at Gauss composition

In this section we will refer to several types of equivalence, so we will say two objects A, B are G-equivalent if there exists $g \in G$ such that $A = B^g$, where G is a group and B^g the image of B after being acted on by g. Note that by this definition, in Section 2 we talked about $\mathrm{SL}_2(\mathbb{Z})$-equivalent binary quadratic forms. We will also switch from multiplicative notation to additive notation for the group of binary quadratic forms, since we know the group is abelian. Furthermore throughout this section we will assume all our spaces are *non-degenerate*, that is, whenever we talk about the discriminant of an object; be it a cube of integers, a quadratic ring or otherwise, we will assume that it is non-zero.

As noted before, there is a link between binary quadratic forms and 2×2 matrices, so one might wonder if we can find anything of interest using $2 \times 2 \times 2$ cube of integers. This is what Bhargava does [Bhargava(2004)]: he considers cubes of integers and explores six different ways these cubes of integers can represent forms; with each of these forms he explores the question of whether a composition law can be associated to the forms so to create a group. We shall explore five different composition laws complete with proofs and examples.

Consider the space $\left(\mathbb{Z}^2\right)^{\otimes 3}$, this has a basis $\{e_i \otimes e_j \otimes e_k : i, j, k \in \{1, 2\}\}$ where e_1, e_2 are the standard $\mathbb{Z}$-basis of $\mathbb{Z}^2$. So using this basis we have that each element of $(\mathbb{Z}^2)^{\otimes 3}$ is uniquely determined by the eight integers $a_{ij,k}$, that is $x = \sum_{i,j,k} a_{ijk}(e_i \otimes e_j \otimes e_k)$. If we let

$$(a, b, c, d, e, f, g, h) = (a_{1,1,1}, a_{1,1,2}, a_{1,2,1}, a_{1,2,2}, a_{2,1,1}, a_{2,1,2}, a_{2,2,1}, a_{2,2,2})$$

then we can can represent every element of $(\mathbb{Z}^2)^{\otimes 3}$ by a $2 \times 2 \times 2$ cube of integers:

$$\begin{tikzcd}
& e \arrow[rr, dash] \arrow[dd, dash] & & f \arrow[dd, dash] \\
a \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[ur, dash] \arrow[dd, dash] & \\
& g \arrow[rr, dash] & & h, \\
c \arrow[ur, dash] \arrow[rr, dash] & & d \arrow[ur, dash] &
\end{tikzcd} \tag{3.1}$$

So $(\mathbb{Z}^2)^{\otimes 3}$ can be identified with the space of all $2 \times 2 \times 2$ cubes of integers.

If we let $\Gamma = (\mathrm{SL}_2(\mathbb{Z}))^3$, we have a right natural action on $(\mathbb{Z}^2)^{\otimes 3}$, that is $\gamma = \gamma_1 \times \gamma_2 \times \gamma_3 \in \Gamma$ gives a map $\gamma_1 \otimes \gamma_2 \otimes \gamma_3 : \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, with the map $\gamma_i : \mathbb{Z}^2 \to \mathbb{Z}^2$ being the usual left action. We want to see what this corresponds to in terms of cubes of integers. Let $A \in (\mathbb{Z}^2)^{\otimes 3}$ and note that A has three different ways to be "represented" by two matrices namely

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix};$$

$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix}, N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix};$$

$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix}, N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}.$$

Let us consider $\gamma \times \mathrm{id} \times \mathrm{id}$ acting on our cube, and for ease of use let us temporarily go back to $a_{i,j,k}$ notation. With this in mind we see that M_1 can be put in correspondence with $\sum a_{1,j,k}(e_1 \otimes e_j \otimes e_k)$, N_2 with $\sum a_{2,j,k}(e_2 \otimes e_j \otimes e_k)$, M_2 with $\sum a_{i,1,k}(e_i \otimes e_1 \otimes e_k)$, ans so on. Let

$$\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

then the map $\gamma : \mathbb{Z}^2 \to \mathbb{Z}^2$ sends $(e_1, e_2) \mapsto (re_1 + se_2, te_1 + ue_2)$, from this we see that the image of $\sum a_{1,j,k}(e_1 \otimes e_j \otimes e_k) + \sum a_{2,j,k}(e_2 \otimes e_j \otimes e_k)$ under $\gamma \times \mathrm{id} \times \mathrm{id}$ is $\sum a_{1,j,k}((re_1 + te_2) \otimes e_j \otimes e_k) + \sum a_{2,j,k}((se_1 + ue_2) \otimes e_j \otimes e_k)$. Regrouping terms together, we get $\sum(ra_{1,j,k} + sa_{2,j,k})(e_1 \otimes e_j \otimes e_k) + \sum(ta_{1,j,k} + ua_{2,j,k})(e_2 \otimes e_j \otimes e_k)$. When putting this back in terms of matrices, we see that $\gamma \times \mathrm{id} \times \mathrm{id}$

sends $(M_1, N_1) \mapsto (rM_1 + sN_1, tM_1 + uN_1)$. If we repeat this argument with $\mathrm{id} \times \gamma \times \mathrm{id}$ and $\mathrm{id} \times \mathrm{id} \times \gamma$, then we see that in general, the natural action is defined as follows: we take an element

$$\gamma = \begin{pmatrix} r_1 & s_1 \\ t_1 & u_1 \end{pmatrix} \times \begin{pmatrix} r_2 & s_2 \\ t_2 & u_2 \end{pmatrix} \times \begin{pmatrix} r_3 & s_3 \\ t_3 & u_3 \end{pmatrix} \in \Gamma$$

then we define the action of γ on A, denoted A^γ, by replacing, in any order, (M_i, N_i) by $(r_iM_i + t_iN_i, s_iM_i + u_iN_i)$. Notice that at each "stage" all the M_i, N_i are affected but from our above discussion we see that the order in which you apply each individual γ_i does not matter.

Example. Let A be the cube which has

$$M_1 = N_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \times \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We calculate A^γ: at the first stage we replace (M_1, N_1) by $(M_1 + N_1, M_1 + 2N_1)$ so we get

$$\begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}, \begin{pmatrix} 3 & 6 \\ 9 & 12 \end{pmatrix},$$

hence $A' = (2, 4, 6, 8, 3, 6, 9, 12)$. Next we need to replace our <u>new</u> M_2 and N_2, being respectively

$$\begin{pmatrix} 2 & 6 \\ 3 & 9 \end{pmatrix}, \begin{pmatrix} 4 & 8 \\ 6 & 12 \end{pmatrix},$$

by $(2M_2+3N_2, M_2+2N_2)$ which gives $A'' = (16, 10, 36, 22, 24, 15, 54, 33)$. Finally we apply the last component of γ, which just negates every entry to find that $A^\gamma = (-16, -10, -36, -22, -24, -15, -54, -33)$. So we have that

$$\begin{tikzcd}
 & & -24 \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & -15 \arrow[dl, dash] \arrow[dd, dash] \\
 & -16 \arrow[rr, dash] \arrow[dd, dash] & & -10 \arrow[dd, dash] & \\
A^\gamma = & & -54 \arrow[rr, dash] \arrow[dl, dash] & & -33, \arrow[dl, dash] \\
 & -36 \arrow[rr, dash] & & -22 &
\end{tikzcd}$$

Definition 3.1. Let $A \in (\mathbb{Z}^2)^{\otimes 3}$ be a cube and M_i, N_i for $i \in \{1, 2, 3\}$ be as above, then we construct three binary quadratic forms Q_i^A, denoted Q_i if A is obvious, by setting $Q_i(x, y) = -\det(M_ix - N_iy)$

Explicitly

$$\begin{aligned} Q_1 &= -((ad - bc)x^2 + (cf + bg - de - ah)xy + (eh - fg)y^2) \\ &= -(\det M_1x^2 + (cf + bg - de - ah)xy + \det N_1y^2). \end{aligned}$$

We recall from Section 2 that the discriminant of a binary quadratic form $ax^2+bxy+cy^2$ is $D = b^2-4ac$. An explicit calculation shows that, given an arbitrary $A \in (\mathbb{Z}^2)^{\otimes 3}$, the discriminant of Q_1, Q_2 and Q_3 is the same, leading to the following definition.

Definition 3.2. We define *the discriminant* of A to be

$$\begin{aligned} D &= \mathrm{Disc}(Q_i) \\ &= a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 - 2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(adfg + bceh) \end{aligned}$$

Lemma 3.3. *Let $A \in (\mathbb{Z}^2)^{\otimes 3}$ give rise to Q_1, Q_2, Q_3 and $\gamma = \gamma_1 \times \gamma_2 \times \gamma_3$ then A^γ gives rises to the three binary quadratic forms $Q_1^{\gamma_1}, Q_2^{\gamma_2}$ and $Q_3^{\gamma_3}$. That is $Q_i^{(A^\gamma)} = (Q_i^A)^{\gamma_i}$.*

Proof. We will only prove this for Q_1 as the exact same argument can be used for Q_2 and Q_3. Let $\gamma = \mathrm{id} \times \gamma_2 \times \gamma_3$, where id is the 2×2 identity matrix. By definition id does not change our original M_1, N_1 while γ_2 (respectively γ_3) just do column (respectively row) operations on M_1, N_1 simultaneously. More precisely if

$$\gamma_2 = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

and we denote the columns of $M_1x - N_1y$ by c_1, c_2, then we have that γ_2 acts by the column operation $\widetilde{c_1} = rc_1 + tc_2$ and $\widetilde{c_2} = \frac{sc_1+(-st+ru)c_2}{r}$. So the determinant of $M_1x - N_1y$ is, using linear algebra, scaled by a factor of $r \cdot \frac{-st+ru}{r} = \det(\gamma_1) = 1$. Hence $\det(M_1x - N_1y)$ is unchanged under γ_2, so Q_1 is unaffected by γ.

Next consider $\gamma = \gamma_1 \times \mathrm{id} \times \mathrm{id}$. In this case M_1, N_1 are only affected by

$$\gamma_1 = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

and an explicit calculation shows that $-\det((rM_1 + tN_1)x - (sM_1 + uN_1)y) = Q_1(rx + sy, tx + uy) = Q_1^{\gamma_1}$ □

So a cube $A \in (\mathbb{Z}^2)^{\otimes 3}$ gives rise to three binary quadratic form with the same discriminant. We want to establish an operation on those three binary quadratic forms so to find a group. Barghava inspired himself from the group law on elliptic curves: if three points P_1, P_2, P_3 on a an elliptic curve are collinear then the sum of P_1, P_2, P_3 is 0

Axiom (The cube law). *For all Q_1^A, Q_2^A, Q_3^A that arise from some $A \in (\mathbb{Z}^2)^{\otimes 3}$ we have that the sum of Q_1^A, Q_2^A, Q_3^A is zero.*

A useful consequence of this axiom is that it leads to an identification of two equivalent binary quadratic forms. By that we mean if $\gamma = \gamma_1 \times \mathrm{id} \times \mathrm{id}$ then, as in the proof, we have two sets of three binary quadratic cubes Q_1, Q_2, Q_3 and $Q_1^{\gamma_1}, Q_2, Q_3$, but we know the sums of these two sets are zero, hence Q_1 becomes identified with $Q_1^{\gamma_1}$. As in Section 2 given a binary quadratic form Q we will denote by $[Q]$ the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of Q. We denote by $C(\left(\mathrm{Sym}^2\mathbb{Z}^2\right)^*; D)$ the set of equivalence classes of primitive binary quadratic forms with discriminant D. Note that $C(\left(\mathrm{Sym}^2\mathbb{Z}^2\right)^*; D)$ is the same as $C(D)$ in section 2, but we now specify $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ to make it explicit that we are considering binary quadratic forms. We use the notation $\mathrm{Sym}^2\mathbb{Z}^2$ to mean that we are looking at the space of 2-variable (i.e., binary) symmetric (if we look at the associated matrix) forms of degree 2 (i.e., quadratic). Furthermore we use $(\dots)^*$ to mean that the associated matrix does not necessarily have entries in $\mathbb{Z}$, in other words, if our quadratic form is (a, b, c), we do not require b to be even.

Theorem 3.4 (Gauss composition). *Let $D \equiv 0, 1 \mod 4$ and let*

$$Q_{\mathrm{id},D} = \begin{cases} x^2 - \frac{D}{4}y^2 & D \equiv 0 \mod 4 \\ x^2 - xy + \frac{1-D}{4}y^2 & D \equiv 1 \mod 4 \end{cases}$$

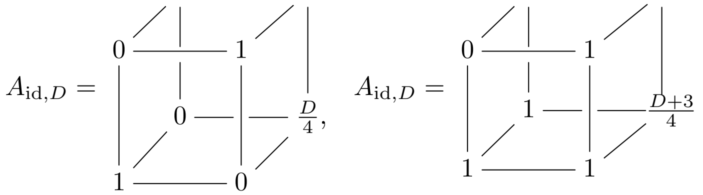
Then there exists a unique binary operation to turn $C(\left(Sym^2\mathbb{Z}^2\right)^*; D)$ into an additive group with:

1. *$[Q_{\mathrm{id},D}]$ is the identity,*
2. *for any cube A of discriminant D such that Q_1^A, Q_2^A, Q_3^A are primitive we have $[Q_1^A] + [Q_2^A] + [Q_3^A] = [Q_{\mathrm{id},D}]$. (Part of the cube law)*

Given Q_1, Q_2, Q_3 with $[Q_1] + [Q_2] + [Q_3] = [Q_{\mathrm{id},D}]$ then there exists a unique, up to Γ-equivalence, cube $A \in (\mathbb{Z}^2)^{\otimes 3}$ of discriminant D such that A gives rise to Q_1, Q_2, Q_3.

Before we prove this, we are going to show that the cube law axiom is equivalent to Dirichlet composition. Hence this theorem is a restatement of the fact that Dirichlet composition turns $C(D)$ into a group, which we have proved in the cases when D is not a square.

Let $A_{\mathrm{id},D}$ be the following cube



depending on whether $D \equiv 0 \mod 4$ or $D \equiv 1 \mod 4$ respectively. Then we note that $Q_{\mathrm{id},D}$, what we have called the principle form in section 2, is such that $A_{\mathrm{id},D}$ gives rise to $Q_1 = Q_2 = Q_3 = Q_{\mathrm{id},D}$.

Definition 3.5. We say that A is *primitive* if the three binary quadratic forms it gives rise to are primitive

Using this definition we can now show how the cube law axiom and Gauss composition are equivalent. If we start with a primitive cube, as in figure (3.1), we note that since the cube is primitive its coefficients have gcd 1. To see this let $G = \gcd(a, b, c, d, e, f, g, h)$ this implies that $G | \gcd(bc - ad, ed + ah - bg - fc, fg - eh) = 1$, where the equality is due to the fact that Q_1 is primitive, which implies that $G = 1$. We use that fact to find $\gamma \in \Gamma$ such that A^γ is of the form $(1, 0, 0, d, 0, f, g, h)$ for some new d, f, g, h by applying the following steps: first let

$$U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

By applying appropriate copies of $U \times \mathrm{id} \times \mathrm{id}$, $\mathrm{id} \times U \times \mathrm{id}$ and $\mathrm{id} \times \mathrm{id} \times U$, we can assume without loss of generality that a is the smallest non-zero absolute entry of A. If a is coprime with either b, c or e, we can use Euclid's algorithm to find a matrix in $\mathrm{SL}_2(\mathbb{Z})$ changing a into 1. If not then apply appropriate copies of $T^n \times \mathrm{id} \times \mathrm{id}$, $\mathrm{id} \times T^n \times \mathrm{id}$ and $\mathrm{id} \times \mathrm{id} \times T^n$ to reduce b, c and e modulo a. We can then replace a with the smallest non-zero absolute entry and repeat the process. We either stop as soon as we have $a = 1$, or if the first case does not occurs when we end up with A being of the form $(a, 0, 0, d, 0, f, g, h)$. In the latter case, notice that $\gcd(a, f) = 1$ for primitivity to hold, and we can apply T to A to get $(a, 0, d, d, f, f, g + h, h)$, but then we are back in the case of $\gcd(a, e) = 1$. Hence we can find $\gamma \in \Gamma$ such that A^γ is of the form $(1, b, c, d, e, f, g, h)$, then use the 1 to reduce b, c and e to 0, i.e., we have

$$\begin{tikzcd}
& 0 \arrow[rr, dash] \arrow[dd, dash] & & f \arrow[dd, dash] \\
1 \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[ur, dash] \arrow[dd, dash] & \\
& g \arrow[rr, dash] \arrow[dl, dash] & & h. \arrow[dl, dash] \\
0 \arrow[rr, dash] & & d &
\end{tikzcd}$$

The three binary quadratic forms this cube gives rises to are

$$\begin{aligned}
Q_1 &= -\begin{vmatrix} x & -fy \\ -gy & dx - hy \end{vmatrix} = -dx^2 + hxy + fgy^2 \\
Q_2 &= -\begin{vmatrix} x & -dy \\ -fy & gx - hy \end{vmatrix} = -gx^2 + hxy + dfy^2 \\
Q_3 &= -\begin{vmatrix} x & -gy \\ -dy & fx - hy \end{vmatrix} = -fx^2 + hxy + dgy^2
\end{aligned}$$

Note that by construction $Q_i^A \in [Q_i]$, and the cube law states that $[Q_1] + [Q_2] = -[Q_3]$. In terms of Dirichlet composition, noting that $\gcd(d, h, fg) = 1$ implies $\gcd(d, g, h) = 1$, we have $[Q_1] + [Q_2] = [-dx^2 + hxy + fgy^2] + [-gx^2 + hxy + dfy^2] = \left[dgx^2 + Bxy + \frac{B^2 - (h^2 + 4dfg)}{4dg} y^2\right]$ for some B that satisfies $B \equiv h \mod 2d, B \equiv h \mod 2g, B^2 \equiv h^2 + 4dfg \mod 2dg$. We can easily see that $B = h$ works hence $[Q_1] + [Q_2] = \left[dgx^2 + hxy - fy^2\right]$, but recall that $ax^2 + bxy + cy^2 \sim cy^2 - bxy + ax^2$, hence $[Q_1] + [Q_2] = [-fx^2 - hxy + dgy^2]$ which in terms of Dirichlet composition we know is $-[Q_3]$. So Dirichlet composition corresponds to the Cube Law.

Proof of first part of Theorem 3.4 in the case D is not a square. The preceding paragraph shows how the cube law is equivalent to Dirichlet composition. So, in the case D is not a square, Dirichlet composition is a binary operation that satisfy the given condition since: we know it is an additive binary operation defined on $C((\mathrm{Sym}^2 \mathbb{Z}^2)^*; D)$; its identity is the equivalence class of the principal form, now denoted $[Q_{\mathrm{id},D}]$; it is equivalent to the cube law. Furthermore, the preceding paragraph shows that if a binary operation satisfy the cube law, then it is Dirichlet composition, proving the uniqueness part of the statement. □

We will not finish the proof of Theorem 3.4 as such, but instead it will be proven as parts of other discussion and proves of later section. We will cover the case of when D is a square as part of the second proof of Theorem 3.6, which we do on page 22. As for the second statement of the theorem, we will show how we can extend Theorem 3.7 to prove this.

3.2 Cubes of integers

Now that we have a definition of primitivity we can use this along with the notation $[A]$ to denote the set of Γ-equivalence classes of A. We will denote this new set of equivalence classes of primitive cubes by $C(\left(\mathbb{Z}^2\right)^{\otimes 3}; D)$. We show that we can equip this set so to form a group.

Theorem 3.6 (Composition of cubes of integers)**.** *Let $D \equiv 0, 1 \mod 4$ and let $A_{\mathrm{id},D}$ be as defined above. Then there exists a unique binary operation that turns $C(\left(\mathbb{Z}^2\right)^{\otimes 3}; D)$ into an additive group such that:*

1. *$[A_{\mathrm{id},D}]$ is the identity,*
2. *for $i = 1, 2, 3$ the maps $[A] \mapsto [Q_i^A]$ are group homomorphism from $C(\left(\mathbb{Z}^2\right)^3; D)$ to $C(\left(Sym^2\mathbb{Z}^2\right)^*; D)$.*

Proof in the case D is not a square. This can be deduced from Theorem 3.4 by defining the addition of cubes as follow. Let A, B be two primitive cubes with discriminant D. Now since $([Q_1^A] + [Q_1^B]) + ([Q_2^A] + [Q_2^B]) + ([Q_3^A] + [Q_3^B]) = [Q_{\mathrm{id},D}]$ in $C(\left(\mathrm{Sym}^2\mathbb{Z}^2\right)^*; D)$ by Theorem 3.4 we have that there exists, up to Γ-equivalence, a unique cube C of discriminant D which gives rise to representatives of $[Q_1^A] + [Q_1^B]$, $[Q_2^A] + [Q_2^B]$, $[Q_3^A] + [Q_3^B]$. We define the composition of $[A]$ and $[B]$ to be $[A] + [B] = [C]$. One can easily see that the composition of cubes directly relates to the composition of binary quadratic forms. By the way we have defined composition of cubes one can easily see that if $f_i([A]) = [Q_i^A]$ then $f_i([A] + [B]) = f_i([C]) = [Q_i^C] = [Q_i^A] + [Q_i^B] = f_i([A]) + f_i([B])$ hence proving 2. For part 1 we know that $A_{\mathrm{id},D}$ gives rise to $Q_{\mathrm{id},D}$ three times, hence by definition and the fact $[Q_{\mathrm{id},D}]$ is the identity we have that $[A_{\mathrm{id},D}]$ is the identity.

Conversely, if we have an other binary operation satisfying 2, then because of the group homomorphism, the binary operation it maps to has to be Dirichlet composition. Moreover, once we have chosen the identity of the group, as part 1 does, then the binary operation has to be unique. □

We are going to later re-prove this theorem, on page 22, the way Bhargava does, as it follows a similar approach to the proof of Dirichlet composition and hence at the same time proves Dirichlet composition including the case when D is a square. While this is a useful theorem it does not give an explicit formula (in the proof we will do later we will see a way of constructing the composition, but it is not practical), much like Theorem 3.4 did not give an explicit formula. But in that case we had showed that the binary operation was the same as Dirichlet's composition to which we have a formula. Lemmermeyer took a more computational based approach to binary quadratic forms, and when he looked at Bhargava's paper he wrote down a theorem [Lemmermeyer(2010), p80] with an explicit formula, namely:

Theorem 3.7. *Let $D \equiv 0$ or $1 \mod 4$. For any pair of primitive binary quadratic form $Q_1 = (a, b, c)$ and $Q_2 = (a', b', c')$ with discriminant D there is a cube A such that $Q_1 = Q_1^A$ and $Q_2 = Q_2^A$.*

More precisely: if $aa' \neq 0$ and if we let $e = \gcd(a, a', \frac{b+b'}{2})$ then there exists an integral solution f, g to the equation

$$\frac{a'f - ag}{e} = \frac{b - b'}{2}$$

such that if we define

$$h = \frac{-f\frac{b+b'}{2} - ec'}{a}$$

then h is integral. Furthermore for all such f, g, h the cube

$$\begin{tikzcd}
 & \frac{a'}{e} \arrow[rr, dash] \arrow[dd, dash] & & \frac{b+b'}{-2e} \arrow[dd, dash] \\
0 \arrow[ur, dash] \arrow[rr, dash] \arrow[dd, dash] & & \frac{a}{e} \arrow[ur, dash] \arrow[dd, dash] & \\
 & g \arrow[rr, dash] & & h \\
e \arrow[ur, dash] \arrow[rr, dash] & & f \arrow[ur, dash] &
\end{tikzcd} \tag{3.2}$$

gives rise to Q_1, Q_2.

