Notes on Bhargava's composition laws

Katherine E. Stange

December 29, 2014

1 Introduction

These are notes to myself and our research seminar on *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*, M. Bhargava, Annals of Mathematics, 159 (2004), 217–250.

2 Composition of Quadratic Forms – Classical Viewpoint

Where by 'classical,' I mean before 2000.

2.1 Quadratic forms

There are some standard facts that need to be collected about quadratic forms. An integral n-ary k-ic form is a $\mathbb{Z}$-linear combination of monomials of degree k in n variables. We will concern ourselves with integral binary quadratic forms, which can all be expressed as

$$aX^2 + bXY + cY^2, \quad a, b, c \in \mathbb{Z}.$$

(Note that some authors require b to be even; we do not.) Such a form is *primitive* if $\gcd(a, b, c) = 1$.

Two such forms are $\mathrm{GL}_2(\mathbb{Z})$-equivalent if one can be obtained from another by an invertible change of variables

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix},$$

i.e. where $a, b, c, d \in \mathbb{Z}$, $ad - bc = \pm 1$. They are $\mathrm{SL}_2(\mathbb{Z})$-equivalent if we further require $ad - bc = 1$. In other words, both $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z})$ act on the collection of primitive integral binary quadratic forms.

Each binary quadratic form has a *discriminant* $b^2 - 4ac$, which is invariant under the $\mathrm{GL}_2(\mathbb{Z})$-action. Hence each equivalence class has a *discriminant*.

The equivalence classes of forms of discriminant D form a finite set, which we will denote $\mathcal{Q}(D)$. To see that it is finite, one studies the *reduction* of quadratic forms, which I'll briefly review now.

A quadratic form $aX^2 + bXY + cY^2$ can be viewed as a function

$$f_{a,b,c} : \mathbb{Z}^2 \to \mathbb{Z}, \quad [x, y] \mapsto ax^2 + bxy + cy^2.$$

This is well defined because it is degree 2 and therefore blind to the change of sign $(x, y) \mapsto (-x, -y)$. The function $f_{a,b,c}$ is an example of a *quadratic form* in the sense of a function satisfying

1. $f(nx) = n^2 f(x), n \in \mathbb{Z}$ for all x,
2. $B(x, y) = f(x + y) - f(x) - f(y)$ is a symmetric bilinear form.

Such a function is called *non-degenerate* if $f(x) \neq 0$ for all $x \neq 0$. It is *positive (negative) definite* if $f(x) > 0$ ($f(x) < 0$) for all $x \neq 0$. It is indefinite if it is non-degenerate but neither positive nor negative definite. The form $f_{a,b,c}$ is...

degenerate	if $D = 0$ or a square
positive or negative definite	if $D < 0$
indefinite	if $D > 0$, nonsquare

There is a separate reduction theory for positive (or negative) definite and indefinite forms. For positive definite forms, the traditional theory is pleasingly simple: there is exactly one so-called *reduced* form in each equivalence class. For $\mathrm{GL}_2(\mathbb{Z})$-equivalence, the condition of reduction is

$$0 \leq b \leq a \leq c.$$

For $\mathrm{SL}_2(\mathbb{Z})$-equivalence (a finer notion), the condition of reduction is

$$0 \leq |b| \leq a \leq c.$$

The extra freedom of GL_2 lets you change the sign of b (by taking $x, y \mapsto x, -y$).

Warning. In what follows Bhargava will change the action and hence equivalence classes slightly. See Section 3.3.

For indefinite forms, there are finitely many reduced forms in each equivalence class, and the notion of SL_2-reduced is that

$$|\sqrt{D} - 2|c|| < b < \sqrt{D}.$$

2.2 Composition of forms

The term *composition of forms* refers to a group law we can impose on $\mathcal{Q}(D)$ via a correspondence with ideal classes. This allows one to do a simple finite calculation (counting reduced forms) to determine the class number of a quadratic field.

Most sources cover the positive definite case, but a reference for both is Henri Cohen, A Course in Compuational Algebraic Number Theory, §5.2. Bhargava changes conventions somewhat in order to unify the positive and negative discriminants.

Theorem 1 (Positive definite case)**.** *There is a bijective correspondence between ideal classes in the ring of integers of the quadratic field K of discriminant $D < 0$, and primitive integral positive definite binary quadratic forms of discriminant D modulo $SL_2(\mathbb{Z})$-equivalence.*

For the indefinite case, we need the *narrow* class group, which is traditionally defined to be the invertible fractional ideals modulo totally positive principal fractional ideals. The term *totally positive* means the generator is positive under all embeddings to $\mathbb{R}$.

Theorem 2 (Indefinite case)**.** *There is a bijective correspondence between* narrow *ideal classes in the ring of integers of the quadratic field K of discriminant $D > 0$, and primitive integral* indefinite *binary quadratic forms of discriminant D modulo $SL_2(\mathbb{Z})$-equivalence.*

