Rings of small rank over a Dedekind domain and their ideals

SENIOR THESIS

Evan O'Dorney
emo916math@gmail.com, (925)998-0239
Advisor: Benedict Gross

July 4, 2015

1 Introduction

The mathematics that we will discuss has its roots in the investigations of classical number theorists—notably Fermat, Lagrange, Legendre, and Gauss (see [8], Ch. I)—who were interested in what integers are represented by expressions such as $x^2 + ky^2$, for fixed k. It became increasingly clear that in order to answer one such question, one had to understand the general behavior of expressions of the form

$$ax^2 + bxy + cy^2.$$

These expressions are now called binary quadratic forms. It was Gauss who first discovered that, once one identifies forms that are related by a coordinate change $x \mapsto px + qy, y \mapsto rx + sy$ (where $ps - qr = 1$), the forms whose *discriminant* $D = b^2 - 4ac$ has a fixed value and which are *primitive*, that is, $\gcd(a, b, c) = 1$, can be naturally given the structure of an abelian group, which has the property that if forms ϕ_1, ϕ_2 represent the numbers n_1, n_2, then their product $\phi_1 * \phi_2$ represents $n_1 n_2$. This group law $*$ is commonly called *Gauss composition.*

Gauss's construction of the product of two forms was quite ad hoc. Since Gauss's time, mathematicians have discovered various reinterpretations of the composition law on binary quadratic forms, notably:

- Dirichlet, who discovered an algorithm simplifying the understanding and computation of the product of two forms, which we will touch on in greater detail (see Example 5.8).
- Dedekind, who by introducing the now-standard notion of an ideal, transformed Gauss composition into the simple operation of multiplying two ideals in a quadratic ring of the form $\mathbb{Z}[(D + \sqrt{D})/2]$;
- Bhargava, who in 2004 astounded the mathematical community by deriving Gauss composition from simple operations on a $2 \times 2 \times 2$ cube [1].

In abstraction, Bhargava's reinterpretation is somewhat intermediate between Dirichlet's and Dedekind's: it shares the integer-based concreteness of Gauss's original investigations, yet it also corresponds to natural constructions in the realm of ideals. One of the highlights of Bhargava's method is that it extends to give group structures on objects beyond binary quadratic forms, hence the title of his paper series, "Higher composition laws." It also sheds light on previously inaccessible conjectures about Gauss composition, such as an estimate for the number of forms of bounded discriminant whose third power is the identity [7].

A second thread that will be woven into this thesis is the study of finite ring extensions of $\mathbb{Z}$, often with a view toward finite field extensions of $\mathbb{Q}$. Quadratic rings (that is, those having

a $\mathbb{Z}$-basis with just two elements) are simply and classically parametrized by a single integer invariant, the *discriminant*. For cubic rings, Delone and Faddeev prove a simple lemma (as one of many tools for studying irrationalities of degree 3 and 4 over $\mathbb{Q}$) parametrizing them by binary cubic forms ([9], pp. 101ff). A similar classification for quartic and higher rings proved elusive until Bhargava, using techniques inspired by representation theory, was able to parametrize quartic and quintic rings together with their cubic and sextic *resolvent* rings, respectively, and thereby compute the asymptotic number of quartic and quintic rings and fields with bounded discriminant [3, 4, 5, 6]. The analytic virtue of Bhargava's method is to map algebraic objects such as rings and ideals to lattice points in bounded regions of $\mathbb{R}^n$, where asymptotic counting is much easier. (Curiously enough, the ring parametrizations seem to reach a natural barrier at degree 5, in contrast to the classical theory of solving equations by radicals where degree 4 is the limit.)

In this thesis, we will focus on two parametrizations that are representative of Bhargava's algebraic techniques in general. The first is the one that generalizes Gauss composition by parametrizing triples (I_1, I_2, I_3) of fractional ideals in a quadratic ring satisfying a condition Bhargava calls being *balanced* by $2 \times 2 \times 2$ boxes of integers. We take some time to explore this balancing condition through theorems and examples. The second parametrization we will focus on is that of quartic rings by pairs of ternary quadratic forms, that is, pairs $(f(x, y, z), g(x, y, z))$ where f and g are quadratic, up to coordinate changes in both the inputs and the outputs.

Bhargava published these results over the integers $\mathbb{Z}$. Since then, experts have wondered whether his techniques apply over more general classes of rings; by far the most ambitious extensions of this sort are Wood's classifications of quartic algebras [13] and ideals in certain n-ic algebras [14] over an arbitrary base scheme S. In this thesis we prove the two aforementioned parametrizations over a Dedekind domain R. The use of a Dedekind domain has the advantage of remaining relevant to the original application (counting number fields and related structures) while introducing some new generality. In particular we find that R may have characteristic 2, the frequent factors of $1/2$ in Bhargava's expositions notwithstanding, and certain appearances of the units $R^\times$ illuminate the shadowy but crucial role of the group $\mathbb{Z}^\times = \{\pm 1\}$ in the corresponding $\mathbb{Z}$-parametrizations.

The remainder of the thesis is structured as follows. In section 2, we set up basic definitions concerning projective modules over a Dedekind domain. In sections 3 and 4, respectively, we generalize to Dedekind base rings two classical parametrizations, namely of quadratic algebras over $\mathbb{Z}$ and of their ideals. In section 5, we prove Bhargava's parametrization of balanced ideal triples (itself a generalization of Gauss composition) over a Dedekind domain. In section 6, we work out in detail a specific example—unramified extensions of $\mathbb{Z}_p$—that allows us to explore the notion of balanced ideal triple in depth. Finally, in sections 7 and 8, we tackle cubic and quartic algebras respectively.

2 Modules and algebras over a Dedekind domain

A *Dedekind domain* is an integral domain that is Noetherian, integrally closed, and has the property that every nonzero prime ideal is maximal. The standard examples of Dedekind domains are the ring of algebraic integers $\mathcal{O}_K$ in any finite extension K of $\mathbb{Q}$; in addition, any field and any principal ideal domain (PID), such as the ring $\mathbb{C}[x]$ of polynomials in one variable, is Dedekind. In this section, we summarize properties of Dedekind domains that we will find useful; for more details, see [10], pp. 9–18.

The salient properties of Dedekind domains were discovered through efforts to generalize prime factorization to rings beyond $\mathbb{Z}$; in particular, every nonzero ideal $\mathfrak{a}$ in a Dedekind domain R is expressible as a product $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ of primes, unique up to ordering. Our motivation for using Dedekind domains stems from two other related properties. Recall that a *fractional ideal* or simply an *ideal* of R is a finitely generated nonzero R-submodule of the fraction field K of

R, or equivalently, a set of the form $a\mathfrak{a}$ where $\mathfrak{a} \subseteq R$ is a nonzero ideal and $a \in K^\times$. (The term "ideal" will from now on mean "(nonzero) fractional ideal"; if we wish to speak of ideals in the ring-theoretic sense, we will use a phrasing such as "ideal $\mathfrak{a} \subseteq R$.") The first useful property is that any fractional ideal $\mathfrak{a} \subseteq K$ has an inverse $\mathfrak{a}^{-1}$ such that $\mathfrak{a}\mathfrak{a}^{-1} = R$. This allows us to form the group $I(R)$ of nonzero fractional ideals and quotient by the group $K^\times/R^\times$ of principal ideals to obtain the familiar *ideal class group,* traditionally denoted $\operatorname{Pic} R$. (For the ring of integers in a number field, the class group is always finite; for a general Dedekind domain this may fail, e.g. for the ring $\mathbb{C}[x,y]/(y^2-(x-a_1)(x-a_2)(x-a_3))$ of functions on a punctured elliptic curve.)

The second property that we will find very useful is that modules over a Dedekind domain are classified by a simple theorem generalizing the classification of finitely generated abelian groups. For our purposes it suffices to discuss torsion-free modules, which we will call lattices.

Definition 2.1. Let R be a Dedekind domain and K its field of fractions. A *lattice* over R is a finitely generated, torsion-free R-module M. If M is a lattice, we will denote by the subscript M_K its K-span $M \otimes_R K$ (except when M is denoted by a symbol containing a subscript, in which case a superscript will be used). The dimension of M_K over K is called the *rank* of the lattice M.

A lattice of rank 1 is a nonzero finitely generated submodule of K, i.e. an ideal; thus isomorphism classes of rank-1 lattices are parametrized by the class group $\operatorname{Pic} R$. The situation for general lattices is not too different.

Theorem 2.2 (see [10], Lemma 1.5, Theorem 1.6, and the intervening Remark)**.** *A lattice M over R is classified up to isomorphism by two invariants: its rank m and its top exterior power $\Lambda^m M$. Equivalently, every lattice is a direct sum $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ of nonzero ideals, and two such direct sums $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$, $\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_n$ are isomorphic if and only if $m = n$ and the products $\mathfrak{a}_1 \cdots \mathfrak{a}_m$ and $\mathfrak{b}_1 \cdots \mathfrak{b}_n$ belong to the same ideal class.*

In this thesis we will frequently be performing multilinear operations on lattices. Using the classification theorem, it is easy to show that these operations behave much more "tamely" than for modules over general rings. Specifically, for two lattices $M = \mathfrak{a}_1 u_1 \oplus \cdots \oplus \mathfrak{a}_m u_m$ and $N = \mathfrak{b}_1 v_1 \oplus \cdots \oplus \mathfrak{b}_n v_n$, we can form the following lattices:

- the tensor product
$$M \otimes N = \bigoplus_{\substack{1 \le i \le m \\ 1 \le j \le n}} \mathfrak{a}_i \mathfrak{b}_j (u_i \otimes v_j);$$
- the symmetric powers
$$\operatorname{Sym}^k M = \bigoplus_{1 \le i_1 \le \cdots \le i_k \le m} \mathfrak{a}_{i_1} \cdots \mathfrak{a}_{i_k} (u_{i_1} \otimes \cdots \otimes u_{i_k})$$
and the exterior powers
$$\Lambda^k M = \bigoplus_{1 \le i_1 < \cdots < i_k \le m} \mathfrak{a}_{i_1} \cdots \mathfrak{a}_{i_k} (u_{i_1} \wedge \cdots \wedge u_{i_k})$$
of ranks $\binom{n+k-1}{k}$ and $\binom{n}{k}$ respectively;
- the dual lattice
$$M^* = \operatorname{Hom}(M, R) = \bigoplus_{1 \le i \le m} \mathfrak{a}_i^{-1} u_i^*;$$

- and the space of homomorphisms

$$\mathrm{Hom}(M,N) \cong M^* \otimes N = \bigoplus_{\substack{1\le i\le m\\ 1\le j\le n}} \mathfrak{a}_i^{-1}\mathfrak{b}_j(u_i^* \otimes v_j).$$

A particular composition of three of these constructions is of especial relevance to the present thesis:

Definition 2.3. If M and N are lattices, then a degree-k *map* $\phi : M \to N$ is an element of $(\mathrm{Sym}^k M^*) \otimes N$. A map to a lattice N of rank 1 is called a *form*.

In terms of the decompositions $M = \mathfrak{a}_1 u_1 \oplus \cdots \oplus \mathfrak{a}_m u_m$ and $N = \mathfrak{b}_1 v_1 \oplus \cdots \oplus \mathfrak{b}_n v_n$, a degree-$k$ map can be written in the form

$$\phi(x_1u_1 + \cdots + x_mu_m) = \sum_{j=1}^{n} \sum_{i_1+\cdots+i_m=k} a_{i_1,\ldots,i_m,j} \cdot x_1^{i_1} \cdots x_m^{i_m} v_j,$$

where the coefficients $a_{i_1,\ldots,i_m,j}$ belong to the ideals $\mathfrak{a}_1^{-i_1} \cdots \mathfrak{a}_m^{-i_m}\mathfrak{b}_j$ needed to make each term's value belong to N. For example, over $R = \mathbb{Z}$, a quadratic map from $\mathbb{Z}^2$ to $\mathbb{Z}$ is a quadratic expression

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

in the coordinates $x, y \in (\mathbb{Z}^2)^*$ on $\mathbb{Z}^2$. Three caveats about this notion are in order:

- Although such a degree-k map indeed yields a function from M to N, it need not be unambiguously determined by this function if R is finite. For instance, if $R = \mathbb{F}_2$ is the field with two elements, the cubic map from $\mathbb{F}_2^2$ to $\mathbb{F}_2$ defined by $\phi(x,y) = xy(x+y)$ vanishes on each of the four elements of $\mathbb{F}_2^2$, though it is not the zero map.
- A degree-k map from M to a lattice containing N whose values lie in N need not be a degree-k map from M to N. For instance,

  $$f(x,y) = \frac{xy(x+y)}{2}$$

  is a cubic map from $\mathbb{Z}^2$ to $\frac{1}{2}\mathbb{Z}$ but not to $\mathbb{Z}$, although it outputs an integer for each pair of integers (x,y).
- Also, one must not confuse $(\mathrm{Sym}^k M^*) \otimes N$ with the space $(\mathrm{Sym}^k M)^* \otimes N$ of symmetric k-ary multilinear functions from M to N. Although both lattices have rank $n\binom{m+k-1}{k}$ and there is a natural map from one to the other (defined by evaluating a multilinear function on the diagonal), this map is not in general an isomorphism. For instance, the quadratic forms $\phi : \mathbb{Z}^2 \to \mathbb{Z}$ arising from a symmetric bilinear form $\lambda((x_1,y_1),(x_2,y_2)) = ax_1x_2 + b(x_1y_2 + x_2y_1) + cy_1y_2$ are exactly those of the form $\phi(x,y) = ax^2 + 2bxy + cy^2$, with middle coefficient even.

