A Parameterization of 3-torsion in Quadratic Number Rings á la Bhargava

Eliot Hodges

Math 280y: Arithmetic Statistics
Final Paper
May 2023
Fabian Gundlach

1. Introduction

It is a fundamental problem in arithmetic statistics to provide asymptotic counts for arithmetic objects. Doing so allows us to ask interesting statistical questions about these objects. For example, for any odd prime p, what is the probability that a random quadratic number field (ordered by discriminant) is ramified at p? On the first problem set, we showed that the number of quadratic number fields of discriminant less than T is asymptotic to $\prod_p(1-\frac{1}{p^2})T$ and used this result to show that the probability in question is $1/(p+1)$.

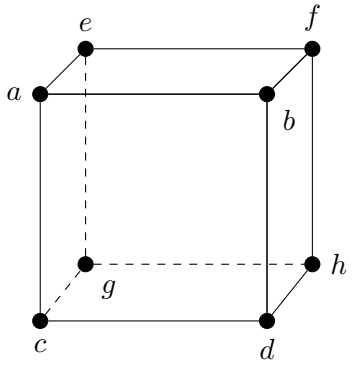
However, actually proving these asymptotics can be quite challenging. Usually, the proof involves finding a nice *parameterization* of the object in question—a bijection from the set of arithmetic objects we are interested in to some set of objects that is easier to count—and then providing an asymptotic count for the second set of objects (usually this involves some kind of sieve argument).

In their seminal paper, *On the density of discriminants of cubic fields* (see [2]), Davenport and Heilbronn proved that the number of cubic fields with discriminant having absolute value less than T is asymptotic to $T/(3\zeta(3))$. Their method, which involves parameterizing cubic number fields by binary cubic forms, along with some class field theory, also gives asymptotics for the 3-torsion in the class groups of quadratic number fields. Proving this result is the motivation for this paper, yet we will not adhere to Davenport and Heilbronn's approach.

Instead, we will present a parameterization of the 3-torsion in the class groups of quadratic number fields due to Bhargava. In his paper (see [1]), *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*, Bhargava generalizes Gauss's famous law of composition of integral binary quadratic forms by deriving a law of composition on $2\times2\times2$ cubes of integers. This more general law of composition on cubes yields four new laws of composition on (1) binary cubic forms, (2) pairs of binary quadratic forms, (3) pairs of quaternary alternating 2-forms, and (4) senary alternating 3-forms. Recall that Gauss composition gives us a parameterization of the class group of a quadratic number field of discriminant D by the $\mathrm{GL}_2(\mathbb{Z})$-orbits of integral binary quadratic forms. Likewise, Bhargava's higher composition laws not only return Gauss's original result but also give several new interesting parameterizations, one of which is the aforementioned parameterization of the 3-torsion in the class group of a quadratic number fields.

2. A group law on cubes

We begin by considering the space of $2\times2\times2$ cubical integer matrices and define a natural action of $\Gamma=\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_2(\mathbb{Z})$ on this space. Denote the space $(\mathbb{Z}^2)^{\otimes3}$ by C_2. Because C_2 is a free abelian group (i.e., $\mathbb{Z}$-module) of rank 8, each element can be represented as a vector (a,b,c,d,e,f,g,h). More intuitively, we may represent the elements of this space by cubes of integers:



(1)

Alternatively, if $\{v_1, v_2\}$ is the standard basis of $\mathbb{Z}^2$, then the elements of C_2 can be written as

$$\sum_{i,j,k} a_{ijk} v_i \otimes v_j \otimes v_k$$

for $1 \leq i, j, k \leq 2$ and $a_{ijk} \in \mathbb{Z}$ instead. However, from here on out, we'll stick to the cubical representation, since this representation is both more convenient and intuitive.

Now, the three planes of symmetry of the cube allow us to partition each cube in C_2 into two 2×2 integral matrices in three ways—Bhargava calls these the *fundamental slicings*. More explicitly, if A denotes the cube in (1), these slicings give us the following pairs of 2×2 matrices:

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

or

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

or

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

It is from these slicings that we define our action of $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ on our space. In particular, we begin by defining how an element of $\mathrm{SL}_2(\mathbb{Z})$ in the ith factor of Γ acts on the cube, and then show that the actions of the three factors of $\mathrm{SL}_2(\mathbb{Z})$ in Γ commute, thus giving us a natural action of Γ on C_2. Let an element

$$\begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

in the ith factor of $\mathrm{SL}_2(\mathbb{Z})$ in Γ act on the cube A by taking $(M_i, N_i) \mapsto (rM_i + sN_i, tM_i + uN_i)$. Checking that the actions of each of the factors commute is straightforward (hint: row and column operations commute), and we omit this detail for the sake of brevity. Therefore, we have a well-defined, natural action of Γ on C_2.