This correspondence is very concrete to describe. Let $K = \mathbb{Q}(\sqrt{D})$ and let I be an ideal of $\mathcal{O}_K$. The ideal I is a rank two $\mathbb{Z}$-module, and the norm $N = N_{K/\mathbb{Q}}$ on $\mathcal{O}_K$ restricts to I. The map

$$f_I : I \to \mathbb{Z}, \quad x \mapsto N(x)/N(I)$$

is a quadratic form. Explicitly, choosing a basis α, β for I with the convention that

$$\frac{\beta\sigma(\alpha) - \alpha\sigma(\beta)}{\sqrt{D}} > 0,$$

where σ is the non-trivial automorphism of S, we can write a quadratic form $aX^2 + bXY + cY^2$ such that

$$f_{a,b,c} : \mathbb{Z}^2 \to \mathbb{Z}$$

is given by

$$f_{a,b,c}(x, y) = f_I(x\alpha + y\beta) = N(x\alpha + y\beta)/N(I).$$

Example 1. *Let $I = (2, 1+\sqrt{-5})$ be an ideal of $\mathbb{Z}[\sqrt{-5}]$ which has discriminant -20. The allowable basis is $\alpha = 2, \beta = 1 - \sqrt{-5}$ since*

$$2 + 2\sqrt{-5} - 2 + 2\sqrt{-5} = 4\sqrt{-5}.$$

The ideal has norm $N(I) = 2$. Then the form is

$$\frac{1}{2}N(2x+(1+\sqrt{-5})y) = \frac{1}{2}(2x+y+\sqrt{-5}y)(2x+y-\sqrt{-5}y) = 2x^2+2xy+3y^2.$$

Note that if we'd taken the conjugate ideal, the necessity of choosing an allowable basis means we would end up with x and y swapped.

Conversely, given a primitive integral binary quadratic form, we can create an ideal:

$$aX^2 + bXY + cY^2 \mapsto \left(a, \frac{b-\sqrt{D}}{2}\right)\alpha,$$

where we choose α to be anything with $sign(N(\alpha)) = sign(a)$ (this condition holds for all α when $D < 0$ and we are in the positive definite case, so it is only required for the $D > 0$). To provide some context to the formula, note that the roots of

$$aX^2 + bX + c$$

are

$$\frac{b \pm \sqrt{D}}{2a}.$$

At least for positive definite forms[1], another way to give the correspondence in this direction is to specify a representative of the fractional ideal class by

$$\mathbb{Z} + \eta\mathbb{Z}$$

where η is an (appropriately chosen) root of $aX^2 + bX + c$.

Example 2. *Consider the form $2x^2 + 2xy + 3y^2$ which has $D = -20$. One obtains the ideal*

$$\left(2, \frac{2-\sqrt{-20}}{2}\right) = (2, 1-\sqrt{-5}).$$

Since $\sqrt{-5}$ has class number 2, this is equivalent to $(2, 1+\sqrt{-5})$.

To verify the theorem, there are a variety of things to check, but none of them are other than straightforward. We should verify that these descriptions of the map in either direction are well defined (especially on equivalence classes), and that they are inverse to one another.

[1] Does this work for indefinite?

3 Composition of Quadratic Forms - Bhargava's Perspective

3.1 Quadratic Rings and Discriminants

A quadratic ring is a commutative ring with unit R having $\mathbb{Z}^2$ as its additive group. More generally, $\mathbb{Z}^n$ gives an n-ic ring. We have a trace and norm

$$Tr : R \to \mathbb{Z}, N : R \to \mathbb{Z}$$

which are just the trace and determinant of the ring endomorphism $x \mapsto \alpha x$ for an element $\alpha \in R$. There's a trace pairing, $\langle \alpha, \beta \rangle := Tr(\alpha\beta)$ and the determinant of its Gram matrix is the *discriminant*. This is always 0 or 1 (mod 4) (Stickelberger).

Given a candidate D for the discriminant, we may find a quadratic ring with that discriminant, by writing

$$S(D) = \mathbb{Z}[\tau]/(\tau^2 - f(\tau))$$

where

$$f(\tau) = \begin{cases} D/4 & D \equiv 0 \pmod 4 \\ (D-1)/4 + \tau & D \equiv 1 \pmod 4 \end{cases}$$

Then one computes that (Bhargava, (13)):

$$S(D) = \begin{cases} \mathbb{Z}[x]/(x^2) & D = 0 \\ \mathbb{Z} \times \mathbb{Z} & D \neq 0 \text{ is a square} \\ \mathbb{Z}[(D + \sqrt{D})/2] & \text{otherwise} \end{cases}$$

This is unique up to isomorphism. But the isomorphism is not canonical; the quadratic ring has a nontrivial automorphism. The remedy is define an oriented quadratic ring, which has one extra piece of data. Then we will obtain a bijection between discriminants and isomorphism classes of oriented quadratic rings, i.e.

Theorem 3 (Bhargava, Theorem 8)**.** *There is a one-to-one correspondence between the set of discriminants (i.e. integers congruent to* 0 *or* 1 *modulo* 4*) and the set of isomorphism classes of oriented quadratic rings, by the association*

$$D \leftrightarrow S(D)$$

where D is the discriminant of $S(D)$.

The reason we work with *oriented* quadratic rings is that then the objects in the equivalence class don't have automorphisms, so that given two such objects, there is a *unique* (hence canonical) isomorphism between them. This allows us to define multiplication of ideals without any ambiguity: if you have an ideal of one ring, you can canonically identify it as an ideal of another, and hence multiply by some ideal in that other ring. In other words, one needs to choose a square root in order to tell which of the two ideals $(1+\sqrt{D})$ or $(1-\sqrt{D})$ you are talking about.

From now on, we write $K = \mathbb{Q} \otimes S$.