2.1 Algebras

An *algebra of rank* n over R is a lattice S of rank n equipped with a multiplication operation giving it the structure of a (unital commutative associative) R-algebra. Since R is integrally closed, the sublattice generated by $1 \in S$ must be primitive (that is, the lattice it generates is maximal for its dimension, and therefore a direct summand of S), implying that the quotient S/R is a lattice of rank $n-1$ and we have a noncanonical decomposition

$$S = R \oplus S/R. \tag{1}$$

We will be concerned with algebras of ranks 2, 3, and 4, which we call quadratic, cubic, and quartic algebras (or rings) respectively.

2.2 Orientations

When learning about Gauss composition over $\mathbb{Z}$, one must sooner or later come to a problem that vexed Legendre (see [8], p. 42): If one considers quadratic forms up to $\mathrm{GL}_2\mathbb{Z}$-changes of variables, then a group structure does not emerge because the conjugate forms $ax^2 \pm bxy + cy^2$, which ought to be inverses, have been identified. Gauss's insight was to consider forms only up to "proper equivalence," i.e. $\mathrm{SL}_2\mathbb{Z}$ coordinate changes. This is tantamount to considering quadratic forms not simply on a rank-2 $\mathbb{Z}$-lattice M, but on a rank-2 $\mathbb{Z}$-lattice equipped with a distinguished generator of its top exterior power $\Lambda^2 M$. For general lattices over Dedekind domains, whose top exterior powers need not belong to the principal ideal class, we make the following definitions.

Definition 2.4. Let $\mathfrak{a}$ be a fractional ideal of R. A rank-n lattice M is of *type* $\mathfrak{a}$ if its top exterior power $\Lambda^n M$ is isomorphic to $\mathfrak{a}$; an *orientation* on M is then a choice of isomorphism $\alpha : \Lambda^n M \to \mathfrak{a}$. The possible orientations on any lattice M are of course in noncanonical bijection with the units $R^\times$. The easiest way to specify an orientation on M is to choose a decomposition $M = \mathfrak{b}_1 u_1 \oplus \cdots \oplus \mathfrak{b}_n u_n$, where the ideals $\mathfrak{b}_i$ are scaled to have product $\mathfrak{a}$, and then declare

$$\alpha(y_1 u_1 \wedge \cdots \wedge y_n u_n) = y_1 \cdots y_n.$$

An orientation on a rank-n R-algebra S is the same as an orientation on the lattice S, or equivalently on the lattice S/R, due to the isomorphism between $\Lambda^n S$ and $\Lambda^{n-1} S/R$ given by

$$1 \wedge v_1 \wedge \cdots \wedge v_{n-1} \mapsto \tilde{v}_1 \wedge \cdots \wedge \tilde{v}_{n-1}.$$

(Here, and henceforth, we use a tilde to denote the image under the quotient map by R, so that the customary bar can be reserved for conjugation involutions. This is opposite to the usual convention where $\tilde{v}$ denotes a lift of v under a quotient map.)

3 Quadratic algebras

Before proceeding to Bhargava's results, we lay down as groundwork two parametrizations that, over $\mathbb{Z}$, were known classically. These are the parametrizations of quadratic algebras and of ideal classes in quadratic algebras. The extension of these to other base rings has been thought about extensively, with many different kinds of results produced (see [12] and the references therein). Here, we prove versions over a Dedekind domain that parallel our cubic and quartic results.

Let S be a quadratic algebra over R. Since S/R has rank 1, the decomposition (1) simplifies to $S = R \oplus \mathfrak{a}\xi$ for an (arbitrary) ideal $\mathfrak{a}$ in the class of $\Lambda^2 S$ and some formal generator $\xi \in S_K$. The algebra is then determined by $\mathfrak{a}$ and a multiplication law $\xi^2 = t\xi - u$, which allows us to describe the ring as $R[\mathfrak{a}\xi]/(\mathfrak{a}^2(\xi^2 - t\xi + u))$, a subring of $K[\xi]/(\xi^2 - t\xi + u)$. Alternatively, we can associate to the ring its norm map

$$N_{S/R} : S \to R, \quad x + y\xi \mapsto x^2 + txy + uy^2.$$

It is evident that this is just another way of packaging the same data, namely two numbers $t \in \mathfrak{a}^{-1}$ and $u \in \mathfrak{a}^{-2}$. The norm map is more readily freed from coordinates than the multiplication table, yielding the following parametrization.

Lemma 3.1. *Quadratic algebras over R are in canonical bijection with rank-2 R-lattices M equipped with a distinguished copy of R and a quadratic form $\phi : M \to R$ that acts as squaring on the distinguished copy of R.*

Proof. Given M and ϕ, the distinguished copy of R must be primitive (otherwise ϕ would take values outside R), yielding a decomposition $M = R \oplus \mathfrak{a}\xi$. Write ϕ in these coordinates as

$$\phi(x + y\xi) = x^2 + txy + uy^2;$$

then the values $t \in \mathfrak{a}^{-1}$ and $u \in \mathfrak{a}^{-2}$ can be used to build a multiplication table on M having the desired norm form (which is unique, as for any fixed coordinate system, the norm form determines t and u, which determine the multiplication table). ■

If there is a second copy of R on which $N_{S/R}$ restricts to the squaring map, it must be generated by a unit of S with norm 1, multiplication by which induces an automorphism of the lattice with norm form. Hence we can eliminate the distinguished copy of R and arrive at the following arguably prettier parametrization:

Theorem 3.2. *Quadratic algebras over R are in canonical bijection with rank-2 R-lattices M equipped with a quadratic form $\phi : M \to R$ attaining the value 1.*

For our applications to Gauss composition it will also be helpful to have a parametrization of *oriented* quadratic algebras. An orientation $\alpha : \Lambda^2 R \to \mathfrak{a}$ can be specified by choosing an element ξ with $\alpha(1 \wedge \xi) = 1$. Since ξ is unique up to translation by $\mathfrak{a}^{-1}$, the parametrization is exceedingly simple.

Theorem 3.3. *For each ideal $\mathfrak{a}$ of R, there is a canonical bijection between oriented quadratic algebras of type $\mathfrak{a}$ and pairs (t, u), where $t \in \mathfrak{a}^{-1}$, $u \in \mathfrak{a}^{-2}$, up to the action of $\mathfrak{a}^{-1}$ via*

$$s.(t, u) = (t + 2s, u + st + s^2)$$

One other fact that will occasionally be useful is that every quadratic algebra has an involutory automorphism defined by $\bar{x} = \operatorname{Tr} x - x$ or, in a coordinate representation

$$S = R[\mathfrak{a}\xi]/(\mathfrak{a}^2(\xi^2 - t\xi + u)),$$

by $\xi \mapsto t - \xi$. (The first of these characterizations shows that the automorphism is well-defined, the second that it respects the ring structure.)

Example 3.4. When $R = \mathbb{Q}$ (or more generally any Dedekind domain in which 2 is a unit), then completing the square shows that oriented quadratic algebras are in bijection with the forms $x^2 - ky^2$, $k \in \mathbb{Q}$, each of which yields an algebra $S = \mathbb{Q}[\sqrt{k}]$ oriented by $\alpha(1 \wedge \sqrt{k}) = 1$.

If we pass to *unoriented* extensions, then we identify $\mathbb{Q}[\sqrt{k}]$ with its rescalings $\mathbb{Q}[f\sqrt{k}] \cong \mathbb{Q}[\sqrt{f^2 k}]$, $f \in \mathbb{Q}^\times$. The resulting orbit space $\mathbb{Q}/(\mathbb{Q}^\times)^2$ parametrizes quadratic number fields, plus the two nondomains

$$\mathbb{Q}[\sqrt{0}] = \mathbb{Q}[\epsilon]/(\epsilon^2) \quad \text{and} \quad \mathbb{Q}[\sqrt{1}] \cong \mathbb{Q} \oplus \mathbb{Q}.$$

Example 3.5. When $R = \mathbb{Z}$, we can almost complete the square, putting a general $x^2 + txy + uy^2$ in the form

$$x^2 - \frac{D}{4}y^2 \quad \text{or} \quad x^2 + xy - \frac{D-1}{4}y^2.$$

Here $D = t^2 - 4u$ is the *discriminant*, the standard invariant used in [1] to parametrize oriented quadratic rings. It takes on all values congruent to 0 or 1 mod 4. It also parametrizes *unoriented* quadratic rings, since each such ring has just two orientations which are conjugate under the ring's conjugation automorphism. The rings of integers of number fields are then parametrized by the *fundamental discriminants* which are not a square multiple of another discriminant, with the exception of 0 and 1 which parametrize $\mathbb{Z}[\epsilon]/\epsilon^2$ and $\mathbb{Z} \oplus \mathbb{Z}$ respectively.

Example 3.6. For an example where discriminant-based parametrizations are inapplicable, consider the field $R = \mathbb{F}_2$ of two elements. Any nonzero quadratic form attains the value 1, and there are three such, namely

$$x^2, \quad xy, \quad \text{and} \quad x^2 + xy + y^2.$$

They correspond to the three quadratic algebras over $\mathbb{F}_2$, respectively $\mathbb{F}_2[\epsilon]/\epsilon^2$, $\mathbb{F}_2 \oplus \mathbb{F}_2$, and $\mathbb{F}_4$.

4 Ideal classes of quadratic algebras

We can now parametrize ideal classes of quadratic algebras, in a way that partially overlaps [12]. To be absolutely unambiguous, we make the following definition for quadratic algebras that need not be domains:

Definition 4.1. Let S be a quadratic algebra over R. A *fractional ideal* (or just an *ideal*) of S is a finitely generated S-submodule of S_K **that spans** S_K **over** K. Two fractional ideals are considered to belong to the same *ideal class* if one is a scaling of the other by a scalar $\gamma \in S_K^\times$. (This is clearly an equivalence relation.) The ideal classes together with the operation induced by ideal multiplication form the *ideal class semigroup*, and the invertible ideal classes form the *ideal class group* $\operatorname{Pic} S$.

The condition in bold means that, for instance, the submodule $R \oplus \{0\} \subseteq R \oplus R$ is not a fractional ideal. Of course, any ideal that is invertible automatically satisfies it.

Theorem 4.2 (cf. [12], Corollary 4.2)**.** *For each ideal $\mathfrak{a}$ of R, there is a bijection between*

- *ideal classes of oriented quadratic rings of type $\mathfrak{a}$, and*
- *rank-2 lattices M equipped with a nonzero quadratic map $\phi : M \to \mathfrak{a}^{-1} \cdot \Lambda^2 M$.*

In this bijection, the ideal classes that are invertible correspond exactly to the forms that are primitive, *that is, do not factor through any proper sublattice of $\mathfrak{a}^{-1} \cdot \Lambda^2 M$.*

Proof. Suppose first that we have a quadratic ring $S = R \oplus \mathfrak{a}\xi$, oriented by $\alpha(1 \wedge \xi) = 1$, and a fractional ideal I of R. Construct a map $\phi : I \to \mathfrak{a}^{-1} \cdot \Lambda^2 I$ by

$$\omega \mapsto \omega \wedge \xi\omega.$$

Here $\xi\omega \in \mathfrak{a}^{-1} I$ so the wedge product lies in $\mathfrak{a}^{-1} \cdot \Lambda^2 I$, and we get a well-defined quadratic map ϕ, scaling appropriately when I is scaled by an element of $S_K^\times$. Note that ϕ is nonzero because, after extending scalars to K, the element $1 \in I_K = S_K$ is mapped to $1 \wedge \xi \neq 0$.

It will be helpful to write this construction in coordinates. Let $I = \mathfrak{b}_1\eta_1 \oplus \mathfrak{b}_2\eta_2$ be a decomposition into R-ideals, and let ξ act on I by the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, that is,

$$\begin{aligned} \xi\eta_1 &= a\eta_1 + c\eta_2 \\ \xi\eta_2 &= b\eta_1 + d\eta_2 \end{aligned} \tag{2}$$

where a, b, c, d belong to the relevant ideals: $a, d \in \mathfrak{a}^{-1}$, $b \in \mathfrak{a}^{-1}\mathfrak{b}_1\mathfrak{b}_2^{-1}$, and $c \in \mathfrak{a}^{-1}\mathfrak{b}_1^{-1}\mathfrak{b}_2$. Then we get

$$\begin{aligned} \phi(x\eta_1 + y\eta_2) &= (x\eta_1 + y\eta_2) \wedge (x\xi\eta_1 + y\xi\eta_2) \\ &= (x\eta_1 + y\eta_2) \wedge (ax\eta_1 + cx\eta_2 + by\eta_1 + dy\eta_2) \\ &= (cx^2 + (d-a)xy - by^2)(\eta_1 \wedge \eta_2) \in \mathfrak{a}^{-1}\mathfrak{b}_1\mathfrak{b}_2(\eta_1 \wedge \eta_2) = \mathfrak{a}^{-1}\Lambda^2 I. \end{aligned} \tag{3}$$

(Now ϕ appears clearly as a tensor in $\operatorname{Sym}^2 I^* \otimes \mathfrak{a}^{-1} \cdot \Lambda^2 M$.)