Proof. We follow closely [Lemmermeyer(2010), pg 67]. The first paragraph is a restatement of the second part of Theorem 3.4. But the second part will give us an explicit construction of a cube with given two quadratic forms, as we will show that f, g can be found using Euclid's algorithm.

Without loss of generality assume $a' \neq 0$. Let A be the cube of figure (3.2) and let M_i, N_i for $i = 1, 2, 3$ be as usual. Notice that $-\det M_1 = a$ and $-\det M_2 = a'$ as required. We also want $b = (\frac{b+b'}{2} - \frac{ag}{e} + \frac{a'f}{e})$ and $b' = (\frac{b+b'}{2} - \frac{a'f}{e} + \frac{ag}{e})$ which can be rearranged as $\frac{b-b'}{2} = \frac{a'f-ag}{e}$. Notice that $\gcd(\frac{a}{e}, \frac{a'}{e}) | \frac{b-b'}{2}$, as $D = b^2 - 4ac = b'^2 - 4a'c'$ implies $ac - a'c' = \left(\frac{b+b'}{2}\right)\left(\frac{b-b'}{2}\right)$ and $\gcd(\frac{a}{e}, \frac{a'}{e}, \frac{b+b'}{2e}) = 1$. Hence we can use Euclid's algorithm to find $f, g \in \mathbb{Z}$ which satisfy the equation $\frac{a'f-ag}{e} = \frac{b-b'}{2}$.

Next we check what the conditions are needed on h so that A is the required cube, that is h needs to be such that $-\det N_1 = \frac{-\frac{b+b'}{2}g - a'h}{e} = c$ and $-\det N_2 = \frac{-f\frac{b+b'}{2} - ah}{e} = c'$. Recalling that $\frac{b^2-b'^2}{4} = ac - a'c'$ (since the two determinants are the same) and that $g = -\left(\frac{b-b'}{2}\right)\left(\frac{e}{a}\right) - \frac{a'f}{a}$ we have

$$\begin{aligned} h &= \frac{-f\frac{b+b'}{2} - ec'}{a} \\ &= \frac{-ag\frac{b+b'}{2}}{aa'} - \left(\frac{b-b'}{2}\right)\left(\frac{b+b'}{2}\right)\left(\frac{e}{aa'}\right) - \frac{ec}{a} \\ &= \frac{-g\frac{b+b'}{2}}{a'} - \frac{e(ac-a'c') - aec}{aa'} \\ &= \frac{-g\frac{b+b'}{2} - ec'}{a'} \end{aligned}$$

Hence the two requirements boil down to showing that there exists f (or g) such that $h \in \mathbb{Z}$, where h is given as in the formula of the theorem. If $\frac{f\frac{b+b'}{2} - ec'}{a} \in \mathbb{Z}$ then we are done. If not notice that $-\frac{ah}{e} = \frac{\frac{b+b'}{2}g}{e} - c \in \mathbb{Z}$ and similarly for $-\frac{a'h}{e} \in \mathbb{Z}$, hence the denominator of h divides $\gcd(\frac{a}{e}, \frac{a'}{e}) = q$, so write $h = \frac{p}{q}$. Note that $\gcd(q, \frac{b+b'}{2e}) = 1$ hence there exists $r \in \mathbb{Z}$ such that $r\frac{b+b'}{2e} \equiv p \mod q$. Let $N_1' = \begin{pmatrix} e' & g' \\ f' & h' \end{pmatrix} = N_1 - \frac{r}{\alpha}M_1$, then by the definition of q we have that $e' = e$, f' and g' are all integers. Furthermore $h' = \frac{p - r\frac{b+b'}{2e}}{q} \in \mathbb{Z}$, $\frac{a'f'-ag'}{e} = \frac{a'(f-\frac{ra}{qe}) - a(g-\frac{ra'}{qe})}{e} = \frac{a'f-ag}{e}$ as required. Hence we have constructed our cube with all entries in $\mathbb{Z}$ which gives rise to our two quadratic forms. □

While the above theorem only gave a construction for A given two binary quadratic forms, we can still extend it to prove the second statement of Theorem 3.4. Given Q_1, Q_2, Q_3 such that their equivalence class sum to 0, we use the above theorem to construct a cube A which gives rise to Q_1 and Q_2. Then we know that Q_3^A is equivalent to Q_3, so there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $(Q_3^A)^\gamma = Q_3$, hence $A^{\mathrm{id} \times \mathrm{id} \times \gamma}$ gives rise to Q_1, Q_2 and Q_3.

We note that to define $[A] + [B]$ where $A, B \in (\mathbb{Z}^2)^{\otimes 3}$ we just need to calculate $[Q_1^A] + [Q_1^{A'}]$ and $[Q_2^A] + [Q_2^{A'}]$ as, as discussed before, the cube constructed from representatives of these two equivalence classes has to give rise to a third binary quadratic form representing $[Q_3^A] + [Q_3^{A'}]$. Hence we can use Theorem 3.7 to write an explicit composition law. Given two primitive cubes of integers A and A' of discriminant D, we know by our discussion in section 3.1 that they are equivalent to the cubes $(1, 0, 0, d, 0, f, g, h)$ and $(1, 0, 0, d', 0, f', g', h')$. Hence we have that $[Q_1^A] + [Q_1^B] = [(d, h, fg)] + [(d', h', f'g')] = [\frac{dd'}{e'^2}x^2 + Bxy + \frac{e'^2(B^2-D)}{4dd'}y^2]$ and, recalling that $[(a, b, c)] = [(c, -b, a)]$, we have $[Q_2^A] + [Q_2^B] = [(df, -h, g)] + [(d'f', -h', g')] = [\frac{dd'ff'}{e^2}x^2 + B'xy + \frac{e^2(B'^2-D)}{4dd'ff'}]$, where B, B' satisfy

$$\begin{array}{rclcrcl} B & \equiv & h \mod 2\frac{d}{e'} & & B' & \equiv & -h \mod 2\frac{df}{e} \\ B & \equiv & h' \mod 2\frac{d'}{e'} & & B' & \equiv & -h' \mod 2\frac{d'f'}{e} \\ B^2 & \equiv & D \mod 4\frac{dd'}{e'^2} & & B'^2 & \equiv & D \mod 4\frac{dd'ff'}{e^2} \end{array}$$

and $e' = \gcd(d, d', \frac{h+h'}{2})$, $e = \gcd(df, df', \frac{h+h'}{2})$. From this we notice that $e'|e$, so let $a = \frac{e}{e'}$, and that $\frac{B+B'}{2} = \frac{ad}{e}m + \frac{df}{e}n = \frac{ad'}{e}m' + \frac{d'f'}{e}n'$ for some $m, n, m', n' \in \mathbb{Z}$. Using the fact that $\gcd(ab, c) = \mathrm{lcm}(a, b)$

if $a|c$ and $b|c$, if we let $G_1 = \gcd(\frac{d}{e'}, \frac{df}{e})$, $G_2 = \gcd(\frac{d'}{e'}, \frac{d'f'}{e})$, $G_3 = \gcd(\frac{d}{e'}, \frac{d'f'}{e})$ and $G_4 = \gcd(\frac{d'}{e'}, \frac{df}{e})$, then we have $\gcd(\frac{a^2dd'}{e^2}, \frac{dd'ff'}{e^2}, \frac{B+B'}{2}) = \mathrm{lcm}(G_1, G_2, G_3, G_4)$. So let $E = \mathrm{lcm}(G_1, G_2, G_3, G_4)$ (notice that E does not depend on B or B') then we know we can find i, j, k that satisfy

$$\frac{dd'(ff'i - a^2j)}{e^2E} = \frac{B - B'}{2}, \quad k = -i\frac{a^2dd'(B + B')}{2e^2} - \frac{Ea^2(B^2 - D)}{4ff'}$$

Then $[A] + [A'] = [A'']$ where A'' is the cube

$$\begin{tikzcd}
& \frac{dd'ff'}{e^2E} \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & \frac{B+B'}{-2E} \arrow[dl, dash] \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & \frac{dd'a^2}{Ee^2} \arrow[dd, dash] & \\
& j \arrow[rr, dash] \arrow[dl, dash] & & k. \arrow[dl, dash] \\
E \arrow[rr, dash] & & i &
\end{tikzcd}$$

The above paragraph, being full with formula which do not look pleasant, can become easily confusing. So we give an example below to illustrate each steps of the above discussion.

Example. Let $A = (11, 6, -7, 77, 5, 1, -3, 39)$ and $B = (-2, -4, 2, 3, -19, -35, -14, -28)$ be two primitive cubes with discriminant $D = -167$. We can apply

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \times \mathrm{id} \times \mathrm{id}$$

to A to get $A' = (1, 4, -1, -1, 5, 1, -3, 39)$. Since we have a 1 as a first entry we can clear b, c and e by using

$$\begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and end up with $A^{\gamma_1} = (1, 0, 0, 3, 0, -19, 2, 17)$ where

$$\gamma_1 = \begin{pmatrix} 1 & -5 \\ -2 & 11 \end{pmatrix} \times \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Similarly we find that $B^{\gamma_2} = (1, 0, 0, 2, 0, -14, 3, 13)$ where

$$\gamma_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} \times \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

This gives rise to the quadratic forms $Q_1^A = -3x^2 + 17xy - 38y^2, Q_2^A = -2x^2 + 17xy - 57y^2$ and $Q_1^B = -2x^2 + 13xy - 42y^2, Q_2^B = -3x^2 + 13xy - 28y^2$. Since $\gcd(-3, -2, 15) = 1$ we can apply Dirichlet's composition on Q_1^A, Q_1^B and Q_2^A, Q_2^B, we just need to find B, B' which satisfy

$$\begin{array}{rclcrcl}
B & \equiv & 17 \mod 6 & \quad & B' & \equiv & 17 \mod 4 \\
B & \equiv & 13 \mod 4 & & B' & \equiv & 13 \mod 6 \\
B^2 & \equiv & -167 \mod 24 & & B'^2 & \equiv & -167 \mod 24
\end{array}$$

One can check that $B = 5$ and $B' = 1$ satisfy these conditions. So we get two new binary quadratic forms $Q_1^C = 6x^2 + 5xy + 8y^2$ and $Q_2^C = 6x^2 + xy + 7y^2$. Now we set $e = \gcd(6, 6, 3) = 3$ and we need to solve$\frac{6f-6g}{3} = 2, 6h = -3f - 3 \cdot 7$. An easy solution is $f = 1, g = 0, h = -4$. Hence $[A] + [B] = [C]$ where $C = (0, 2, 3, 1, 2, -1, 0, -4)$. In turns of cubes:

$$\left[\begin{tikzcd}
& 5 \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & 1 \arrow[dl, dash] \arrow[dd, dash] \\
11 \arrow[rr, dash] \arrow[dd, dash] & & 6 \arrow[dd, dash] & \\
& -3 \arrow[rr, dash] \arrow[dl, dash] & & 39 \arrow[dl, dash] \\
-7 \arrow[rr, dash] & & 77 &
\end{tikzcd}\right] + \left[\begin{tikzcd}
& -19 \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & -35 \arrow[dl, dash] \arrow[dd, dash] \\
-2 \arrow[rr, dash] \arrow[dd, dash] & & -4 \arrow[dd, dash] & \\
& -14 \arrow[rr, dash] \arrow[dl, dash] & & -28 \arrow[dl, dash] \\
2 \arrow[rr, dash] & & 3 &
\end{tikzcd}\right] = \left[\begin{tikzcd}
& 2 \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & -1 \arrow[dl, dash] \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & 2 \arrow[dd, dash] & \\
& 0 \arrow[rr, dash] \arrow[dl, dash] & & -4 \arrow[dl, dash] \\
3 \arrow[rr, dash] & & 1 &
\end{tikzcd}\right]$$

We can check that $[Q_3^A]+[Q_3^B]=[-19x^2+17xy+6y^2]+[-14x^2+13xy+6y^2]=[4x^2-5xy+12y^2]=[Q_3^C]$. For this we calculate that $Q_3^A+Q_3^B=266x^2+321xy+97y^2$, recalling that $(a,b,c)\sim(c,-b,a)$ and $(a,b,c)\sim(a,b+2an,an^2+bn+c)$, we see that $(266,321,97)\sim(97,-321,266)\sim(97,67,12)\sim(12,-67,97)\sim(12,5,4)\sim(4,-5,12)$ hence $[Q_3^C]=[266x^2+321xy+97y^2]$ as expected.

Theorem 3.8. *The inverse of the equivalence class containing $A=(a,b,c,d,e,f,g,h)$ is the equivalence class containing $-A=(a,-b,-c,d,-e,f,g,-h)$.*

Proof. We calculate that $Q_1^A=(bc-ad)x^2+(de+ah-cf-bg)xy+(eh-fg)y^2=-Q_1^{-A}$ and $Q_2^A=-Q_2^{-A}$. Hence $[Q_1^A]+[Q_1^{-A}]=[Q_2^A]+[Q_2^{-A}]=[Q_{\mathrm{id},D}]$, forcing $[A]+[-A]=[A_{\mathrm{id},D}]$. □

3.3 Another proof of Theorem 3.6

We are now going to prove Theorem 3.6 in a similar way to the proof of Theorem 2.18, in such a way to cover the case when D is square. Recall though that throughout this paper we exclude the case $D=0$. To do this we will need to generalise our notion of orders and introduce the new concept of quadratic rings, which we will use for the remainder of this paper.

Definition 3.9. A *quadratic ring* $\mathcal{O}$ is a (commutative) ring isomorphic as an additive group to $\mathbb{Z}^2$.

From the definition, we have that $\mathcal{O}$ has has rank 2 in $\mathbb{Z}$, furthermore as $\mathcal{O}$ is a ring $1\in\mathcal{O}$. So $\mathcal{O}$ has a basis of the form $[1,\tau]$, since $\tau^2\in\mathcal{O}$ we have that τ solves a quadratic equation $x^2+bx+c=0$ with $b,c\in\mathbb{Z}$.

Definition 3.10. The *discriminant* of a quadratic ring $\mathcal{O}=[1,\tau]$ is $D=b^2-4c$, where b,c are such that $\tau^2+b\tau+c=0$.

A quadratic ring $\mathcal{O}$ of discriminant D is said to be *oriented* if a choice of $\sqrt{D}\in\mathcal{O}\setminus\mathbb{Z}$ has been made.

For this paper, we will assume, unless stated otherwise, that our rings are oriented. Note that D is congruent to 0 or 1 mod 4. Conversely given $D\in\mathbb{Z}$ such that $D\equiv\epsilon \mod 4$ with $\epsilon\in\{0,1\}$, then there exists a unique, up to orientation preserving isomorphism, oriented quadratic ring, namely $\mathcal{O}=[1,\tau]$ where $\tau^2=\epsilon\tau+\frac{D-\epsilon}{4}$. Let us define the conjugate of an element $\alpha=x+\tau y\in\mathcal{O}$, denoted by $\overline{\alpha}$, to be $x+\overline{\tau}y$, where $\overline{\tau}$ is the other root (not in $\mathbb{Z}$) to the equation $x^2-\epsilon x-\frac{D-\epsilon}{4}=0$. With this we define a map $\pi:\mathcal{O}\to\mathbb{Z}$, by $\pi(\alpha)=\frac{\alpha-\overline{\alpha}}{\sqrt{D}}$ and we say an element $\alpha\in\mathcal{O}$ to be positive if $\pi(\alpha)>0$. While we will not need to actually choose $\sqrt{D}$, all our work only requires a choice to have been made, we assume from here on that we take the positive square root, that is $\pi(\sqrt{D})>0$.

Notice how quadratic rings are a natural extension to the definition of orders in Section 2. To see this note that if the discriminant D is square-free and not 1 then $\mathcal{O}$ is just the maximal order $\mathcal{O}_K$ of $K=\mathbb{Q}(\sqrt{D})$. More generally if D is not a square then $D=f^2D_0$ and $x^2+fD_0x+\frac{f^2D_0-f^2D_0}{4}$ is a quadratic polynomial with discriminant D and root $f\omega_k$, using the notation of Section 2.4. So $\mathcal{O}$ is an order of the quadratic field $\mathbb{Q}(\sqrt{D})$. For the remainder of this paper we will let $K:=\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{O}$. In the case that $\mathcal{O}$ has a non-square discriminant $D=f^2D_0$, then using the fact $\mathcal{O}$ is an order, we have that $K=\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{D_0})$.

We use the same definition of fractional ideals and oriented ideals for quadratic rings as we did for orders. Hence we also have the same definition for the narrow class group of a quadratic ring $\mathcal{O}$, that is, $C^+(\mathcal{O})$ is the set of equivalence classes of invertible oriented fractional ideals of $\mathcal{O}$.

Recall that the Cube Law Axiom was taken as an analogy of collinear points on an elliptic curve. For a similar reason we are going to define what it means for three fractional ideals to be *collinear*, the reason for the term being that they will end up being in correspondence with binary quadratic forms that add up to 0.

Definition 3.11. Let $\mathcal{O}$ be a quadratic ring, we say the fractional ideals I_1,I_2,I_3 are *collinear* if $I_1I_2I_3\subseteq\mathcal{O}$ and $N(I_1)N(I_2)N(I_3)=1$

If all three ideals are invertible then we have in fact equality, i.e., $I_1I_2I_3=\mathcal{O}$. In the same way we define equivalence of oriented fractional ideals we have the following definition.

Definition 3.12. We say two triples of collinear fractional oriented ideals, (I_1,I_2,I_3) and (I_1',I_2',I_3'), are *equivalent* if there exists $\alpha_1,\alpha_2,\alpha_3\in K$ such that $I_i=\alpha_iI_i'$ for $i=1,2,3$.

We will denote the set of equivalence classes of collinear triples of oriented invertible fractional ideals of an oriented quadratic ring $\mathcal{O}$, by $C(\mathrm{Col}^3_{1,1,1};\mathcal{O})$. This can easily be seen to be a group when we equip it with the binary operation $(I_1,I_2,I_3)\cdot(I_1',I_2',I_3')=(I_1I_1',I_2I_2',I_3I_3')$. The notation $\mathrm{Col}^3_{1,1,1}$, stands for the fact that we are considering three objects that are collinear, furthermore the $1,1,1$ represent that we do not require our three ideals to be equal to each other, a requirement that we will impose in later cases. We will now state and prove a theorem that will also prove Theorem 3.6.

Theorem 3.13. *Let $D\equiv 0,1 \mod 4$ and $\mathcal{O}$ the oriented ring of discriminant D. Then there is a bijection between $C((\mathbb{Z}^2)^{\otimes 3};D)$ and $C(\mathrm{Col}^3_{1,1,1};\mathcal{O})$.*

Proof. We are going to follow the ideas established by [Bhargava(2004), p 17]. For the moment let us forget that we need our cubes to be primitive and our ideals to be invertible, we will deal with that later on in the proof. Let (I_1,I_2,I_3) be a representative of an equivalence class of collinear triple of fractional ideals of the quadratic ring $\mathcal{O}$ and let $D=\mathrm{Disc}(\mathcal{O})$. Let $1,\tau$ be a positively oriented basis of $\mathcal{O}$ such that $\tau^2=\epsilon\tau+\frac{D-\epsilon}{4}$, with $\epsilon\in\{0,1\}$ and $\epsilon\equiv D \mod 4$. Let α_1,α_2; β_1,β_2; and γ_1,γ_2 be correctly oriented basis of I_1,I_2 and I_3 respectively, since $I_1I_2I_3\subseteq\mathcal{O}$ we have the following eight equations

$$\alpha_i\beta_j\gamma_k=c_{i,j,k}+a_{i,j,k}\tau \tag{3.3}$$

with $a_{i,j,k},c_{i,j,k}\in\mathbb{Z}$. We define a map mapping (I_1,I_2,I_3) to a cube A by setting

$$A=(a_{1,1,1},a_{1,1,2},a_{1,2,1},a_{1,2,2},a_{2,1,1},a_{2,1,2},a_{2,2,1},a_{2,2,2}).$$

We show that this map is well defined. Suppose that we choose another basis for I_1, say $r\alpha_1+t\alpha_2, s\alpha_1+u\alpha_2$ with $ru-st=1$ (our change of basis needs to be in $\mathrm{SL}_2(\mathbb{Z})$ so to keep the correct orientation of I_1). Then we have that our triple gives rise to $A^{\gamma\times\mathrm{id}\times\mathrm{id}}$, where

$$\gamma=\begin{pmatrix} r & s\\ t & u\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}).$$

Hence changing the basis of the three ideals does not change the equivalence class of A. Furthermore if we take an equivalent triple, say $\kappa_1I_1,\kappa_2I_2,\kappa_3I_3$, since they need also to be collinear we have that $N(\kappa_1)N(\kappa_2)N(\kappa_3)=1$, in other words $\kappa_1\kappa_2\kappa_3$ is a unit in $\mathcal{O}$, hence our cube A does not change. So we have shown that the map is well defined. Notice that the above map can be defined as $a_{i,j,k}=\pi(\alpha_i\beta_j\gamma_k)$.

Next we show that the cube has discriminant D. To this end, we show that the equations (3.3) imply $\mathrm{Disc}(A)=N(I_1)^2N(I_2)^2N(I_3)^2\mathrm{Disc}(\mathcal{O})$. This can be checked by direct arithmetic using the formula of the discriminant of A, the formula for the norm of an ideal and the set of equations (3.3). There is a more interesting approach done by [Bhargava(2004), p 18]. Start with the special case $I_1=I_2=I_3=\mathcal{O}$, $\alpha_1=\beta_1=\gamma_1=1$ and $\alpha_2=\beta_2=\gamma_2=\tau$, this gives rise to the cube $A_{\mathrm{id},D}$ from which we can easily see that $\mathrm{Disc}(A)=\mathrm{Disc}(\mathcal{O})$. Now suppose we change I_1 to a general oriented fractional ideal $[\alpha_1,\alpha_2]$, this is done by a transformation $T^T\in\mathrm{GL}_2(\mathbb{Q})$. Then the new cube A is obtained by transforming $A_{\mathrm{id},D}$ by $T\times\mathrm{id}\times\mathrm{id}$. If we let

$$T=\begin{pmatrix} r & s\\ t & u\end{pmatrix}$$

then we know from the proof of Theorem 3.3 that $Q_1^A=Q_{\mathrm{id},D}^T$ and $Q_2^A=Q_3^A=\det(T)Q_{\mathrm{id},D}$, so we have that the discriminant of all three binary quadratic forms are scaled by a factor of $\det(T)^2=N(I_1)^2$. Hence, recalling that the discriminant of A is the same as the discriminant of Q_i^A, we have that the discriminant of A is multiplied by a factor of $N(I_1)^2$. Again using the proof of Theorem 3.3, we can find a similar result for changing I_2, I_3 from our current cube A, hence proving that for all cube A we have $\mathrm{Disc}(A)=N(I_1)^2N(I_2)^2N(I_3)^2\mathrm{Disc}(\mathcal{O})$. But since our ideals are collinear, and hence $N(I_1)N(I_2)N(I_3)=1$, we have $\mathrm{Disc}(A)=\mathrm{Disc}(\mathcal{O})$.