3.2 Orientation of quadratic rings and bases

There's an isomorphism $\overline{\pi} : S/\mathbb{Z} \to \mathbb{Z}$ for each oriented quadratic ring, and this map changes (by the automorphism $1 \mapsto -1$ of $\mathbb{Z}$) when you change the orientation of your ring. Let σ be the non-trivial automorphism of S. Then define

$$\pi(x) = Tr(x/\sqrt{D}) = \frac{x - \sigma(x)}{\sqrt{D}}.$$

which has kernel $\mathbb{Z}$. One is only able to define this by choosing $\sqrt{D}$ to denote one of the two possible candidates in S. If we choose the other candidate, we alter this map by a sign. This also gives a notion of *oriented basis* for any rank two K-submodule of K. The basis $(1, \tau)$ of K is positively oriented if $\pi(\tau) > 0$. Other bases are oriented according to their relation to $(1, \tau)$: these two have the same orientation if and only if the change of basis matrix has determinant $+1$.

Note, for later, that with our choice of τ,

$$\pi(a + b\tau) = b.$$

3.3 Forms and Bhargava's GL_2 and SL_2 actions

Bhargava uses the notation $(\mathrm{Sym}^k \mathbb{Z}^n)^*$ for n-ary k-ic forms with coefficients in $\mathbb{Z}$. In particular, he will study binary quadratic forms as $(\mathrm{Sym}^2 \mathbb{Z}^2)^*$. He makes a remark about the use of *; Jonathan and I can't figure out how this corresponds to anything standard.

For the moment assume $D < 0$. Bhargava considers all negative and positive definite forms of a given discriminant together. This inflates the number of equivalence classes by a factor of two with respect to SL_2-equivalence (since a positive definite form cannot be changed to a negative definite form and vice versa).

For GL_2-equivalence (for all D), he will change the action so that one also multiplies by the determinant of the matrix. So, for example, the map $X \mapsto -X, Y \mapsto -Y$ takes the form $aX^2+bXY+cY^2$ to $-aX^2-bXY-cY^2$. Therefore, by considering GL_2-equivalence in this fashion for $D < 0$, he recovers the usual number of SL_2-equivalence classes of positive definite forms.

Bhargava writes $\mathrm{Cl}((\mathrm{Sym}^2 \mathbb{Z}^2)^*; D)$ for the SL_2-equivalence classes of forms of discriminant D. It is important to remember that for $D < 0$, this is twice the size one classically would mean by SL_2-equivalence classes.

3.4 Oriented ideals and the narrow class group

Definition 1. *An* oriented ideal *of S is a pair (I, ϵ) where I is a fractional ideal of S of rank two as $\mathbb{Z}$-module, and $\epsilon \in \{\pm 1\}$. Its* orientation *is ϵ. Two oriented ideals (I, ϵ) and (I', ϵ') are* equivalent *if $I = \kappa I'$ and $\epsilon = \mathrm{sign}(N(\kappa))\epsilon'$ for some $\kappa \in K^*$.*

Oriented ideals have a norm, defined as $|L/I| \cdot |L/S|^{-1}\epsilon(I)$, where L is any lattice in K containing S and I.

The *narrow class group* $\mathrm{Cl}^+(S)$ is defined as the set of invertible oriented ideals of S, with componentwise multiplication, modulo equivalence. It is most interesting for $D > 0$ where $N(\kappa)$ may be positive or negative. In the case of a quadratic imaginary field, (I, ϵ) and $(I, -\epsilon)$ are never equivalent, so that $\mathrm{Cl}^+(S) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{Cl}(S)$.

In the negative discriminant case, this is non-standard. But it lets us unify the two statements of the form-ideal correspondence.

3.5 Composition of forms

Now we can state the correspondence between forms and class groups in Bhargava's language. The first theorem is most general and includes, for example, non-invertible ideals and non-irreducible quadratic forms.

Theorem 4 (Bhargava I, Theorem 9)**.** *There is a canonical bijection between the set of nondegenerate $\mathrm{SL}_2(\mathbb{Z})$-orbits on the space $(\mathrm{Sym}^2 \mathbb{Z}^2)^*$ of integer-valued binary quadratic forms, and the set of isomorphism classes of pairs (S, I) where S is a non-degenerate oriented quadratic ring (i.e. non-zero discriminant) and I is a (not necessarily invertible) oriented ideal class of S. Under this bijection, the discriminant of a binary quadratic form equals the discriminant of the corresponding quadratic ring.*

In particular, if we restrict to the case we described classically, we have

Theorem 5 (Bhargava 1, Theorem 10)**.** *The above bijection restricts to a correspondence*

$$\mathrm{Cl}((\mathrm{Sym}^2 \mathbb{Z}^2)^*; D) \leftrightarrow \mathrm{Cl}^+(S(D)),$$

which is an isomorphism of groups.

He points out that if you want to use GL_2 equivalence (as modified by him), then you recover the regular class group.

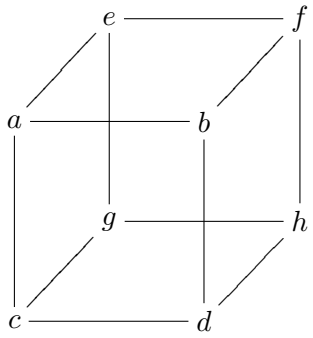
4 Bhargava's cubical perspective on the group law

4.1 Overview

Bhargava's cubes (really, elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$) are meant to represent instances of the group law. From each cube, one can extract three quadratic forms whose classes sum to zero. If one has three such classes, one can construct a Bhargava cube. In the end, he demonstrates this by finding an explicit bijection between cubes and triples of 'balanced ideals.' But the cubes in some sense give the definition of the group law on quadratic forms by 'bare hands,' instead of by transfer of structure. First we'll examine that perspective, before addressing the correspondence with ideals that provides a proof.