We now seek to reconstruct the ideal I from its associated quadratic form. Given an ideal $\mathfrak{a}$, a lattice $M = \mathfrak{b}_1\eta_1 \oplus \mathfrak{b}_2\eta_2$, and a quadratic map $\phi(x\eta_1 + y\eta_2) = (px^2 + qxy + ry^2)(\eta_1 \wedge \eta_2)$ to $\mathfrak{a}^{-1} \cdot \Lambda^2 M$, we may choose $a = 0$, $b = -r$, $c = p$, and $d = q$ to recover an action (2) of ξ on R yielding the form ϕ. By (3), this action is unique up to adding a constant to a and d, which simply corresponds to a change of basis $\xi \mapsto \xi + a$. Next, by the Cayley-Hamilton theorem, the formal expression $\xi^2 - q\xi + pr$ annihilates M, so M is a module over the ring $S = R[\mathfrak{a}\xi]/(\mathfrak{a}^2(\xi^2 - q\xi + pr))$ corresponding to the quadratic form $x^2 + qxy + pry^2$. The last step is to embed M into S_K, or equivalently, to identify M_K with S_K. For this, we divide into cases based on the kind of ring that S_K is, or equivalently the factorization type of the polynomial $f(x) = x^2 - qx + pr$ over K.

- If f is irreducible, then S_K is a field, and M_K is an S_K-vector space of dimension 1, isomorphic to S_K.
- If f has two distinct roots, then $S_K \cong K \oplus K$. There are three different S_K-modules having dimension 2 as K-vector spaces: writing I_1 and I_2 for the two copies of K within S_K, we can describe them as $I_1 \oplus I_1$, $I_2 \oplus I_2$, and $I_1 \oplus I_2$. But on the first two, every element of S_K acts as a scalar. If M_K were one of these, then the quadratic form $\phi(\omega) = \omega \wedge \xi\omega$ would be identically 0, which is not allowed. So $M_K \cong I_1 \oplus I_2 \cong S_K$.
- Finally, if f has a double root, then $S_K \equiv K[\epsilon]/\epsilon^2$. There are two S_K-modules having dimension 2 as a K-vector space: $K\epsilon \oplus K\epsilon$ and S_K. On $K\epsilon \oplus K\epsilon$, S_K acts by scalars and we get a contradiction as before. So $M_K \cong S_K$.

This shows that there is always at least one embedding of M into S_K. To show there is at most one up to scaling, we need that every automorphism of S_K as an S_K-module is given by multiplication by a unit. But this is trivial (the image of 1 determines everything else).

It will be convenient to have as well an explicit reconstruction of an ideal from its associated quadratic form. First change coordinates on M such that $p \neq 0$. (If $r \neq 0$, swap $\mathfrak{b}_1\eta_1$ and $\mathfrak{b}_2\eta_2$; if $p = 0$ but $q \neq 0$, translate $\eta_2 \mapsto \eta_2 + t\eta_1$ for any nonzero $t \in \mathfrak{b}_1\mathfrak{b}_2^{-1}$.) Then the ideal

$$I = \mathfrak{b}_1 + \mathfrak{b}_2\left(\frac{\xi}{p}\right) \tag{4}$$

of the ring $S = R[\mathfrak{a}\xi]/(\mathfrak{a}^2(\xi^2 - q\xi + pr))$ corresponding to the norm form $x^2 + qxy + pry^2$ is readily seen to yield the correct quadratic form.

We now come to the equivalence between invertibility of ideals and primitivity of forms. Suppose first that $\phi : M \to \mathfrak{a}^{-1} \cdot \Lambda^2 M$ is imprimitive, that is, there is an ideal $\mathfrak{a}'$ strictly containing $\mathfrak{a}$ such that ϕ actually arises from a quadratic map $\phi' : M \to \mathfrak{a}'^{-1} \cdot \Lambda^2 M$. Following through the (first) construction, we see that ϕ and ϕ' give the same ξ-action on $I = M$ but embed it as a fractional ideal in two different rings, $S = R \oplus \mathfrak{a}\xi$ and $S' = R \oplus \mathfrak{a}'\xi$. We naturally have $S_K \cong S'_K \cong K[\xi]/(\xi^2 - q\xi + pr)$, and S is a subring of S'. Suppose I had an inverse J as an S-ideal. Then since I is an S'-ideal, the product $IJ = S$ must be an S'-ideal, which is a contradiction.

Conversely, suppose that ϕ is primitive and I has been constructed using (4). Consider the conjugate ideal

$$\bar{I} = \mathfrak{b}_1 + \mathfrak{b}_2\frac{\bar{\xi}}{p} = \mathfrak{b}_1 + \mathfrak{b}_2\frac{q - \xi}{p}$$

and form the product

$$\begin{aligned} I\bar{I} &= \left(\mathfrak{b}_1 + \mathfrak{b}_2\frac{\xi}{p}\right)\left(\mathfrak{b}_1 + \mathfrak{b}_2\frac{q-\xi}{p}\right) \\ &= \mathfrak{b}_1^2 + \mathfrak{b}_1\mathfrak{b}_2\frac{\xi}{p} + \mathfrak{b}_1\mathfrak{b}_2\frac{q-\xi}{p} + \mathfrak{b}_2^2\frac{\xi\bar{\xi}}{p^2} \\ &= \frac{1}{p}(p\mathfrak{b}_1^2 + q\mathfrak{b}_1\mathfrak{b}_2 + r\mathfrak{b}_2^2 + \xi\mathfrak{b}_1\mathfrak{b}_2). \end{aligned}$$

The first three terms in the parenthesis are all fractional ideals in K. The condition that ϕ maps into $\mathfrak{a}^{-1} \cdot \Lambda^2 I$ is exactly that these lie in $\mathfrak{a}^{-1}\mathfrak{b}_1\mathfrak{b}_2$, and the condition of primitivity is that they do not all lie in any smaller ideal, that is, their sum is $\mathfrak{a}^{-1}\mathfrak{b}_1\mathfrak{b}_2$. So

$$I\bar{I} = \frac{\mathfrak{b}_1\mathfrak{b}_2}{p}(\mathfrak{a}^{-1} + R\xi) = \frac{\mathfrak{a}^{-1}\mathfrak{b}_1\mathfrak{b}_2}{p} \cdot S. \tag{5}$$

We conclude that

$$I^{-1} = \mathfrak{a}\mathfrak{b}_1^{-1}\mathfrak{b}_2^{-1}p\bar{I} = \alpha(\Lambda^2 I)^{-1}\bar{I}$$

is an inverse for I. ■

Note that our proof of the invertibility-primitivity equivalence shows something more: that *any* fractional ideal I of a quadratic algebra S is invertible when considered as an ideal of a certain larger ring S', found by "canceling common factors" in its associated quadratic form. The following relation is worth noting:

Corollary 4.3. *If I is an ideal of a quadratic algebra S and $S' = \operatorname{End} I \subseteq S_K$ is its ring of endomorphisms, then*

$$I\bar{I} = \frac{\alpha(\Lambda^2 I)}{\alpha(\Lambda^2 S')} \cdot S'.$$

Proof. The ring S' is the one occurring in the proof that imprimitivity implies noninvertibility, provided that the ideal $\mathfrak{a}'$ is chosen to be as large as possible (i.e. equal to $(p\mathfrak{b}_1^2 + q\mathfrak{b}_1\mathfrak{b}_2 + r\mathfrak{b}_2^2)^{-1}$), so that I is actually invertible with respect to S'. This S' must be the endomorphism ring $\operatorname{End} I$, or else I would be an ideal of an even larger quadratic ring.[1]

Viewing α, by restriction, as an orientation on S', we have $\alpha(\Lambda^2 S') = \mathfrak{a}'$ and the formula is reduced to that for I^{-1} above. ■

Example 4.4. If $R = \mathbb{Z}$ (or more generally any PID), then the situation simplifies to $\mathfrak{a} = \mathbb{Z}$ and $M = \mathbb{Z}^2$, and we recover a bijection between ideal classes and binary quadratic forms. But the theorem also requires us, when changing coordinates on M, to change coordinates on $\Lambda^2 M$ appropriately; that is, ideal classes are in bijection with $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary quadratic forms $\phi : \mathbb{Z}^2 \to \mathbb{Z}$, not under the natural action but under the twisted action

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \phi\right)(x, y) = \frac{1}{ad - bc} \cdot \phi(ax + cy, bx + dy).$$

(Compare [8], p. 142 and [12], Theorem 1.2.)

For an example not commonly encountered in the literature, take the order $S = \mathbb{Z}[5i]$ in the domain $\mathbb{Z}[i]$. Its ideal classes correspond simply to $\mathrm{GL}_2(\mathbb{Z})$-orbits of quadratic forms $px^2 + qxy + ry^2$ having discriminant $q^2 - 4pr = -100$. Using the standard theory of "reduction" of quadratic forms developed by Lagrange (see [8], pp. 26ff.), we may limit our search to the bounded domain where $|q| \leq r \leq p$ and find that there are precisely three, with three corresponding ideal classes:

$$\begin{aligned} \phi_1(x, y) &= x^2 + 25y^2 && \leftrightsquigarrow S = \mathbb{Z}[5i] \\ \phi_2(x, y) &= 2x^2 + 2xy + 13y^2 && \leftrightsquigarrow A = \mathbb{Z}\langle 5, 1 + i\rangle \\ \phi_3(x, y) &= 5x^2 + 5y^2 && \leftrightsquigarrow B = \mathbb{Z}[i]. \end{aligned}$$

The first two ideals, which correspond to primitive forms, are invertible (indeed $A \cdot iA = S$); the third is not. In fact we can build a multiplication table for the ideal class semigroup.

$\cdot$	S	A	B
S	S	A	B
A	A	S	B
B	B	B	B

[1] We here need that $\operatorname{End} I$ is finitely generated and hence a quadratic ring. This is obvious, as it is contained in $x^{-1}I$ for any $x \in S_K^\times \cap I$.

5 Ideal triples

We turn now to one of Bhargava's most widely publicized contributions to mathematics, the reinterpretation of Gauss's 200-year-old composition law on primitive binary quadratic forms in terms of simple operations on a $2 \times 2 \times 2$ box of integers. In fact, Bhargava produced something rather more general: a bijection ([1], Theorem 1) that takes *all* $2 \times 2 \times 2$ boxes satisfying a mild nondegeneracy condition, up to the action of the group

$$\Gamma = \left\{ (M_1, M_2, M_3) \in (\mathrm{GL}_2\mathbb{Z})^3 : \prod_i \det M_i = 1 \right\},$$

to triples of fractional ideals (I_1, I_2, I_3) in a quadratic ring S that are *balanced,* that is, satisfy the two conditions

(a) $I_1 I_2 I_3 \subseteq S$;

(b) $N(I_1)N(I_2)N(I_3) = 1$. Here $N(I)$ is the norm of the ideal I, defined by the formula $N(I) = [A : I]/[A : S]$ for any $\mathbb{Z}$-lattice A containing both S and I.[2]

The ideals I_i are unique up to a scaling by constants $\gamma_i \in S_{\mathbb{Q}}^{\times}$ of product 1.

Our task will be to generalize this result to an arbitrary Dedekind domain. First, to remedy the definition of balanced, we need a workable replacement for the notion of ideal norm. We use a notion of balanced based on the exterior square of the ideal, yielding a special case of the definition used in [14]:

Definition 5.1. A triple of fractional ideals I_1, I_2, I_3 of an R-algebra S is *balanced* if

(a) $I_1 I_2 I_3 \subseteq S$;

(b) the image of $\Lambda^2 I_1 \otimes \Lambda^2 I_2 \otimes \Lambda^2 I_3$ in $(\Lambda^2 S_K)^{\otimes 3}$ is precisely $(\Lambda^2 S)^{\otimes 3}$.

The objects that we will use on the other side of the bijection are, as one might expect, not merely 8-tuples of elements from R, because the class group intrudes. The appropriate notion is as follows:

Definition 5.2. Let $\mathfrak{a}$ be an ideal class of R. A *Bhargava box* of type $\mathfrak{a}$ over R consists of the following data:

- three rank-2 lattices M_1, M_2, M_3;
- an orientation isomorphism $\theta : \Lambda^2 M_1 \otimes \Lambda^2 M_2 \otimes \Lambda^2 M_3 \to \mathfrak{a}^3$;
- a trilinear map $\beta : M_1 \otimes M_2 \otimes M_3 \to \mathfrak{a}$ satisfying the following nondegeneracy condition: for any nonzero $x \in M_i$, the bilinear map from the other two M_j to I induced by fixing one argument to be x is nonzero.