We need to verify that the map mapping I_1,I_2,I_3 to A gives rise to exactly one set of equivalence classes of cubes, i.e., we need to prove the map is both surjective and injective. To show this we fix a cube $A=(a_{1,11},a_{1,1,2},\ldots,a_{2,2,1},a_{2,2,2})$ of discriminant D and consider the set of equations (3.3). As we have only $a_{i,j,k}$ determined, the set of equations seems to be made of mostly indetermined variables, namely $\alpha_i,\beta_j,\gamma_k$ and $c_{i,j,k}$. We will show that in fact the cube determines all these indeterminate, proving surjectivity, but also we will show that the $\alpha_i, \beta_j, \gamma_k$ that A gives rise to gives a unique equivalence class of collinear triples, hence proving injectivity. First we show that A determines the $c_{i,j,k}$. Since we are in a commutative ring we have

$$(\alpha_i\beta_j\gamma_k)(\alpha_{i'}\beta_{j'}\gamma_{k'}) = (\alpha_{i'}\beta_j\gamma_k)(\alpha_i\beta_{j'}\gamma_{k'}) = (\alpha_i\beta_{j'}\gamma_k)(\alpha_{i'}\beta_j\gamma_{k'}) = (\alpha_i\beta_j\gamma_{k'})(\alpha_{i'}\beta_{j'}\gamma_{k'}),$$

so for example $(\alpha_1\beta_1\gamma_1)(\alpha_2\beta_2\gamma_2) = (\alpha_2\beta_1\gamma_1)(\alpha_1\beta_2\gamma_2)$ which implies $(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau)$. We can use the property of commutativity to write out nine different possible equations, see the appendix for which nine and why. With those nine equations, once we multiplied them out, we can equate the coefficients of 1 and the coefficients of τ to get a total of 18 linear and quadratic equations. Solving those 18 equations in terms of $c_{i,j,k}$ and using the fact that we need $N(I_1)N(I_2)N(I_3) > 0$, since $[1, \tau]$ is positively oriented, we find that there exists a unique solution, see appendix, given by:

$$\begin{aligned} c_{i,j,k} &= (i'-i)(j'-j)(k'-k) \\ &\quad [a_{i',j,k}a_{i,j',k}a_{i,j,k'} + \frac{1}{2}a_{i,j,k}(a_{i,j,k}a_{i',j',k'} - a_{i',j,k}a_{i,j',k'} - a_{i,j',k}a_{i',j,k'} - a_{i,j,k'}a_{i',j',k})] \\ &\quad -\frac{1}{2}a_{i,j,k}\epsilon \end{aligned} \tag{3.4}$$

where $\{i, i'\} = \{j, j'\} = \{k, k'\} = \{1, 2\}$ and $\epsilon \in \{1, 0\}$ with $\epsilon \equiv D \mod 4$.

Now that we have the $a_{i,j,k}, c_{i,j,k}$ we can determine appropriate $\alpha_i, \beta_j, \gamma_k$ which yields the correct $a_{i,j,k}, c_{i,j,k}$ under the set of equations (3.3). One can see that, since $\alpha_1(\alpha_2\beta_j\gamma_k) = \alpha_2(\alpha_1\beta_j\gamma_k)$, the ratio $\alpha_1 : \alpha_2$ is determined by the ratio $(c_{1,j,k} + a_{1,j,k}\tau) : (c_{2,j,k} + a_{2,j,k}\tau)$, and this is true for any fixed $j, k \in \{1, 2\}$. Similarly we can determined the ratio $\beta_1 : \beta_2$ by the ratio $(c_{i,1,k} + a_{i,1,k}\tau) : (c_{i,2,k} + a_{i,2,k}\tau)$ for any fixed $i, k \in \{1, 2\}$. Once α_i and β_j have been chosen, we can determine γ_k by the set of equations (3.3). Note that while $\alpha_i, \beta_j, \gamma_k$ are only determined up to scalars in K, this does not matter as we are we want collinear triples of oriented fractional ideals up to equivalence. So if we can show that in fact the $\mathbb{Z}$-module generated by α_1, α_2, the $\mathbb{Z}$-module generated by β_1, β_2 and the $\mathbb{Z}$-module generated by γ_1, γ_2 are in fact fractional ideals of $\mathcal{O}$, then we have showed that to any cube A, there exists a collinear triple of oriented fractional ideals which maps to it, showing surjectivity of the map. Furthermore, due to the uniqueness of the solution (3.4), we have that the equivalence class of collinear ideals mapping to A is unique, which, with a bit more thoughts, shows injectivity. To see that we have proved injectivity suppose we have two collinear triple of oriented fractional ideals, say (I_1, I_2, I_3) and (J_1, J_2, J_3), which maps to A and A^γ respectively, where $\gamma = \gamma_1 \times \gamma_2 \times \gamma_3 \in \Gamma$. Then we can change the basis of J_1, J_2, J_3 by $\gamma_1^{-1}, \gamma_2^{-1}$ and γ_3^{-1} respectively so that (J_1, J_2, J_3) maps to A, by the work we did at the beginning of the proof. But since the equivalence class of collinear ideals mapping to A is unique, we have that (I_1, I_2, I_3) and (J_1, J_2, J_3) must be equivalent.

To check that the $\mathbb{Z}$-module generated by α_1, α_2, the $\mathbb{Z}$-module generated by β_1, β_2 and the $\mathbb{Z}$-module generated by γ_1, γ_2 are fractional ideals of $\mathcal{O}$, we need to check that they are $\mathcal{O}$-modules, so we need to show that they are closed under multiplication by τ. To this end let us fix $\alpha_i = (c_{i,1,1} + a_{i,1,1}\tau)$, $\beta_j = (c_{2,j,2} + a_{2,j,2}\tau)$, forcing $\gamma_1 = \beta_1^{-1}$ and $\gamma_2 = \alpha_2^{-1}$. Moreover let us denote by $Q_i = a_ix^2 + b_ixy + c_iy^2$, the three binary quadratic forms associated to A. An explicit calculation, see appendix for example of the first one, shows that we have in fact

$$\begin{aligned} \tau\alpha_1 &= \frac{b_1 + \epsilon}{2}\alpha_1 + a_1\alpha_2 \\ -\tau\alpha_2 &= c_1\alpha_1 + \frac{b_1 - \epsilon}{2}\alpha_2 \end{aligned}$$

where ϵ is as usual. Similar equations can be worked out for the basis of I_2, I_3. So in particular we have showed that I_1, I_2, I_3 are fractional ideals of $\mathcal{O}$.

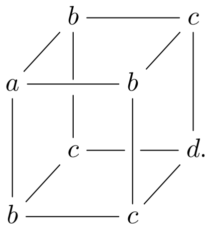
All the above work did not require our ideals to be invertible or our cubes to be primitive, so the above map is a bijection between equivalence classes of collinear triples of ordered fractional ideals of $\mathcal{O}$ and equivalence classes of cubes of discriminant D. To finish the proof of the theorem as stated, i.e., that the bijection is between $C(\mathrm{Col}^3_{1,1,1}; \mathcal{O})$ and $C((\mathbb{Z}^2)^{\otimes 3}; D)$, we need to show that primitive cubes are mapped from invertible ideals. We recall that if a cube is primitive, then it is equivalent to a cube $A = (1, 0, 0, d, 0, f, g, h)$. We use the above map to find the ideals which maps to it, specifically if we let $I_1 = [c_{1,1,1} + a_{1,1,1}\tau, c_{2,1,1} + a_{2,1,1}\tau]$ and $I_2 = [c_{1,1,2} + a_{1,1,2}\tau, c_{1,2,2,} + a_{1,2,2}\tau]$, then we find that $I_1 = [fg, \frac{h+\sqrt{D}}{2}]$ and $I_2 = [df, \frac{h+\sqrt{D}}{2}]$. On the other hand we know that the first two binary quadratic forms A gives rise to are $-dx^2+hxy+fgy^2 \sim fgx^2-hxy+dy^2$ and $-gx^2+hxy+dfy^2 \sim dfx^2-hxy-gy^2$. So we have Gauss composition by defining a map which maps I_i to Q_i, which is the same map as in section 2. Since we know from the work in section 2 that this map is well defined, and that if Q_i is primitive then I_i is invertible, we have by definition that A being primitive means all the Q_i's are, hence we have that indeed the ordered collinear ideals are invertible. On the other hand if (I_1, I_2, I_3) are all invertible then due by Gauss composition they correspond to primitive binary quadratic forms. Since by definition A is primitive if its associated binary quadratic forms are, we have that collinear triples of oriented fractional ideals maps to primitive cubes of integers. Hence we have finished proving that there is a bijection between $C((\mathbb{Z}^2)^{\otimes 3}; D)$ and $C(\mathrm{Col}^3_{1,1,1}; \mathcal{O})$. □

This proof had several aim. One was to see Bhargava's neat approach which we are going to use for a few more proofs, that is to think about these objects in more algebraic and abstract terms. We showed along the way that each I correspond to one of the binary quadratic forms associated to the cube of integers. Furthermore this theorem can be used to prove both Theorem 3.4 and Theorem 3.6. To see how this proves the first theorem, notice that under the bijection mapping equivalence classes of ideals and equivalence classes of binary quadratic forms we have that $\mathcal{O}$ maps to $[Q_{\mathrm{id},D}]$. We also have that for any primitive cube A, then the three ideals it gives rise to satisfies $I_1 I_2 I_3 = \mathcal{O}$, so the unique group law which satisfy point 1 and 2 of Theorem 3.4, is the one that correspond to multiplication of oriented ideals under the bijection $C^+(\mathcal{O})$. Finally, we have that given any three ideals I_1, I_2, I_3 such that $I_1 I_2 I_3 = \mathcal{O}$, then they map to a primitive cube A which gives rise to Q_1, Q_2, Q_3, the three primitive binary quadratic forms which corresponds to the ideals. Hence we have also proven the last statement of Theorem 3.4.

As for proving Theorem 3.6, this follows from the given bijection, as the three maps of part 2, translate into the map sending $(I_1, I_2, I_3) \to I_i \in C^+(\mathcal{O})$, which we know is a group homomorphism. We have also showed that $(\mathcal{O}, \mathcal{O}, \mathcal{O})$ maps to $A_{\mathrm{id},D}$ in the proof, so the unique binary operation satisfying the theorem, is the one that correspond to multiplication of collinear triple of invertible oriented fractional ideals. We also note out of interest that we have a natural bijection from $C(\mathrm{Col}^3_{1,1,1}; \mathcal{O}) \to C^+(\mathcal{O}) \times C^+(\mathcal{O})$ defined by $(I_1, I_2, I_3) \mapsto (I_1, I_2)$, with inverse defined by $(I_1, I_2) \mapsto (I_1, I_2, (I_1 I_2)^{-1})$.

3.4 Binary cubic forms

We now move on to binary cubic forms. In the same way that we have previously described that a symmetric 2 × 2 matrix can represent a binary quadratic form $ax^2 + 2bxy + cy^2$, we can have a symmetric 2 × 2 × 2 "matrix", or what we have called a cube, to represent a binary cubic form $ax^3 + 3bx^2y + 3cxy^2 + dy^3$, namely using the triply symmetric cube:



If M_i, N_i are as defined as in subsection 3.1 then $ax^3 + 3bx^2y + 3cxy^2 + dy^3 = (\underline{x}^T M_i \underline{x}, \underline{x}^T N_i \underline{x})\underline{x}$ for all $i \in \{1, 2, 3\}$, where $\underline{x} = (x, y)$ is a column vector. In the same spirit as $\mathrm{Sym}^2 \mathbb{Z}^2$ denoted the set of binary quadratic forms we use $\mathrm{Sym}^3 \mathbb{Z}^2$ to denote the set of binary cubic forms. Using the correspondence between binary cubic forms and triply symmetric cube we have a natural inclusion $\iota : \mathrm{Sym}^3 \mathbb{Z}^2 \to \left(\mathbb{Z}^2\right)^{\otimes 3}$.

Definition 3.14. The discriminant of $C(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ is $D = a^2d^2 - 3b^2c^2 + 4b^3d + 4ac^3 - 6abcd$

We say a binary cubic form $C(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ is *primitive* if the corresponding triply symmetric cube $\iota(C)$ is primitive.

If we calculate the three binary quadratic form that $\iota(C)$ gives rise to we see that

$$\begin{aligned} Q_1^{\iota(C)} = Q_2^{\iota(C)} = Q_3^{\iota(C)} &= -\begin{vmatrix} ax-by & bx-cy \\ bx-cy & cx-dy \end{vmatrix} \\ &= -((ac-b^2)x^2 + (bc-ad)xy + (bd-c^2)y^2) \end{aligned}$$

hence we have that C is primitive if and only if $\gcd(ac-b^2, bc-ad, bd-c^2) = 1$. We define an $\mathrm{SL}_2(\mathbb{Z})$ action on C as follows: Let

$$\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

then $C^\gamma(x,y) = C(rx+sy, tx+uy)$. As usual if we let $[C]$ denote the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of C (noting that this gives rise to the $\overline{\Gamma}$-equivalence class of $\iota(C)$ where $\overline{\Gamma} = \{\gamma \times \gamma \times \gamma : \gamma \in \mathrm{SL}_2(\mathbb{Z})\} \leq \Gamma$) and $C(\mathrm{Sym}^3 \mathbb{Z}^2; D)$ denote the set of equivalence class of primitive binary cubic forms with discriminant D, then we have the following theorem.

Theorem 3.15 (Composition of binary cubic forms). *Let $D \cong 0, 1 \mod 4$ and let $C_{\mathrm{id},D}$ be defined as*

$$C_{\mathrm{id},D} = \begin{cases} 3x^2y + \frac{D}{4}y^3 & D \cong 0 \mod 4 \\ 3x^2y + 3xy^2 + \frac{D+3}{4}y^3 & D \cong 1 \mod 4 \end{cases}$$

then there exists a binary operation which turns $C(\mathrm{Sym}^3 \mathbb{Z}^2; D)$ into an additive group such that

1. *$[C_{\mathrm{id},D}]$ is the identity,*

2. *the map given by $[C] \mapsto [\iota(C)]$ is a group homomorphism from $C(\mathrm{Sym}^3 \mathbb{Z}^2; D)$ to $C((\mathbb{Z}^2)^{\otimes 3}; D)$.*

Remark. At this point the reader might be surprised by the omission of the word *unique* in the above theorem, but we will show in the example after the proof that the map described in 2. is non-injective in certain cases. Hence we can construct different binary operations that will satisfy the given conditions. This will be remedied as in the proof we will give a bijection between $C(\mathrm{Sym}^3 \mathbb{Z}^2; D)$ and a group, hence we will have a natural binary operation. So when talking about the composition of binary cubic form, except in the next example, we will mean composition with respect to this natural binary operation.

Proof. Again we follow [Bhargava(2004), p 21], which is in the same style as the proof of Theorem 3.13. To this end let us introduce $C(\mathrm{Col}_1^3; \mathcal{O})$ to denote the set of equivalence classes of the pair (I, δ), where I is an ordered invertible fractional ideal of $\mathcal{O}$ and $\delta \in K^* = (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q})^*$ such that $I^3 = \delta\mathcal{O}$ and $N(I)^3 = N(\delta)$. Here two pairs (I, δ) and (I', δ') are equivalent if there exists $\alpha \in K$ such that $I' = \alpha I$ and $\delta' = \alpha^3 \delta$. The notation is meant to represent the fact that we give one ideal, hence the subscript 1, but we require this ideal to be a "triple collinear", hence the Col^3. The words "triple collinear" are quoted, as we are not actually using the property of collinearity (otherwise $I^3 = \mathcal{O}$) but something that looks very much like it. We can easily turn $C(\mathrm{Col}_1^3; \mathcal{O})$ into a group when we equip it with the multiplication $(I, \delta) \cdot (I', \delta') = (II', \delta\delta')$.

Under this notation we will show that there is a bijection between $C(\mathrm{Sym}^3 \mathbb{Z}^2; D)$ and $C(\mathrm{Col}_1^3; \mathcal{O})$, where $\mathcal{O}$ is oriented quadratic ring of discriminant D, as then the proof will be straightforward. As in the proof of Theorem 3.13, we will ignore, and not use, the fact that our ideals need to be invertible and our binary cubic need to be primitive for the time being. Let $1, \tau$ be a positively oriented basis of the oriented order $\mathcal{O}$ of discriminant D, such that $\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$, where $\epsilon \in \{0, 1\}$ and $\epsilon \equiv D \mod 4$. Fix the pair (I, δ) of oriented fractional ideal and invertible element of K, such that $I^3 \subseteq \delta\mathcal{O}$ (we do not necessarily have equality when the the ideal is not invertible) and $N(I)^3 = N(\delta)$. We know that I needs to be positively oriented for $I^3 \subseteq \delta\mathcal{O}$ to hold, so let α, β be a positively oriented basis of I. Since $I^3 \subseteq \delta\mathcal{O}$, we know that

$$\begin{aligned} \alpha^3 &= \delta(c_0 + a_0\tau), \\ \alpha^2\beta &= \delta(c_1 + a_1\tau), \\ \alpha\beta^2 &= \delta(c_2 + a_2\tau), \\ \beta^3 &= \delta(c_3 + a_3\tau), \end{aligned} \tag{3.5}$$

for some $a_i, c_i \in \mathbb{Z}$. We define a map mapping (I, δ) to the binary cubic form $C(x,y) = (a_0, a_1.a_2, a_3) = a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3$. We need to check this map is well defined. For this if we let $\pi : \mathcal{O} \to \mathbb{Z}$ be defined as before, $\pi(\zeta) = \frac{\zeta - \overline{\zeta}}{\sqrt{D}}$, then we have

$$\begin{aligned}
\pi\left(\frac{(\alpha x + \beta y)^3}{\delta}\right) &= \frac{(\frac{\alpha^3}{\delta} - \frac{\overline{\alpha}^3}{\overline{\delta}})x^3 + 3(\frac{\alpha^2\beta}{\delta} - \frac{\overline{\alpha}^2\overline{\beta}}{\overline{\delta}})x^2y + 3(\frac{\alpha\beta^2}{\delta} - \frac{\overline{\alpha}\overline{\beta}^2}{\overline{\delta}})xy^2 + (\frac{\beta^3}{\delta} - \frac{\overline{\beta}^3}{\overline{\delta}})y^3}{\sqrt{D}} \\
&= \frac{(\tau - \overline{\tau})(a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3) + (1-1)(c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3)}{\sqrt{D}} \\
&= \frac{(\tau - \overline{\tau})(a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3)}{\tau - \overline{\tau}} \\
&= C(x,y)
\end{aligned}$$

Hence we can use the map π to give a basis-free description of $C(x,y)$ as the map $(I,\delta) \to \mathbb{Z}$ defined by $(\zeta, \delta) \mapsto \pi(\frac{\zeta^3}{\delta})$. So if we change α, β by an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ to another basis of I (again we have that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ as the new basis needs to be positively oriented), then we change $C(x,y)$ by the same element γ, that is, the equivalence class of $C(x,y)$ is independent of the choice of basis for I. Conversely, if $C'(x,y)$ is in the same equivalence class of $C(x,y)$, then $C' = C^{\gamma}$, for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and C' can be obtain from I as described above with the change of basis by γ. Finally if we take another pair equivalent to (I,δ), say $(\kappa I, \kappa^3\delta)$, then we find that the κ^3 cancel each other out in the set of equations (3.5), hence the pair $(\kappa I, \kappa^3\delta)$ map to the same cube $C(x,y)$ as (I,δ).

We show that the discriminant of $C(x,y)$ is D. Similar as in the proof of 3.13, we show that the equations (3.5) give the identity $\mathrm{Disc}(C(x,y)) = N(I)^6 N(\delta)^{-2} \mathrm{Disc}(\mathcal{O})$. Start with the special case $I = \mathcal{O} = [1,\tau]$ and $\delta = 1$, this gives rise to the binary cubic form $C_{\mathrm{id},D}$ from which we can easily see that $\mathrm{Disc}(C(x,y)) = \mathrm{Disc}(\mathcal{O})$. Now suppose we change I to a general (positively) oriented fractional ideal $[\alpha, \beta]$ by a transformation $T \in \mathrm{GL}_2(\mathbb{Q})$,

$$T = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

Then the new binary cubic form C is obtained by transforming $C_{\mathrm{id},D}$, by that same element, i.e., in the case $D \equiv 0 \mod 4$ we have $C(x,y) = (3r^2t + t^3\frac{D}{4}, r^2u + 2rst + \frac{D}{4}t^2u, s^2t + 2rsu + \frac{D}{4}tu^2, 3s^2u + \frac{D}{u}u^3)$. We can then calculate that the discriminant of $C(x,y)$ is $(ru - st)^6 D = \det(T)^6 D$. Since $N(I) = \det(T)$, we have that changing ideal scales the discriminant of $C(x,y)$ by a factor of $N(I)^6$. On the other hand if we change 1 to $\delta = a + b\overline{\tau}$, we have that, using equations (3.5), our new cube is $C(x,y) = \frac{1}{N(\delta)}(b, a, \frac{D}{4}b, \frac{D}{4}a)$, (again this case is for $D \equiv 0 \mod 4$) and we calculate that the discriminant is

$$\frac{1}{N(\delta)^4}(4a^4(\frac{D}{4}) - 8a^2b^2(\frac{D}{4})^2 + 4b^4(\frac{D}{4})^3) = \frac{D}{N(\delta)^4}(a^2 - b^2\frac{D}{4})^2 = \frac{D}{N(\delta)^2}.$$

So changing δ scales the discriminant by $N(\delta)^{-2}$, and since the changing I does not affect our argument for changing δ and vice versa, we have proved that $\mathrm{Disc}(C(x,y)) = N(I)^6 N(\delta)^{-2} \mathrm{Disc}(\mathcal{O})$. But we have that $N(I)^3 = N(\delta)$, hence $\mathrm{Disc}(C(x,y)) = \mathrm{Disc}(\mathcal{O})$.

We now show that the above map is bijection, by showing that each equivalence classes of pairs (I,δ) map to exactly one set of equivalence classes of binary cubic forms, i.e, we need to prove the map is both surjective and injective. To show this we fix a binary quadratic form $C(x,y) = (a_0, a_1, a_2, a_3)$ of discriminant D and we consider the set of equations (3.5). As we only have a_i determined, the set of equations seems to be made of mostly indetermined variables, namely c_i, α, β and δ. We will show that in fact the binary cubic form determines all these indeterminate, proving surjectivity, but also we will show that the α, β, δ that A can give rise to give a unique equivalence class of collinear triples.