Given any cube $A \in C_2$, we may associate to A three binary quadratic forms,

$$Q_i(x, y) = Q_i^A(x, y) := -\det(xM_i - yN_i)$$

for $1 \leq i \leq 3$. Because acting by the subgroup $\{\mathrm{id}\} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \subset \Gamma$ is the same as applying row and column operations to M_1 and N_1, we see that Q_1 is invariant under the action of this subgroup, implying that the value of $-\det(xM_1 - yN_1)$ is unchanged. The subgroup $\mathrm{SL}_2(\mathbb{Z}) \times \{\mathrm{id}\} \times \{\mathrm{id}\}$ acts on Q_1 in the usual way: $(M, 1, 1) \cdot Q_1(x, y) = Q_1(M^T(x, y))$ (i.e., we apply Q_1 to the vector given by applying M^T to (x, y)). Thus, we see that the discriminant $\mathrm{disc}(Q_1)$ of Q_1 is an invariant for our Γ-action on $C_2 = \mathbb{Z} \otimes \mathbb{Z} \otimes \mathbb{Z}$. A computation tells us that $\mathrm{disc}(Q_2)$ and $\mathrm{disc}(Q_3)$ are both equal to $\mathrm{disc}(Q_1)$ (in fact, $\mathrm{disc}(Q_1)$ is the unique polynomial invariant for this action; see page 220 of [1] or [3]), and thus we may unambiguously define the discriminant of our cube A to be

$$\mathrm{disc}(A) = \mathrm{disc}(Q_1).$$

Another computation tells us $\mathrm{disc}(A)$ explicitly:

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

Now, consider the free abelian group on the set of primitive binary quadratic forms of discriminant D (recall that primitive means the coefficients of the form are relatively prime) and quotient by the subgroup generated by the forms $Q_1^A + Q_2^A + Q_3^A$ for each Q_i^A a primitive quadratic form given by the same cube A with $\mathrm{disc}(A) = D$.

By imposing this additional condition, the $\mathrm{SL}_2(\mathbb{Z})$-equivalent forms (under the standard action) are identified with each other. In other words, $\mathrm{SL}_2(\mathbb{Z})$-equivalent forms are "cube equivalent." To see why this is the case, let $\gamma = (\gamma_1, 1, 1) \in \Gamma$, and let A be a cube giving the three forms Q_1, Q_2, Q_3. Then γA gives the three forms Q_1', Q_2, Q_3, and another explicit computation tells us that $Q_1' = \gamma_1 Q_1$. In the quotient group described in the paragraph above, $Q_1 + Q_2 + Q_3$ and $Q_1' + Q_2 + Q_3$ are both sent to 0, and hence, Q_1 and Q_1' are identified. It remains to show that any such integral binary quadratic form $f(x, y) = rx^2 + sxy + ty^2$ actually arises as Q_1^A for some cube A. But this can be easily seen by computing Q_1^A for

$$A = (a, b, c, d, e, f, g, h) = (r, 0, 0, 1, s, -t, 1, 0).$$

This allows us to think of the group law in the quotient group as a law of addition which descends to a law of addition on the $\mathrm{SL}_2(\mathbb{Z})$-orbits of of binary quadratic forms of discriminant D. In fact, choosing an appropriate identity element makes this set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D into a group!

In particular, we have the following. From here on out, for any binary quadratic form Q, let $[Q]$ denote its $\mathrm{SL}_2(\mathbb{Z})$-equivalence class.

Theorem 2.1. *Let D be any integer congruent to 0 or 1 mod 4. Suppose $Q_{\mathrm{id},D}$ is any primitive binary quadratic form with discriminant D such that there is a cube A_0 with the property that $Q_1^{A_0} = Q_2^{A_0} = Q_e^{A_0} = Q_{\mathrm{id},D}$. Then there exists a unique group law on the set of $\mathrm{SL}_2(\mathbb{Z})$-orbits of primitive binary quadratic forms of discriminant D with the following significance.*

(1) $[Q_{\mathrm{id},D}]$ is the additive identity;

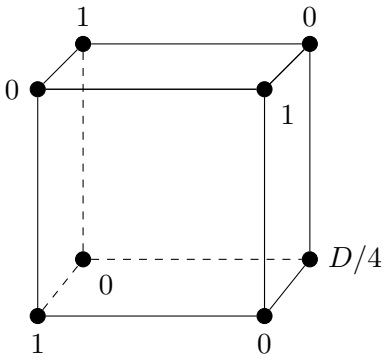
(2) For any cube A with $\mathrm{disc}(A) = D$ and Q_1^A, Q_2^A, Q_3^A primitive, then $[Q_1^A] + [Q_2^A] + [Q_3^A] = [Q_{\mathrm{id},D}]$. On the other hand, if Q_1, Q_2, Q_3 are such that $[Q_1] + [Q_2] + [Q_3] = [Q_{\mathrm{id},D}]$, then there exists a cube A of discriminant D such that $Q_i^A = Q_i$ for all i, and A is unique up to Γ-equivalence.