If we choose a decomposition of each M_i into a direct sum $\mathfrak{b}_{i1} \oplus \mathfrak{b}_{i2}$ of ideals, then θ becomes an isomorphism from $\prod_{i,j} \mathfrak{b}_{ij}$ to $\mathfrak{a}^3$ (which we may take to be the identity), while β is determined by eight coefficients

$$\beta_{ijk} \in \mathfrak{b}_{1i}^{-1} \mathfrak{b}_{2j}^{-1} \mathfrak{b}_{3k}^{-1} \mathfrak{a}.$$

Thus we stress that, in spite of all the abstraction, our parameter space indeed still consists of $2 \times 2 \times 2$ boxes of numbers lying in certain ideals contained in K.

[2] This should not be confused with the ideal generated by the norms of the elements of I. Even over $\mathbb{Z}$, the two notions differ: $2 \cdot \mathbb{Z}[i]$ is an ideal of norm 2 in the ring $\mathbb{Z}[2i]$, but every element of $2 \cdot \mathbb{Z}[i]$ has norm divisible by 4.

Theorem 5.3 (cf. [1], Theorem 1; [14], Theorem 1.4)**.** *For each ideal $\mathfrak{a}$ of R, there is a bijection between*

- *balanced triples (I_1, I_2, I_3) of ideals in an oriented quadratic ring S of type $\mathfrak{a}$, up to scaling by factors γ_1, γ_2, $\gamma_3 \in S_K^\times$ with product 1;*
- *Bhargava boxes of type $\mathfrak{a}$.*

Remark. Two balanced ideal triples may be inequivalent for the purposes of this bijection even if corresponding ideals belong to the same class (see Example 5.8d). Consequently a Bhargava box cannot be described as corresponding to a balanced triple of ideal *classes.*

Proof. The passage from ideals to the Bhargava box is simple and derived directly from [1]. Given a balanced triple (I_1, I_2, I_3) in a quadratic ring S with an orientation $\alpha : \Lambda^2 S \to \mathfrak{a}$, construct the trilinear map

$$\begin{aligned} \beta : I_1 \otimes I_2 \otimes I_3 &\to \mathfrak{a} \\ x \otimes y \otimes z &\mapsto \alpha(1 \wedge xyz). \end{aligned}$$

This, together with the identification θ coming from condition (b) of Definition 5.1, furnishes the desired Bhargava box.

We seek to invert this process and reconstruct the ring S, the orientation α, and the ideals I_i uniquely from the Bhargava box. We begin by reconstructing the quadratic forms $\phi_i : M_i \to \mathfrak{a}^{-1} \cdot \Lambda^2 M_i$ corresponding to the ideals I_i. For this we first use β to map M_1 to $\mathrm{Hom}(M_2 \otimes M_3, \mathfrak{a})$, in other words $\mathrm{Hom}(M_2, \mathfrak{a}M_3^*)$. We then take the determinant, which is a quadratic map to $\mathrm{Hom}(\Lambda^2 M_2, \Lambda^2(\mathfrak{a}M_3^*)) \cong \mathfrak{a}^2 \cdot \Lambda^2 M_2^* \otimes \Lambda^2 M_3^*$, which can be identified via $-\theta$ (note the sign change) with $\mathfrak{a}^{-1}\Lambda^2 M_1$. We thus get a quadratic form $\phi_1' : M_1 \to \mathfrak{a}^{-1}\Lambda^2 M_1$. We claim that if the Bhargava box arose from a triple of ideals, then this is the natural form $\phi_1 : x \mapsto x \wedge \xi x$ on I_1. For convenience we will extend scalars and prove the equality as one of forms on $M_1^K \cong S_K$. To deal with ϕ_1', we must analyze

$$\beta(x) = (y \mapsto (z \mapsto \alpha(1 \wedge xyz))) \in \mathrm{Hom}(M_2^K, M_3^{K*}).$$

Now whereas M_2^K is naturally identifiable with S_K, to deal with $M_3^{K*} \cong S_K^*$ we have to bring in the symmetric pairing $\alpha(1 \wedge \bullet\bullet) : S_K \otimes_K S_K \to K$, which one easily checks is nondegenerate and thus identifies S_K^* with S_K. So we have transformed $\beta(x)$ to the element

$$\beta'(x) = (y \mapsto xy) \in \mathrm{Hom}_K(S_K, S_K).$$

We then take the determinant, which equals the norm $N(x) \in K \cong \mathrm{Hom}_K(\Lambda^2 S_K, \Lambda^2 S_K)$. This is to be compared to

$$\phi_1(x) = x \wedge \xi x = N(x)(1 \wedge \xi) = \alpha^{-1}(N(x)).$$

It then remains to check that we have performed the identifications properly, that is, that the four isomorphisms

$$\begin{array}{ccc} K & \xleftarrow{\ \alpha\ } & \Lambda^2(M_1^K \otimes_{S_K} M_2^K) \\ {\scriptstyle \alpha\otimes\alpha}\uparrow & & \downarrow{\scriptstyle \wedge^2(x\otimes y \mapsto \alpha(xy\bullet))} \\ \Lambda^2 M_1^K \otimes \Lambda^2 M_2^K & \xrightarrow{\ -\theta\ } & \Lambda^2 M_3^{K*} \end{array}$$

are compatible. In particular we discover that the pairing $\alpha(1 \wedge \bullet\bullet)$ is given in the basis $\{1, \xi\}$ by the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & \mathrm{Tr}\,\xi \end{bmatrix}$$

of determinant -1, explaining the compensatory minus sign that must be placed on θ.

Now write $M_i = \mathfrak{b}_{i1}\eta_{i1} \oplus \mathfrak{b}_{i2}\eta_{i2}$ where $\theta : \prod_{i,j} \mathfrak{b}_{ij} \to \mathfrak{a}^3$ may be assumed to be the identity map, and express β in these coordinates as

$$\beta\left(\sum_{i,j,k} x_{ijk}\eta_{1i}\eta_{2j}\eta_{3k}\right) = \sum_{i,j,k} a_{ijk}x_{ijk}.$$

It will be convenient to create the single-letter abbreviations $a = a_{111}$, $b = a_{112}$, $c = a_{121}$, continuing in lexicographic order to $h = a_{222}$. Then ϕ_1 sends an element $x\eta_{11} + y\eta_{12} \in M_1$ to the determinant

$$-\det\begin{bmatrix} ax+ey & bx+fy \\ cx+gy & dx+hy \end{bmatrix} = (bc-ad)x^2 + (bg+cf-ah-de)xy + (fg-eh)y^2.$$

This means that the I_1 that we are searching for necessarily has a ξ-action given by the matrix

$$\begin{bmatrix} ah+de & eh-fg \\ bc-ad & bg+cf \end{bmatrix} \tag{6}$$

where we have added a scalar matrix such that the trace $ah+bg+cf+de$, and indeed the entire characteristic polynomial

$$F(x) = x^2 - (ah+bg+cf+de)x + abgh + acfh + adeh + bcfg + bdeg + cdef - adfg - bceh, \tag{7}$$

is symmetric under permuting the roles of M_1, M_2, and M_3. In other words, we have found a single ring $S = R[\mathfrak{a}\xi]/\mathfrak{a}^2F(\xi)$ of which M_1, M_2, and M_3 are modules, under the ξ-action (6) and its symmetric cousins

$$\begin{bmatrix} ah+cf & ch-dg \\ be-af & bg+de \end{bmatrix} \text{ on } M_2 \text{ and } \begin{bmatrix} ah+bg & bh-df \\ ce-ag & cf+de \end{bmatrix} \text{ on } M_3.$$

The next step is is the construction of the elements τ_{ijk} that will serve as the products $\eta_{1i}\eta_{2j}\eta_{3k}$ of the ideal generators. Logically, it begins with a "voilà" (compare [1], p. 235):

$$\tau_{ijk} = \begin{cases} -a_{\bar{i}jk}a_{i\bar{j}k}a_{ij\bar{k}} - a_{ijk}^2 a_{\bar{i}\bar{j}\bar{k}} - a_{ijk}\bar{\xi}, & i+j+k \text{ odd}, \\ a_{\bar{i}jk}a_{i\bar{j}k}a_{ij\bar{k}} + a_{ijk}^2 a_{\bar{i}\bar{j}\bar{k}} + a_{ijk}\xi, & i+j+k \text{ even}. \end{cases}$$

Here $\bar{i}$, $\bar{j}$, $\bar{k}$ are shorthand for $3-i$, etc., while $\bar{\xi}$ denotes the Galois conjugate $\mathrm{Tr}(\xi)-\xi$. Bhargava apparently derived this formula (in the case $R = \mathbb{Z}$) by solving the natural system of quadratic equations ($\tau_a\tau_d = \tau_b\tau_c$ and so on). For our purposes it suffices to note that this formula is well-defined over any Dedekind domain (in contrast to [1] where there is a denominator of 2) and yields a trilinear map $\tilde{\beta} : M_1 \otimes M_2 \otimes M_3 \to S$, defined by

$$\tilde{\beta}\left(\sum_{i,j,k} x_{ijk}\eta_{1i}\eta_{2j}\eta_{3k}\right) = \sum_{i,j,k} \tau_{ijk}x_{ijk},$$

with the property that following with the projection $\alpha(1 \wedge \bullet) : S \to \mathfrak{a}$ gives back β. We claim that $\tilde{\beta}$, in addition to being R-trilinear, is S-trilinear under the newfound S-actions on the M_i. This is a collection of calculations involving the action of ξ on each factor, for instance

$$(ah+de)\tau_a + (bc-ad)\tau_e = \xi\tau_a$$

(where we have taken the liberty of labeling the τ_{ijk} as $\tau_a, \ldots, \tau_h$ in the same manner as the a_{ijk}). This is routine, and all the other edges of the box can be dealt with symmetrically. So, extending scalars to K, we get a map

$$\tilde{\beta} : M_1^K \otimes_{S_K} M_2^K \otimes_{S_K} M_3^K \to S_K.$$

Since each M_i is isomorphic to a fractional ideal, each M_i^K is isomorphic to S_K and thus so is the left side. Also, it is easy to see that $\tilde{\beta}$ is surjective or else β would be degenerate. So once two identifications $\iota_1 : M_1 \to I_1$, $\iota_2 : M_2 \to I_2$ are chosen, the third $\iota_3 : M_3 \to I_3$ can be scaled such that $\tilde{\beta}(x \otimes y \otimes z) = \iota_1(x)\iota_2(y)\iota_3(z)$ and hence $\beta(x \otimes y \otimes z) = \alpha(1 \wedge \iota_1(x)\iota_2(y)\iota_3(z))$ is as desired.

We have now constructed a triple (I_1, I_2, I_3) of fractional ideals such that the map $\alpha(1 \wedge \bullet\bullet\bullet) : I_1 \otimes I_2 \otimes I_3 \to K$ coincides with β. Two verifications remain:

- That $I_1 I_2 I_3 \subseteq S$. Since $I_1 I_2 I_3$ is the R-span of the eight τ_{ijk}, this is evident from the construction of the τ_{ijk}.
- That $\prod_i \Lambda^2(I_i) = \prod_i \Lambda^2(S)$, and more strongly that the diagram

$$\begin{array}{ccc} \bigotimes_i \Lambda^2(M_i) & \xrightarrow{\prod_i \iota_i} & \bigotimes_i \Lambda^2(I_i) \\ & \searrow^{\theta} & \downarrow{\scriptstyle \alpha^{\otimes 3}} \\ & & K \end{array}$$

  commutes. This is a verification similar to that which showed the correspondence of the forms ϕ_i. Indeed, if we had recovered a triple of ideals that produced the correct β but the wrong θ, then the ϕ's as computed from β and the two θ's would have to mismatch.

This concludes the proof that each Bhargava box corresponds to at least one balanced triple. We must also prove that two balanced triples (I_1, I_2, I_3) and (I_1', I_2', I_3') yielding the same Bhargava box must be equivalent; but here we are helped greatly by the results that we have already proved. Namely, since the forms ϕ_i associated to the ideals match, these ideals must lie in the same oriented quadratic ring S and there must be scalars $\gamma_i \in S_K^\times$ such that $I_i' = \gamma_i I_i$. We may normalize such that $\gamma_2 = \gamma_3 = 1$. Then, for all $x \in I_1, y \in I_2, z \in I_3$,

$$0 = \beta(xyz) - \beta(xyz) = \alpha(1 \wedge xyz) - \alpha(1 \wedge \gamma_1 xyz) = \alpha(1 \wedge (1 - \gamma_1)xyz).$$

In other words, we have $(1 - \gamma_1)x \in K$ for every $x \in I_1 I_2 I_3$. Extending scalars, we get the same for all $x \in K I_1 I_2 I_3 = S_K$ which implies $1 - \gamma = 0$. ■

It is natural to think about what happens when the datum θ is removed from the Bhargava box. As one easily verifies, multiplying θ by a unit $u \in R^\times$ is equivalent to multiplying the orientation α of S by u^{-1} while keeping the same ideals I_i. Accordingly, we have the following corollary, which we have chosen to state with a representation-theoretic flavor:

Corollary 5.4. *Balanced triples of ideals (I_1, I_2, I_3) of types $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ in an (unoriented) quadratic extension S of type $\mathfrak{a}$, up to equivalence, are parametrized by* $\mathrm{GL}(M_1) \times \mathrm{GL}(M_2) \times \mathrm{GL}(M_3)$*-orbits of trilinear maps*

$$\beta : M_1 \otimes M_2 \otimes M_3 \to \mathfrak{a},$$

where M_i is the module $R \oplus \mathfrak{a}_i$, satisfying the nondegeneracy condition of Definition 5.2.