First we show that $C(x,y)$ determines the c_i. Since we are in a commutative ring we have that $(\alpha^2\beta)^2 = \alpha^3\alpha\beta^2$ and $(\alpha\beta^2)^2 = \alpha^2\beta\beta^3$. By expanding them using equations (3.5), recalling that $\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$, and equating the coefficients of τ and the coefficients of 1, we get the following 4 linear and quadratic equations:

$$\begin{aligned}
c_0c_2 + a_0a_2\frac{D-\epsilon}{4} &= c_1^2 + a_1^2\frac{D-\epsilon}{4} \\
c_0a_2 + c_2a_0 + \epsilon a_0a_2 &= 2c_1a_1 + \epsilon a_1^2 \\
c_1c_3 + a_1a_3\frac{D-\epsilon}{4} &= c_2^2 + a_2^2\frac{D-\epsilon}{4} \\
c_1a_3 + c_3a_1 + \epsilon a_1a_3 &= 2c_2a_2 + \epsilon a_2^2
\end{aligned}$$

We can use SAGE 4.8, which uses Maxima [Stein et al.(2012), SAGE], to solve this set of equations and find four different solutions. Recalling that the basis α, β was positively oriented, hence that $\pi(\alpha\overline{\beta}) > 0$. we can try each of the four solutions and see that only one solutions works, namely:

$$\begin{aligned}
c_0 &= \frac{1}{2}(2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 - \epsilon a_0) \\
c_1 &= \frac{1}{2}(a_1^2a_2 - 2a_0a_2^2 + a_0a_1a_3 - \epsilon a_1) \\
c_2 &= -\frac{1}{2}(a_1a_2^2 - 2a_1^2a_3 + a_0a_2a_3 + \epsilon a_2) \\
c_3 &= -\frac{1}{2}(2a_2^3 - 3a_1a_2a_3 + a_0a_3^2 + \epsilon a_3) \qquad (3.6)
\end{aligned}$$

where again $\epsilon \equiv D \mod 4$, with $\epsilon \in \{0, 1\}$. Now that we have c_i and a_i, we can determine appropriate α, β which yields the correct c_i and a_i under the set of equations (3.5). One can see that, since equations (3.5) implies $\frac{\alpha}{\beta} = \frac{c_0+a_0\tau}{c_1+a_1\tau} = \frac{c_1+a_1\tau}{c_2+a_2\tau} = \frac{c_2+a_2\tau}{c_3+a_3\tau}$, we have that the ratio $\alpha : \beta$ is determined. Hence α, β are determined, up to a scalar factor in K. Once α, β have been fixed, then δ is determined, and it is clear that if we scale both α and β by κ, then δ change by a factor of κ^3. If we can show that the $\mathbb{Z}$-module generated by α, β is in fact a fractional ideal of $\mathcal{O}$, then we have showed for every binary cubic form $C(x, y)$, there exists an oreitned fractional ideal and δ which maps to it, showing surjectivity. Furthermore, due to the uniqueness of the solution for the c_i, we have that the equivalence class of collinear pair (I, δ) mapping to A is unique, which, with a bit more thoughts, shows injectivity. To see that we have proved injectivity, suppose we have two collinear pairs, say (I, δ) and (I', δ'), which maps to $C(x, y)$ and $C^\gamma(x, y)$ respectively. Then we can change the basis of I' by γ^{-1} so that I' maps to $C(x, y)$. Then by the uniqueness of the equivalence class of collinear pairs which maps to $C(x, y)$, we have that (I, δ) and (I', δ') are equivalent.

To check that the $\mathbb{Z}$-module generated by α, β is a fractional ideal of $\mathcal{O}$, we need to check that it is an $\mathcal{O}$-module, so we need to show that they are closed under multiplication by τ. To this end let us fix $\alpha = (c_1 + a_1\tau)$, $\beta = (c_2 + a_2\tau)$, then $\delta = \alpha\beta$. We can use direct calculation to show that:

$$\begin{aligned}
\alpha\tau &= \frac{a_0a_3 - a_1a_2 + \epsilon}{2}\alpha + (a_1^2 - a_0a_2)\beta \\
-\beta\tau &= (a_2^2 - a_1a_3)\alpha + \frac{a_0a_3 - a_1a_2 - \epsilon}{2}\beta,
\end{aligned}$$

see the appendix for an example on how to check the first equality.

All the above work did not require I to be invertible nor our binary cubic form to be primitive, so the above map is a bijection between equivalence classes of collinear pairs (I, δ) of $\mathcal{O}$ and equivalence classes of binary cubic forms. So to finish our claim that there is a bijection between $C(\mathrm{Sym}^3\,\mathbb{Z}^2; D)$ and $C(\mathrm{Col}_1^3; \mathcal{O})$, we need to show that the pair (I, δ) map to a primitive cube when I is invertible, and that primitive cubes are mapped from a pair where the ideal is invertible. For this we consider the map $[C] \to [\imath(C)]$, and have a look at what this translate to in terms of oriented fractional ideals. Using equations (3.4) and equations (3.6), we find that in fact $c_{1,1,1} = c_0$, $c_{1,1,2} = c_{1,2,1} = c_{2,1,1} = c_1$, $c_{1,2,2} = c_{2,1,2} = c_{2,2,1} = c_2$ and $c_{2,2,2} = c_3$. Hence it is not hard to see that the map $[C] \mapsto [\imath(C)]$ correspond to the map sending the equivalence class of (I, δ) to the equivalence class of (I, I, I). Now by definition a binary cubic form $C$is primitive if and only if $\imath(C)$ is, but a cube is primitive if and only if its three ideals are invertible, hence C is primitive if and only if I is invertible. So we have proved that there is a bijection between $C(\mathrm{Sym}^3\,\mathbb{Z}^2; D)$ and $C(\mathrm{Col}_1^3; \mathcal{O})$.

This is proves the theorem as along with the bijection, we saw that $(\mathcal{O}, 1)$ maps to $C_{\mathrm{id},D}$, and that the group homomorphism $C(\mathrm{Col}_1^3; \mathcal{O}) \to C(\mathrm{Col}_{1,1,1}^3; \mathcal{O})$ correspond to the map $[C] \mapsto [\imath(C)]$. Hence the binary operation satisfying the theorem, is the one that correspond to multiplication of pairs (I,δ) under the bijection between $C(\mathrm{Col}_1^3;\mathcal{O})$ and $C(\mathrm{Sym}^3\,\mathbb{Z}^2;D)$. □

Before we move on we consider the map which sends the equivalence class of (I,δ) to the equivalence class of I in $C_3^+(\mathcal{O})$, where $C_3^+(\mathcal{O})$ denotes the subgroup of $C^+(\mathcal{O})$ whose elements have order dividing 3, i.e., the set of equivalence classes of ideals I such that $I^{3k}=\mathcal{O}$. We note that the map $C(\mathrm{Col}_1^3;\mathcal{O})\to C_3^+(\mathcal{O})$ is quite clearly surjective, but it is not injective. If (I,δ) maps to the identity in $C_3^+(\mathcal{O})$ then $I=\mathcal{O}$, but there is no condition on δ. Now two pairs (I,δ) and (I',δ') are equivalent if there exists $\kappa\in K$ such that $\kappa I'=I$ and $\kappa^3\delta'=\delta$. The only κ such that $\kappa\mathcal{O}=\mathcal{O}$ is if $\kappa\in\mathcal{O}^*$, hence the kernel has for cardinality the number of units over the number of units which are cubes. This map highlight the fact why the map $[C]\mapsto[\imath(C)]$ is not injective, and what we expect the kernel to be. In the next example we show directly that this map is not injective and show how this gives rise to different groups.

Example. Consider the set $C(\mathrm{Sym}^3\,\mathbb{Z}^2;229)$, we are going to show that the map $C(\mathrm{Sym}^3\,\mathbb{Z}^2;229)\to C((\mathbb{Z}^2)^{\otimes 3};229)$ defined by $[C]\mapsto[\imath(C)]$ is not injective. Following this we will give two different binary operations that turn $C(\mathrm{Sym}^3\,\mathbb{Z}^2;229)$ into a group satisfying the conditions of the theorem. Let (a_0,a_1,a_2,a_3) denote the binary cubic form $a_0x^3+3a_1x^2y+3a_2xy^2+y^3$, then $C(\mathrm{Sym}^3\,\mathbb{Z}^2;229)$ has 9 elements which can be represented by

$(0,1,1,58)$	$(1,2,-1,5)$	$(1,-2,-1,-5)$
$(1,0,1,15)$	$(1,0,3,-11)$	$(-2,1,1,6)$
$(1,0,1,-15)$	$(-2,-1,1,-6)$	$(1,0,3,11)$

which we will also refer to as $(C_{0,0},C_{0,1},C_{0,2},\dots,C_{2,2})$, e.g., $C_{0,1}=(1,0,1,15)$. The above table was found using the bijection given in the above theorem, as it was easier to find the elements of $(\mathrm{Col}_1^3;\mathbb{Z}[\frac{1+\sqrt{229}}{2}])$, but for the sake of the example, we will forget the ideals and δ associated to each binary cubic form. We will now show that $[\imath(C_{i,0})]=[\imath(C_{i,1})]=[\imath(C_{i,0})]$, it will be easier to do this if we use the bijection between $C((\mathbb{Z}^2)^{\otimes 3};D)$ and $C((I_1,I_2,I_3);\mathcal{O})$ where $\mathcal{O}$ is the oriented quadratic ring of discriminant D. Let $1,\tau$ be a positively oriented basis of $\mathcal{O}$ with $\tau^2=\tau+57$.

For $C_{0,0}$ we have that $\imath(C_{0,0})=(0,1,1,1,1,1,1,58)$, if we use equation (3.4) we find that $\{c_{i,j,k}\}=(1,0,0,57,0,57,57,57)$. We let $\alpha_1=c_{1,1,1}+a_{1,1,1}\tau=1$, $\alpha_2=c_{2,1,1}+a_{2,1,1}\tau=\tau$,$\beta_1=c_{2,1,2}+a_{2,1,2}\tau=57+\tau$, $\beta_2=c_{2,2,2}+a_{2,2,2}\tau=57+58\tau$ and from them construct $I_1=[\alpha_1,\alpha_2]=[1,\tau]$, $I_2=[\beta_1,\beta_2]=[57+\tau,57+58\tau]$ and $I_3=[\beta_1^{-1},\alpha_2^{-1}]=[\frac{58-\tau}{3249},\frac{-1+\tau}{57}]$. We check that $I_1I_2I_3=\mathcal{O}$ as required, (hence $N(I_1)N(I_2)N(I_3)=1$), so $[\imath(C_{1,1})]$ correspond to the equivalence class of the collinear triple (I_1,I_2,I_3). Using the exact same process we find that a representative of the equivalence class of collinear triples that correspond to $[\imath(C_{i,j})]$:

$C_{i,j}$	(I_1,I_2,I_3)	label
$(0,1,1,58)$	$\big([1,\tau],[57+\tau,57+58\tau].\,\big[\frac{58-\tau}{3249},\frac{-1+\tau}{57}\big]\big)$	(I_1,I_2,I_3)
$(1,0,1,15)$	$([7+\tau,-1],[-8+\tau,-121+15\tau],[7+\tau,-1])$	(I_1',I_2',I_3')
$(1,0,1,-15)$	$([-8+\tau,-1],[7+\tau,-106+15\tau],[-8+\tau,-1])$	(I_1'',I_2'',I_3'')
$(1,2,-1,5)$	$\big([13+\tau,1+2\tau],[22-\tau,-29+5\tau],\big[\frac{21+\tau}{405},\frac{-3+2\tau}{225}\big]\big)$	(J_1,J_2,J_3)
$(1,0,3,-11)$	$\big([-6+\tau,-9],[15+3\tau,-82-11\tau],\big[\frac{-6+\tau}{81},\frac{-1}{9}\big]\big)$	(J_1',J_2',J_3')
$(-2,-1,1,-6)$	$\big([-15-2\tau,-3-\tau],[-12+\tau,47-6\tau],\big[\frac{-11-\tau}{75},\frac{4-\tau}{45}\big]\big)$	(J_1'',J_2'',J_3'')
$(1,-2,-1,-5)$	$\big([-14+\tau,3-2\tau],[-21-\tau,-24-5\tau],\big[\frac{-22+\tau}{405},\frac{-1-2\tau}{225}\big]\big)$	(K_1,K_2,K_3)
$(-2,1,1,6)$	$\big([17-2\tau,-4+\tau],[11+\tau,41+6\tau],\big[\frac{12-\tau}{75},\frac{3+\tau}{45}\big]\big)$	(K_1',K_2',K_3')
$(1,0,3,-11)$	$\big([5+\tau,-9],[-18+3\tau,-93+11\tau],\big[\frac{5+\tau}{81},\frac{-1}{9}\big]\big)$	(K_1'',K_2'',K_3'')

We can now verify that in fact $I_1=I_1'=I_1''=\mathcal{O}$; $\frac{1}{57+\tau}I_2=I_2'=I_2''=\mathcal{O}$; $(57+\tau)I_3=I_3'=I_3''=\mathcal{O}$. Hence $[\imath(C_{0,0})]=[\imath(C_{0,1})]=[\imath(C_{0,2})]$ as required. We also check that $\frac{3-\tau}{25}J_1=J_1'=J_1''$; $J_2=J_2'=\frac{73-7\tau}{25}J_2''$; $J_3=\frac{-3+2\tau}{25}J_3'=\frac{24+5\tau}{81}J_3''$, implying that $[\imath(C_{1,0})]=[\imath(C_{1,1})]=[\imath(C_{1,2})]$. Finally $\frac{1+2\tau}{25}K_1=K_1'=K_1''$; $K_2=\frac{66+7\tau}{25}K_2'=K_2''$; $K_3=\frac{-29+5\tau}{81}K_3'=\frac{1+\tau}{25}K_3''$, implying that $[\imath(C_{2,0})]=[\imath(C_{2,1})]=[\imath(C_{2,2})]$.

So we have showed that the map sending $[C]$ to $[\imath(C)]$ is not always injective. We can now construct a binary operation such that $C(\mathrm{Sym}^3\,\mathbb{Z}^2;229)\cong C_9$ and the map becomes a group homomorphism. Define the map $\phi:C(\mathrm{Sym}^3\,\mathbb{Z}^2;229)\to\mathbb{Z}/9\mathbb{Z}$ by $[C_{i,j}]\mapsto i+3j$, this is clearly a bijection and it gives rise to a unique binary operation, which we will denote $+_9$. We now see easily that $[C] \mapsto [\imath(C)]$ is a group homomorphism

On the other had we can construct a second binary operation such that $C(\operatorname{Sym}^3 \mathbb{Z}^2; 229) \cong C_3 \times C_3$ and the map f is still a group homomorphism. Define the map $\psi : C(\operatorname{Sym}^3 \mathbb{Z}^2; 229) \to \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ by $[C_{i,j}] \mapsto (i, j)$. It is easy to see that the map defined by $[C] \mapsto [\imath(C)]$ is still a group homomorphism

While the example above shows that we do not have a unique binary operation, the proof of the previous theorem gave a natural binary operation to use, which we will call the composition, that is the one that under the bijection correspond to $(I, \delta) \cdot (I', \delta') = (II', \delta\delta')$. Let us calculate the composition of two binary cubic forms. Let $C(x, y) = a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3$ and $C'(x, y) = b_0x^3 + 3b_1x^2y + 3b_2xy^2 + b_3y^3$ be two binary cubic forms of discriminant $D = a_0^2a_3^2 - 3a_1^2a_2^2 - 6a_0a_1a_2a_3 + 4(a_0a_2^3 + a_1^3a_3)$. Let $\mathcal{O} = [1, \tau]$ such that $\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$, where $\epsilon \in \{0, 1\}$, $\epsilon \equiv D \mod 4$. Defining c_i as in theorem for $C(x, y)$ and d_i for $C'(x, y)$, we let $I = [c_1 + a_1\tau, c_2 + a_2\tau] = [\alpha, \beta]$ and $I' = [d_1 + b_1\tau, d_2 + b_2\tau] = [\alpha', \beta']$. Then $\delta = \alpha\beta, \delta' = \alpha'\beta'$.We now need to calculate $(II', \delta\delta')$. Now $\delta\delta'$ is clear to calculate, but II' is slightly harder. We will use binary quadratic composition, but we need to be careful that we do end up with II' and not an ideal equivalent to it, otherwise our $\delta\delta'$ would also need to change. Recall from section 2 that a binary quadratic form attached to $I = [\alpha, \beta] = \alpha[1, \frac{\beta}{\alpha}]$ is $\frac{N(\alpha x + \beta y)}{N(I)}$. If we let the binary quadratic forms corresponding to $[1, \frac{\beta}{\alpha}], [1, \frac{\beta'}{\alpha'}]$ to be f, f' respectively we have

$$\begin{aligned} f &= \frac{N(\alpha)x^2 + \operatorname{Tr}(\alpha\overline{\beta})xy + N(\beta)y^2}{N(I)}, \\ f' &= \frac{N(\alpha')x^2 + \operatorname{Tr}(\alpha'\overline{\beta}')xy + N(\beta')y^2}{N(I')}. \end{aligned}$$

Calculating their composition and recalling that to the ideal attached to the binary quadratic form (a, b, c) is $[a, \frac{-b+\sqrt{D}}{2}]$, we find that

$$\left[1, \frac{\beta}{\alpha}\right] \left[1, \frac{\beta'}{\alpha'}\right] = \frac{N(I)N(I')e^2}{N(\alpha\alpha')} \left[\frac{N(\alpha\alpha')}{N(I)N(I')e^2}, \frac{-B + \sqrt{D}}{2}\right]$$

with $B = \frac{1}{eN(I)N(I')}(n_1N(\alpha)\operatorname{Tr}(\alpha'\overline{\beta}') + n_2N(\alpha')\operatorname{Tr}(\alpha\overline{\beta}) + n_3\frac{\operatorname{Tr}(\alpha\overline{\beta})\operatorname{Tr}(\alpha'\overline{\beta}') + N(I)N(I')D}{2}) \mod \frac{2N(\alpha\alpha')}{e^2N(I)N(I')}$, where $e = \gcd(\frac{N(\alpha)}{N(I)}, \frac{N(\alpha')}{N(I)'}, \frac{N(I')\operatorname{Tr}(\alpha\overline{\beta}) + N(I)\operatorname{Tr}(\alpha'\overline{\beta}')}{2N(I)N(I')})$ and n_1, n_2, n_3 are such that $n_1\frac{N(\alpha)}{N(I)} + n_2\frac{N(\alpha')}{N(I')} + n_3\frac{N(I')\operatorname{Tr}(\alpha\overline{\beta}) + N(I)\operatorname{Tr}(\alpha'\overline{\beta}')}{2N(I)N(I')} = e$. Then because of the factor of α and α' we left out, we have

$$II = \frac{\alpha\alpha'}{e}\frac{N(I)N(I')e^2}{N(\alpha\alpha')} \left[\frac{N(\alpha\alpha')}{N(I)N(I')e^2}, \frac{-B + \sqrt{D}}{2}\right]$$

Recalling that $\sqrt{D} = 2\tau - \epsilon$, we have the following set of formulas (from rearranging equations(3.5)):

$$\begin{aligned} \widetilde{c_0} + \widetilde{a_0}\tau &= \frac{(\alpha\alpha')^2}{\beta\beta'e^3} \\ \widetilde{c_1} + \widetilde{a_1}\tau &= \frac{(\alpha\alpha')^2}{\beta\beta'e} \cdot \frac{N(I)N(I')}{N(\alpha\alpha')} \cdot \left(\frac{-B - \epsilon}{2} + \tau\right) \\ \widetilde{c_2} + \widetilde{a_2}\tau &= \frac{(\alpha\alpha')^2}{\beta\beta'}\frac{N(I)^2N(I')^2e}{N(\alpha\alpha')^2} \cdot \left(\frac{-B - \epsilon}{2} + \tau\right)^2 \\ \widetilde{c_3} + \widetilde{a_3}\tau &= \frac{(\alpha\alpha')^2}{\beta\beta'} \cdot \frac{N(I)^3N(I')^3e^3}{N(\alpha\alpha')^3}\left(\frac{-B - \epsilon}{2} + \tau\right)^3 \end{aligned}$$

Hence our the composition of $C(x, y)$ and $C'(x, y)$ will be $\widetilde{C}(x, y) = \widetilde{a_0}x^3 + 3\widetilde{a_1}x^2y + 3\widetilde{a_2}xy^2 + \widetilde{a_3}y^3$.

Example. Let us compose the two binary cubic forms $C(x, y) = x^3 + 6x^2y - 3xy^2 + 5y^3$ and $C'(x, y) = -2x^3 + 3x^2y + 3xy^2 + 6y^3$, notice that this is $C_{1,0}$ and $C_{2,1}$ of the previous example, so we have $D = 229$ and $\epsilon = 1$, hence $\tau^2 = \tau + 57$. First we calculate the corresponding c_1, c_2, c_1', c_2'. Using (3.6) we find that $c_1 = 1$, $c_2 = 22$, $c_1' = -4$ and $c_2' = 11$, giving us the ideals $I = [\alpha, \beta] = [1 + 2\tau, 22 - \tau]$ and

$I' = [\alpha', \beta'] = [-4+\tau, 11+\tau]$. We can now calculate $N(I) = 45$, $N(I') = 15$, $N(\alpha) = -225$, $N(\alpha') = -45$, $\mathrm{Tr}(\alpha\overline{\beta}) = 315$ and $\mathrm{Tr}(\alpha'\overline{\beta'}) = -195$. So we set $e = \gcd(-5, -3, -3) = 1$ and it follows that we can pick $n_1 = 1, n_2 = -2, n_3 = 0$ giving $B = 107 \mod 30 = 17$. Putting this together we have

$$\begin{aligned}
\widetilde{c_0} + \widetilde{a_0}\tau &= 107 - 11\tau \\
\widetilde{c_1} + \widetilde{a_1}\tau &= (107 - 11\tau) \cdot \frac{1}{15} \cdot (-9 + \tau) \\
\widetilde{c_2} + \widetilde{a_2}\tau &= (107 - 11\tau) \cdot \frac{1}{225} \cdot (138 - 17\tau) \\
\widetilde{c_3} + \widetilde{a_3}\tau &= (107 - 11\tau) \cdot \frac{1}{3375} \cdot (-2211 + 274\tau)
\end{aligned}$$

meaning that $\widetilde{a_0} = -11$, $\widetilde{a_1} = 13$, $\widetilde{a_2} = -14$ and $\widetilde{a_3} = 15$. So $[x^3 + 6x^2y - 3xy^2 + 5y^3] + [-2x^3 + 3x^2y + 3xy^2 + 6y^3] = [-11x^3 + 39x^2y - 42xy^2 + 15y^3] = [C''(x, y)]$. Now if we apply the element

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

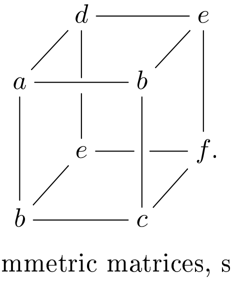
to $C''(x, y)$, we find that $C''(x, x+y) = x^3 + 3xy^2 + 15y^3 = C_{0,1}$ in our example, leading to think that $C(\mathrm{Sym}^3 \mathbb{Z}^2; 229) \cong C_3 \times C_3$. We can in fact check that this is the case.