The usual choice of identity element is

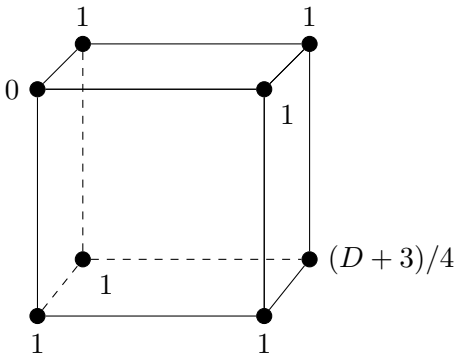
$$Q_{\mathrm{id},D} = x^2 - \frac{D}{4}y^2 \quad \text{or} \quad Q_{\mathrm{id},D} = x^2 - xy + \frac{1-D}{4}y^2,$$

which (must) correspond to the following cubes:
(2)

$A_{\mathrm{id},D} =$



$A_{\mathrm{id},D} =$

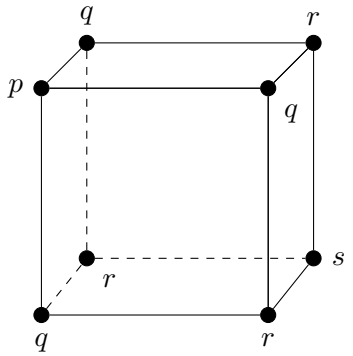


respectively. The two options for $Q_{\mathrm{id},D}$ correspond to the cases $D \equiv 0 \bmod 4$ and $D \equiv 1 \bmod 4$, respectively.

Theorem 2.1 also tells us that the cubes of discriminant D giving rise to triples of primitive quadratic forms form a group as well. We call a cube *projective* if Q_i^A is primitive for $1 \leq i \leq 3$. Let $[A]$ denote the Γ-orbit of A. The following is an easy consequence of Theorem 2.1:

Theorem 2.2. *Suppose D is any integer congruent to 0 or 1 mod 4. Let $A_{\mathrm{id},D}$ be the cube defined by (2). There exists a unique group law on the set of Γ-equivalence classes of projective cubes of discriminant D with the following significance. (1) $[A_{\mathrm{id},D}]$ is the identity element; (2) the map $[A] \mapsto [Q_i^A]$ is a group homomorphism to the group from Theorem 2.1 for $1 \leq i \leq 3$. Denote this group by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$.*

While we will not prove Theorem 2.1 or Theorem 2.2, the law of composition on cubes gives a natural law of composition on $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms with triplicate central coefficients, $px^3 + 3qx^2y + 3rxy^2 + sy^3$. Let $\mathrm{Sym}^3 \mathbb{Z}^2$ denote the space of binary cubic forms with triplicate central coefficients. To each such binary cubic form, we associate the triply-symmetric cube



(3)

which gives us a natural inclusion $\iota : \mathrm{Sym}^3 \mathbb{Z}^2 \to \mathbb{Z} \otimes \mathbb{Z} \otimes \mathbb{Z}$.

The inclusion ι along with the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathrm{Sym}^3 \mathbb{Z}^2$ and the Γ-action on C_2 begs the question: is there a way of viewing the action of $M \in \mathrm{SL}_2(\mathbb{Z})$ on a binary cubic form $C \in \mathrm{Sym}^3 \mathbb{Z}^2$ as the action of an element $\gamma \in \Gamma$ on $\iota(C)$? In general, if $C \in \mathrm{Sym}^3 \mathbb{Z}^2$, then $\gamma \cdot \iota(C)$ is not necessarily in the image of ι. This makes sense, since $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ and we only have an $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathrm{Sym}^3 \mathbb{Z}^2$, rather than a Γ-action. However, ι is $\mathrm{SL}_2(\mathbb{Z})$-equivariant if we restrict to a specific subgroup of Γ isomorphic to $\mathrm{SL}_2(\mathbb{Z})$. Consider the natural inclusion of $\mathrm{SL}_2(\mathbb{Z}) \hookrightarrow \Gamma$ given by $M \mapsto (M, M, M)$, and note that the image of this inclusion is isomorphic to $\mathrm{SL}_2(\mathbb{Z})$. We see that $(M, M, M) \cdot \iota(C) = \iota(M \cdot C)$, implying that ι is a $\mathrm{SL}_2(\mathbb{Z})$-equivariant map, as desired.