4.2 The Cubes

Bhargava represents elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ as cubes of eight integers:



meaning (where v_1, v_2 is the standard basis of $\mathbb{Z}^2$),

$$av_1 \otimes v_1 \otimes v_1 + bv_1 \otimes v_2 \otimes v_1 + cv_2 \otimes v_1 \otimes v_1 + dv_2 \otimes v_2 \otimes v_1$$

$$+ev_1 \otimes v_1 \otimes v_3 + fv_1 \otimes v_2 \otimes v_2 + gv_2 \otimes v_1 \otimes v_2 + hv_2 \otimes v_2 \otimes v_2.$$

We can slice the cube into two slices of bread in three possible ways:

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

or

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

or

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

He defines an action on such cubes by $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$. A matrix $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ in the ith factor of $\mathrm{SL}_2(\mathbb{Z})$ acts on the cube by replacing the bread slices M_i, N_i with $rM_i + sN_i$ and $tM_i + uN_i$. (That is, instead of row operations and column operations, we have bread slice operations.)

4.3 Interpreting cubes as triples of quadratic forms

Define

$$Q_i(x, y) = -\det(xM_i - yN_i).$$

Q_i is transformed to its SL_2-equivalent forms by the action of the i-th factor of SL_2. It is invariant under the SL_2 action by the other two factors of SL_2. One finds that the discriminant of all three forms are equal and preserved under the $\mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$ action.

Let's call any cube for which the three resultant forms are primitive a *projective cube*.

4.4 The composition of quadratic forms

Now we do the composition of quadratic forms by bare hands[2]: *Three equivalence classes of forms add to the trivial class if and only if they correspond to the three perspectives on some cube of eight integers.* In other words, take the free abelian group on primitive integral binary quadratic forms of a fixed discriminant D and take the quotient by all sums

$$Q_1 + Q_2 + Q_3$$

arising from any projective cube. We automatically identify forms with their equivalent forms, since for any equivalent forms Q_1 and Q_1', there exist cubes

[2]Gauss and Dirchlet etc. did this too, and the cube approach is not without precedent in their formulae, even if they didn't draw cubes. See Lemmermeyer's notes.

with $Q_2 = Q_2'$ and $Q_3 = Q_3'$. This law doesn't directly identify any forms with the identity. For example, consider a group of order 3, say $\mathbb{Z}/3\mathbb{Z}$. The group laws of the form $x + y + z = id$ are exactly

$$0 + 1 + 2 = id, \quad 0 + 0 + 0 = id, \quad 1 + 1 + 1 = id, \quad 2 + 2 + 2 = id$$

There's nothing to break the symmetry here[3]

However, we can choose as an identity any form Q_{id} which appears from all three perspectives on some cube. Taking the quotient by Q_{id}, we obtain a group. Bhargava shows that this gives a group law on equivalence classes (classes don't get identified further).

Bhargava demonstrates some such identity cubes which give exactly Gauss' version of composition.

The above group (with his choice of identity) is exactly $\mathrm{Cl}((\mathrm{Sym}^2 \mathbb{Z}^2)^*; D)$. In particular, this is made up only of classes of primitive forms. It will be proven by setting up a correspondence between cubes (not just projective[4] ones) with certain data on quadratic rings.

5 Cubes and triples of balanced ideals

Let $S = S(D)$ and write $K = \mathbb{Q} \otimes_{\mathbb{Z}} S$, i.e. S is a quadratic ring and K is its quadratic algebra (e.g. ring of integers and field of fractions). The way to the proof is through a correspondence between cubes and triples of so-called 'balanced' ideals (a proxy for ideals that sum to zero; in fact, it is just ideals that sum to zero in the ring of integers case, plus a consistency condition on which representatives we choose simultaneously).

5.1 Balanced ideals

Definition 2 (Bhargava, §3.3)**.** *A triple (I_1, I_2, I_3) of oriented ideals of S is* balanced *if $I_1 I_2 I_3 \subset S$ and $N(I_1)N(I_2)N(I_3) = 1$. Two such triples (I_1, I_2, I_3) and (I_1', I_2', I_3') are equivalent if $I_i = \kappa_i I_i'$ for some $\kappa_i \in K$. (Note that then $N(\kappa_1\kappa_2\kappa_3) = 1$.)*

In the case of ideals in a quadratic ring of integers, balance is equivalent to their product being trivial in the narrow class group and the representatives of the classes being chosen so that their norms multiply to 1. Remember that the norm involves the orientation.

[3] The same happens with elliptic curves: until you pick a point to serve as identity, you don't yet have a group.

[4] meaning all three of the associated forms are primitive

5.2 The main theorem

Write $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$.

Theorem 6 (Bhargava, Theorem 11)**.** *There is a canonical bijection between the set of nondegenerate Γ-orbits on the space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ of cubes, and the set of isomorphism classes of pairs $(S, (I_1, I_2, I_3))$, where S is a nondegenerate oriented quadratic ring and (I_1, I_2, I_3) is an equivalence class of balanced triples of oriented ideals of S. Under this bijection, the discriminant of an integer cube equals the discriminant of the corresponding quadratic ring.*

We'll now outline the proof. The correspondence is constructed explicitly.