Theorem 3.16. *The inverse of the equivalence class containing the primitive binary cube $C(x, y) = (a, b, c, d) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ is the equivalence class containing the primitive binary cube $-C(x, y) = (a, -b, c, -d) = ax^3 - 3bx^2y + 3cxy^2 - dy^3$.*

Proof. Let us calculate the pairs (I, δ) associated to each of the two cubes. For this end we use equations (3.6), and where $a_0 = a, a_1 = b, a_2 = c$ and $a_3 = d$. Notice that $c_0' = \frac{1}{2}(-2b^3 + 3abc - a^2d - \epsilon a) = -c_0 - a\epsilon$. Similarly we find $c_1' = c_1 + \epsilon b, c_2' = -c_2 - \epsilon c$ and $c_3' = c_3 + \epsilon d$. If we let $I = [\alpha, \beta] = [c_0 + a\tau, c_1 + b\tau]$, then $I' = [-c_0 - (\epsilon - \tau)a, c_1 + (\epsilon - \tau)b] = [-\overline{\alpha}, \overline{\beta}]$. This means that $\delta = \alpha^2$ and $\delta'^2 = \overline{\alpha}^2$. Now we recall from Theorem 2.15 that the inverse to $I = [\alpha, \beta]$ is $\frac{a}{N(\alpha)}\overline{I}$, and furthermore we have since seen that $a = \frac{N(\alpha)}{N(I)}$. In our case, making sure we orient $\overline{I}$ positively to keep with in line with I, we have the inverse of I is $\frac{1}{N(\alpha)}[-\overline{\alpha}, \overline{\beta}]$. So we calculate that $II' = N(I)II^{-1} = N(I)\mathcal{O}$. Now $N(I)^3 = N(\delta)$, but $N(\delta) = N(\alpha)^2 = \delta\delta'$, so the pair $(1, \mathcal{O})$ is equivalent to the pair $(\delta\delta', II')$, meaning that our cubes are inverses of each other. □

3.5 Pairs of binary quadratic forms

We now have a quick look at pairs of binary quadratic forms. The idea is that for binary cubic forms we looked at triply symmetric cube and found a subgroup of Γ which act on this triply symmetric cubes and preserved the triple symmetry. In this case we will look at double symmetry, that is a cube that when looking at two of the binary quadratic forms associated to them, they are the same. Such cubes take the form



This cube can be sliced into two 2×2 symmetric matrices, so they can be viewed as a pair of binary quadratic forms $(ax^2 + 2bxy + cy^2, dx^2 + 2exy + fy^2)$ (as opposed to looking at the normal binary quadratic forms associated to such a cube). Let us denote the space of pairs of binary quadratic forms with an even middle coefficients by $\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2$ (Here $\mathbb{Z}^2$ denotes the fact that we are using pairs and $\mathrm{Sym}^2 \mathbb{Z}^2$ the fact that we are using binary quadratic forms with even middle coefficient as appose to $(\mathrm{Sym}^2 \mathbb{Z}^2)^*$ which allowed odd middle coefficients). Then we have the natural inclusion map $\jmath$:

$\mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2 \to (\mathbb{Z}^2)^{\otimes 3}$. We can equip this set with an $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-action by $(f(x,y), g(x,y))^\gamma = (rf^{\gamma_2}(x,y) + tg^{\gamma_2}(x,y), sf^{\gamma_2}(x,y) + ug^{\gamma_2}(x,y))$ where

$$\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \times \gamma_2 \in \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$$

and $f^{\gamma_2}(x,y)$ denotes the usual $\mathrm{SL}_2(\mathbb{Z})$-action on binary quadratic forms. Note that under the inclusion map $\jmath$, the group action is transformed by the map $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \to \Gamma$ defined by $(\gamma_1, \gamma_2) \mapsto (\gamma_1, \gamma_2, \gamma_2)$. If both $f(x,y)$ and $g(x,y)$ are primitive (under the normal definition of primitive for binary quadratic form) then we can see that $\jmath(f(x,y), g(x,y))$ is a primitive cube.

Definition 3.17. We define the *discriminant* of $((a,2b,c),(d,2e,f))$ to be $D = c^2d^2 + a^2f^2 - 2afcd - 4(aebf + bdce - ace^2 - b^2fd)$. This is in fact the discriminant of the cube $\jmath(f(x,y), g(x,y))$

If we denote the $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-equivalence classes of $P \in \mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2$ by $[P]$, and the set of equivalence class of pairs of primitive binary quadratic forms by $C(\mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2; D)$ we have the following theorem.

Theorem 3.18 (Composition of pairs of binary quadratic forms)**.** *Let $D \equiv 0, 1 \mod 4$ and let*

$$P_{\mathrm{id},D} = \begin{cases} (2xy, x^2 + \frac{D}{4}y^2) & D \equiv 0 \mod 4 \\ (2xy + y^2, x^2 + 2xy + \frac{D+3}{4}y^2) & D \equiv 1 \mod 4 \end{cases}$$

Then there exists a unique binary operation to turn $C(\mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2; D)$ into an an additive group with:

1. *$[P_{\mathrm{id},D}]$ is the identity,*
2. *the map given by $[P] \mapsto [\jmath(P)]$ is a group homomorphism from $C(\mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2; D)$ to $C((\mathbb{Z}^2)^{\otimes 3}; D)$*

Proof. For this proof we use $\mathrm{Col}^3_{1,1}$ to denotes the set of triple collinear invertible oriented fractional ideals (I_1, I_2, I_2), that is, we use Col^3 to denote the fact we need three ideals to be collinear, while $1,1$ stands for the fact only at most two of them are different. Let $C(\mathrm{Col}^3_{1,1}; \mathcal{O})$ be the group of equivalence classes of $\mathrm{Col}^3_{1,1}$, we claim that there is a bijection between $C(\mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2; D)$ and $C(\mathrm{Col}^3_{1,1}; \mathcal{O})$ where $\mathcal{O}$ is the oriented ring of discriminant D. The proof of this claim is the same as the previous two proofs and so we only give a sketch of it in the appendix.

With this bijection in mind, we can define another bijection, this time between $C(\mathrm{Col}^3_{1,1}; \mathcal{O}) \to C^+(\mathcal{O})$, by sending the equivalence class of (I_1, I_2, I_2) to the equivalence class of I_2. This is clearly bijective as the inverse defined by the equivalence class of I maps to the equivalence class of $((I^2)^{-1}, I, I)$, is well defined. Translating this back into forms we have a group isomorphism between $C(\mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2; D) \to C((\operatorname{Sym}^2 \mathbb{Z}^2)^*; D)$ defined by $[P] \mapsto [Q_2^{\jmath(P)}]$. This group isomorphism is enough to prove the theorem, as $[P_{\mathrm{id},D}]$ is clearly isomorphic to $[Q_{\mathrm{id},D}]$, furthermore the isomorphism $[P] \mapsto [Q_2^{\jmath(P)}]$ is the composition of $[P] \mapsto [\jmath(P)]$ and $[A] \mapsto [Q_2^A]$. Since we know the second of these two map is a group homomorphism and that the composition is an isomorphism, we have that the first of these two maps needs to be an injective group homomorphism, proving part 2. Hence the unique binary operation is the one corresponding to the unique binary operation on $C((\operatorname{Sym}^2 \mathbb{Z}^2)^*; D)$. □

We can use the group isomorphism to compose two pairs of primitive binary quadratic forms. Before we do that it would be useful to see the inverse of $[P] \mapsto [Q_3^{\jmath(P)}]$. If we start with a primitive binary quadratic form (a,b,c) then we need to find a cube such that $Q_2 = Q_3 = (a,b,c)$. If we use Theorem 3.7, we can see that we let $e = \gcd(a,b)$ and$f = g$ be such that $h = \frac{-fb-ec}{a} \in \mathbb{Z}$. This leads to the inverse being defined as $(a,b,c) \mapsto ((0, \frac{2a}{e}, \frac{b}{e}), (e, 2f, \frac{fb-ec}{a}))$.

Let $P = ((a,2b,c),(d,2e,f))$ and $P' = ((a',2b',c'),(d',2e',f'))$ be two pairs of primitive binary quadratic forms. Then we calculate that

$$\begin{aligned} Q_3^{\jmath(P)} &= (db - ae)x^2 + (af - dc)xy + (ec - bf)y^2 \\ Q_3^{\jmath(P')} &= (d'b' - a'e')x^2 + (a'f' - d'c')xy + (e'c' - b'f')y^2 \end{aligned}$$

Then we let $E = \gcd(db - ae, d'b' - a'e', \frac{1}{2}(af + a'f' - dc - d'c'))$, n_1, n_2, n_3 be such that $n_1(db - ae) + n_2(d'b' - a'e') + \frac{n_3}{2}(af + a'f' - dc - d'c') = e$ and set $B = \frac{1}{E}(n_1(db - ae)(a'f' - d'c') + n_2(d'b' - a'e')(af - dc) + \frac{n_3}{2}((af - dc)(a'f' - d'c') + D))$, then

$$Q_3^{\jmath(P)} + Q_3^{\jmath(P')} \quad = \quad \frac{(db - ae)(d'b' - a'e')}{E^2} x^2 + Bxy + \frac{E^2(B^2 - D)}{4(db - ae)(d'b' - a'e')} y^3.$$

Unfortunately, this does not simplify much more.

Example. Let us compose $P = ((-5, 2{\cdot}2, -3), (0, 2{\cdot}1, -3))$ and $P' = ((-11, 2{\cdot}12, -13), (0, 2{\cdot}7, -17))$, that is $P = (-5x^2 + 4xy - 3y^2, 2xy - 3y^2)$ and $P' = (-11x^2 + 24xy - 13y^2, 14xy - 17y^2)$. We can calculate that the discriminant $D = 165$. We have

$$\begin{aligned} Q_3^{\jmath(P)} &= 5x^2 + -15xy + 3y^2, \\ Q_3^{\jmath(P')} &= 77x^2 + 187xy + 113y^2. \end{aligned}$$

Then we see that $\gcd(5, 77, 86) = 1$ and that we can let $n_1 = 31, n_2 = -2, n_3 = 0$. So we set $B = 31 \cdot 5 \cdot 187 - 2 \cdot 77 \cdot -15 \mod 2 \cdot 5 \cdot 77 = 495$. Hence we have

$$Q_3^{\jmath(P)} + Q_3^{\jmath(P')} = 385x^2 + 495xy + 159y^2.$$

From here we let $e = \gcd(385, 495) = 55$, and we need to find f such that $h = \frac{-495f - 8745}{385}$ is integral. One can check that we can let $f = 1$. Hence $[P] + [P'] = [((0, 14, 9), (55, 2, -24))]$. Writing out in full:

$$[(-5x^2 + 4xy - 3y^2, 2xy - 3y^2)] + [(-11x^2 + 24xy - 13y^2, 14xy - 17y^2)] = [(14xy + 9y^2, 55x^2 + 2xy - 24y^2)]$$

Theorem 3.19. *The inverse of the* $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$*-equivalence class containing* $P = ((a, 2b, c), (d, 2e, f)) \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2$ *is the* $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$*-equivalence class containing* $-P = ((a, -2b, c), (-d, 2e, -f))$.

Proof. We use the isomorphisms between $C(\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2; D)$ and $C((\mathrm{Sym}^2 \mathbb{Z}^2)^*; D)$. We have $[P] + [-P] \mapsto [Q^P] + [Q^{-P}] = [(db - ae, af - dc, ec - bf)] + [(db - ae, -(af - dc), ec - bf)] = [Q^P] - [Q^P] = 0$, hence $[P] + [-P] = 0$. □

3.6 Pairs of quaternary alternating 2-forms

We will now look at a fourth way of constructing a form from our $2 \times 2 \times 2$ cube of integers, but to start our motivation we need to take a different look at $(\mathbb{Z}^2)^{\otimes 3}$. Recall from Linear Algebra that the dual of V, denoted $V^\vee$, is the group $\mathrm{Hom}_\mathbb{Z}(V, \mathbb{Z})$ of $\mathbb{Z}$-linear maps from V to $\mathbb{Z}$, furthermore if V is finite dimensional then there is, once we have chosen a basis of V, a natural isomorphism between V and $V^\vee$. Also recall from Rings and Modules that $\mathrm{Hom}_\mathbb{Z}(V \otimes W, C) = \mathrm{Bilin}_\mathbb{Z}(V \times W, C)$. We say a linear map ϕ is *alternating* if $\phi(v_1, \ldots, v_i, v_{i+1}, \ldots, v_n) = -\phi(v_1, \ldots, v_{i+1}, v_i, \ldots, v_n)$ for all $v_j \in V$ and any $i \in [1, n]$, or alternatively if the associated matrix M is skew-symmetric, i.e., such that $M^T = -M$. We now formally define *the wedge product*:

Definition 3.20. Let V be a $\mathbb{Z}$-module and $T(V)$ denote the tensor algebra of V, that is the set of finite sum of $v \otimes u$ with $v, u \in V$. Let $I \lhd T(V)$ be the ideal generated by all elements of the form $v \otimes v, v \in V$. Then *the wedge product* of V is $\wedge(V) = T(V)/I$. The wedge product of two elements $u, v \in V$ is $u \wedge v = u \otimes v \mod I$.

We let $\wedge^k(V)$ denote the k^{th} wedge product, which is the vector subspace of $\wedge(V)$ spanned by elements of the form $v_1 \wedge v_2 \wedge \cdots \wedge v_k$ with $v_i \in V$.

One can see that the wedge product map $V \times V \to \wedge^2 V$ is alternating, so we have $\mathrm{Hom}_\mathbb{Z}(V \wedge V, C) = \mathrm{AltBilin}_\mathbb{Z}(V \times V, C)$. This extends to $\mathrm{Hom}_\mathbb{Z}(\wedge^k V, C) =$ (alternating bilinear forms on V^k). If V is finite dimensional and we have chosen a basis for it, we can use the isomorphism between V and $V^\vee$ to define an isomorphism between $(\wedge^k V)^\vee$ and $\wedge^k(V^\vee)$.

For ease of notation, let L_i for $i \in \{1, 2, 3\}$ denote a copy of $(\mathbb{Z}^2)^\vee$, since L_i is finite dimensional we have $L_i^\vee = \mathbb{Z}^2$. With this setup we can think of $(\mathbb{Z}^2)^{\otimes 3}$ as the space of $\mathbb{Z}$-trilinear map $L_1 \times L_2 \times L_3 \to \mathbb{Z}$. Given a trilinear map $\phi : L_1 \times L_2 \times L_3 \to \mathbb{Z}$ we can construct a new trilinear map $\overline{\phi} : L_1 \times (L_2 \oplus L_3) \times (L_2 \oplus L_3) \to \mathbb{Z}$ given by $\overline{\phi}(r, (s, t), (u, v)) = \phi(r, s, v) - \phi(r, u, t)$, which is alternating in the second and third variable (i.e, $\overline{\phi}(r, (s, t), (u, v)) = -\overline{\phi}(r, (u, v), (s, t))$). Let us use Bhargava's notation

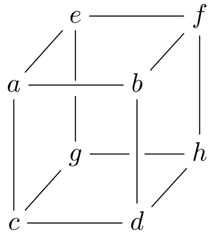
$\mathrm{id}\otimes\wedge_{2,2}$ to denote the map which takes ϕ to $\overline{\phi}$, where id represent the fact that the first variable stays fixed, while $\wedge_{2,2}$ denotes the fact we "fused" (Bhargava's terminology) together the second and third variable, so that they alternate. So we have a map $\mathrm{Trili}_{\mathbb{Z}}(L_1\times L_2\times L_3,\mathbb{Z})\to(L_1\otimes\wedge^2(L_2\times L_3))^\vee=(L_1)^\vee\otimes\mathrm{AltBilin}_{\mathbb{Z}}((L_2\times L_3)^2,\mathbb{Z})$. If we fix the basis of L_i to be the dual of the standard basis of $\mathbb{Z}^2$, then we can use the isomorphism $L_1\cong\mathbb{Z}^2$ and $L_2\times L_3\cong\mathbb{Z}^4$. This means we have a $\mathbb{Z}$-linear map $\mathrm{id}\otimes\wedge_{2,2}:(\mathbb{Z}^2)^{\otimes 3}\to\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$, which takes $2\times2\times2$ cubes of integers to pairs of alternating 2-forms. We want to see how this map acts more visually so let us denote the basis of L_i by d_1,d_2, such that $d_j(e_i)=\delta_{ij}$, where e_1,e_2 is the standard $\mathbb{Z}$-basis of $\mathbb{Z}^2$, and fix $A=(a,b,c,d,e,f,g,h)\in(\mathbb{Z}^2)^{\otimes 3}$. Let us restrict ourselves to

$$M_1=\begin{pmatrix}a&b\\c&d\end{pmatrix},$$

then $\phi\in\mathrm{Bilin}_{\mathbb{Z}}(L_2\times L_3,\mathbb{Z})$ is defined by $\phi(d_i,d_j)=a(d_i(e_1)\otimes d_j(e_2))+b(d_i(e_1)\otimes d_j(e_2))+c(d_i(e_2)\otimes d_j(e_1))+d(d_i(e_2)\otimes d_j(e_2))$, and $\overline{\phi}((s,t),(u,v))=\phi(s,v)-\phi(u,t)$. With this we can calculate that $\overline{\phi}((d_i,0),(d_j,0))=\phi(d_i,0)-\phi(d_j,0)=0$, $\phi((d_1,0),(0,d_1))=\phi(d_1,d_1)-\phi(0,0)=a-0=a$, $\phi((d_1,0),(0,d_2))=\phi(d_1,d_2)-\phi(0,0)=b$ and so on. Repeating the argument on

$$N_1=\begin{pmatrix}e&f\\g&h\end{pmatrix},$$

we get:



$$\to\left(\begin{bmatrix}0&0&a&b\\0&0&c&d\\-a&-c&0&0\\-b&-d&0&0\end{bmatrix},\begin{bmatrix}0&0&e&f\\0&0&g&h\\-e&-g&0&0\\-f&-h&0&0\end{bmatrix}\right).$$

Let $\Gamma'=\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_4(\mathbb{Z})$, then Γ' acts on $\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$ in the following way: let $(F_1,F_2)\in\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$ and

$$\gamma=\begin{pmatrix}r&s\\t&u\end{pmatrix}\times\gamma_1\in\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_4(\mathbb{Z}),$$

then $(F_1,F_2)^\gamma=(rF_1^{\gamma_1}+tF_2^{\gamma_1},sF_1^{\gamma_1}+uF_2^{\gamma_1})$, where $F_1^{\gamma_1}=\gamma_1^TF_1\gamma_1$ as usual (that is the action on a binary quadratic form Q was $\gamma^TS\gamma$ where S is the associated matrix to Q). We denote the Γ'-equivalence class of (F_1,F_2) by $[(F_1,F_2)]$. Back to the map $\mathrm{id}\otimes\wedge_{2,2}$, we want to see how the group action on $2\times2\times2$ cubes of integers translate to the group action on $\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$. To this end we consider first how $\gamma_1\times\mathrm{id}\times\mathrm{id}\in\Gamma$ acts on $A=(a,b,c,d,e,f,g,h)$, it is quite clear that this correspond to $\gamma_1\times\mathrm{id}\in\Gamma'$ acting on $(\mathrm{id}\otimes\wedge_{2,2})(A)$. Now we look at $\mathrm{id}\times\gamma_2\times\mathrm{id}\in\Gamma$, this gives rise to

$$\left(\begin{bmatrix}0&0&ar+bt&as+bu\\0&0&cr+dt&cs+du\\-ar-bt&-cr-dt&0&0\\-as-bu&-cs-du&0&0\end{bmatrix},\begin{bmatrix}0&0&er+ft&es+fu\\0&0&gr+ht&gs+hu\\-er-ft&-gr-ht&0&0\\-es-fu&-gs-hu&0&0\end{bmatrix}\right),$$

$$\text{when }\gamma_2=\begin{pmatrix}r&s\\t&u\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}).$$

We can see that this corresponds to the action of $\mathrm{id}\times\gamma_2'\in\Gamma'$ where

$$\gamma_2'=\begin{pmatrix}\gamma_2&0\\0&\mathrm{id}\end{pmatrix}\text{ or equivalently }\begin{pmatrix}\mathrm{id}&0\\0&\gamma_2\end{pmatrix}\in\mathrm{SL}_4(\mathbb{Z}).$$

Similarly when considering how $\mathrm{id}\times\mathrm{id}\times\gamma_3\in\Gamma$ acts on A, we find that this corresponds to the action of $\mathrm{id}\times\gamma_3'\in\Gamma'$ where

$$\gamma_3'=\begin{pmatrix}\gamma_3&0\\0&\mathrm{id}\end{pmatrix}\text{ or equivalently }\begin{pmatrix}\mathrm{id}&0\\0&\gamma_3\end{pmatrix}\in\mathrm{SL}_4(\mathbb{Z}).$$

With this in mind it is not hard to see that that

$$(\mathrm{id}\otimes\wedge_{2,2})(A^{\gamma_1\times\gamma_2\times\gamma_3}) \quad = \quad ((\mathrm{id}\otimes\wedge_{2,2})(A))^{\gamma_1\times(\gamma_2\oplus\gamma_3)} \text{ where } \gamma_2\oplus\gamma_3 = \begin{pmatrix}\gamma_2 & 0\\ 0 & \gamma_3\end{pmatrix} \in \mathrm{SL}_4(\mathbb{Z}).$$

So the map $\mathrm{id}\otimes\wedge_{2,2}$ gives rise to a well defined map sending $[A]$ to $[(\mathrm{id}\otimes\wedge_{2,2})(A)]$.

Definition 3.21. We say that an element $(F_1, F_2) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ is *primitive* if it is Γ'-equivalent to $(\mathrm{id}\otimes\wedge_{2,2})(A)$ for some primitive cube A.

The determinant of a skew-symmetric matrix, M, can be calculated to be a square, so we can define a define a function $\mathrm{Pfaff}(M) = \sqrt{\det(M)}$, where the sign of the square root is taken such that $\mathrm{Pfaff}(I) = 1$, where

$$I = \begin{pmatrix} 0 & \mathrm{id}\\ -\mathrm{id} & 0\end{pmatrix}.$$

So to any pair $(F_1, F_2) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ we can associate a binary quadratic form $Q = Q^{(F_1,F_2)}$ by setting $-Q(x, y) = \mathrm{Pfaff}(F_1x - F_2y)$. If we let

$$F_1 = \begin{bmatrix} 0 & p & a & b\\ -p & 0 & c & d\\ -a & -c & 0 & q\\ -b & -d & -q & 0\end{bmatrix} \qquad F_2 = \begin{bmatrix} 0 & r & e & f\\ -r & 0 & g & h\\ -e & -g & 0 & s\\ -f & -h & -s & 0\end{bmatrix},$$

then explicit calculation shows

$$-Q(x, y) \quad = \quad (pq - ad + bc)x^2 + (ps + rq - ah - ed + cf + bg)xy + (rs - eh + gf).$$

Notice that if $(F_1, F_2) = (\mathrm{id}\otimes\wedge_{2,2})(A)$ then $-Q = Q_1^A$ (where Q_1^A is as in the subsection on page 14), since in this case we have $p = q = r = s = 0$. We set the discriminant of (F_1, F_2) to be $\mathrm{Disc}((F_1, F_2)) = \mathrm{Disc}(Q)$.

We use $C(\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4, D)$ to denote the set of Γ'-equivalence classes of primitive pairs of quaternary alternating 2-forms (M, N) with discriminant D.