Thus, a binary cubic form $C \in \mathrm{Sym}^3 \mathbb{Z}^2$ is said to be *projective* if $\iota(C)$ is projective. If C is given by $C(x, y) = px^3 + 3qx^2y + 3rxy^2 + sy^3$ and is projective, then the corresponding forms $Q_i^{\iota(C)}$ are all given by

$$H(x, y) = -\frac{1}{36} \begin{vmatrix} C_{xx} & C_{xy} \\ C_{yx} & C_{yy} \end{vmatrix} = (q^2 - pr)x^2 + (ps - qr)xy + (r^2 - qs)y^2.$$

It follows that C is projective if and only if H is primitive. Thus, for C to be projective, it suffices to check whether $\gcd(q^2 - pr, ps - qr, r^2 - qs) = 1$.

Note that ι introduces a discrepancy: for some binary cubic form $C \in \mathrm{Sym}^3 \mathbb{Z}^2$, there are now two different ways of defining $\mathrm{disc}(C)$. In particular, $\mathrm{disc}(C)$ could denote the discriminant of C as a polynomial or its discriminant as a cube, which differ by a factor of -27. From here on out, assume that $\mathrm{disc}(C)$ refers to $\mathrm{disc}(\iota(C))$, the discriminant of the cube $\iota(C)$. We will see why this viewpoint is useful when we prove Theorem 3.1.

Depending on whether D is 0 or 1 mod 4, the identity cubes (2) are given by

$$C_{\mathrm{id},D} = 3x^2y + \frac{D}{4}y^3 \quad \text{or} \quad C_{\mathrm{id},D} = 3x^2y + 3xy^2 + \frac{D+3}{4}y^3$$

respectively. As usual, let $[C]$ denote the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of $C \in \mathrm{Sym}^3 \mathbb{Z}^2$.

Theorem 2.3. *Suppose D is any integer congruent to 0 or 1 mod 4. Let $C_{\mathrm{id},D}$ be as in the above. Then there exists a unique group operation on the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of projective binary cubic forms C of discriminant D with the following significance. (1) $[C_{\mathrm{id},D}]$ is the additive identity; (2) the map $[C] \mapsto [\iota(C)]$ is a group homomorphism to $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$. Denote this group by $\mathrm{Cl}(Sym^3 \mathbb{Z}^2; D)$.*

3. Parameterizations

This section will be entirely devoted to proving the following theorem, from which most of our results follow. In the following, recall that by $\mathrm{disc}(f)$ we mean $\mathrm{disc}(\iota(f))$, the discriminant of f when viewed as a cube (rather than as a binary cubic form).

Theorem 3.1. *There exists a canonical bijection between*

$$\{f \in Sym^3 \mathbb{Z}^2 \mid \mathrm{disc}(f) \neq 0\}/\mathrm{SL}_2(\mathbb{Z})$$

and the equivalence classes of triples (S, I, δ), where S is a nondenerate (discriminant nonzero) oriented quadratic ring, I is a fractional ideal of S, and δ is some element in $(S \otimes \mathbb{Q})^\times$ with the following properties: $I^3 \subset \delta S$ and $N(I)^3 = N(\delta)$. Moreover, for $f \in Sym^3 \mathbb{Z}^2$, $\mathrm{disc}(f)$ is equal to the discriminant of the corresponding quadratic ring.

By *quadratic ring*, we mean a commutative ring (with unit) whose underlying structure as an additive group is $\mathbb{Z}^2$ (the name *quadratic ring* comes from the fact that the classical example of such a ring is the ring of integers of a quadratic number field). For any α in such a quadratic ring R, the trace of α, denoted $\mathrm{tr}(\alpha)$, is the trace of the linear map $R \to R$ given by multiplication by α. As in algebraic number theory, if $\{\alpha_i\}$ is a $\mathbb{Z}$-basis for R, we say that $\det(\mathrm{tr}(\alpha_i \alpha_j)_{i,j}) \in \mathbb{Z}$ is the *discriminant* of R, which we denote using $\mathrm{disc}(R)$. This quantity is independent of the basis we choose.

Recall that all quadratic rings have exactly two automorphisms. Stickelberger's criterion tells us that $\mathrm{disc}(R)$ is congruent to 0 or 1 mod 4. Conversely, given any integer D congruent to 0 or 1 mod 4, there is a unique quadratic ring with discriminant D. Thus, we have a parameterization of isomorphism classes of quadratic rings by the elements of $\mathbb{Z}$ congruent to 0 or 1 mod 4, but this parameterization is not quite ideal since quadratic rings have two automorphisms (in the number field case, this corresponds to the fact that $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(-\sqrt{D})$, i.e., we have two choices for $\sqrt{D}$) while the elements of $\mathbb{Z}$ in question only have one. In other words, we have a parameterization up to noncanonical isomorphism.