5.3 Making a cube from balanced ideals

Let $S = \mathbb{Z} + \tau\mathbb{Z}$ as before. Choose integral bases (α_1, α_2), (β_1, β_2) and (γ_1, γ_2) for each of the ideals. The orientation of the basis is chosen to match the orientation of the ideals. We form a cube by writing (Bhargava, (15))

$$\alpha_i \beta_j \gamma_k = c_{ijk} + a_{ijk}\tau$$

and then a_{ijk} forms the cube! Another way to say this is that a cube corresponds to a trilinear mapping

$$I_1 \times I_2 \times I_3 \to \mathbb{Z}, (x, y, z) \mapsto \pi(xyz).$$

The cube is formed of the images under this map of the various tuples of basis elements, and therefore these 8 values determine the map by linearity.

The action of Γ on cubes corresponds exactly with the action of Γ on the bases of the three ideals.

Bhargava says equivalence on triples leaves the cube unchanged. This doesn't make a lot of sense to me, though, since the cube can change even if the triple of ideals doesn't, by picking a new basis. He probably means up to equivalence. But what if $\kappa_1 = i$, and $\kappa_2 = \kappa_3 = 1$ in $\mathbb{Z}[i]$. This swaps real and imaginary parts. How is it obvious the result is an equivalent cube?

5.4 Recovering the balanced ideals from their cube

Bhargava has already explained how to recover the ideals: take the quadratic forms obtained from each of the three perspectives. (Of course, I'm conflating forms with ideals already; in his paper he reproves Gauss composition as a consequence of his cubes and balanced ideals correspondence.) We'll

now show that this recovers the same ideals you put into your cube in the last section. This argument is not in Bhargava.

Consider the bilinear pairing

$$\mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}, \quad (a, b) \mapsto \pi(ab).$$

The Gram matrix of this pairing has determinant -1, with respect to an integral basis of $\mathcal{O}_K$. This pairing is very natural: it is the pairing

$$\mathcal{O}_K \times \mathcal{O}_K \to \bigwedge^2 \mathcal{O}_K, \quad (a, b) \mapsto a \wedge \overline{b}$$

This is because $\bigwedge^2 \mathcal{O}_K$ and $\mathcal{O}_K/\mathbb{Z}$ are isomorphic via $a \wedge b \mapsto \pi(a\overline{b})$ and $x \mapsto x \wedge 1$.

This pairing restricts to any pair of ideals $I_1 = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ and $I_2 = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2$, where we are choosing a basis oriented according to the orientation of the ideals. The resulting Gram matrix

$$\left(\pi(\alpha_i\beta_j)\right)_{i,j}.$$

has determinant $-N(I_1)N(I_2)$ (here, norm is the norm of oriented ideals). Let $\gamma \in \mathcal{O}_K$. Then the matrix

$$\left(\pi(\gamma\alpha_i\beta_j)\right)_{i,j}.$$

is exactly the pairing's Gram matrix when applied to $\gamma I_1 \times I_2$. Since I is taken to γI by a linear transformation of determinant $N(\gamma)$, this matrix has determinant

$$-N(\gamma)N(I_1)N(I_2).$$

The conclusion is this. Suppose we form a cube from balanced ideals I_1, I_2, I_3. If we write our third ideal $K = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$, then the matrix

$$X\left(\pi(\gamma_1\alpha_i\beta_j)\right)_{i,j} - Y\left(\pi(\gamma_2\alpha_i\beta_j)\right)_{i,j}$$

is exactly the pairing matrix for $(X\gamma_1 - Y\gamma_2)I_1 \times I_2$. It has determinant

$$-N(X\gamma_1 - Y\gamma_2)N(I_1)N(I_2) = -N(X\gamma_1 - Y\gamma_2)/N(I_3)$$

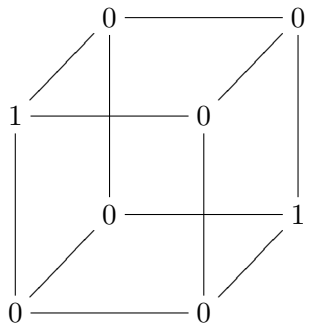
which is exactly the negative of the quadratic form for the ideal I_3. But this determinant is also the quadratic form Q_3 from the cube, by definition. Similarly, the oriented ideals I_1 and I_2 correspond to the forms Q_1 and Q_2.

In other words, if we form a cube from balanced ideals I_1, I_2 and I_3, then the quadratic forms Q_1, Q_2 and Q_3 defined from the cube recover the ideals.

5.5 All cubes give balanced ideals

From a given cube we can extract three quadratic forms. I propose to show that these are balanced. First, I will show that their product J is an integral ideal. From the cube, which has integer entries, and the fact that the products of the generators of the I_i span J over $\mathbb{Z}$, we see that $\pi(J) \subset \mathbb{Z}$. I claim that this is a necessary and sufficient condition for an ideal to be integral. If it is integral, this is immediate. If $\pi(J) \subset \mathbb{Z}$, but we have some $a + b\tau \notin S$, then it must be the case that $a \notin \mathbb{Z}$ and $b = \pi(a + b\tau) \in \mathbb{Z}$. But then $a\tau \in J$ has $\pi(a\tau) \notin \mathbb{Z}$.

The idea is to extend scalars to the quadratic algebra $K = \mathbb{Q} \otimes S$. When these are extended, the cube can be diagonalized, meaning, by an action of $\mathrm{SL}_2(K) \times \mathrm{SL}_2(K) \times \mathrm{SL}_2(K)$, we can put it in the form



corresponding to the three forms XY, XY, XY. Explicitly, find the two roots e_i, e_i' of Q_i. By assumption, that K-linear combination of the generators α_1, α_2 of I_1 has zero norm (here we are taking the norm on $K \otimes S$, meaning $N(x \otimes y) = x^2 \otimes y\sigma(y)$), i.e. $N(e_i \otimes \alpha_1 + e_i' \otimes \alpha_2) = 0$. A computation reveals that $e_i = \alpha_2$, $e_i' = -\alpha_1$, both in K. Therefore, under a suitable change of basis defined over K, the form becomes XY. Do this with each form Q_i, and then apply the appropriate changes of basis in the corresponding factors of $\mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$. The result is the cube above (this is a straightforward computation).