Theorem 3.22 (Composition of pairs of quaternary alternating 2-forms.). *Let $D \equiv 0$ or $1 \mod 4$ and let $F_{\mathrm{id},D} = (F_1, F_2)_{\mathrm{id},D} := (\mathrm{id}\otimes\wedge_{2,2})(A_{\mathrm{id},D})$. Then there exists a unique binary operation which turns $C(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D)$ into an additive group such that:*

1. *$[(F_1, F_2)_{\mathrm{id},D}]$ is the identity,*
2. *There is a group homomorphism $C((\mathbb{Z}^2)^{\otimes 3}, D) \to C(\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4, D)$ defined by $[A] \mapsto [(\mathrm{id}\otimes\wedge_{2,2})(A)]$*
3. *There is a group homomorphism $C(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4, D) \to C((\mathrm{Sym}^2\mathbb{Z}^2)^*, D)$ defined by $[(F_1, F_2)] \mapsto [Q^{(F_1,F_2)}]$*

Proof. We know the map of 2. is well defined by our discussion before the theorem. Furthermore since an element $F \in C(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D)$ is primitive, we know that there exists a primitive cube A such that $[(\mathrm{id}\otimes\wedge_{2,2})(A)] = [F]$. Hence this map is clearly surjective. From this it follows that the map gives rise to a unique binary operation, which clearly has $[F_{\mathrm{id},D}]$ as the identity. As for the homomorphism of part 3., it is constructed by finding A such that $[(\mathrm{id}\otimes\wedge_{2,2})(A)] = [(F_1, F_2)]$ and sending $[A]$ to $[Q_1^A]$. To show that the homomorphism of part 3. is well defined, we can after long and tedious calculation of elements in $[(F_1, F_2)_{\mathrm{id},D}]$, show that the map acts trivially on the kernel of the map $[A] \mapsto [(\mathrm{id}\otimes\wedge_{2,2})(A)]$. Hence by the fundamental theorem of homomorphism of groups we have that the map $[(F_1, F_2)] \mapsto [Q^{(F_1,F_2)}]$ is well defined. □

Due to the tedious and long calculation, while the rest of the above proof seemed fairly easy, this was not a very enlightening. In fact, we can take a more interesting, if less straight-forward approach, by constructing a bijection in the same style we have been doing so far, this will also prove something stronger. But for this we need to extend some of the notions we applied to ideals into more general module of a quadratic ring. So let $\mathcal{O}$ be an oriented quadratic ring and $K = \mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Q}$.

Definition 3.23. We define a *rank n ideal* of $\mathcal{O}$ to be an $\mathcal{O}$-module of K^n having rank $2n$ as a $\mathbb{Z}$-module, hence it can be written as $[\alpha_1, \beta_1, \dots, \alpha_n, \beta_n]$, with $\alpha_i, \beta_i \in K^n$

Two rank n ideals are said to be in the same *rank n ideal class* if there exists an element $\lambda \in \mathrm{GL}_n(K)$ mapping one to the other.

This is a generalisation of fractional ideals which are rank 1 ideals by that definition and the definition of rank n ideal class is compatible with fractional ideal class since $\mathrm{GL}_1(K) \cong K^*$. With rank n ideals also comes the idea of oriented rank n ideals, like in the case of fractional ideals. Recall that $I = [\alpha, \beta]$ is positively oriented if $\frac{\overline{\alpha}\beta - \alpha\overline{\beta}}{\sqrt{D}} > 0$, which is equivalent to the determinant of the matrix transforming $[1, \tau]$ to $[\alpha, \beta]$ being positive. So in the same spirit we define:

Definition 3.24. The basis of a rank n ideal $M = [\alpha_1, \beta_1, \dots, \alpha_n, \beta_n]$ is *positively oriented* (respectively *negatively* oriented*) if* the matrix transforming

$$[(1, 0, \dots, 0), (\tau, 0, \dots, 0), (0, 1, \dots, 0), (0, \tau, \dots, 0), \dots (0, 0, \dots 1), (0, 0, \dots, \tau)]$$

to M has positive determinant (respectively negative determinant).

As usual the norm of an oriented rank n ideal M is defined to be the index of M in $\mathcal{O}^n$, to be more precise $N(M) = |L/M| \cdot |L/\mathcal{O}|^{-1}$ where L is any lattice in K^n which contains both $\mathcal{O}^n$ and M.

Let $\mathrm{Det}(M)$ denote the ideal in $\mathcal{O}$ generated by all elements of the form $\det(x_1, \dots, x_n)$ where $x_i \in M \subseteq K^n$ and det is the canonical map $(K^n)^n \to K$ defined by taking the determinant.

In particular if $M \cong I_1 \oplus \cdots \oplus I_n \subseteq K^n$ for some ideals $I_1, \dots, I_n$ in $\mathcal{O}$ then $\mathrm{Det}(M) = I_1 \dots I_n$. With this we can see that we can say, in the same spirit of a triple collinear oriented fractional ideals, a k-tuple of oriented $\mathcal{O}$-ideals $M_1, \dots M_n$ of ranks $n_1, \dots, n_k$ respectively is *collinear* if $\mathrm{Det}(M_1) \dots \mathrm{Det}(M_k) \subseteq \mathcal{O}$ and $N(M_1) \dots N(M_k) = 1$. Similarly we say two such collinear k-tuples $(M_1, \dots, M_k)$ and $(M_1', \dots, M_k')$ to be equivalent if there exists elements $\lambda_1, \dots, \lambda_k$ in $\mathrm{GL}_{n_1}(K), \dots, \mathrm{GL}_{n_k}(K)$ respectively such that $M_i' = \lambda_i M_i$ for all i.

In the same spirit as before, let us use the notation $\mathrm{Col}^2_{1,2}$ to denote the set of collinear pairs (I, M), where I is an oriented rank 1 ideal and M an oriented rank 2 ideal. Then we denote the set of equivalence classes of collinear oriented invertible pairs of ideals of rank 1 and 2 respectively, (I, M), of a quadratic ring $\mathcal{O}$ by $C(\mathrm{Col}^2_{1,2}; \mathcal{O})$ and we get the following theorem.

Theorem 3.25. *There is a bijection between $C(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D)$ and $C(\mathrm{Col}^2_{1,2}; \mathcal{O})$ where $\mathcal{O}$ is the oriented quadratic ring of discriminant D.*

Proof. As usual this will follow the work of Bhargava [Bhargava(2004), p 24]. For the moment let us forget the conditions of primitive and invertible. As usual let $\mathcal{O}$ be and oritented ring and let D be its discriminant. Let $1, \tau$ be a positively oriented basis of $\mathcal{O}$ (with $\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$), and let (I, M) be such that $I\mathrm{Det}(M) \subseteq \mathcal{O}$ and $N(I)N(M) = 1$. Let α_1, α_2 be a correctly oriented basis of I and let $\beta_1, \beta_2, \beta_3, \beta_4$ be a correctly oriented basis of M. Since (I, M) are a collinear pair, we can use the fact that $I\mathrm{Det}(M) \subseteq \mathcal{O}$ to write a priori 32 equations:

$$\alpha_i \det(\beta_j, \beta_k) = c^{(i)}_{j,k} + a^{(i)}_{j,k}\tau \tag{3.7}$$

for $i \in \{1, 2\}$, $j, k \in \{1, 2, 3, 4\}$ and $c^{(i)}_{j,k}, a^{(i)}_{j,k} \in \mathbb{Z}$. Noticing that $\det(\beta_j, \beta_j) = 0 \forall j$ we have $c_{j,j} = a_{j,j} = 0$, furthermore since $\det(\beta_j, \beta_k) = -\det(\beta_k, \beta_j)$ (Linear Algebra), we have that $c^{(i)}_{j,k} = -c^{(i)}_{k,j}$ and $a^{(i)}_{j,k} = -a^{(i)}_{k,j}$ cutting the number of unknown constant down to 24. Set $F_i = \{a^{(i)}_{j,k}\}_{j,k} \in M_4(K), i \in \{1, 2\}$, by our previous two comment we have that the diagonal entries of F_i are 0 and $F_i^T = -F_i$, so they are both 2-alternating forms. Hence $F = (F_1, F_2) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ is our desired pair of quaternary alternating 2-forms.

If we choose another basis for I, M, we are applying a change of basis by an element $\gamma \in \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z}) = \Gamma'$, again the element has to be in $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$ to keep the orientation of I and M the same, and by constructions of the map we can see that this will simply change F by the same element γ. Hence our map is well defined and independent of choice of basis. Furthermore, if we take an equivalence set $(\kappa_1 I, \kappa_2 M)$, since we have that $N(\kappa_1)N(\det(\kappa_2)) = 1$, we have that they map to the same F. So our map is well defined and independent of the choice of basis.

We show that F has discriminant D, by showing that equations (3.7) implies $\text{Disc}(F) = N(I)^2N(M)^2\text{Disc}(\mathcal{O})$. First if we let $I = [1, \tau]$ and $M = [(1,0), (\tau, 0), (0,1), (0, \tau)]$, we see that $F = F_{\text{id},D}$, in which case the identity holds. Now suppose we change I to a general rank 1 ideal $[\alpha, \beta]$ by a an element

$$T = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \text{SL}_2(\mathbb{Z}),$$

this changes $F_{\text{id},D} = (F_1, F_2)$ to $(rF_1 + tF_2, sF_1 + uF_2)$, hence, once we have calculated the quadratic form associated to it, changes the discriminant by a factor of $\det(T)^2 = N(I)^2$. Similarly, if we change M to a general rank 2 ideal, then we find that the discriminant is scaled by $N(M)^2$. Hence giving the identity $\text{Disc}(F) = N(I)^2N(M)^2\text{Disc}(\mathcal{O})$. But since $N(I)N(M) = 1$, we have that $\text{Disc}(F) = \text{Disc}(\mathcal{O})$.

As usual, we want to show that under this map every equivalence classes (I, M) get map to exactly one $[F]$. For this end we fix $F = (F_1, F_2) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ with $F_i = \{a^{(i)}_{j,k}\}$ and consider the set of equations (3.7). We first need to following identity, that can easily be check through direct calculation: If v_1, v_2, v_3, v_4 are four planar coordinates then $\det(v_1, v_3) \cdot \det(v_2, v_4) = \det(v_1, v_2) \cdot \det(v_3, v_4) + \det(v_1, v_4) \cdot \det(v_2, v_3)$. We can use this identity to write

$$\alpha_i \det(\beta_k, \beta_m) \cdot \alpha_j \det(\beta_l, \beta_n) = \alpha_{i'} \det(\beta_k, \beta_l) \cdot \alpha_{j'} \det(\beta_m, \beta_n) + \alpha_{i''} \det(\beta_k, \beta_n)\alpha_{j''} \det(\beta_l, \beta_m)$$

for $u, j \in \{1, 2\}$, $k, l, m, n \in \{1, 2, 3, 4\}$ and (i', j') and (i'', j'') are any ordered pairs equal either to (i, j) or (j, i). If we expand this with all the different possible combination and equates the τ and 1 separately we gets 94 linear and quadratic equations. Bhargava states [Bhargava(2004), p 25] that these 94 equations plus the condition that $N(I)N(M) > 0$ give the following unique solution:

$$\begin{aligned} c^{(i)}_{j,k} &= (i - i')[a^{(i')}_{j,k}\text{Pfaff}(F_i) \\ &\quad -\frac{1}{2}a^{(i)}_{j,k}(\text{Pfaff}(F_1 + F_2) - \text{Pfaff}(F_1) - \text{Pfaff}(F_2))] - \frac{1}{2}a^{(i)}_{j,k}\epsilon \end{aligned} \tag{3.8}$$

where $\{i, i'\} = \{1, 2\}$, $j, k \in \{1, 2, 3, 4\}$ and $\epsilon \in \{0, 1\}$ as usual.

Once the $a^{(i)}_{j,k}$ and $c^{(i)}_{j,k}$ are know we can determine α_i and β_j. First notice that equations (3.7) implies that $\alpha_1 : \alpha_2 = (c^{(1)}_{j,k} + a^{(1)}_{j,k}\tau) : (c^{(1)}_{j,k} + a^{(2)}_{j,k}\tau)$ for $j, k \in \{1, 2, 3, 4\}$, we know the right hand side of the equation is the same for all $j, k \in \{1, 2, 3, 4\}$ due to the restrictions of equations (3.7). So α_1, α_2 are uniquely determined up to a scalar factor in K, hence we can set $\alpha_i = c^{(i)}_{1,2} + a^{(i)}_{1,2}\tau$ for $i = 1, 2$. Once we have fixed our choice of α_1, α_2, we can use equations (3.7) to determine the values of $\det(\beta_j, \beta_k)$. Hence $\beta_1, \beta_2, \beta_3, \beta_4$ are uniquely determined as elements of K^2 up to a factor of $\text{SL}_2(K)$, since $\det(\gamma \cdot (\beta_j, \beta_k)) = \det(\beta_j, \beta_k)$ for $\gamma \in \text{SL}_2(K)$. Once we have showed that these two $\mathbb{Z}$-modules are modules over $\mathcal{O}$, then we have showed that to any pair of alternating quaternary 2-forms, there exists a collinear pair (I, M) which maps to it, showing surjectivity of the map. Futhermore, due to the uniqueness of the solution (3.8), we have that the equivalence class of collinear pair (I, M) mapping to F is unique, which as before shows injectivity.

We need to check that these two $\mathbb{Z}$-modules, one with basis α_1, α_2, the other with basis $\beta_1, \beta_2, \beta_3, \beta_4$ are modules over $\mathcal{O}$. As with previous proofs we can use direct calculation to show the structure of $I = [\alpha_1, \alpha_2]$ is determined by

$$\begin{aligned} \tau\alpha_1 &= \frac{b_1 + \epsilon}{2}\alpha_1 + a_1\alpha_2 \\ -\tau\alpha_2 &= c_1\alpha_1 + \frac{b_1 - \epsilon}{2}\alpha_2 \end{aligned}$$

where $-\text{Pfaff}(F_1x - F_2y) = a_1x^2 + b_1xy + r_1y^2$. Let us use $\text{sgn}(i, j, k, l)$ to denote the sign of the permutation (i, j, k, l) of $(1, 2, 3, 4)$, for example $\text{sgn}(2, 1, 3, 4) = -1$ and $\text{sgn}(3, 2, 4, 1) = 1$. As we have fixed $\alpha_i = c^{(i)}_{1,2} + a^{(i)}_{1,2}\tau$, we can let $\beta_1 = (1, 0)$ and $\beta_2 = (0, 1)$ forcing $\beta_3 = (a_3 + b_3\tau, c_3 + d_3\tau), \beta_4 = (a_4 + b_4\tau, c_4 + d_4\tau)$ where $a_i + b_i\tau = \alpha_2^{-1}(c^{(1)}_{2,i} + a^{(1)}_{2,i}\tau)$ and $c_i + d_i\tau = \alpha_1^{-1}(c^{(1)}_{1,i} + a^{(1)}_{1,i}\tau)$. We can now check, after some long calculations that

$$\tau\beta_i = \sum_{j=1}^{4} t_{ij}\beta_j$$

where

$$t_{ij} = \begin{cases} \operatorname{sgn}(i,j,k,l)(a^{(1)}_{i,l}a^{(2)}_{i,k} - a^{(1)}_{i,k}a^{(2)}_{i,l}) & i \neq j \\ \frac{1}{2}\sum_{\substack{j,k,l \\ k<l}} \operatorname{sgn}(i,j,k,l)(a^{(1)}_{k,l}a^{(2)}_{i,j} - a^{(1)}_{i,j}a^{(2)}_{k,l}) + \frac{1}{2}\epsilon & j = i \end{cases}$$

Hence we have that M is in fact an $\mathcal{O}$-module.

We have showed that given $F \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$, we construct a, up to equivalence, unique pair of collinear ideals of rank $1, 2$ respectively, which under the map given by equations (3.7) maps to F. Let us consider now the map $\mathrm{id} \otimes \wedge_{2,2}$. Consider $A = (a,b,c,d,e,f,g,h) \in (\mathbb{Z}^2)^{\otimes 3}$, this correspond to (I_1, I_2, I_3) where $I_1 = [c_{1,1,1} + a\tau, c_{2,1,1} + e\tau]$, $I_2 = [c_{2,1,2} + f\tau, c_{2,2,2} + h\tau]$,$I_3 = [(c_{2,1,2} + f\tau)^{-1}, (c_{2,1,1} + e\tau)^{-1}]$ and $c_{i,j,k}$ is given by equation (3.3). On the other hand $(\mathrm{id} \otimes \wedge_{2,2})(A)$ correspond to (I, M) where $I = [c^{(1)}_{1,3} + a\tau, c^{(2)}_{1,3} + e\tau]$, (we can not use $c^{(i)}_{1,2} + a^{(i)}_{1,2}\tau$ as it is zero and hence not invertible in K), and $M = [(0, c^{(2)}_{1,4} + f\tau), (0, c^{(2)}_{2,4} + h\tau), ((c^{(2)}_{1,4} + f\tau)^{-1}, 0), ((c^{(2)}_{1,3} + e\tau)^{-1}, 0)]$, (we use a slightly different basis for M than expected for ease of calculation, one can easily check that (I, M) is a collinear pair giving $(\mathrm{id} \otimes \wedge_{2,2})(A)$). Notice that $M = I_2 \oplus I_3$ meaning that the map $(\mathrm{id} \otimes \wedge_{2,2})$ correspond to the map which sends $((I_1, I_2, I_3), \mathcal{O})$ to $((I_1, I_2 \oplus I_3), \mathcal{O})$. Furthermore a theorem by Bass [Bass(1962), Thm 1.7] states: Let R be a Noetherian integral domain, then every torsion free R-module is a direct sum of modules of rank one if and only if all finitely generated ideals of R have at most two generators. In our case, $\mathcal{O}$ is a Noetherian ring with all fractional ideal having rank two, hence any torsion free $\mathcal{O}$-module M can be written as the direct sum of two fractional ideal. This means that the map sending $((I_1, I_2, I_3, \mathcal{O})$ to $((I_1, I_2 \oplus I_3), \mathcal{O})$ is surjective, i.e., $\mathrm{id} \otimes \wedge_{2,2}$ is a surjective group map.

None of the above required primitivity or invertibility, so to complete our proof, we need to show that invertible ideals give rise to primitive pairs of quaternary alternating 2-forms. To do this we use the above map $\mathrm{id} \otimes \wedge_{2,2}$. Since a primitive pair of quaternary alternating 2-forms comes from a primitive cube, and that a primitive cube is in bijection with invertible oriented fractional ideals we have that $(I_1, I_2 \oplus I_3)$ have to be invertible. On the other hand since invertible ideals are only equivalent to invertible ideal, an either I or M is not invertible, then they can not give rise to a primitive pair of quaternary alternating 2-forms. Hence here completes the proof that there is an isomorphism between the group $C(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D)$ and $C(\mathrm{Col}^2_{1,2}; \mathcal{O})$.

To finish proving Theorem (3.22) we finally, show that $[(F_1, F_2)] \to [Q^{(F_1,F_2)}]$ is a group homomorphism. $(F_1, F_2) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ correspond to pairs $((I, M), \mathcal{O})$ with (I, M) being a collinear pair, in particular $I\mathrm{Det}(M) = \mathcal{O}$. Serre's cancellation theorem [Serre(1957), Prop 7] states that a module of rank k over a dimension 1 ring $\mathcal{O}$ is uniquely determined by its determinant. In our case since from the previous paragraph we know $M = I_2 \oplus I_3$ and using the fact that $I\mathrm{Det}M = II_2I_3 = \mathcal{O}$, we have that any pair $((I, M), \mathcal{O})$ is in fact of the form $((I, I^{-1} \oplus \mathcal{O}), \mathcal{O})$. Hence we have a bijection sending $((I, M), \mathcal{O})$ to $(I, \mathcal{O})$, which correspond to the bijection $C(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4, D) \to C((\mathrm{Sym}^2 \mathbb{Z}^2)^*, D)$ which is defined by $[(F_1, F_2)] \to [Q^{(F_1,F_2)}]$ □

Corollary 3.26. *Every element in* $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ *is* Γ'*-equivalent to* $(\mathrm{id} \otimes \wedge_{2,2})(A)$ *for some cube* $A \in (\mathbb{Z}^2)^{\otimes 3}$.

Corollary 3.27. *There is an isomorphism of groups* $C(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4) \to C((\mathrm{Sym}^2 \mathbb{Z}^2)^*, D)$ *defined by* $[(F_1, F_2)] \mapsto [Q^{(F_1,F_2)}]$.

The second corollary is the most surprising one of the two, although the first one is quite important in its own right. The advantage of having gone through all this work to show the isomorphism is that along the way we saw the inverse of the map defined by $[(F_1, F_2)] \mapsto [Q^{(F_1,F_2)}]$. It is the map correspond to $I \mapsto (I, I^{-1} \oplus \mathcal{O})$. Using the bijection between binary quadratic forms and fractional oriented ideals, if we let $\mathcal{O} = [1, \tau]$ we have $I = [a, \frac{-b-\epsilon}{2} + \tau]$ and hence $I^{-1} = \frac{1}{a}[a, \frac{-b-\epsilon}{2} + \overline{\tau}]$. With some direct calculations we see that this gives the map

$$(a,b,c) \mapsto \left(\begin{bmatrix} 0 & 0 & 0 & a \\ 0 & 0 & -1 & -\frac{\epsilon+b}{2} \\ 0 & 1 & 0 & 0 \\ -a & \frac{\epsilon+b}{2} & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & \frac{\epsilon-b}{2} \\ 0 & 0 & 0 & c \\ -1 & 0 & 0 & 0 \\ \frac{-\epsilon+b}{2} & -c & 0 & 0 \end{bmatrix} \right)$$

where $\epsilon \in \{0, 1\}$ and $\epsilon \equiv b^2 \mod 4$ as usual (since $D = b^2 - 4ac$). The entry c was due to the calculation $(\frac{-b-\epsilon}{2})(\frac{-b-\epsilon}{2a}) + (\frac{-b-\epsilon}{2a})\epsilon - \frac{D-\epsilon}{4a} = \frac{b^2-D}{4a} = c$. We can now look at how to compose two primitive pairs of alternating quaternary alternating 2-forms. Let F and F' be two such forms of discriminant D, with associated binary quadratic forms

$$\begin{aligned} -Q^F &= (pq-ad+bc)x^2+(-ps-rq+ah+ed-cf-bg)xy+(rs-eh+gf), \\ -Q^{F'} &= (p'q'-a'd'+b'c')x^2+(-p's'-r'q'+a'h'+e'd'-c'f'-b'g')xy+(r's'-e'h'+g'f'). \end{aligned}$$

Then we set $E = \gcd(pq-ad+bc, p'q'-a'd'+b'c', \frac{1}{2}(-ps-p's'-rq-r'q'+ah+a'h'-c'f'-bg-b'g'))$ and we let n_1, n_2, n_3 be as usual. Then the composition of F and F' is

$$\left(\begin{bmatrix} 0 & 0 & 0 & A \\ 0 & 0 & -1 & -\frac{\epsilon+B}{2} \\ 0 & 1 & 0 & 0 \\ -A & \frac{\epsilon+B}{2} & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 & \frac{\epsilon-B}{2} \\ 0 & 0 & 0 & C \\ -1 & 0 & 0 & 0 \\ \frac{-\epsilon+B}{2} & -C & 0 & 0 \end{bmatrix}\right),$$

where

$$\begin{aligned} A &= \frac{(pq-ad+bc)(p'q'-a'd'+b'c')}{E^2} \\ B &= \frac{n_1}{E}(pq-ad+bc)(-p's'-r'q'+a'h'+e'd'-c'f'-b'g') \\ &\quad +\frac{n_2}{E}(p'q'-a'd'+b'c')(-ps-rq+ah+ed-cf-bg) \\ &\quad +\frac{n_3}{2E}((-ps-rq+ah+ed-cf-bg)(-p's'-r'q'+a'h'+e'd'-c'f'-b'g')-D) \\ C &= \frac{E^2(B^2-D)}{4(pq-ad+bc)(p'q'-a'd'+b'c')} \end{aligned}$$

Again, unfortunately not much cancellation or simplification seems possible, but we show in the next example that the calculations are not hard.