To rectify this situation, we consider *oriented quadratic rings*, which are defined to be quadratic rings where a specific choice of isomorphism $\bar{\pi} : S/\mathbb{Z} \to \mathbb{Z}$ has been made. Such a ring only has one automorphism, and it follows that any two oriented quadratic rings with the same discriminant are canonically isomorphic. Equivalently, we see that a quadratic ring is oriented once we choose $\sqrt{D}$. Such a choice determines a canonical projection $\pi : S \to \mathbb{Z}$ given by $\pi(x) = \mathrm{tr}(x/\sqrt{D}) = (x - \bar{x})/\sqrt{D}$, where $\bar{x}$ denotes the image of x under the nontrivial automorphism of S (in the case of number fields, this is the Galois conjugate of x). This projection π must have kernel $\mathbb{Z}$ and thus induces an isomorphism $\bar{\pi} : S/\mathbb{Z} \to \mathbb{Z}$, implying that these two viewpoints are the same.

Another solution to this issue is the following. We may define a (trivial) $\mathbb{Z}^\times$-action of integers, and then parameterize quadratic rings by the $\mathbb{Z}^\times$-orbits of this action. This way, the stabilizer of each integer in $\mathbb{Z}$ is the correct group, $\mathbb{Z}/2\mathbb{Z}$. Thus, there is no longer a need to pick an orientation and we can instead use an action of $\mathrm{GL}_2(\mathbb{Z})$. In this case, $\mathrm{GL}_2(\mathbb{Z})$ acts on a binary quadratic

form by $M \cdot f(x,y) \mapsto \frac{1}{\det(M)} f(M^T(x,y))$. One advantage of this viewpoint is that, in the case of Gauss composition, we get a bijection between $\mathrm{GL}_2(\mathbb{Z})$-orbits of primitive binary quadratic forms of discriminant D and the class group of $S(D)$, $\mathrm{Cl}(S(D))$. When using the action of $\mathrm{SL}_2(\mathbb{Z})$, our bijection is between $\mathrm{SL}_2(\mathbb{Z})$-orbits of primitive binary quadratic forms of discriminant D and the narrow class group of $S(D)$, $\mathrm{Cl}^+(S(D))$. While this difference is mainly aesthetic, it is perhaps easier to see the usefulness of the $\mathrm{GL}_2(\mathbb{Z})$ approach at first glance. We consider $\mathrm{SL}_2(\mathbb{Z})$-orbits, however, because this setup is slightly cleaner in terms of exposition.

Now, recall that any quadratic ring S can be written as $\mathbb{Z} + \mathbb{Z}\tau$, where the multiplication is given by

$$\tau^2 = \frac{D}{4} \quad \text{or} \quad \tau^2 = \frac{D-1}{4} + \tau,$$

depending on whether or not D is congruent to 0 or 1 mod 4. We define what it means for a basis to be *oriented*: Given a quadratic ring $S = \mathbb{Z} + \mathbb{Z}\tau$, we say that the basis $\{1, \tau\}$ of S is *positively oriented* if $\pi([\tau]) > 0$. Then, we say that any pair of linearly independent elements $\alpha, \beta \in K = S \otimes \mathbb{Q}$ is *positively oriented* if the linear map taking $(1, \tau) \mapsto (\alpha, \beta)$ has positive determinant. We define the *norm* of an ideal I of a quadratic ring S to be the following: let (α, β) be a $\mathbb{Z}$-basis of I, and let $M \in \mathrm{GL}_2(\mathbb{Q})$ be the linear map taking $(1, \tau) \mapsto (\alpha, \beta)$. Let $N(I) = \det(M)$. Finally, let (S, I, δ) and (T, J, ϵ) be two triples as in Theorem 3.1. We say that these triples are equivalent if there exists some isomorphism $\phi : S \to T$ and element $\kappa \in T \otimes \mathbb{Q}$ such that $J = \kappa\phi(I)$ and $\epsilon = \kappa^3\phi(\delta)$. Checking that this is indeed an equivalence relation is not difficult. We are now ready to prove Theorem 3.1.