5.1 Relation with the class group

In [1], after establishing a bijection between balanced ideal triples and $2 \times 2 \times 2$ cubes (Theorem 1), Bhargava proceeds to Theorem 2, which establishes a group law on the cubes themselves, or rather on the subset of those that are "projective," i.e. correspond to triples of invertible ideals. This structure is easily replicated in our situation: it is only necessary to verify that the product of two balanced triples of invertible ideals is balanced. In fact, a weaker condition suffices.

Lemma 5.5. *Let (I_1, I_2, I_3) and (J_1, J_2, J_3) be balanced triples of ideals of a quadratic ring S, with each I_i invertible. Then the ideal triple (I_1J_1, I_2J_2, I_3J_3) is also balanced.*

Proof. We clearly have

$$I_1J_1 \cdot I_2J_2 \cdot I_3J_3 = (I_1I_2I_3)(J_1J_2J_3) \subseteq S,$$

establishing (a) of Definition 5.1. For (b), the key is to use Corollary 4.3 to get a handle on the exterior squares of the I_iJ_i. We have $\operatorname{End} I_i = S$; each $S_i = \operatorname{End} J_i$ is a quadratic ring with $S \subseteq S_i \subseteq S_K$. Then since

$$\operatorname{End} J_i \subseteq \operatorname{End} I_iJ_i \subseteq \operatorname{End} I_i^{-1}I_iJ_i = \operatorname{End} J_i,$$

we see that $\operatorname{End} I_iJ_i = S_i$ as well. Then

$$\frac{\alpha(\Lambda^2(I_iJ_i))}{\alpha(S_i)}S_i = I_iJ_i \cdot \overline{I_iJ_i} = I_i\overline{I_i} \cdot J_i\overline{J_i} = \alpha(\Lambda^2 I_i)S \cdot \frac{\alpha(\Lambda^2 J_i)}{\alpha(S_i)}S_i = \frac{\alpha(\Lambda^2 I_i)\alpha(\Lambda^2 J_i)}{\alpha(S_i)}S_i.$$

Intersecting with K, we get

$$\alpha(\Lambda^2(I_iJ_i)) = \alpha(\Lambda^2 I_i)\alpha(\Lambda^2 J_i).$$

We can now multiply and get

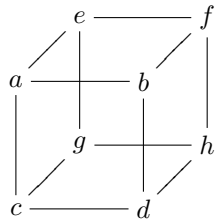
$$\prod_i \alpha(\Lambda^2(I_iJ_i)) = \prod_i \alpha(\Lambda^2 I_i) \cdot \prod_i \alpha(\Lambda^2 J_i) = R,$$

so (I_1J_1, I_2J_2, I_3J_3) is balanced. ∎

Corollary 5.6 (cf. [1], Theorems 2 and 12)**.** *The Bhargava boxes which belong to a fixed ring S (determined by the quadratic form (7)) and which are primitive (in the sense of having all three associated quadratic forms primitive) naturally form a group isomorphic to $(\operatorname{Pic} S)^2$.*

Corollary 5.7. *The Bhargava boxes which belong to a fixed ring S naturally have an action by $(\operatorname{Pic} S)^2$.*

Example 5.8. When $R = \mathbb{Z}$ (or more generally any PID), we can simplify the notation of a Bhargava box by taking each $M_i = \mathbb{Z}^2$, so that θ is without loss of generality the standard orientation $\Lambda^2(\mathbb{Z}^2)^{\otimes 3} \xrightarrow{\sim} \mathbb{Z}$, and β is expressible as a box

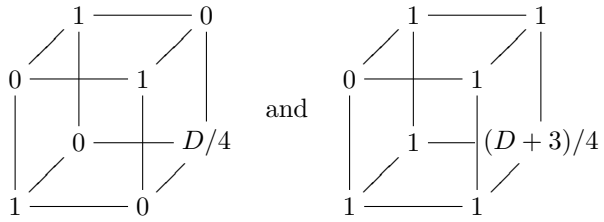


of integers. The three forms ϕ_i are then obtained by slicing β into two 2×2 matrices and taking the determinant of a general linear combination as described in [1], Section 2.1:

$$\phi_1(x, y) = -\det\left(x\begin{bmatrix} a & b \\ c & d \end{bmatrix} + y\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right).$$

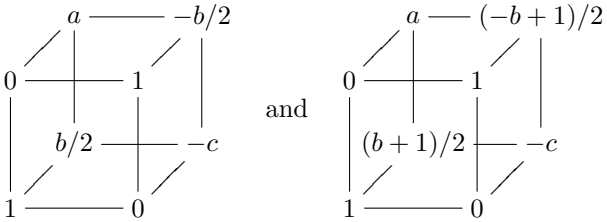
We recapitulate the boxes having the greatest significance in [1] and in the theory of quadratic forms generally:

(a) The boxes



(for D even and odd respectively), have as all three of their associated quadratic forms $x^2 - (D/4)y^2$ and $x^2 + xy - (D-1)/4 \cdot y^2$ respectively, the defining form of the ring S of discriminant D. They correspond to the balanced triple (S, S, S). These are the "identity cubes" of [1], equation (3).

(b) The boxes



(for b even and odd respectively), have as two of their associated quadratic forms the conjugates

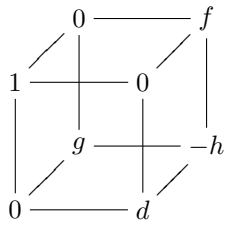
$$ax^2 + bxy + cy^2 \quad \text{and} \quad ax^2 - bxy + cy^2$$

and as the third associated form the form $x^2 - (D/4)y^2$ or $x^2 + xy - (D-3)/4 \cdot y^2$ defining the ring S of discriminant $D = b^2 - 4ac$. These boxes express the fact that the triple

$$(S, I, \alpha(\Lambda^2 I)^{-1}\bar{I})$$

is always balanced (compare Corollary 4.3). If $\gcd(a, b, c) = 1$, we also get that I and $\bar{I}$ represent inverse classes in the class group and that, correspondingly, $ax^2 + bxy + cy^2$ and $ax^2 - bxy + cy^2$ are inverse under Gauss's composition law on binary quadratic forms.

(c) The box



has as associated quadratic forms

$$\begin{aligned}
\phi_1(x, y) &= -dx^2 + hxy + fgy^2 \\
\phi_2(x, y) &= -gx^2 + hxy + dfy^2 \\
\phi_3(x, y) &= -fx^2 + hxy + dgy^2.
\end{aligned}$$

As Bhargava notes ([1], p. 249), Dirichlet's simplification of Gauss's composition law was essentially to prove that any pair of primitive binary quadratic forms of the same discriminant can be put in the form (ϕ_1, ϕ_2), so that the multiplication relation that we derive from this box,

$$\phi_1 * \phi_2 = -fx^2 - hxy + dgy^2 \text{ (or, equivalently, } dgx^2 + hxy - fy^2),$$

encapsulates the entire multiplication table for the class group.

(d) For some examples not found in the classical theory of primitive forms, we consider the non-Dedekind domain $S = \mathbb{Z}[5i]$, whose ideal class semigroup was computed above (Example 4.4). Let us find all balanced triples that may be formed from the ideals

$$S = \mathbb{Z}[5i], \quad A = \mathbb{Z}\langle 5, 1+i\rangle, \quad B = \mathbb{Z}[i]$$

of S. We compute

$$\alpha(\Lambda^2 S) = \mathbb{Z}, \quad \alpha(\Lambda^2 A) = \mathbb{Z}, \quad \alpha(\Lambda^2 B) = \frac{1}{5}\mathbb{Z}.$$

For each triple (I_1, I_2, I_3) of ideal class representatives, finding all balanced triples of ideals in these classes is equivalent to searching for all $\gamma \in S_K^\times$ satisfying $\gamma \cdot I_1 I_2 I_3 \subseteq S$ which have the correct norm

$$\langle N(\gamma)\rangle = \frac{1}{\alpha(\Lambda^2 I_1) \cdot \alpha(\Lambda^2 I_2) \cdot \alpha(\Lambda^2 I_3)}$$

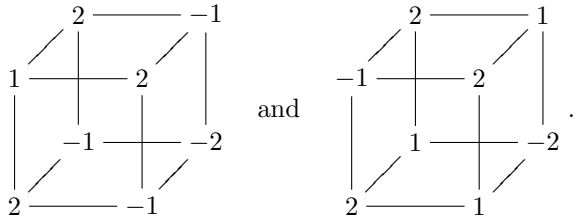
(the right side is an ideal of $\mathbb{Z}$, so $N(\gamma)$ is hereby determined up to sign, and as we are in a purely imaginary field, $N(\gamma) > 0$).

Using the class B zero or two times, we get four balanced triples

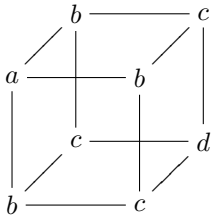
$$(S, S, S), \quad (S, A, iA), \quad (S, B, 5B), \quad \text{and} \quad (A, B, 5B),$$

each of which yields one Bhargava box. We get no balanced triples involving the ideal class B just once; indeed, it is not hard to show in general that if two ideals of a balanced triple are invertible, so is the third.

The most striking case is $I_1 = I_2 = I_3 = B$, for here there are two multipliers γ of norm 125 that send $B^3 = \mathbb{Z}[i]$ into $\mathbb{Z}[5i]$, namely $10 + 5i$ and $10 - 5i$ (we could also multiply these by powers of i, but this does not change the ideal B). The balanced triples $(B, B, (10+5i)B)$ and $(B, B, (10-5i)B$ are inequivalent under scaling, although corresponding ideals belong to the same classes. Thus we get two inequivalent Bhargava boxes with the same three associated forms, namely



(e) The triply symmetric boxes



correspond to balanced triples of ideals that all lie in the same class; those that are *projective*—that is, whose associated forms are primitive—correspond to invertible ideal classes whose third power is the trivial class. This correspondence was used to prove estimates for the average size of the 3-torsion of class groups in [7]. Our work suggests that similar methods may work for quadratic extensions of rings besides $\mathbb{Z}$.

6 Another example: p-adic rings

Example 6.1. It is instructive to look at the local rings $R = \mathbb{Z}_p$, where for simplicity we assume $p \geq 3$. Thanks to the large supply of squares, the corresponding field $K = \mathbb{Q}_p$ has but five (unoriented) quadratic extensions, namely those obtained by adjoining a square root of 0, 1, p, u, and pu where u is an arbitrary non-square modulo p. The quadratic ring extensions S of R then break up into five classes according to the corresponding extension S_K of K. We will work out one representative case, namely the oriented ring extensions $S_n = \mathbb{Z}_p[p^n\sqrt{u}]$ corresponding to the unique unramified extension $L = K[\sqrt{u}]$ of degree 2.

For any fractional ideal I of S_n, we can pick an element of I of minimal valuation (recalling that L possesses a unique extension of the valuation on K) and scale it to be 1. Then $S_n \subseteq I \subseteq S_0$, since $S_0 = \mathbb{Z}_p[\sqrt{u}]$ is the valuation ring, and it is easy to see that the only possible ideals are the subrings $S_0, S_1, \ldots, S_n$. In particular S_n is the only invertible ideal class, and the class group $\operatorname{Pic} S$ is trivial.