Example. Let us compose the folloiwng two pairs of quaternary alternating 2-forms, F and F', which gives rise to the binary quadratic forms

$$-Q^F = (10{\cdot}0-(-5){\cdot}9+7{\cdot}(-3))x^2+(-10{\cdot}1-4{\cdot}0+(-5){\cdot}(-5)+(-4){\cdot}9-(-3){\cdot}8-7{\cdot}0)xy+(4{\cdot}1-(-4){\cdot}(-5)+0{\cdot}8)y^2 = 24x^2+3xy$$

$$-Q^{F'} = (3{\cdot}1-0{\cdot}0+0{\cdot}0)x^2+(-3{\cdot}(-5)-0{\cdot}1+0{\cdot}11+(-5){\cdot}0-0{\cdot}11-0{\cdot}(-5))xy+(0{\cdot}(-5)-(-5){\cdot}11+(-5){\cdot}11)y^2 = 3x^2+15xy-11$$

We calculate the discriminant $D = 1545$, hence $\epsilon = 1$, and $E = \gcd(24, 3, 9) = 3$, so we let $n_1 = n_3 = 0$ and $n_2 = 1$. Therefore we get $B = \frac{1}{3}(3 \cdot 3) = 3$, $A = 8$ and $C = \frac{9-1545}{4\cdot 8} = -48$. Hence

$$\begin{aligned} &\left[\left(\begin{bmatrix} 0 & 10 & -5 & 7 \\ -10 & 0 & -3 & 9 \\ 5 & 3 & 0 & 0 \\ -7 & -9 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 4 & -4 & 8 \\ -4 & 0 & 0 & -5 \\ 4 & 0 & 0 & 1 \\ -8 & -5 & -1 & 0 \end{bmatrix}\right)\right] + \left[\left(\begin{bmatrix} 0 & 3 & 0 & 0 \\ -3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -5 & 11 \\ 0 & 0 & -5 & 11 \\ 5 & 5 & 0 & -5 \\ 11 & 11 & 5 & 0 \end{bmatrix}\right)\right] \\ = &\left[\left(\begin{bmatrix} 0 & 0 & 0 & 24 \\ 0 & 0 & -1 & -2 \\ 0 & 1 & 0 & 0 \\ -24 & 2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -16 \\ -1 & 0 & 0 & 0 \\ 1 & 16 & 0 & 0 \end{bmatrix}\right)\right] + \left[\left(\begin{bmatrix} 0 & 0 & 0 & 3 \\ 0 & 0 & -1 & -8 \\ 0 & 1 & 0 & 0 \\ -3 & 8 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & -7 \\ 0 & 0 & 0 & -110 \\ -1 & 0 & 0 & 0 \\ 7 & 110 & 0 & 0 \end{bmatrix}\right)\right] \\ &= \left[\left(\begin{bmatrix} 0 & 0 & 0 & 8 \\ 0 & 0 & -1 & -2 \\ 0 & 1 & 0 & 0 \\ -8 & 2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -48 \\ -1 & 0 & 0 & 0 \\ 1 & 48 & 0 & 0 \end{bmatrix}\right)\right] \end{aligned}$$

Theorem 3.28. *The inverse of the class containing $F \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ is the class containing $-F \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$, where:*

$$F = \left(\begin{bmatrix} 0 & p & a & b \\ -p & 0 & c & d \\ -a & -c & 0 & q \\ -b & -d & -q & 0 \end{bmatrix}, \begin{bmatrix} 0 & r & e & f \\ -r & 0 & g & h \\ -e & -g & 0 & s \\ -f & -h & -s & 0 \end{bmatrix}\right), -F = \left(\begin{bmatrix} 0 & p & -a & b \\ -p & 0 & c & -d \\ a & -c & 0 & q \\ -b & d & -q & 0 \end{bmatrix}, \begin{bmatrix} 0 & -r & e & -f \\ r & 0 & -g & h \\ -e & g & 0 & -s \\ f & -h & s & 0 \end{bmatrix}\right)$$

Proof. Notice that $[Q^F] = [(pq-ad+bc)x^2+(-ps-rq+ah+ed-cf-bg)xy+(rs-eh+gf)]$ while $[Q^{-F}] = [(pq-ad+bc)x^2-(-ps-rq+ah+ed-cf-bg)xy+(rs-eh+gf),]$. So $[Q^{-F}] = -[Q^F]$, hence $[F]+[-F] = 0$. □

3.7 Diagrams

To summarise this section, we started with cubes of integers and we have constructed five different objects. Between these objects we constructed the following discriminant-preserving maps:

$$\begin{tikzcd}
 & \operatorname{Sym}^3 \mathbb{Z}^2 \arrow[d, hook, "\imath"] & \\
 & (\mathbb{Z}^2)^{\otimes 3} \arrow[dl, "\mathrm{id} \otimes \wedge_{2,2}"'] \arrow[d, two heads, "A \mapsto Q_i^A"'] & \\
\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4 \arrow[r, "(F_1,F_2) \mapsto Q^{(F_1,F_2)}"'] & (\operatorname{Sym}^2 \mathbb{Z}^2)^* & \mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2 \arrow[l, "P \mapsto Q_3^{\jmath(P)}"] \arrow[ul, hook, "\jmath"']
\end{tikzcd}$$

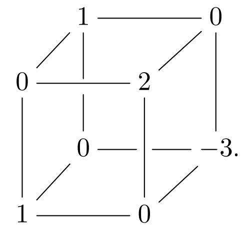
The map $\imath$ and $\jmath$ were the natural inclusion discussed in subsection 3.4 and 3.5 respectively. It also quite clear that the map sending A to Q_i^A is surjective, since we have by Theorem 3.4 we can always construct cube that will give rise to (a, b, c) and $(a, -b, c)$. This diagram in turn creates 5 groups with the following group homomorphisms:

$$\begin{tikzcd}
 & C(\operatorname{Sym}^3 \mathbb{Z}^2; D) \arrow[d, "\alpha"] & \\
 & C((\mathbb{Z}^2)^{\otimes 3}; D) \arrow[dl, two heads, "\gamma"'] \arrow[d, two heads, "\beta_i"] & \\
C(\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4; D) \arrow[r, "\cong", "\delta"'] & C((\operatorname{Sym}^2 \mathbb{Z}^2)^*; D) & C(\mathbb{Z}^2 \otimes \operatorname{Sym}^2 \mathbb{Z}^2; D) \arrow[l, "\cong"', "\epsilon"] \arrow[ul, hook, "\zeta"']
\end{tikzcd}$$

This diagram only commutes in the left triangle when taking the map β_1, while for the right triangle you need to take the map β_3. On the way we showed that:

- the map α, defined by $[C] \mapsto [\imath(C)]$ is neither injective, see the example in Section 3.4, nor surjective. In the following example, we show, using two different method, a cube which has no preimages.:

  Example. Consider the cube

  of discriminant -24. We want to show that it is not equivalent to a triply symmetric cube.

  For the first method we stay within $C((\mathbb{Z}^2)^{\otimes 3}; -24)$. Note that if $A^{\gamma_1 \times \gamma_2 \times \gamma_3} = B$ where B is a triply symmetric cube, then $B = (A^{\mathrm{id} \times \gamma_2 \gamma_1^{-1} \times \gamma_3 \gamma_1^{-1}})^{\gamma_1 \times \gamma_1 \times \gamma_1}$, so if B is triply symmetric, then so is $B^{\gamma_1^{-1} \times \gamma_1^{-1} \times \gamma_1^{-1}} = A^{\mathrm{id} \times \gamma_2 \gamma_1^{-1} \times \gamma_3 \gamma_1^{-1}}$. Hence we just need to show that A^γ is not a triply symmetric cube for any $\gamma \in \mathrm{id} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$. Suppose there exists

  $$\gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} r_2 & s_2 \\ t_2 & u_2 \end{pmatrix} \times \begin{pmatrix} r_3 & s_3 \\ t_3 & u_3 \end{pmatrix} \in \mathrm{id} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}),$$

  such that A^γ is a triply symmetric cube, then using the triple symmetry of the cube and calculating A^γ we have the following set of equality:

  $$\begin{aligned} 2u_2 r_3 + s_2 t_3 &= 2t_2 s_3 + r_2 u_3 = r_2 r_3 - 3t_2 t_3, \\ 2u_2 s_3 + s_2 u_3 &= s_2 r_3 - 3u_2 t_3 = r_2 s_3 - 3t_2 u_3. \end{aligned}$$

If we rearrange the second equality of the first line we have $r_2(u_3 - r_3) = t_2(-3t_3 - 2s_3)$, so multiplying $r_2u_2 - s_2t_2 = 1$ by $u_3 - r_3$ we have $t_2(-3t_3 - 2s_3)u_2 - t_2(u_3 - r_3)s_2 = (u_3 - r_3)$. The left hand side is $t_2((s_2r_3 - 3u_2t_3) - (2u_2s_3 + s_2u_3)) = 0$, so we must have $u_3 = r_3$ and $t_2(-3t_3 - 2s_3) = 0$. We have two cases:

Case 1. $t_2 \neq 0$: In which case $3t_3 = -2s_3$. Since we have $r_3u_3 - s_3t_3 = 1$, we need to solve $r_3^2 + \frac{2}{3}s_3^2 = 1$, which has only the solutions $r_3 = u_3 = \pm 1$ and $t_3 = s_3 = 0$. Substituting all of this back into the equations above, we find $2u_2 = r_2$ and $s_2 = -3t_2$. Again since we have $r_2u_2 - s_2t_2 = 1$ we find $2u_2^2 + 3u_2^2 = 1$, which has no solution over $\mathbb{Z}$.

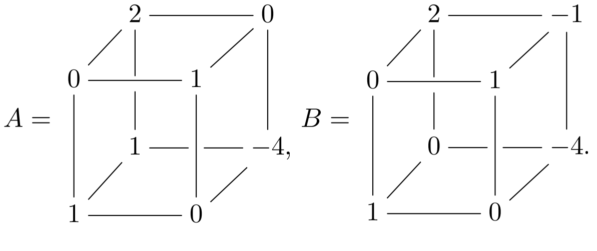
Case 2. $t_2 = 0$: In which case we have $r_2 = u_2 = \pm 1$. Looking at the second set of equality we find $2u_2s_3 + s_2r_3 = s_2r_3 - 3u_2t_3$, since $u_2 \neq 0$ this implies $s_3 = -3t_3$. Then as in the first case we find, since $r_3 = u_3$, that $r_3 = u_3 = \pm 1$ and $t_3 = s_3 = 0$, leading again to a lack of solution

We have showed that no such γ can exist, hence A is not equivalent to a triply symmetric cube, hence there is not binary cubic form C such that $[\alpha(C)] = [A]$.

For the second method we use the group isomorphism that we have constructed in this paper. We will see that this is quicker and much easier than the above method. Let us use equations (3.4) to construct the triple collinear oriented invertible fractional ideals which correspond to A. Let τ be such that $\tau^2 = -6$ (since $8 \equiv 0 \mod 4$), we calculate that $c_{1,1,1} = 2$, $c_{2,1,1} = 0$, $c_{2,1,2} = -6$, $c_{2,2,2} = 0$. Hence we have $I_1 = [2, \tau]$, $I_2 = [-6, -3\tau]$ and $I_3 = -\frac{1}{6}[1, \tau]$. Now quite clearly I_3 is equivalent to $\mathcal{O} = [1, \tau]$. On the other hand we claim that I_1 is not principal. This is due to the fact that $N(2) = 4, N(\tau) = 6$, hence any element α which would generate I_1, needs to have norm dividing 2. Since $I \neq \mathcal{O}$, we have that α is not a unit, furthermore, due to the fact that $N(a + b\tau) = a^2 + 6b^2$, we have that no element of $\mathcal{O}$ has norm 2. Hence such an α does not exist and I_1 is not principal. Since I_1 is not equivalent to I_3, we have that (I_1, I_2, I_3) can not be in the image of (I, δ) for any I or δ. This examples shows how easier it is to work using the bijection. We also have some free information, namely that Q_1^A is equivalent to Q_2^A, since $I_2 = -3I_1$, and we know that Q_3^A is equivalent to the principal binary quadratic form.

- The maps β_i, defined by $[A] \mapsto [Q_i^A]$ for $i = 1, 2, 3$ are all surjective. This is due to the fact that, for β_1, the lower right triangle commutes, and due to the isomorphism of ϵ, we have that β_1 has to be surjective. Since the three maps are the same up, up to a composition with an automorphism on $C((\mathbb{Z}^2)^{\otimes 3}; D)$. It is clearly not injective as one group is isomorphism to $C^+(\mathcal{O})^2$ while the second group is isomorphic to $C^+(\mathcal{O})$. Still we use the following example to illustrate how to argue without using the isomorphism, and to show two non-equivalent cubes which give rise to the same three binary quadratic forms.

Example. Consider the two following cubes of discriminant -31:



We calculate $Q_1^A = x^2 - xy + 8y^2 = Q_1^B$, so we have $\beta_1(A) = \beta_1(B)$. On the other hand $Q_2^A = 2x^2 + xy + 4y^2$ while $Q_2^B = 2x^2 - xy + 4y^2$, since they are both in reduced form, we know that they are not $\mathrm{SL}_2(\mathbb{Z})$-equivalent. Now suppose $[A] = [B]$, then there is $\gamma = \gamma_1 \times \gamma_2 \times \gamma_3 \in \Gamma$ such that $B = A^\gamma$, but we recall that $Q_i^{(A^\gamma)} = (Q_i^A)^{\gamma_i}$, so in particular if $B = A^\gamma$ then $Q_2^B = (Q_2^A)^{\gamma_2}$. Which is a contradiction since we have Q_2^B and Q_2^A are not equivalent. Hence we have $[A] \neq [B]$ but $[\beta_1(A)] = [Q_1^A] = [Q_1^B] = [\beta_1(B)]$ showing that β_1 is not injective. A similar argument can be used to show that neither β_2, β_3 are injective. An interesting point to note is that $Q_3^A = 2x^2 - xy + 4y^2$ and $Q_3^B = 2x^2 + xy + 4y^2$, hence while A and B are not equivalent they both give rise to the same three binary quadratic forms.

- The map γ, defined by $[A] \mapsto [(\mathrm{id} \otimes \wedge_{2,2})(A)]$, is surjective, by Corollary 3.26, but not injective, consider the following example

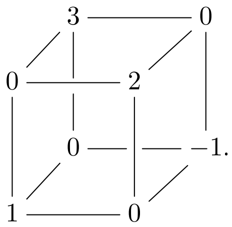
  Example. Let us use the same two cube of discriminant -31 as above. Then if we find the pairs of quaternary alternating 2-forms they map two and calculate their associated binary quadratic forms: $Q^{\gamma(A)} = x^2 - xy + 8y^2 = Q_1^A = Q_1^B = Q^{\gamma(B)} = x^2 - xy + 8y^2$. Since they are the same we have that $\gamma(A)$ and $\gamma(B)$ are equivalent, hence γ is not injective.

- The map δ, defined by $[F] \mapsto [Q^F]$, is an isomorphism, by Corollary 3.27.

- The map ϵ, defined by $[P] \mapsto [Q^P]$, is an isomorphism, by Theorem 3.18.

- The map ζ, defined by $[P] \mapsto [\jmath(P)]$, is injective, as seen in the proof of Theorem 3.18. It is not surjective, consider the following example:

  Example. Let us consider the following cube of discriminant -24



  We want to show that this cube is not equivalent to a doubly symmetric cube. Notice that if $A^{\gamma_1 \times \gamma_2 \times \gamma_3} = B$ a doubly symmetry cube, then $A^{\mathrm{id} \times \mathrm{id} \times \gamma_3 \gamma_2^{-1}} = B^{\gamma_1^{-1} \times \gamma_2^{-1} \times \gamma_2^{-1}}$, which is also a doubly symmetric cube. Hence it is enough to show that there are no $\gamma \in \mathrm{id} \times \mathrm{id} \times \mathrm{SL}_2(\mathbb{Z})$ such that A^γ is a doubly symmetry cube. To see this, suppose that

$$\gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

  is such that A^γ is a doubly symmetry cube. Calculating A^γ we see that we have $2r = u$ and $-s = 3t$. Since we also need $ru - st = 1$, we need to solve $2r^2 + 3t^2 = 1$. This has no solution in $\mathbb{Z}$, hence there is no γ such that A^γ, is doubly symmetric. So there is no pair of binary quadratic form, P, such that $[\zeta(P)] = [A]$.

We can also look at the diagram in terms of the groups in a quadratic ring, note that in all the map description we are talking about the equivalence class represented by:

$$\begin{tikzcd}
 & C(\mathrm{Col}_1^3;\mathcal{O}) \arrow[r, "(I,\delta)\mapsto(I)"] \arrow[d, "(I,\delta)\mapsto(I,I,I)"'] & C_3^+(\mathcal{O}) \\
C^+(\mathcal{O}) \times C^+(\mathcal{O}) \arrow[r, shift left, "(I_1,I_2)\mapsto(I_1,I_2,(I_1I_2)^{-1})"] & C(\mathrm{Col}_{1,1,1}^3;\mathcal{O}) \arrow[l, shift left, "(I_1,I_2,I_3)\mapsto(I_1,I_2)"] \arrow[dl, "(I_1,I_2,I_3)\mapsto(I_1,I_2\oplus I_3)"'] \arrow[d, "(I_1,I_2,I_3)\mapsto(I_i)"] & \\
C(\mathrm{Col}_{1,2}^2;\mathcal{O}) \arrow[r, shift left, "(I,M)\mapsto(I)"] & C^+(\mathcal{O}) \arrow[l, shift left, "(I)\mapsto(I,I^{-1}\oplus M)"] \arrow[r, shift left, "(I)\mapsto((I^2)^{-1},I)"] & C(\mathrm{Col}_{1,1}^3;\mathcal{O}) \arrow[l, shift left, "(I_1,I_2)\mapsto(I_2)"] \arrow[ul, "(I_1,I_2,I_2)\mapsto(I_1,I_2,I_2)"']
\end{tikzcd}$$

4 Conclusion and Further Work

In this paper we saw the construction of 5 different groups and their links to ideals and modules of quadratic rings. As mentioned before Bhargava take this further and goes on to explore cubic, quartic and quintic rings, where he goes on to find many more interesting and important results. In section 2 we talked a bit about reduction theory for positive definite binary quadratic forms, this is something that we could explore further for binary cubic forms. It would also be interesting to study the effect reducing pairs of binary quadratic forms have on the binary quadratic form they are associated to. This would also link nicely with the idea of how to determine when two forms are equivalent, especially in the case of binary cubic forms as we can not link them to binary quadratic forms.

Better yet we have a strong tool to analyse pairs of quaternary alternating 2-forms, that is, we can use the the bijection with binary quadratic forms. We can study the link between a single quaternary alternating 2-form, by letting the second map be of the form

$$\begin{pmatrix} 0 & \mathrm{id} \\ -\mathrm{id} & 0 \end{pmatrix},$$

as then the pair is certainly primitive. In fact such a pair gives rise to the binary quadratic form $(bc - ad)x^2 + (a + d)xy + y^2$. So given a quaternary alternating 2-form given by the matrix

$$\left(\begin{array}{cc|cc} 0 & p & \multicolumn{2}{c}{\multirow{2}{*}{M}} \\ -p & 0 & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{$-M^T$}} & 0 & q \\ & & -q & 0 \end{array}\right)$$

with $M \in \mathrm{GL}_2(\mathbb{Z})$, the binary quadratic form associated to it is $-\det(M)x^2 + \mathrm{Tr}(M)xy + y^2$. Most of the composition we have seen ended up with big formula and variable everywhere, yet when we did the examples, there was not much work to do. For that reason it would be interesting to explore each composition in a lot more details and see if we can establish certain relations, such as congruence, that the composition would need to satisfy.

References

[Bass(1962)] H. Bass. Torsion free and projective modules. *Trans. Amer. Math. Soc.*, 102: 319–327, 1962. ISSN 0002-9947. URL http://www.ams.org/journals/tran/1962-102-02/S0002-9947-1962-0140542-0/S0002-9947-1962-0140542-0.pdf.

[Bhargava(2004)] M. Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004. ISSN 0003-486X. doi: 10.4007/annals.2004.159.217. URL http://dx.doi.org/10.4007/annals.2004.159.217.

[Cox(1989)] D. A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. ISBN 0-471-50654-0; 0-471-19079-9. Fermat, class field theory and complex multiplication.

[Dirichlet(1871)] P. Dirichlet. *Vorlesungen über zahlentheorie.* F. Vieweg und sohn, 1871.

[Gauss(1986)] C. F. Gauss. *Disquisitiones arithmeticae.* Springer-Verlag, New York, 1986. ISBN 0-387-96254-9. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[Lemmermeyer(2010)] F. Lemmermeyer. Binary quadratic forms; an elementary approach to the arithmetic of elliptic and hyperelliptic curves (preprint). 2010. URL http://www.rzuser.uni-heidelberg.de/~hb3/publ/bf.pdf.

[Serre(1957)] J. Serre. Modules projectifs et espaces fibrés a fibre vectorielle. *Séminaire Dubreil-Pisot*, 58, 1957. URL http://www.numdam.org/item?id=SD_1957-1958__11_2_A9_0.

[Shanks(1989)] D. Shanks. On Gauss and composition. I, II. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 163–178, 179–204. Kluwer Acad. Publ., Dordrecht, 1989.

[Stein et al.(2012)] W. Stein et al. *Sage Mathematics Software (Version 4.8).* The Sage Development Team, 2012. URL http://www.sagemath.org. Uses The Maxima Group http://maxima.sourceforge.net/.