Proof of Theorem 3.1. We'll begin by showing how to construct a binary cubic form given a triple (S, I, δ). Let $S = \mathbb{Z} + \mathbb{Z}\tau$ and let (α, β) form a positively oriented $\mathbb{Z}$-basis for I. In particular, depending on whether $\mathrm{disc}(S)$ is congruent to 0 or 1 mod 4, let τ be such that $\tau^2 - D/4 = 0$ or $\tau^2 - \tau + \frac{1-D}{4} = 0$, respectively. We see that I^3 is generated as a $\mathbb{Z}$-module by the four products $\alpha^3, \alpha^2\beta, \alpha\beta^2, \beta^3 \in I^3 \subset \delta S$. Since $I^3 \subset \delta S$, we may write

$$\alpha^{3-i}\beta^i = \delta(c_i + a_i\tau) \quad \text{for } 0 \le i \le 3 \tag{4}$$

and $a_i, c_i \in \mathbb{Z}$. We associate to (S, I, δ) the binary cubic form

$$C(x,y) = a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3 \in \mathrm{Sym}^3 \mathbb{Z}^2.$$

Firstly, we need to check is that $C(x,y)$ does not depend on our choice of bases (α, β) for I and $(1, \tau)$ for $\mathbb{Z}$. To see this, we claim that $C(x,y) = \pi((\alpha x + \beta y)^3)$, where π is the associated canonical projection $\pi : S \to \mathbb{Z}$. This follows from simply applying π to

$$(\alpha x + \beta y)^3 = \alpha^3x^3 + 3\alpha^2\beta x^2y + 3\alpha\beta^2xy^2 + \beta y^3$$

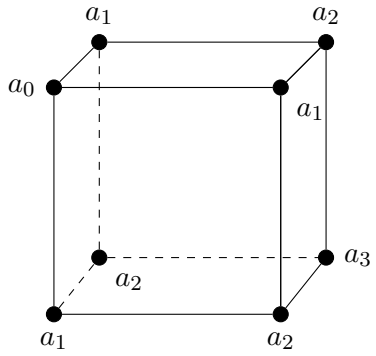
(recall the definition of the a_i's). Therefore, we may define C in a basis free manner: as the map from $I \to \mathbb{Z}$ taking $\zeta \mapsto \pi(\zeta^3)$. Given another (positively oriented) basis (α', β') of I, let $M \in \mathrm{SL}_2(\mathbb{Z})$ be the change of basis matrix taking (α, β) to (α', β'). Our basis-free description of C then tells us that changing bases to (α', β') will just change $C(x,y)$ to $M \cdot C(x,y) = C(M^T(x,y))$, implying that the $\mathrm{SL}_2(\mathbb{Z})$-orbit associated to (S, I, δ) is independent of the choice of basis for I. Moreover, we may realize $M \cdot C(x,y)$ by changing our basis of I to $M(\alpha, \beta)$. Now, let (S, I, δ) and (T, J, ϵ) be two equivalent triples so that there exists an isomorphism $\phi : S \to T$ and element $\kappa \in T \otimes \mathbb{Q}$ such that $J = \kappa\phi(I)$ and $\epsilon = \kappa^3\phi(\delta)$. We claim that both triples give rise to the same cubic forms $C(x,y)$; we consider the cubic form associated to (T, J, ϵ) given by the basis $\alpha' = \kappa\phi(\alpha), \beta' = \kappa\phi(\beta)$ for J. Let $\tau' = \phi(\tau)$, and note that

$$(\alpha')^{3-i}(\beta')^i = \kappa^3\phi(\alpha^{3-i}\beta^i) = \kappa^3\phi(\delta)(c_i + a_i\tau') = \epsilon(c_i + a_i\tau') \in J.$$

It follows that the form associated to (T, J, ϵ) is exactly $C(x,y)$.

Now, we prove that the map defined in the above, from equivalence classes of triples (S, I, δ) to $\mathrm{SL}_2(\mathbb{Z})$-orbits of $\mathrm{Sym}^3 \mathbb{Z}^2$, is indeed a bijection.

To do this, consider some form $C(x, y) \in \mathrm{Sym}^3 \mathbb{Z}^2$. We will show that there is exactly one triple (S, I, δ) (up to equivalence) that gives the form $C(x, y)$ under the map described in the above. Recall from Section 2 that $C(x, y)$ corresponds to the cube of integers $\iota(C)$,



to which we can assign a well-defined discriminant $\mathrm{disc}(C) = \mathrm{disc}(\iota(C))$. Recall from earlier that the discriminant of C is not the discriminant of C as a polynomial. Rather, it is the discriminant of the unique cube we may associate to C, $\iota(C)$. Also recall the system (4) from earlier, and note that, with C fixed, only the a_i's are determined (with everything else indeterminant).