We now enumerate the balanced triples that can be built out of these ideals. A balanced triple is formed from two sorts of data: three ideal classes S_i, S_j, S_k; and a scale factor γ such that $\gamma S_i S_j S_k \subseteq S$ and

$$\langle N(\gamma)\rangle = \frac{1}{\alpha(\Lambda^2 S_i)\alpha(\Lambda^2 S_j)\alpha(\Lambda^2 S_k)}.$$

Computing

$$\alpha(\Lambda^2 S_i) = \alpha(1 \wedge p^i\sqrt{u}) = \left\langle p^{i-n}\right\rangle,$$

we get that $N(\gamma)$ has valuation $p^{3n-i-j-k}$ and in particular (since L is unramified)

$$i + j + k \equiv n \mod 2. \tag{8}$$

Write $3n - i - j - k = 2s$. Then $\gamma = p^s\gamma'$ where $\gamma' \in S_0^\times$. To avoid needless repetition of arguments, we assume $i \leq j \leq k$, and then $\gamma S_i S_j S_k = p^s\gamma' S_i$. Let $\gamma' = a + b\sqrt{u}$ where $a, b \in \mathbb{Z}_p$. Since $p^s\gamma' S_i$ is clearly contained in S_0, the condition for it to lie in S_n is that the irrational parts of its generators

$$p^s\gamma' \cdot 1 = p^s a + p^s b\sqrt{u} \quad \text{and} \quad p^s\gamma' \cdot p^i = p^{i+s}bu + p^{i+s}a\sqrt{u}$$

are divisible by p^n, that is,

$$v_p(a) \geq n - s - i \quad \text{and} \quad v_p(b) \geq n - s.$$

Since a and b cannot both be divisible by p, we must have $n - s - i \leq 0$, which can also be written as a sort of triangle inequality:

$$(n - j) + (n - k) \geq n - i. \tag{9}$$

If this holds, then the restrictions on γ' are now merely that $p^{n-s}|b$, that is, $\gamma' \in S_t^\times$ where $t = \max\{n - s, 0\}$. But if γ' is multiplied by a unit in $S_i^\times$, then the corresponding balanced triple is merely changed to an equivalent one. So the balanced triples are in bijection with the

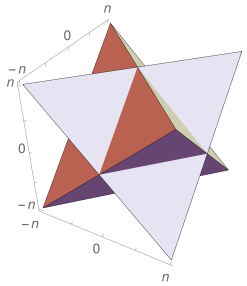


Figure 1: Stella octangula showing the range of ideal triples in $\mathbb{Z}_p[p^n\sqrt{u}]$ that are balanced

quotient $S_t^\times/S_i^\times$. Since the index of $S_i^\times$ in $S_0^\times$ is $p^{i-1}(p+1)$ $(i \geq 1)$, we have that there are precisely

$$B_{ijk} = \begin{cases} p^{i-t} & i \geq t > 0 \\ p^{i-1}(p+1) & i > t = 0 \\ 1 & i = t = 0 \end{cases}$$

classes of Bhargava boxes whose associated ideals are of the classes S_i, S_j, S_k, or equivalently, whose associated quadratic forms are

$$p^{n-i}x^2 - up^{n+i}y^2, \quad p^{n-j}x^2 - up^{n+j}y^2, \quad p^{n-k}x^2 - up^{n+k}y^2.$$

For beauty's sake let us examine one other angle of looking at the balanced triples. If we extend the notation S_i $(i \in \mathbb{Z})$ to denote the $\mathbb{Z}_p$-module generated by 1 and $p^i\sqrt{u}$ for every $i \in \mathbb{Z}$, then S_i is an ideal of the ring S_n exactly when $-n \leq i \leq n$. Of course $S_{-i} = p^{-i}\sqrt{u} \cdot S_i$ so we get no further ideal classes. But the admissible values of i, j, and k now range in the stella octangula (Figure 1) formed by reflecting the graph of (9) over the three coordinate planes, as well as the diagonal planes $i = j$, $i = k$, $j = k$. Indeed, the triples (i, j, k) such that some scaling of (S_i, S_j, S_k) is balanced are exactly the points of the lattice defined by (8) lying within the stella octangula. In such a case, one such balanced triple can be given by

$$(S_i, S_j, p^s S_k) \quad \text{or} \quad (S_i, S_j, p^s\sqrt{u}S_k)$$

according as (i, j, k) belongs to one or the other of the two tetrahedra making up the stella octangula.

7 Cubic algebras

The second main division of our paper has as its goal the parametrization of quartic algebras. We begin with cubic algebras, for there the parametrization is relatively simple and will also furnish the desired ring structure on the cubic resolvents of our quartic rings. The parametrization was done by Delone and Faddeev for cubic domains, by Gan, Gross, and Savin for cubic rings over $\mathbb{Z}$, and by Deligne over an arbitrary scheme ([13], p. 1074 and the references therein). Here we simply state and prove the result over a Dedekind domain, taking advantage of the construction in [3], section 3.9.

Theorem 7.1 (cf. [2], Theorem 1; [13], Theorem 2.1; [11], Proposition 5.1 and the references therein)**.** *Let R be a Dedekind domain. There is a canonical bijection between cubic algebras over R and pairs consisting of a rank-2 R-module M and a cubic map $\phi : M \to \Lambda^2 M$.*

Proof. Given the cubic ring C, we let $M = C/R$ so $\mathfrak{a} = \Lambda^2 M \cong \Lambda^3 C$ is an ideal class. Consider the map $\tilde{\phi} : C \to \mathfrak{a}$ given by $x \mapsto 1 \wedge x \wedge x^2$. This is a cubic map, and if x is translated by an element $a \in R$, the map does not change. Hence it descends to a cubic map $\phi : M \to \mathfrak{a}$. We will show that each possible ϕ corresponds to exactly one ring C.

Fix a decomposition $M = \mathfrak{a}_1\tilde{\xi}_1 \oplus \mathfrak{a}_2\tilde{\xi}_2$ of M into ideals. Any C can be written as $R \oplus M = R \cdot 1 \oplus \mathfrak{a}_1\xi_1 \oplus \mathfrak{a}_2\xi_2$ as an R-module, where the lifts ξ_1 and ξ_2 are unique up to adding elements of $\mathfrak{a}_1^{-1}$ and $\mathfrak{a}_2^{-1}$ respectively. Then the remaining structure of C can be described by a multiplication table

$$\begin{aligned} \xi_1^2 &= \ell + a\xi_1 + b\xi_2 \\ \xi_1\xi_2 &= m + c\xi_1 + d\xi_2 \\ \xi_2^2 &= n + e\xi_1 + f\xi_2. \end{aligned}$$

It should be remarked that this is not literally a multiplication table for C, but rather for the corresponding K-algebra $C_K = C \otimes_R K$, which does literally have $\{1, \xi_1, \xi_2\}$ as a K-basis. For C to be closed under this multiplication, the coefficients must belong to appropriate ideals ($\ell \in \mathfrak{a}_1^{-2}$, $a \in \mathfrak{a}_1^{-1}$, etc.).

Note that the basis change $\xi_1 \mapsto \xi_1 + t_1$, $\xi_2 \mapsto \xi_2 + t_2$ ($t_i \in \mathfrak{a}_i^{-1}$) diminishes c and d by t_2 and t_1, respectively (as well as wreaking greater changes on the rest of the multiplication table). Hence there is a unique choice of the lifts ξ_1 and ξ_2 such that $c = d = 0$.

We now examine the other piece of data that we are given, the cubic map ϕ describable in these coordinates as

$$\begin{aligned} \phi(x\tilde{\xi}_1 + y\tilde{\xi}_2) &= 1 \wedge (x\xi_1 + y\xi_2) \wedge (x\xi_1 + y\xi_2)^2 \\ &= 1 \wedge (x\xi_1 + y\xi_2) \wedge ((\ell + a\xi_1 + b\xi_2)x^2 + mxy + (n + e\xi_1 + f\xi_2)y^2)) \\ &= (bx^3 - ax^2y + fxy^2 - ey^3)(1 \wedge \xi_1 \wedge \xi_2). \end{aligned}$$

Thus, in our situation, specifying ϕ is equivalent to specifying the four coefficients a, b, e, and f. It therefore suffices to prove that, for each quadruple of values $a \in \mathfrak{a}_1^{-1}$, $b \in \mathfrak{a}_1^{-2}\mathfrak{a}_2$, $e \in \mathfrak{a}_1\mathfrak{a}_2^{-2}$, $f \in \mathfrak{a}_2^{-1}$, there is a unique choice of values ℓ, m, n, completing the multiplication table. The only conditions on the multiplication table that we have not used are the associative laws $(\xi_1^2)\xi_2 = \xi_1(\xi_1\xi_2)$ and $\xi_1(\xi_2^2) = (\xi_1\xi_2)\xi_2$. Expanding out these equations reveals the unique solution $\ell = -ae$, $m = -be$, $n = -bf$, which indeed belong to the correct ideals. So from the map ϕ we have constructed a unique cubic ring C. ∎

Example 7.2. Here we briefly summarize the most important examples over $R = \mathbb{Z}$, where the cubic map $\phi : M \to \Lambda^2 M$ reduces to a binary cubic form $\phi : \mathbb{Z}^2 \to \mathbb{Z}$, up to the twisted action of the group $\mathrm{GL}_2\mathbb{Z}$ by

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \phi\right)(x, y) = \frac{1}{ad - bc} \cdot \phi(ax + cy, bx + dy).$$

- The trivial ring $\mathbb{Z}[\epsilon_1, \epsilon_2]/(\epsilon_1^2, \epsilon_1\epsilon_2, \epsilon_2^2)$ corresponds to the zero form 0.
- Rings which are not domains correspond to reducible forms (e.g. $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ corresponds to $xy(x + y)$), and rings which have nontrivial nilpotents correspond to forms with repeated roots.
- A monogenic ring $\mathbb{Z}[\xi]/(\xi^3 + a\xi^2 + b\xi + c)$ corresponds to a form $x^3 + ax^2y + bxy^2 + cy^3$ with leading coefficient 1. Accordingly a form which does not represent the value 1 corresponds to a ring that is not monogenic; for instance, the form $5x^3 + 7y^3$ (which attains only values $\equiv 0, \pm 2 \bmod 7$) corresponds to the subring $\mathbb{Z}[\sqrt[3]{5^2 \cdot 7}, \sqrt[3]{5 \cdot 7^2}]$ of the field $\mathbb{Q}[\sqrt[3]{5^2 \cdot 7}] = \mathbb{Q}[\sqrt[3]{5 \cdot 7^2}]$, proving that this ring (which is easily checked to be the full ring of integers in this field) is not monogenic.

- If a form ϕ corresponds to a ring C, then the form $n \cdot \phi$ corresponds to the ring $\mathbb{Z} + nC$ whose generators are n times as large. Hence the content $\mathrm{ct}(\phi) = \gcd(a, b, c, d)$ of a form $\phi(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ equals the *content* of the corresponding ring C, which is defined as the largest integer n such that $C \cong \mathbb{Z} + nC'$ for some cubic ring C'. The notion of content (which is also not hard to define for cubic algebras over general Dedekind domains) will reappear prominently in our discussion of quartic algebras (see section 8.2).

8 Quartic algebras

Our next task is to generalize Bhargava's parametrization of quartic rings with a cubic resolvent in [3], and in particular to formalize the notion of a cubic resolvent. The concept was first developed as part of the theory of solving equations by radicals, in which it was noted that if a, b, c, and d are the unknown roots of a quartic, then

$$ab + cd, \quad ac + bd, \quad \text{and} \quad ad + bc$$

satisfy a cubic whose coefficients are explicit polynomials in those of the original quartic. Likewise, if $Q \supseteq \mathbb{Z}$ is a quartic ring embeddable in a number field, the useful resolvent map

$$x \mapsto (\sigma_1(x)\sigma_2(x) + \sigma_3(x)\sigma_4(x), \sigma_1(x)\sigma_3(x) + \sigma_2(x)\sigma_4(x), \sigma_1(x)\sigma_4(x) + \sigma_2(x)\sigma_3(x))$$

lands in a cubic subring of $\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$, where $\sigma_1, \ldots, \sigma_4$ are the four embeddings $Q \hookrightarrow \mathbb{C}$. The question then arises of what the proper notion of a resolvent map is in case Q is not a domain. In section 2.1 of [3], Bhargava defines from scratch a workable notion of Galois closure of a ring, providing a rank-24 algebra in which the resolvent can be defined. Alternatively (section 3.9), Bhargava sketches a way of axiomatizing the salient properties of a resolvent map. It is the second method that we develop here.

Definition 8.1 (cf. [13], p. 1069)**.** Let R be a Dedekind domain, and let Q be a quartic algebra over R. A *resolvent* for Q consists of a rank-2 R-lattice M, an R-module isomorphism $\theta : \Lambda^3(Q/R) \to \Lambda^2 M$, and a quadratic map $\phi : Q/R \to M$ satisfying the relation

$$\theta(x \wedge y \wedge xy) = \phi(x) \wedge \phi(y) \tag{10}$$

for all $x, y \in Q$.

Example 8.2. For the prototypical example of a resolvent, take $Q = R^{\oplus 4}$ and $C = R^{\oplus 3}$. Let θ identify the standard orientations on these lattices, and let ϕ be given by the roots

$$\phi(a, b, c, d) = (ab + cd, ac + bd, ad + bc)$$

of the classical resolvent of the quartic $(x - a)(x - b)(x - c)(x - d)$. Many more examples can be derived from this (see Example 8.10).