A Appendix

A.1 Calculations to the proof of 3.13

A.1.1 Solving the 18 equations

We show the calculations which leads to the formula for the $c_{i,j,k}$. We start with the nine equations (which we get by writing out all possible equation and removing the redundant one, that is the one that appears several time, or the one where we have the same thing on both side):

$$\begin{array}{rcl}
(\alpha_1\beta_1\gamma_1)(\alpha_2\beta_2\gamma_2) &=& (\alpha_2\beta_1\gamma_1)(\alpha_1\beta_2\gamma_2)\\
(\alpha_1\beta_1\gamma_1)(\alpha_2\beta_2\gamma_2) &=& (\alpha_1\beta_2\gamma_1)(\alpha_2\beta_1\gamma_2)\\
(\alpha_1\beta_1\gamma_1)(\alpha_2\beta_2\gamma_2) &=& (\alpha_1\beta_1\gamma_2)(\alpha_2\beta_2\gamma_1)\\
(\alpha_1\beta_1\gamma_1)(\alpha_1\beta_2\gamma_2) &=& (\alpha_1\beta_2\gamma_1)(\alpha_1\beta_1\gamma_2)\\
(\alpha_1\beta_1\gamma_1)(\alpha_2\beta_1\gamma_2) &=& (\alpha_1\beta_1\gamma_2)(\alpha_2\beta_1\gamma_1)\\
(\alpha_1\beta_1\gamma_1)(\alpha_2\beta_2\gamma_1) &=& (\alpha_1\beta_2\gamma_1)(\alpha_2\beta_1\gamma_1)\\
(\alpha_2\beta_2\gamma_2)(\alpha_2\beta_1\gamma_1) &=& (\alpha_2\beta_1\gamma_2)(\alpha_2\beta_2\gamma_1)\\
(\alpha_2\beta_2\gamma_2)(\alpha_1\beta_2\gamma_1) &=& (\alpha_1\beta_2\gamma_2)(\alpha_2\beta_2\gamma_1)\\
(\alpha_2\beta_2\gamma_2)(\alpha_1\beta_1\gamma_2) &=& (\alpha_2\beta_1\gamma_2)(\alpha_1\beta_2\gamma_2)
\end{array}$$

giving us the respective nine equation of the form $(c_{i,j,k} + a_{i,j,k}\tau)(c_{i',j',k'} + a_{i',j',k'}\tau) = (c_{i',j,k} + a_{i',j,k}\tau)(c_{i,j',k'} + a_{i,j',k'}\tau)$. Now we recall that $\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$ where $\epsilon \equiv D \mod 4$, $\epsilon \in \{0,1\}$, and that

$$\begin{array}{rcl}
D &=& a_{1,1,1}^2 a_{2,2,2}^2 + a_{1,1,2}^2 a_{2,2,1}^2 + a_{1,2,1}^2 a_{2,1,2}^2 + a_{2,1,1}^2 a_{1,2,2}^2\\
&& -2(a_{1,1,1}a_{1,1,2}a_{2,2,1}a_{2,2,2} + a_{1,1,1}a_{1,2,1}a_{2,1,2}a_{2,2,2} + a_{1,1,1}a_{2,1,1}a_{1,2,2}a_{2,2,2}\\
&& \quad +a_{1,1,2}a_{1,2,2}a_{2,1,1}a_{2,2,1} + a_{1,1,2}a_{2,1,2}a_{1,2,1}a_{2,2,1} + a_{1,2,1}a_{1,2,2}a_{2,1,1}a_{2,1,2})\\
&& +4(a_{1,1,1}a_{1,2,2}a_{2,1,2}a_{2,2,1} + a_{2,2,1}a_{2,1,2}a_{1,2,2}a_{2,2,2}),
\end{array}$$

we expand the equations and equate the coefficients of τ and the coefficients of 1.

$$\begin{array}{rcl}
c_{1,1,1}c_{2,2,2} + \dfrac{D-\epsilon}{4}a_{1,1,1}a_{2,2,2} &=& c_{2,1,1}c_{1,2,2} + \dfrac{D-\epsilon}{4}a_{2,1,1}a_{1,2,2}\\
c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + \epsilon a_{1,1,1}a_{2,2,2} &=& c_{2,1,1}a_{1,2,2} + c_{1,2,2}a_{2,1,1} + \epsilon a_{2,1,1}a_{1,2,2}\\
c_{1,1,1}c_{2,2,2} + \dfrac{D-\epsilon}{4}a_{1,1,1}a_{2,2,2} &=& c_{1,2,1}c_{2,1,2} + \dfrac{D-\epsilon}{4}a_{1,2,1}a_{2,1,2}\\
c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + \epsilon a_{1,1,1}a_{2,2,2} &=& c_{1,2,1}a_{2,1,2} + c_{2,1,2}a_{1,2,1} + \epsilon a_{1,2,1}a_{2,1,2}\\
c_{1,1,1}c_{2,2,2} + \dfrac{D-\epsilon}{4}a_{1,1,1}a_{2,2,2} &=& c_{1,1,2}c_{2,2,1} + \dfrac{D-\epsilon}{4}a_{1,1,2}a_{2,2,1}\\
c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + \epsilon a_{1,1,1}a_{2,2,2} &=& c_{1,1,2}a_{2,2,1} + c_{2,2,1}a_{1,1,2} + \epsilon a_{2,2,1}a_{1,1,2}\\
c_{1,1,1}c_{1,2,2} + \dfrac{D-\epsilon}{4}a_{1,1,1}a_{1,2,2} &=& c_{1,2,1}c_{1,1,2} + \dfrac{D-\epsilon}{4}a_{1,2,1}a_{1,1,2}\\
c_{1,1,1}a_{1,2,2} + c_{1,2,2}a_{1,1,1} + \epsilon a_{1,1,1}a_{1,2,2} &=& c_{1,2,1}a_{1,1,2} + c_{1,1,2}a_{1,2,1} + \epsilon a_{1,1,2}a_{1,2,1}\\
c_{1,1,1}c_{2,1,2} + \dfrac{D-\epsilon}{4}a_{1,1,1}a_{2,1,2} &=& c_{1,1,2}c_{2,1,1} + \dfrac{D-\epsilon}{4}a_{1,1,2}a_{2,1,1}
\end{array}$$

$$\begin{aligned}
c_{1,1,1}a_{2,1,2} + c_{2,1,2}a_{1,1,1} + \epsilon a_{1,1,1}a_{2,1,2} &= c_{1,1,2}a_{2,1,1} + c_{2,1,1}a_{1,1,2} + \epsilon a_{1,1,2}a_{2,2,1} \\
c_{1,1,1}c_{2,2,1} + \frac{D-\epsilon}{4}a_{1,1,1}a_{2,2,1} &= c_{1,2,1}c_{2,1,1} + \frac{D-\epsilon}{4}a_{1,2,1}a_{2,1,1} \\
c_{1,1,1}a_{2,2,1} + c_{2,2,1}a_{1,1,1} + \epsilon a_{1,1,1}a_{2,2,1} &= c_{1,2,1}a_{2,1,1} + c_{2,1,1}a_{1,2,1} + \epsilon a_{2,1,1}a_{1,2,1} \\
c_{2,2,2}c_{2,1,1} + \frac{D-\epsilon}{4}a_{2,2,2}a_{2,1,1} &= c_{2,1,2}c_{2,2,1} + \frac{D-\epsilon}{4}a_{2,1,2}a_{2,2,1} \\
c_{2,2,2}a_{2,1,1} + c_{2,1,1}a_{2,2,2} + \epsilon a_{2,2,2}a_{2,1,1} &= c_{2,1,2}a_{2,2,1} + c_{2,2,1}a_{2,1,2} + \epsilon a_{2,1,2}a_{2,2,1} \\
c_{2,2,2}c_{1,2,1} + \frac{D-\epsilon}{4}a_{2,2,2}a_{1,2,1} &= c_{1,1,2}c_{2,2,1} + \frac{D-\epsilon}{4}a_{1,1,2}a_{2,2,1} \\
c_{2,2,2}a_{1,2,1} + c_{1,2,1}a_{2,2,2} + \epsilon a_{2,2,2}a_{1,2,1} &= c_{1,1,2}a_{2,2,1} + c_{2,2,1}a_{1,1,2} + \epsilon a_{1,1,2}a_{2,2,1} \\
c_{2,2,2}c_{1,1,2} + \frac{D-\epsilon}{4}a_{2,2,2}a_{1,1,2} &= c_{2,1,2}c_{1,2,2} + \frac{D-\epsilon}{4}a_{2,1,2}a_{1,1,2} \\
c_{2,2,2}a_{1,1,2} + c_{1,1,2}a_{2,2,2} + \epsilon a_{2,2,2}a_{1,1,2} &= c_{2,1,2}a_{1,2,2} + c_{1,2,2}a_{2,1,2} + \epsilon a_{2,1,2}a_{1,2,2}
\end{aligned}$$

We can then use a computer program (SAGE 4.8 which used Maxima took roughly 24hr on a standard computer [Stein et al.(2012), SAGE]) to find that there are two solutions. Since we have the condition that $N(I_1)N(I_2)N(I_3) > 0$, we can try both solution and notice that only one works, hence we have a unique solution, which, when looking at the coefficients and sign of each solution, can be condensed into the formula:

$$\begin{aligned}
c_{i,j,k} &= (i'-i)(j'-j)(k'-k) \\
&\quad [a_{i',j,k}a_{i,j',k}a_{i,j,k'} + \frac{1}{2}a_{i,j,k}(a_{i,j,k}a_{i',j',k'} - a_{i',j,k}a_{i,j',k'} - a_{i,j',k}a_{i',j,k'} - a_{i,j,k'}a_{i',j',k})] \\
&\quad -\frac{1}{2}a_{i,j,k}\epsilon
\end{aligned}$$

where $\{i, i'\} = \{j, j'\} = \{k, k'\} = \{1, 2\}$, and $\epsilon \in \{0, 1\}$ with $\epsilon \equiv D \mod 4$.

A.1.2 Showing I_1, I_2, I_3 are fractional ideals.

If $I_1 = [\alpha_1, \alpha_2] = [c_{1,1,1} + a_{1,1,1}\tau, c_{2,1,1} + a_{2,1,1}\tau]$ and $Q_1 = a_1x^2 + b_1xy + cy^2$, we want to show the equalities

$$\begin{aligned}
\tau\alpha_1 &= \frac{b_1+\epsilon}{2}\alpha_1 + a_1\alpha_2 \\
-\tau\alpha_2 &= c_1\alpha_2 + \frac{b_1-\epsilon}{2}\alpha_2,
\end{aligned}$$

where $\epsilon \equiv D \mod 4$, $\epsilon \in \{0, 1\}$. For ease of use, let $A = (a, b, c, d, e, f, g, h)$ and we recall the following formula:

$$D = a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 - 2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(adfg + bceh)$$

by definition of D;

$$\begin{aligned}
a_1 &= bc - ad \\
b_1 &= de + ah - cf - bg \\
c_1 &= fg - eh
\end{aligned}$$

by definition of Q_1;

$$\begin{aligned}
c_{1,1,1} &= bce + \frac{1}{2}a(ah - cf - bg - de) - \frac{1}{2}a\epsilon \\
c_{2,1,1} &= -afg - \frac{1}{2}e(ed - ah - cf - bg) - \frac{1}{2}e\epsilon
\end{aligned}$$

by using formula (3.4);

$$\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$$

by definition of τ. From this we can calculate, recalling that $\epsilon^2 = \epsilon$:

$$\begin{aligned}
\frac{b_1+\epsilon}{2}\alpha_1 + a_1\alpha_2 &= \frac{de+ah-cf-bg+\epsilon}{2}(c_{1,1,1}+a\tau) + (bc-ad)(c_{2,1,1}+e\tau) \\
&= \frac{1}{4}(a^2deh + a^3h^2 - a^2cfh - a^2bgh - acdef - a^2cfh + ac^2f^2 + abcfg \\
&\quad -abdeg - a^2bgh + abcfg + ab^2g^2 - ad^2e^2 - a^2deh + acdef + abdeg \\
&\quad -ade\epsilon - a^2h\epsilon + acf\epsilon + abg\epsilon + a^2h\epsilon - acf\epsilon - abg\epsilon - ade\epsilon - a\epsilon) \\
&\quad +\frac{1}{2}(bcde^2 + abceh - bc^2ef - b^2ceg + bce\epsilon + (ade + a^2h - acf - abg + a\epsilon)\tau \\
&\quad -bcde^2 + abceh + bc^2ef + b^2ceg + ae^2d^2 - a^2deh - acdef - abdeg - bce\epsilon + ade\epsilon) \\
&\quad +(-abcfg + a^2dfg + (bce - ade)\tau) \\
&= \frac{1}{4}(a^3h^2 - 2a^2cfh - 2a^2bgh + ac^2f^2 + 2abcfg + ab^2g^2 - ad^2e^2 - 2ade\epsilon - a\epsilon \\
&\quad +4abceh + 2ae^2d^2 - 2a^2deh - 2acdef - 2abdeg + 2ade\epsilon - 4abcfg + 4a^2dfg \\
&\quad +(2ade + 2a^2h - 2acf - 2abg + 2a\epsilon + 4bce - 4ade)\tau) \\
&= \frac{1}{4}(aD - a\epsilon) + \frac{1}{4}(2a(-de + ah - cf - bg) - 2a\epsilon + 4a\epsilon + 4bce)\tau \\
&= (c_{1,1,1} + a\epsilon)\tau + \frac{D-\epsilon}{\tau}a \\
&= \tau(c_{1,1,1} + a\tau) \\
&= \tau\alpha_1
\end{aligned}$$

We can use the same approach for $-\alpha_2\tau = c_1\alpha_1 + \frac{b_1-\epsilon}{2}\alpha_2$. While we will not got through the calculations to show

$$\begin{aligned}
\tau\beta_1 &= \frac{b_2+\epsilon}{2}\beta_1 + a_2\beta_2 \\
-\tau\beta_2 &= c_2\beta_1 + \frac{b_2-\epsilon}{2}\beta_2 \\
\tau\gamma_1 &= \frac{b_3+\epsilon}{2}\gamma_3 + a_3\gamma_2 \\
-\tau\gamma_2 &= c_3\gamma_1 + \frac{b_3-\epsilon}{2}\gamma_2
\end{aligned}$$

we will write down the following equations that are needed to check that they are correct.

$$\begin{aligned}
I_2 &= [\beta_1, \beta_2] = [c_{2,1,2} + f\tau, c_{2,2,2} + h\tau] \\
I_3 &= [\gamma_1, \gamma_2] = [\beta_1^{-1}, \alpha_2^{-1}] = \left[\frac{c_{2,1,2} + f\epsilon - f\tau}{c_{2,1,2}^2 + \epsilon f c_{2,1,2} - \frac{D-\epsilon}{4}f^2}, \frac{c_{2,1,1} + e\epsilon - e\tau}{c_{2,1,1}^2 + \epsilon e c_{2,1,1} - \frac{D-\epsilon}{4}e^2}\right] \\
a_2 &= ce - ag \\
b_2 &= ah + bg - ed - cf \\
c_2 &= df - bh \\
a_3 &= be - af \\
b_3 &= ah + cf - de - bg \\
c_3 &= gd - ch \\
c_{2,1,2} &= bhe + \frac{1}{2}f(fc - ah - de - bg) - \frac{1}{2}f\epsilon \\
c_{2,2,2} &= -dfg - \frac{1}{2}h(ah - de - bg - cf) - \frac{1}{2}h\epsilon
\end{aligned}$$

A.2 Calculation to prove in Theorem 3.15

We need to show that, in the set up of Theorem 3.15, the following equality holds:

$$\begin{aligned} \alpha\tau &= \frac{a_0a_3 - a_1a_2 + \epsilon}{2}\alpha + (a_1^2 - a_0a_2)\beta \\ -\beta\tau &= (a_2^2 - a_1a_3)\alpha + \frac{a_0a_3 - a_1a_2 - \epsilon}{2}\beta \end{aligned}$$

where $\alpha = c_1 + a_1\tau$ and $\beta = c_2 + a_2\tau$. For ease of notation we let $(a, b, c, d) = (a_0, a_1, a_2, a_3)$. We recall that $\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$, where $\epsilon \equiv D \mod 4$, $\epsilon \in \{0, 1\}$ and by definition

$$D = a^2d^2 - 3b^2c^2 + 4ac^3 + 4b^3d - 6abcd$$

Using formula (3.6) we find that

$$\begin{aligned} c_1 &= \frac{1}{2}(b^2c - 2ac^2 + abd - \epsilon b) \\ c_2 &= -\frac{1}{2}(bc^2 - 2b^2d + acd + \epsilon c) \end{aligned}$$

We can now calculate that, using the fact $\epsilon^2 = \epsilon$,

$$\begin{aligned} \frac{ad - bc + \epsilon}{2}(c_1 + b\tau) + (b^2 - ac)(c_2 + c\tau) &= \frac{1}{4}(ab^2cd - b^3c^2 - 2a^2c^2d + 2abc^3 + a^2bd^2 - ab^2cd \\ &\quad +\epsilon b^2c - 2\epsilon ac^2 + \epsilon abd - \epsilon abd + \epsilon b^2c - \epsilon b) \\ &\quad +\frac{1}{2}(adb\tau - b^2c\tau + \epsilon b\tau - b^3c^2 + 2b^4d - ab^2cd - \epsilon b^2c \\ &\qquad +abc^3 - 2ab^2cd + a^2c^2d + \epsilon ac^2) \\ &\quad +(b^2c\tau - ac^2\tau) \\ &= \frac{1}{4}(-b^3c^2 - 2a^2c^2d + 2abc^3 + a^2bd^2 + 2\epsilon b^2c - 2\epsilon ac^2 - \epsilon b \\ &\quad -2b^3c^2 + 4b^4d - 6ab^2cd - 2\epsilon b^2c + 2abc^3 + 2a^2c^2d + 2\epsilon ac^2 \\ &\quad \tau(2adb - 2b^2c - 2\epsilon b + 4\epsilon b + 4b^2c - ac^2)) \\ &= \frac{1}{4}(b(-3b^2c^2 + 4ac^3 + a^2d^2 + 4b^3d - 6abcd) - \epsilon b) \\ &\quad +\tau(\frac{1}{2}(adb - b^2c - \epsilon b - ac^2 + 2b^2c) + \epsilon b) \\ &= \frac{1}{4}(D - \epsilon)b + \tau(c_1 + \epsilon b) \\ &= c_1\tau + b(\epsilon\tau + \frac{D-\epsilon}{4}) \\ &= \tau\alpha \end{aligned}$$

Similar calculation can be done for $-\beta\tau$ using all the information already given.

A.3 Proof of the bijection between $C(\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2; D)$ and $C(\mathrm{Col}^3_{1,1}; \mathcal{O})$

As this is similar to the proofs of Theorem (3.13) and Theorem (3.15), we only give a sketch proof here, pointing out the important formula that are needed. As usual let $\mathcal{O} = [1, \tau]$ be positively oriented of discriminant D. Then take (I_1, I_2, I_2) to be a representative of an element of $C(\mathrm{Col}^3_{1,1}; \mathcal{O})$, and let $I_1 = [\alpha_1, \alpha_2]$ and $I_2 = [\beta_1, \beta_2]$ be correctly oriented basis, in particular I_1 has to be positively oriented. Then we have the following six equations

$$\begin{aligned} \alpha_i\beta_1^2 &= c_{i,0} + a_{i,0}\tau \\ \alpha_i\beta_1\beta_2 &= c_{i,1} + a_{i,1}\tau \\ \alpha_i\beta_2^2 &= c_{i,2} + a_{i,2}\tau \end{aligned} \tag{A.1}$$

for some $c_{i,j}, a_{i,j} \in \mathbb{Z}$. Then we claim that the map sending the equivalence class of (I_1, I_2, I_2) to the equivalence class of $P = ((a_{1,0}, 2a_{1,1}, a_{1,2}), (a_{2,0}, 2a_{2,1}, a_{2,2})) = (a_{1,0}x^2 + 2a_{1,1}xy + a_{1,2}y^2, a_{2,0}x^2 +$

$2a_{2,1}xy+a_{2,2}y^2)$ is the bijection we require. We can see that if we change the basis of I_1 by $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ (as it needs to keep the correct orientation), then we change P by $\gamma \times \mathrm{id}$, while if we change the basis of I_2 by $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ then we change P by $\mathrm{id} \times \gamma$. Furthermore if we change to another set of equivalent triple, then we still map to P. So this map is well defined.

We show that P has discriminant D, by using the same process as before and showing that the equations (A.1) gives rise to the equality $\mathrm{Disc}(P) = N(I_1)^2 N(I_2)^4 \mathrm{Disc}(\mathcal{O})$. But since $I_1, I_2, I_2$are collinear, we have $N(I_1)N(I_2)^2 = 1$.

We show that the map is injective and surjective by showing that every P is map unto by exactly one equivalence class of $C(\mathrm{Col}^3_{1,1};\mathcal{O})$. To this end fix $P = ((a_{1,0}, 2a_{1,1}, a_{1,2}), (a_{2,0}, 2a_{2,1}, a_{2,2}))$ and consider equations (A.1). As usual we show that all the indeterminate $c_{i,j}, \alpha_i$ and β_j are determined by $a_{i,j}$. We start by finding $c_{i,j}$ in terms of $a_{i,j}$. Since we are in a commutative ring, the following 5 equations holds $(\alpha_i\beta_1\beta_2)^2 = (\alpha_i\beta_1^2)(\alpha_1\beta_2^2)$ and $(\alpha_1\beta_1\beta_2)(\alpha_2\beta_1\beta) = (\alpha_1\beta_1^2)(\alpha_2\beta_2^2) = (\alpha_2\beta_1^2)(\alpha_1\beta_2^2)$. Expanding them using equations (A.1), recalling that $\tau^2 = \epsilon\tau + \frac{D-\epsilon}{4}$ and equating coefficients of τ and 1 we have a total of 10 equations. Solving those 10 equations, using [Stein et al.(2012), SAGE], give two solutions. But recalling that $N(I_1) > 0$ we have the following unique solution:

$$\begin{aligned}
c_{i,0} &= (i'-i)[a_{i,1}^2 a_{i',0} - a_{i,0}a_{1,1}a_{2,1} + \frac{1}{2}(a_{i,0}^2 a_{i',2} - a_{i,2}a_{1,0}a_{2,0} - a_{i,0}\epsilon)] \\
c_{i,1} &= (i'-i)\frac{1}{2}[a_{i,1}a_{1,0}a_{2,2} + a_{i,1}a_{2,0}a_{1,2} - 2a_{i,0}a_{i',1}a_{i,2} - a_{i,1}\epsilon] \\
c_{i,2} &= (i'-i)[a_{i,1}^2 a_{i',2} - a_{i,2}a_{1,1}a_{2,1} + \frac{1}{2}(a_{i,2}^2 a_{i',0} - a_{i,0}a_{1,2}a_{2,2} - a_{i,2}\epsilon)]
\end{aligned}$$

As before we notice that the ration $\beta_1 : \beta_2$ is determined by the ratio $c_{i,0} + a_{i,0}\tau : c_{i,1} + a_{i,1}\tau$, and so the $\mathbb{Z}$-modules are determined up to scalars in K. We finally check that these two $\mathbb{Z}$-modules are fractional ideals of $\mathcal{O}$ by checking they are closed under multiplication by τ. Once again we can show that:

$$\begin{aligned}
\alpha_1\tau &= \frac{a_{1,0}a_{2,2} + a_{2,0}a_{1,2} - 2a_{1,1}a_{2,1} + \epsilon}{2}\alpha_1 + (a_{1,1}^2 - a_{1,0}a_{1,2})\alpha_2 \\
-\alpha_2\tau &= (a_{2,1}^2 - a_{2,0}a_{2,2})\alpha_1 + \frac{a_{1,0}a_{2,2} + a_{2,0}a_{1,2} - 2a_{1,1}a_{2,1} - \epsilon}{2}\alpha_2 \\
\beta_1\tau &= \frac{a_{1,0}a_{2,2} - a_{1,2}a_{2,0} + \epsilon}{2}\alpha_1 + (a_{2,0}a_{1,1} - a_{1,0}a_{2,1})\alpha_2 \\
-\beta_2\tau &= (a_{2,1}a_{1,2} - a_{1,1}a_{2,2})\alpha_1 + \frac{a_{1,0}a_{2,2} - a_{1,2}a_{2,0} - \epsilon}{2}\alpha_2
\end{aligned}$$

To show that invertible ideals maps to primitive pairs of binary quadratic forms, we use the group homomorphism $(I_1, I_2, I_2) \mapsto (I_1, I_2, I_2)$ between $C(\mathrm{Col}^3_{1,1};\mathcal{O})$ and $C(\mathrm{Col}^3_{1,1,1};\mathcal{O})$, and the fact that primitive pairs of binary quadratic forms correspond to primitive cubes. This finish the sketch proof that there is a bijection between $C(\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2; D)$ and $C(\mathrm{Col}^3_{1,1};\mathcal{O})$