To see that $C(x, y)$ determines the ring S, recall that it suffices to show that $\mathrm{disc}(S)$ is determined (recall S is a quadratic ring) by our system (4). To do so, we will need the identity

$$\mathrm{disc}(C) = N(I)^6 N(\delta)^{-2} \mathrm{disc}(S).$$

We first prove the identity in the special case where we take $I = S$ and $\delta = 1$. As before, write $S = S(D) = \mathbb{Z} + \mathbb{Z}\tau$, and consider the special (simple) case where $I = S$, $\alpha = 1$, and $\beta = \tau$. In this case, it is easy to check that $C(x, y) = C_{\mathrm{id},D}$; note that the cube $C_{\mathrm{id},D}$ has discriminant $N(\delta)^2 D = \mathrm{disc}(S)$ (the $N(\delta)^2$ factor comes from scaling everything by δ and taking the discriminant). Hence, we have that $\mathrm{disc}(C) = N(\delta)^{-2} D = N(\delta)^{-2} \mathrm{disc}(S)$, as desired.

For the general case, assume that I is now a general ideal of S with $\mathbb{Z}$-basis (α, β). We may write $(\alpha, \beta) = M(1, \tau)$ for some $M \in \mathrm{SL}_2(\mathbb{Q})$, and we see that the cube in (4) is given by applying $(M, M, M) \in \Gamma$ to $C_{\mathrm{id},D}$. For the sake of brevity, we omit checking the details explicitly (lots of gross algebra). If we act on the cube $C_{id,D}$ one factor at a time (i.e., first by (M, e, e), then (e, M, e), and finally (e, e, M); recall that the actions of the factors of Γ commute), another computation shows that acting by (M, e, e) multiplies the quadratic form $Q_2^{(M,e,e)C_{id,D}}$ by $\det(M) = N(I)$. This multiplies the discriminant of $(M, e, e)C_{\mathrm{id},D}$ by $N(I)^2$. Similarly, acting by (e, M, e) and (e, e, M) both scale the discriminant by $N(I)^2$; this establishes the identity in full generality. Now, our assumption that $N(I)^3 = N(\delta)$ tells us that $\mathrm{disc}(C) = \mathrm{disc}(S)$, implying that $\mathrm{disc}(S)$ (and thus S itself) is determined by our form C.

Next, we show that the c_i's are also uniquely determined by C. Rewrite $(\alpha^2\beta)^2 = \alpha^3 \cdot \alpha\beta$ and $(\alpha\beta^2)^2 = \alpha^2\beta \cdot \beta^3$; these identities follow from the commutativity and associativity of S. Using (4), we may rewrite both of these equations to give two linear and two quadratic equations in our four variables c_0, c_1, c_2, c_3. As long as (α, β) has positive orientation, we can show that this system has exactly one solution. We'll illustrate this for the case where $\tau^2 = D/4$; the other case is similar.

Rewriting the two identities as suggested above, we see that

$$(c_1^2 + a_1^2 D/4) + 2a_1c_1\tau = (c_0c_2 + a_0a_2D/4) + (a_2c_0 + a_0c_2)\tau$$
$$(c_2^2 + a_2^2 D/4) + 2a_2c_2\tau = (c_3c_1 + a_3a_1D/4) + (a_1c_3 + a_3c_1)\tau.$$

This gives the following system of equations

$$2a_1c_1 = a_2c_0 + a_0c_2 \tag{5}$$
$$2a_2c_2 = a_1c_3 + a_3c_1 \tag{6}$$
$$c_1^2 + a_1^2D/4 = c_0c_2 + a_0a_2D/4 \tag{7}$$
$$c_2^2 + a_2^2D/4 = c_3c_1 + a_3a_1D/4. \tag{8}$$

Finally, the requirement that (α, β) has positive orientation tells us that the map taking $1 \mapsto \alpha$ and $\tau \mapsto \beta$ must have positive determinant. While α and β are undetermined still, we note that the map taking $1 \mapsto 1$ and $\tau \mapsto \beta/\alpha$ has the same determinant as the aforementioned map. By considering

$$\frac{\beta}{\alpha} = \frac{\beta^2\alpha}{\alpha\beta^2} = \frac{c_2 + a_2\tau}{c_1 + a_1\tau},$$

some computation shows that the condition (α, β) is of positive orientation if and only if

$$a_2c_1 - a_1c_2 > 0.$$

Now, (5) and (6) are linear equations that allow us to write c_0 and c_3, respectively, in terms of c_1 and c_2. Plugging these into (7) and (8) gives us two quadrics in c_1 and c_2. Using a computer, we can compute that there is exactly common root of these quadrics subject to the condition $a_2c_1 - a_1c_2 > 0$. In particular, we find that there are four common solutions to the two quadrics; note that solutions must come in pairs, since if $(c_0, \ldots, c_3)$ is a solution to the system above, then so is its negative, $(-c_0, \ldots, -c_3)$. One of the solutions (exhibited below), along with its negative, is integral, and the other two involve $\sqrt{D}$. In the case that $D = \mathrm{disc}(S) = \mathrm{disc}(C)$ is not a square, $\sqrt{D}$ is irrational, and neither of these additional solutions are possible, since the c_i's are necessarily integral. Thus, we have a unique solution satisfying $a_2c_1 > a_1c_2$ (we can compute that the solution given below indeed satisfies this inequality when $D \equiv 0 \bmod 4$). However, in the case where D is a square, this argument breaks down. In this case, there are only two solutions in which α and β are linearly independent (we'll show later that we may take $\alpha = c_1 + a_1\tau$ and $\beta = c_2 + a_2\tau$), which are the solution given below and its negative.