8.1 Resolvent to ring

Our first result is that the resolvent encapsulates the data of the ring:

Theorem 8.3 (cf. [3], Theorem 1 and Proposition 10; [13], Corollary 1.2)**.** *Let $\tilde{Q}$ and M be R-lattices of ranks 3 and 2 respectively. Let $\theta : \Lambda^3\tilde{Q} \to \Lambda^2 M$ be an isomorphism, and let $\phi : \tilde{Q} \to M$ be a quadratic map. Then there is a unique quartic ring Q with an isomorphism $Q/R \cong \tilde{Q}$ such that (M, θ, ϕ) is a cubic resolvent for Q.*

Proof. Write $\tilde{Q} = \mathfrak{a}_1\tilde{\xi}_1 \oplus \mathfrak{a}_2\tilde{\xi}_2 \oplus \mathfrak{a}_3\tilde{\xi}_3$ as usual. The ring Q will of course be $R \oplus \mathfrak{a}_1\xi_1 \oplus \mathfrak{a}_2\xi_2 \oplus \mathfrak{a}_3\xi_3$ as an R-module, with a multiplication table

$$\xi_i\xi_j = c_{ij}^0 + \sum_{k=1}^{3} c_{ij}^k \xi_k$$

where $c_{ij}^0 \in \mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}$ and $c_{ij}^k \in \mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\mathfrak{a}_k$. The 18 coefficients c_{ij}^k are subject to the expansion of the relation (10):

$$\left(\sum_i x_i\tilde{\xi}_i\right) \wedge \left(\sum_j y_j\tilde{\xi}_j\right) \wedge \left(\sum_{i,j,k} x_i y_j c_{ij}^k \tilde{\xi}_k\right) = \theta^{-1}\left(\phi\left(\sum_i x_i\tilde{\xi}_i\right) \wedge \phi\left(\sum_j y_j\tilde{\xi}_j\right)\right). \quad (11)$$

Write

$$\phi(x_1\xi_1 + x_2\xi_2 + x_3\xi_3) = \sum_{1\le i\le j\le 3} \mu_{ij} x_i x_j$$

where $\mu_{ij} \in \mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}M$. Then define

$$\lambda_{k\ell}^{ij} = \theta^{-1}(\mu_{ij} \wedge \mu_{k\ell}) \in \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\mathfrak{a}_k^{-1}\mathfrak{a}_\ell^{-1}.$$

We can now expand both sides of (11) as polynomials in the x's and y's times $\tilde{\xi}_1 \wedge \tilde{\xi}_2 \wedge \tilde{\xi}_3$, getting

$$\begin{vmatrix} x_1 & y_1 & \sum_{i,j} c_{ij}^1 x_i y_j \\ x_2 & y_2 & \sum_{i,j} c_{ij}^2 x_i y_j \\ x_3 & y_3 & \sum_{i,j} c_{ij}^3 x_i y_j \end{vmatrix} = \sum_{i\le j} \sum_{k\le \ell} \lambda_{k\ell}^{ij} x_i x_j y_k y_\ell,$$

and equate coefficients of each biquadratic monomial $x_i x_j y_k y_\ell$. Due to the skew-symmetry of each side, all terms involving $x_i^2 y_i^2$ or $x_i x_j y_i y_j$ cancel, and the remaining 30 equations group into 15 matched pairs. They are summarized as follows, where (i, j, k) denotes any permutation of $(1, 2, 3)$ and $\epsilon = \pm 1$ its sign:

$$\begin{aligned} c_{ii}^j &= \epsilon\lambda_{ik}^{ii} \\ c_{ij}^k &= \epsilon\lambda_{ii}^{jj} \\ c_{ij}^j - c_{ik}^k &= \epsilon\lambda_{ii}^{jk} \\ c_{ii}^i - c_{ij}^j - c_{ik}^k &= \epsilon\lambda_{ik}^{ij}. \end{aligned} \quad (12)$$

At first glance it may seem that one can add a constant a to c_{ij}^j and c_{ij}^k, while adding $2a$ to c_{ii}^i, to derive a three-parameter family of solutions from a single one; but this is merely the transformation induced by the change of lift $\xi_i \mapsto \xi_i + a$ for $\tilde{\xi}_i$. So there is essentially only one solution. (It could be normalized by taking e.g. $c_{12}^1 = c_{23}^2 = c_{31}^3 = 0$, although we do not use this normalization here, preferring to save time later by keeping the indices 1, 2, and 3 in complete symmetry.)

The constant terms c_{ij}^0 of the multiplication table are as yet undetermined. They must be deduced from the associative law. There are several ways to compute each c_{ij}^0, and to prove that they agree, along with all the other relations implied by the associative law, is the final step in the construction of the quartic ring Q. Our key tool is the *Plücker relation* relating the wedge products of four vectors in a 2-dimensional space:

$$(a \wedge b)(c \wedge d) + (a \wedge c)(d \wedge b) + (a \wedge d)(b \wedge c) = 0,$$

or, as we will use it,

$$\lambda_{bb'}^{aa'}\lambda_{dd'}^{cc'} + \lambda_{cc'}^{aa'}\lambda_{bb'}^{dd'} + \lambda_{dd'}^{aa'}\lambda_{cc'}^{bb'} = 0.$$

To give succinct names to these relations among the λ's, note that $aa', \ldots, dd'$ are four of the six unordered pairs that can be formed from the symbols 1, 2, and 3, and the relation is nontrivial only when these four pairs are distinct. Consequently we denote it by $\mathrm{Pl}(ee', ff')$, where ee' and ff' are the two pairs that do not appear in it. Then $\mathrm{Pl}(ee', ff')$ as a polynomial in the λ's is unique up to sign, and we will never have occasion to fix a sign convention.

We are now ready to derive the associative law from the Plücker relations. Of course this is a task that could be left to a computer, but since we will soon be deriving the Plücker relations from the associative law, we find it advisable to present the process at least in summary form. Here it is:

$$\begin{gathered}
[(\xi_i\xi_i)\xi_j - (\xi_i\xi_j)\xi_i]_k = \mathrm{Pl}(jk, kk) \\
[(\xi_i\xi_j)\xi_k - (\xi_i\xi_k)\xi_j]_i = \mathrm{Pl}(ij, ik)
\end{gathered}$$

$$\begin{array}{ccc}
[(\xi_i\xi_i)\xi_j - (\xi_i\xi_j)\xi_i]_j & [(\xi_i\xi_j)\xi_i - (\xi_i\xi_i)\xi_j]_i \xrightarrow{\mathrm{Pl}(ij,kk)} [(\xi_i\xi_j)\xi_k - (\xi_j\xi_k)\xi_i]_k \\
\Big\downarrow{\scriptstyle \mathrm{Pl}(jj,kk)} & \Big\downarrow{\scriptstyle \mathrm{Pl}(ik,jk)} \qquad\qquad \Big\downarrow{\scriptstyle \mathrm{Pl}(ik,jk)} \\
[(\xi_i\xi_i)\xi_k - (\xi_i\xi_k)\xi_i]_j & [(\xi_i\xi_j)\xi_j - (\xi_j\xi_j)\xi_i]_j \xrightarrow{\mathrm{Pl}(ij,kk)} [(\xi_i\xi_j)\xi_k - (\xi_j\xi_k)\xi_i]_k
\end{array} \tag{13}$$

And here is the explanation:

- The notation $[\omega]_i$ denotes the coefficient of ξ_i when ω is expressed in terms of the basis $\{1, \xi_1, \xi_2, \xi_3\}$.
- Each of the first two equations is a direct calculation. For instance:

$$\begin{aligned}
[(\xi_i\xi_i)\xi_j - (\xi_i\xi_j)\xi_i]_k &= [(c_{ii}^0 + c_{ii}^i\xi_i + c_{ii}^j\xi_j + c_{ii}^k\xi_k)\xi_j - (c_{ij}^0 + c_{ij}^i\xi_i + c_{ij}^j\xi_j + c_{ij}^k\xi_k)\xi_i]_k \\
&= c_{ii}^i c_{ij}^k + c_{ii}^j c_{jj}^k + c_{ii}^k c_{jk}^k - c_{ij}^i c_{ii}^k - c_{ij}^j c_{ij}^k - c_{ij}^k c_{ik}^k \\
&= (c_{ii}^i - c_{ij}^j - c_{ik}^k)c_{ij}^k + c_{ii}^k(c_{jk}^k - c_{ij}^i) + c_{ii}^j c_{jj}^k \\
&= \epsilon(\lambda_{ik}^{ij}\lambda_{ii}^{jj} - \lambda_{ij}^{ii}\lambda_{jj}^{ik} + \lambda_{ik}^{ii}\lambda_{ij}^{jj}) \\
&= \mathrm{Pl}(jk, kk).
\end{aligned}$$

- The two lower diagrams show the instances of the associative law that produce a summand of c_{ii}^0 or c_{ij}^0, respectively. Each node in the diagrams yields a formula for c_{ii}^0 or c_{ij}^0 (having no denominator, and consequently belonging to the correct ideal $\mathfrak{a}_i^{-2}$ resp. $\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}$); and where two nodes are joined by a line, the *difference* between the two corresponding formulas is expressible as a Plücker relation.

We have now proved all of the associative law except the constant terms; that is, we now have that $(xy)z - x(yz) \in R$ for all $x, y, z \in Q$. Attacking the constant terms in the same manner as above leads to considerably heavier computations, which could be performed by computer (compare [3], top of p. 1343). Alternatively, we may use the following trick. Let $i, j, k \in \{1, 2, 3\}$ be any indices, and let $h \in \{1, 2, 3\}$ be an index distinct from k. Then using the already-proved ξ_h-component of the associative law,

$$\begin{aligned}
\xi_i(\xi_j\xi_k) - \xi_j(\xi_i\xi_k) &= [\xi_h(\xi_i(\xi_j\xi_k)) - \xi_h(\xi_j(\xi_i\xi_k))]_h \\
&= [(\xi_h\xi_i)(\xi_j\xi_k) - (\xi_h\xi_j)(\xi_i\xi_k)]_h \\
&= [((\xi_h\xi_i)\xi_j)\xi_k - ((\xi_h\xi_j)\xi_i)\xi_k]_h.
\end{aligned}$$

This last is necessarily zero, since it consists of the number $(\xi_h\xi_i)\xi_j - (\xi_h\xi_j)\xi_i \in R$ multiplied by ξ_k, and thus has no ξ_h-component. ■

8.2 Ring to resolvent

Now we will conversely create a resolvent given a quartic ring Q by reversing our steps. The first few steps are easy: writing $Q = R \oplus \mathfrak{a}_1\xi_1 \oplus \mathfrak{a}_2\xi_2 \oplus \mathfrak{a}_3\xi_3$, the multiplication table can be encoded in a family of c_{ij}^k's, from which the fifteen values $\lambda_{k\ell}^{ij}$ are determined through (12). These $\lambda_{k\ell}^{ij}$ satisfy the fifteen Plücker relations by (13). The target M of our resolvent map is also determined: its rank is 2, and its top exterior power must be $\Lambda^3(Q/R)$. It then remains to construct the vectors $\mu_{ij} \in \mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}M$ such that their pairwise exterior products $\mu_{ij} \wedge \mu_{k\ell}$ have the specified value $\lambda_{k\ell}^{ij}$.

There is one ring Q for which this problem takes a striking turn: the *trivial* ring $Q = R[\mathfrak{a}_1\epsilon_1, \mathfrak{a}_2\epsilon_2, \mathfrak{a}_3\epsilon_3]/\sum_{i,j}(\mathfrak{a}_i\mathfrak{a}_j\epsilon_i\epsilon_j)$ where all c's and thus all λ's are zero. Here the six μ_{ij} can be chosen independently from any one-dimensional subspace of M_K. For all other systems of λ's, the family of resolvent maps is much smaller, as we will now prove.

Lemma 8.4. *Fix a rank-2 R-lattice M and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ of R ($n \geq 2$). Let λ_{ij}, $1 \leq i < j \leq n$ be elements of $\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\Lambda^2 M$ satisfying the Plücker relations*

$$\lambda_{ij}\lambda_{k\ell} + \lambda_{i\ell}\lambda_{jk} = \lambda_{ik}\lambda_{j\ell}.$$

Define the ideal

$$\mathfrak{c} = (\Lambda^2 M)^{-1} \sum_{i<j} \lambda_{ij}\mathfrak{a}_i\mathfrak{a}_j;$$

that is, it is the smallest ideal such that each λ_{ij} belongs not merely to $\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\Lambda^2 M$, but to $\mathfrak{c}\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\Lambda^2 M$.

If $\mathfrak{c} \neq 0$, then the possible choices of elements $\mu_i \in \mathfrak{a}_i^{-1}M$ such that $\mu_i \wedge \mu_j = \lambda_{ij}$ are in noncanonical bijection with the disjoint union

$$\coprod_{R \supseteq \mathfrak{a} \supseteq \mathfrak{c}} R/\mathfrak{a}.$$

Proof. Some λ_{ij} is nonzero, without loss of generality λ_{12}. Let V be an abstract K-vector space of dimension 2. We construct vectors $v_1, \ldots, v_n$ whose exterior products are proportional to the λ's as follows. First let (v_1, v_2) be a basis of V. Then, for $3 \leq i \leq n$, take

$$v_i = \frac{-\lambda_{2i}v_1 + \lambda_{1i}v_2}{\lambda_{12}}$$

to give the products $v_1 \wedge v_i$ and $v_2 \wedge v_i$ the desired values. The remaining λ_{ij} have not been used, but their values were forced by the Plücker relations anyway, so we have a system of v_i such that

$$v_i \wedge v_j = \frac{\lambda_{ij}}{\lambda_{12}} \cdot v_1 \wedge v_2.$$

Consider the R-module

$$M_0 = \sum_{i=1}^{n} \mathfrak{a}_i v_i.$$

It is a lattice (finitely generated, torsion-free, and of rank 2), and its exterior square is

$$\Lambda^2 M_0 = \sum_{i<j} \mathfrak{a}_i\mathfrak{a}_j(v_i \wedge v_j) = \sum_{i<j} \mathfrak{a}_i\mathfrak{a}_j \frac{\lambda_{ij}}{\lambda_{12}} v_1 \wedge v_2 = \mathfrak{c} \cdot \Lambda^2 M \cdot \frac{v_1 \wedge v_2}{\lambda_{12}}.$$

If $\mathfrak{c}$ happens to be the unit ideal, then M_0 can be identified with M (in essentially only one way), and the v_i are the elements of $\mathfrak{a}_i^{-1}M$ that we seek. In general, we must embed M_0 into M or, what is essentially the same thing, embed M into V such that the image contains M_0. Since

the v_i are unique up to $\mathrm{GL}_2 K$-equivalence, each embedding of the latter sort yields a distinct solution. So the lemma is reduced to the following problem:

Given a rank-2 lattice M_0 and an ideal $\mathfrak{c} \subseteq R$, how can we parametrize lattices M ($M_0 \subseteq M \subseteq M_K$) satisfying $\Lambda^2 M = \mathfrak{c}^{-1}\Lambda^2 M_0$?