Write $x = \alpha_2 \otimes \alpha_1 - \alpha_1 \otimes \alpha_2$, which is an element of norm zero. In fact, it is what I'll call 'left-zero'. In other words, under the isomorphism

$$K \otimes K \simeq K \times K, \quad a \otimes b \mapsto (ab, a\sigma(b)),$$

the left coordinate is zero. This implies the norm is zero.

It is a computation to verify that $\pi(x) = -N(I_1)$. Similarly, define y and z for the other two ideals, and find that $\pi(y) = -N(I_2)$ and $\pi(z) = -N(I_3)$.

In fact (although π is not in general multiplicative), one can compute that it is multiplicative on elements that are left-zero. Therefore,

$$1 = \pi(xyz) = -N(I_1)N(I_2)N(I_3)$$

from which we conclude that the ideals are balanced! Except for a sign?

This would need to be extended to the non ring-of-integers case, but with that accomplished, this provides a new proof of Bhargava's main bijection that is much less computational.

5.6 Cubes have a group law

Balanced triples come with a group law (coordinatewise). We restrict to projective modules. The resulting group is isomorphic to

$$\mathrm{Cl}^+(S) \times \mathrm{Cl}^+(S)$$

by $(I_1, I_2, I_3) \mapsto (I_1, I_2)$. The correspondence of Bhargava's theorem then gives us a group law on cubes.

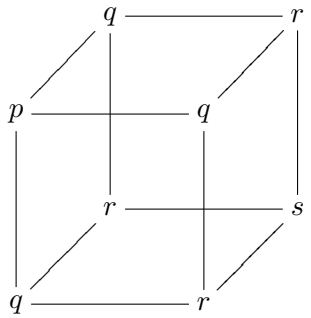
Theorem 7 (Bhargava, Theorem 12)**.**

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \simeq \mathrm{Cl}^+(S(D)) \times \mathrm{Cl}^+(S(D)).$$

Bhargava uses these theorems to recover the usual correspondence between forms and ideals in the classical case.

6 Binary cubic forms

A binary cubic form $px^3 + 3qx^2y + 3rxy^2 + sy^3$ can be associated to a cube



The association is that a cubic form is the diagonal of a trilinear form in much the same way a quadratic form is the diagonal of a bilinear form. In

other words, starting by viewing a *symmetric* cube as a *symmetric* trilinear form

$$\phi : \mathbb{Z}^2 \times \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}$$

we get a new cubic form:

$$\overline{\phi} : \mathbb{Z}^2 \to \mathbb{Z}$$

by

$$\overline{\phi}(x) = \phi(x, x, x).$$

Symmetry isn't required for this construction, but if we require symmetry then this construction has an inverse, given explicitly by

$$\phi(x, y, z) = \frac{1}{6}\left(\overline{\phi}(x + y + z) - \overline{\phi}(x + y) - \overline{\phi}(y + z) - \overline{\phi}(z + x) + \overline{\phi}(x) + \overline{\phi}(y) + \overline{\phi}(z)\right).$$

For ϕ to have integer coefficients, the interior coefficients of the cubic form must be divisible by 3. The fact that k-ic quadratic forms are in bijection with symmetric k-linear forms (at least over a field) is called *polarization*. At any rate, this inverse is an inclusion from binary cubic forms given in the form above (with interior coefficients divisible by 3), into cubes:

$$\mathrm{Sym}^3 \mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$$

A cubic form is projective if its cube is so.

Note a footnote[5].

Theorem 8 (Bhargava, Theorem 13)**.** *SL_2 orbits of* $\mathrm{Sym}^3 \mathbb{Z}^2$ *are in bijection with equivalence classes of (S, I, δ) where S is a nondegenerate oriented quadratic ring, I is an ideal of S, and δ is an invertible element of $S \otimes \mathbb{Q}$ such that $I^3 \subseteq \delta \cdot S$ and $N(I)^3 = N(\delta)$. The discriminant of the cubic form class is the discriminant of S.*

Equivalence: $(S, I, \delta) \sim (\phi(S), \kappa\phi(I), \kappa^3\phi(\delta))$ where ϕ is an isomorphism of oriented quadratic rings and $\kappa \in \mathbb{Q} \otimes \phi(S)$.

As a result, we have the following, concerning the 3-part Cl_3 of the class group:

[5]Bhargava writes $\mathrm{Sym}^3 \mathbb{Z}^2$ for cubic binary forms, but as far as I can tell (in consultation with Jonathan), this ought to be $\mathrm{Sym}^3((\mathbb{Z}^2)^*)$. Then symmetric trilinear forms would be $(\mathrm{Sym}^3(\mathbb{Z}^2))^*$, which is isomorphic, almost (it depends whether you require the interior coefficients of the form to be divisible by 3). Bhargava seems to have this backwards from what I'm suggesting here, and I don't understand why.

Theorem 9 (Bhargava, Corollary 14)**.** *There's a surjective group homomorphism*

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

Namely, the form goes to the module I in the corresponding triple $(S(D), I, \delta)$. The kernel has cardinality $|U/U^3|$ where U is the unit group of $S(D)$.