This unique solution to the system in question is given by

$$c_0 = \frac{2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 - \varepsilon a_0}{2},$$
$$c_1 = \frac{a_1^2a_2 - 2a_0a_2^2 + a_0a_1a_3 - \varepsilon a_1}{2},$$
$$c_2 = -\frac{a_1a_2^2 - 2a_1^2a_3 + a_0a_2a_3 + \varepsilon a_2}{2},$$
$$c_3 = -\frac{2a_2^3 - 3a_1a_2a_3 + a_0a_3^2 + \varepsilon a_3}{2},$$

where $\varepsilon = 0$ or $\varepsilon = 1$ if $D \equiv 0$ or $D \equiv 1 \bmod 4$, respectively. Therefore, the c_i's are also entirely determined by our form C.

We also see that (4) implies that

$$\frac{\alpha^2\beta}{\alpha\beta^2} = \frac{\alpha}{\beta} = \frac{c_1 + a_1\tau}{c_2 + a_2\tau} \tag{9}$$

This tells us that α and β are determined (uniquely) up to scaling by elements of $S \otimes \mathbb{Q}$. Fix an α and β, say $\alpha = c_1 + a_1\tau$ and $\beta = c_2 + a_2\tau$, and note that this uniquely determines δ by (4). If we rescale α and β by some $\kappa \in S \otimes \mathbb{Q}$, then we see that we must rescale δ by κ^3. Hence, we have a unique triple (S, I, δ) (up to equivalence) that is sent to the form C under the mapping defined at the beginning of the proof.

There is one last thing to check: I, as we have written it, is simply the $\mathbb{Z}$-module generated by α and β, not necessarily an ideal. To rectify this, we show that I is an ideal of S; we may actually write down the S-module structure on I explicitly. Using our explicit expressions for α and β, $\alpha = c_1 + a_1\tau$ and $\beta = c_2 + a_2\tau$, in addition to our expressions for c_i's in terms of the a_i, we see that

$$\tau\alpha = \frac{q+\varepsilon}{2}\alpha + p\beta$$

and

$$-\tau\beta = r\alpha + \frac{q-\varepsilon}{2}\beta,$$

where

$$p = a_1^2 - a_0a_2, \quad q = a_0a_3 - a_1a_2, \quad r = a_2^2 - a_1a_3$$

and where $\varepsilon = 0$ or $\varepsilon = 1$ in accordance with whether D is congruent to 0 or 1 mod 4, respectively. We note that the quadratic form Q associated to the binary cubic form C (viewed as an integral cube) is exactly

$$Q(x, y) = px^2 + qxy + ry^2.$$

Therefore, I is indeed an ideal of S, and we are done. □

4. Consequences

The following are immediate consequences of Theorem 3.1. Let $\mathrm{Cl}_3(R)$ denote the 3-torsion (i.e., the elements with order dividing 3) in the ideal class group of an integral domain R.

Corollary 4.1. *Denote the quadratic ring of discriminant D by $S(D)$. There is a natural surjective group homomorphism*

$$\mathrm{Cl}(Sym^3\,\mathbb{Z}^2; D) \twoheadrightarrow \mathrm{Cl}_3(S(D)).$$

The cardinality of the kernel of this homomorphism is $|U/U^3|$, where U is the group of units in $S(D)$.

The case where $S(D)$ is the ring of integers of a quadratic number field K is significant and the main goal of this paper:

Corollary 4.2. *Let D be a disriminant of a quadratic number field K. Then there is a canonical surjective homomorphism*

$$\mathrm{Cl}_3(Sym^3\,\mathbb{Z}^2; D) \twoheadrightarrow \mathrm{Cl}_3(K).$$

The kernel of this map has size

$$\begin{cases} 1 & \text{if } D < -3; \\ 3 & \text{otherwise.} \end{cases}$$

References

[1] Bhargava, M. Higher composition laws i: A new view on gauss composition, and quadratic generalizations. *Annals of Mathematics 159*, 1 (2004), 217–250.

[2] Davenport, H., and Heilbronn, H. On the density of discriminants of cubic fields. ii. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences 322*, 1551 (1971), 405–420.

[3] Hilbert, D. Theory of algebraic invariants, 1993.