This recovers a classical number theory fact if we are in the case of a ring of integers (Bhargava, Corollary 15).

6.1 The explicit bijection

Suppose $\eta^3 = \delta$. If one takes

$$I_1, I_2, I_3 = \frac{1}{\eta}(\alpha\mathbb{Z} + \beta\mathbb{Z}),$$

then one obtains this bijection from the bijection of cubes with balanced ideals. The problem is that δ needn't be a cube, but this can be dealt with. The cubic form then is the map

$$C : I \to \mathbb{Z}, \quad \zeta \mapsto \pi(\zeta^3).$$

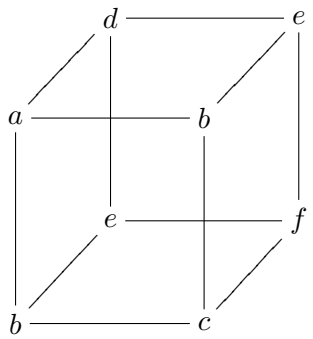
This doesn't appear to have a δ in it, but recall that $I^3 \subset \delta S$ and $N(I)^3 = N(\delta)$ (in other words, we don't have free choice on δ once I is determined).

7 Pairs of binary quadratic forms

We write $\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2$ for pairs of binary quadratic forms. Here we require the middle coefficient to be even, i.e. these are really symmetric bilinear forms over $\mathbb{Z}$.

Theorem 10 (Bhargava, Theorem 16)**.** *There is a canonical bijection between the set of nondegenerate $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ orbits on $\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^2$, and the set of isomorphism classes of balanced triples $(S, (I_1, I_2, I_3))$ where $I_2 = I_3$. Discriminants correspond.*

Taking $I_2 = I_3$ imposes a symmetry on the cube:



In other words, slicing in the correct of the three dimensions, one obtains two symmetric matrices: these are the two symmetric bilinear forms giving the quadratic forms. The identity pair for $D \equiv 0 \pmod 4$ is

$$2xy, \quad x^2 + \frac{D}{4}y^2.$$

The equivalence classes of projective cubes with this symmetry form a group

$$\mathrm{Cl}^+(\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}; D)$$

There's an isomorphism

$$\mathrm{Cl}^+(\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}; D) \to \mathrm{Cl}^+((\mathrm{Sym}^2 \mathbb{Z}^2)^*; D).$$

This is obtained by taking the cube to one of the associated quadratic forms. In fact, a cube with this sort of symmetry will have $Q_2 = Q_3$, so we take it to $Q_2 = Q_3$ (instead of Q_1)[6].

8 Pairs of quaternary alternating 2-forms

8.1 How a cube is a pair of alternating forms

Closely following Bhargava, section 2.6.

A quaternary alternating 2-form is an alternating form in four variables, meaning elements of $\wedge^2\mathbb{Z}^4$, or maps

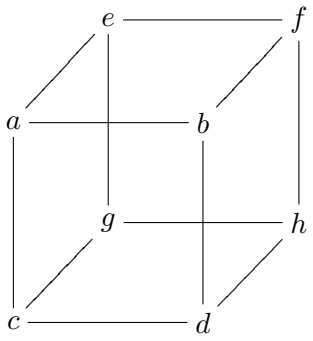
$$B : \mathbb{Z}^4 \times \mathbb{Z}^4 \to \mathbb{Z}$$

[6]Think about this in the case where balanced really means product equal to (1): then Q_1 is always associated to a square ideal, so you wouldn't get the whole class group.

having the property that B is linear in each coordinate and

$$B(u,u) = 0, \text{ equivalently, } B(u,v) = -B(v,u)$$

(alternating is the same as skew-symmetric when characteristic is not 2). Hence an alternating 2-form is given by a matrix with skew-symmetry ($A^T = -A$). Here's a way to see a cube as a pair of quaternary alternating 2-forms (Bhargava, equation (10)):



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

It is apparent that one may not realize all possible pairs of forms this way (since the forms in the equation always have 8 zero entries, for example). However, Bhargava assures us that every pair of forms is equivalent to a pair in this shape.

Here's how the cube gives a form in a more algebraic way. View a cube as a trilinear map, as before:

$$\phi : L_1 \times L_2 \times L_3 \rightarrow \mathbb{Z}$$

where L_i are rank 2 $\mathbb{Z}$-modules. We build from this a different $\mathbb{Z}$-trilinear map:

$$\overline{\phi} : L_1 \times (L_2 \oplus L_3) \times (L_2 \oplus L_3) \rightarrow \mathbb{Z}$$

according to the formula

$$\overline{\phi}(r,(s,t),(u,v)) = \phi(r,s,v) - \phi(r,u,t).$$

This is skew-symmetric in the second and third variables. This map $\phi \rightarrow \overline{\phi}$ is actually a map

$$id \otimes \wedge_{2,2} : \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \wedge^2(\mathbb{Z}^2 \oplus \mathbb{Z}^2) = \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4,$$

taking cubes to pairs of alternating forms.

8.2 Actions on cubes and pairs of forms

Two pairs of forms, i.e. elements of $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$, are equivalent if they are in the same $\Gamma' = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$ orbit, i.e. change of variables on the forms themselves, together with replacement by unimodular linear combinations of the forms (i.e. we are really considering the span of the two forms; change of basis in this space).

With Γ as before acting on cubes, the action will take a pair of forms to an equivalent pair. Bhargava shows that the map from cubes to forms is surjective onto the Γ' orbits. We call the image of a projective cube, and all its equivalent pairs, projective.

8.3 Discriminants

The space $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ has a unique polynomial invariant for the action of Γ', called the discriminant. Specifically, it is

$$\mathrm{Disc}(\mathrm{Pfaff}(Mx - Ny))$$

where (M, N) is the pair of alternating matrices[7].

This discriminant is the same as that of the cube the pair came from.

Denote the collection of projective pairs of discriminant D by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D)$.

8.4 The main bijection

Theorem 11 (Bhargava, Theorem 17)**.** *There is a canonical bijection between the set of nondegernate Γ' orbits on $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ and the set of isomorphism classes of pairs $(S, (I, M))$ where S is a nondegenerate oriented quadratic ring, (I, M) is an equivalence class of balanced pairs of oriented ideals of S having ranks 1 and 2 respectively. Discriminants correspond.*

Some clarification on terminology is in order here. A rank n ideal of S is a rank $2n$ $\mathbb{Z}$-module contained as an S-submodule in K^n. Equivalence is isomorphism as S-modules (the isomorphisms are elements of $\mathrm{GL}_n(K)$). These can also be oriented.

The notion of *balanced* (ranks can be mixed, i.e. M_i has rank n_i etc.) is:

$$\mathrm{Det}(M_1) \cdots \mathrm{Det}(M_k) \subset S, \quad N(M_1) \cdots N(M_k) = 1$$

[7]The Pfaffian is the square root of the determinant, where sign is chosen so that $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ has positive Pfaffian

This requires explaining Norm and Det, which we will do in a moment. Equivalence of balanced k-tuples is as before – elements λ_i of $\mathrm{GL}_{n_i}(K)$ taking M_i to M_i'. This entails that the determinants of the λ_i have a product of norm 1.

Norm is $|L/M| \cdot |L/S|^{-1}\epsilon(M)$ where ϵ is the orientation, and L is any lattice of K^n containing S^n and M. (Bhargava gives this definition for ideals, i.e. rank one ideals; it is equivalent to what you think, but lets you define things for fractional ideals without passing to integral ideals.)

The map Det takes ideals of rank n to ideals of rank 1. If M has rank n, then for every n-tuple $(x_1, \ldots, x_n) \in M^n$, we can write $\det(x_1, \ldots, x_n)$ in terms of usual map

$$\det : (K^n)^n \to K.$$

The ideal Det is the ideal generated by all $\det(x_1, \ldots, x_n)$.

We obtain an isomorphism of groups

Theorem 12 (Bhargava, Theorem 6)**.**

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D) \to \mathrm{Cl}((\mathrm{Sym}^4 \mathbb{Z}^2)^*; D)$$

8.5 The correspondence

The map

$$id \otimes \wedge_{2,2} : \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$$

corresponds through the correspondence of Bhargava's Theorem 17 with

$$(S, (I_1, I_2, I_3)) \mapsto (S, (I_1, I_2 \oplus I_3)).$$

The isomorphism of groups comes from the map

$$(S, (I, M)) \mapsto (S, I)$$

on the side of ideals[8]. On the side of forms, it is

$$(M, N) \mapsto -\mathrm{Pfaff}(Nx - My).$$

[8]Bhargava uses a cancellation theorem of Serre to show that $(S, (I, M))$ is always of the form $(S, (I, S \oplus I^{-1}))$.

9 Senary alternating 3-forms

In other words, alternating AKA skew-symmetric trinary forms in six variables. Again, we take a trilinear map

$$\phi : L_1 \times L_2 \times L_3 \to \mathbb{Z},$$

and construct a new trilinear map

$$\overline{\phi} : (L_1 \oplus L_2 \oplus L_3)^3 \to \mathbb{Z}$$

according to the formula

$$\overline{\phi}((r_1, r_2, r_3), (s_1, s_2, s_3), (t_1, t_2, t_3)) = \mathrm{Det}_\phi(r, s, t) := \sum_{\sigma \in S_3} (-1)^\sigma \phi(r_{\sigma(1)}, s_{\sigma(2)}, t_{\sigma(3)}).$$

This map $\phi \mapsto \overline{\phi}$ corresponds to

$$\wedge_{2,2,2} : \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \to \wedge^3(\mathbb{Z}^2 \oplus \mathbb{Z}^2 \oplus \mathbb{Z}^2) = \wedge^3 \mathbb{Z}^6.$$

The action on the latter is $\mathrm{SL}_6(\mathbb{Z})$ and as in the last case, $\wedge_{2,2,2}$ is surjective on equivalence classes. Again, one unique polynomial invariant called the *discriminant* (same as that of cube under this map). Again, projective means coming from a projective cube.

We get

$$\mathrm{Cl}(\wedge^3 \mathbb{Z}^6; D)$$

but it turns out to be always trivial! For fundamental discriminants, all forms are projective so there's only one form up to $\mathrm{SL}_6(\mathbb{Z})$-equivalence.

Theorem 13 (Bhargava, Theorem 18)**.** *There is a canonical bijection between the set of nondegenerate* $\mathrm{SL}_6(\mathbb{Z})$*-orbits on the space* $\wedge^3 \mathbb{Z}^6$ *and the set of isomorphism classes of pairs* (S, M) *where* S *is a nondegenerate oriented quadratic ring and* M *is an equivalence class of balanced ideals of* S *having rank* 3*. Discriminants correspond.*

Under the correspondence, turning a cube into a form corresponds to

$$(S, (I_1, I_2, I_3)) \mapsto (S, I_1 \oplus I_2 \oplus I_3).$$

Bhargava calls this 'fusing' the three rank 1 ideals into a rank 3 ideal.