Note that we must have $M \subseteq \mathfrak{c}^{-1}M_0$, since $M \wedge M_0 \subseteq M \wedge M = \mathfrak{c}^{-1}\Lambda^2 M_0$. Pick a decomposition $\mathfrak{c}^{-1}M_0 \cong \mathfrak{d}_1 \oplus \mathfrak{d}_2$. Then consider the map $\pi : M \to \mathfrak{d}_1$ that is the restriction of projection to the first factor. We have $\ker \pi = \{0\} \times \mathfrak{a}\mathfrak{d}_2$ and $\operatorname{im} \pi = \mathfrak{b}\mathfrak{d}_1$ for some ideals $\mathfrak{a}, \mathfrak{b}$ subject to the familiar behavior of top exterior powers in exact sequences:

$$\mathfrak{c}^{-1}\Lambda^2 M_0 = \Lambda^2 M = \mathfrak{a}\mathfrak{d}_2 \wedge \mathfrak{b}\mathfrak{d}_1 = \mathfrak{a}\mathfrak{b}\mathfrak{c}^{-2}\Lambda^2 M_0,$$

that is, $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$. Now if $\mathfrak{a}$ and $\mathfrak{b}$ are fixed, the lattice M is determined by a picking a coset in $\mathfrak{d}_2/\mathfrak{a}\mathfrak{d}_2$ for the preimage of each point $b \in \operatorname{im} \pi$; this is determined by an R-module map

$$\mathfrak{b}\mathfrak{d}_1 \to \mathfrak{d}_2/\mathfrak{a}\mathfrak{d}_2$$

or, since $\mathfrak{c}\mathfrak{d}_1$ is necessarily in the kernel,

$$\mathfrak{b}\mathfrak{d}_1/\mathfrak{c}\mathfrak{d}_1 \to \mathfrak{d}_2/\mathfrak{a}\mathfrak{d}_2.$$

We can identify both the domain and the target of this map with $R/\mathfrak{a}$ via the standard result that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a Dedekind domain R, then $\mathfrak{a}/\mathfrak{a}\mathfrak{b} \cong R/\mathfrak{b}$. (Proof: Use the Chinese Remainder Theorem to find $a \in \mathfrak{a}$ that has minimal valuation with respect to each of the primes dividing $\mathfrak{b}$. Then a generates $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$, and $a \mapsto 1$ is the desired isomorphism.) Then the desired parameter space is $\mathrm{Hom}_R(R/\mathfrak{a}, R/\mathfrak{a}) \cong R/\mathfrak{a}$. Letting $\mathfrak{a}$ vary yields the claimed bijection. ∎

As the reader may have guessed, the ideal $\mathfrak{c}$ can be identified with the *content* of the ring Q as defined in a way mirroring Bhargava ([3], Definition 14):

Theorem 8.5 (cf. [3], Corollary 4)**.** *Let Q be a nontrivial quartic R-algebra. Then*

(*a*) *there is an ideal $\mathfrak{c}$, called the* content *of Q, characterized by the following property: For each ideal $\mathfrak{a} \subseteq R$, there exists a quartic R-algebra Q' such that $Q \cong R + \mathfrak{a}Q'$ if and only if $\mathfrak{a} \supseteq \mathfrak{c}$.*

(*b*) *The cubic resolvents (M, θ, ϕ), up to isomorphism, are in noncanonical bijection with the disjoint union*

$$\coprod_{R \supseteq \mathfrak{a} \supseteq \mathfrak{c}} R/\mathfrak{a}.$$

Proof. Here the only new assertion is the reinterpretation of the ideal $\mathfrak{c}$. The existence of the content ideal is a classical result, but here we re-prove it in a way that automatically links it to the $\mathfrak{c}$ of Lemma 8.4.

If Q' is defined by a decomposition $Q' = R \oplus \mathfrak{a}_1\xi_1 \oplus \mathfrak{a}_2\xi_2 \oplus \mathfrak{a}_3\xi_3$ and multiplication coefficients c_{ij}^k, then $R + \mathfrak{a}Q'$ can be described by the same multiplication coefficients, but on the underlying lattice $R \oplus \mathfrak{a}\mathfrak{a}_1\xi_1 \oplus \mathfrak{a}\mathfrak{a}_2\xi_2 \oplus \mathfrak{a}\mathfrak{a}_3\xi_3$. Here we note that the c_{ij}^k belong to $\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\mathfrak{a}_k$ although the new lattice demands only that they belong to $\mathfrak{a}^{-1}\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\mathfrak{a}_k$.

Reversing this process, we see that if $Q = R \oplus \mathfrak{a}_1\xi_1 \oplus \mathfrak{a}_2\xi_2 \oplus \mathfrak{a}_3\xi_3$ is defined by a family of coefficients c_{ij}^k or, equivalently, $\lambda_{k\ell}^{ij}$, then we can produce a ring Q' with $Q = R + \mathfrak{a}Q'$ if and only if all $\lambda_{k\ell}^{ij}$ belong to $\mathfrak{a}$ times the ideals $\mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}\mathfrak{a}_k^{-1}\mathfrak{a}_\ell^{-1}\Lambda^2 M$ where they belong, in other words

$$(\Lambda^2(M))^{-1} \sum_{i,j,k,\ell} \lambda_{k\ell}^{ij}\mathfrak{a}_i\mathfrak{a}_j\mathfrak{a}_k\mathfrak{a}_\ell \subseteq \mathfrak{a}.$$

But the left-hand side is precisely the ideal $\mathfrak{c}$ in Lemma 8.4.

To achieve complete rigor, we ought to make $(1, \xi_1, \xi_2, \xi_3)$ a *normal* basis, that is, $c_{12}^1 = c_{23}^2 = c_{31}^3 = 0$, so that the c-system and the λ-system are in exact bijection; we should also remark that, by construction, the c_{ij}^0 always belong to the correct ideals if the other c_{ij}^k do. ∎

Bhargava proved ([3], Corollary 4) that the number of cubic resolvents of a quartic ring over $\mathbb{Z}$ is the sum of the divisors of its content. Likewise, we now have:

Corollary 8.6. *If Q is a nontrivial quartic algebra over the ring of integers of a number field, the number of cubic resolvents of Q equals the sum of the norms of the divisors of its content.*

We also have the following:

Corollary 8.7. *Every quartic algebra over a Dedekind domain possesses at least one cubic resolvent.*

8.3 The cubic ring structure of the resolvent

In contrast to the classical presentation, the resolvent maps we have constructed take their values in *modules*, without any explicit connection to a ring. In fact, there is the structure of a cubic ring already latent in a resolvent. It can be revealed by the following trick of multilinear algebra (compare [13], p. 1076). First pick a decomposition $Q' = \mathfrak{a}_1\tilde{\xi}_1 \oplus \mathfrak{a}_2\tilde{\xi}_2 \oplus \mathfrak{a}_3\tilde{\xi}_3$, and let $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \cong \Lambda^3 Q' \cong \Lambda^2 M$. Writing

$$\phi(x_1\tilde{\xi}_1 + x_2\tilde{\xi}_2 + x_3\tilde{\xi}_3) = \sum_{i\le j} x_i x_j \mu_{ij} \quad (\mu_{ij} \in \mathfrak{a}_i^{-1}\mathfrak{a}_j^{-1}M),$$

consider the determinant

$$\begin{aligned}\Delta &= 4\det\begin{bmatrix} \mu_{11} & \frac{1}{2}\mu_{12} & \frac{1}{2}\mu_{13} \\ \frac{1}{2}\mu_{12} & \mu_{22} & \frac{1}{2}\mu_{23} \\ \frac{1}{2}\mu_{13} & \frac{1}{2}\mu_{23} & \mu_{33}\end{bmatrix} \\ &= 4\mu_{11}\mu_{22}\mu_{33} + \mu_{12}\mu_{13}\mu_{23} - \mu_{11}\mu_{23}^2 - \mu_{22}\mu_{13}^2 - \mu_{33}\mu_{12}^2 \quad \in \mathfrak{a}^{-2}\operatorname{Sym}^3 M\end{aligned}$$

(the two expressions are equal except when $\operatorname{char} K = 2$, in which case the first becomes purely motivational). Next, the $\Lambda^2 M \cong \mathfrak{a}$-valued pairing $\wedge$ on M gives an identification of M with $\mathfrak{a}M^*$, so we can transform

$$\mathfrak{a}^{-2}\operatorname{Sym}^3 M \cong \mathfrak{a}^{-2}\operatorname{Sym}^3(\mathfrak{a}M^*) = \mathfrak{a}\operatorname{Sym}^3(M^*) \cong \operatorname{Sym}^3(M^*) \otimes \Lambda^2(M).$$

Thus Δ yields a cubic map $\delta : M \to \Lambda^2 M$, which by Theorem 7.1 is equivalent to a cubic ring C with an identification $C/R \cong M$. That δ is independent of the chosen basis $(\tilde{\xi}_1, \tilde{\xi}_2, \tilde{\xi}_3)$ follows from properties of the determinant, at least when $\operatorname{char} K \neq 2$.

Two theorems concerning this cubic ring structure we will state without proof, since they are mere polynomial identities already implied by Bhargava's work over $\mathbb{Z}$:

Theorem 8.8 (cf. [3], equation (30))**.** *Let Q be a quartic ring, and let C be the cubic ring whose structure is determined by the resolvent map data $\theta : \Lambda^3(Q/R) \to \Lambda^2(C/R)$ and $\phi : Q/R \to C/R$. For any element $x \in Q$ and any lift $y \in C$ of the element $\phi(x) \in C/R$, we have the equality*

$$\theta(x \wedge x^2 \wedge x^3) = y \wedge y^2.$$

As Bhargava notes, this identity may be used as an alternative to Theorem 7.1 to determine the multiplicative structure on C; it works in all cases over $\mathbb{Z}$ except when Q has nilpotents.

We end with a theorem concerning discriminants, which until now have been conspicuously absent from our discussion, in direct contrast to Bhargava's presentation. Recall that the discriminant of a $\mathbb{Z}$-algebra Q with a $\mathbb{Z}$-basis $(\xi_1, \ldots, \xi_n)$ is defined as the determinant of the matrix $[\operatorname{Tr}(\xi_i\xi_j)]_{i,j}$. In like manner, define the *discriminant* of a rank-n R-algebra Q to be the map

$$\operatorname{disc}(Q) : x_1 \wedge \cdots \wedge x_n \mapsto \det[\operatorname{Tr}(x_i x_j)]_{i,j}.$$

It is quadratic and thus can be viewed as an element of $(\Lambda^n Q^*)^{\otimes 2}$, a rank-1 lattice that is not in general isomorphic to R. The discriminants of a quartic ring and its cubic resolvent are "equal" in precisely the way one might hope:

Theorem 8.9 (cf. [3], Proposition 13)**.** *Let Q, C, θ be as above. The isomorphism*

$$(\theta^*)^{\otimes 2} : (\Lambda^2(C/R)^*)^{\otimes 2} \to (\Lambda^3(Q/R)^*)^{\otimes 2}$$

carries $\operatorname{disc} C$ *to* $\operatorname{disc} Q$*.*

Example 8.10. Once again, we recapitulate the situation over $\mathbb{Z}$. Here, once bases $Q/R = \mathbb{Z}\xi_1 \oplus \mathbb{Z}\xi_2 \oplus \mathbb{Z}\xi_3$ and $C/R = \mathbb{Z}\eta_1 \oplus \mathbb{Z}\eta_2$ have been fixed so that θ is given simply by $\xi_1 \wedge \xi_2 \wedge \xi_3 \mapsto \eta_1 \wedge \eta_2$, the resolvent map ϕ can be written as a pair of ternary quadratic forms, or, even more pictorially, as a pair of symmetric matrices

$$\begin{bmatrix} a_{11} & \frac{1}{2}a_{12} & \frac{1}{2}a_{13} \\ \frac{1}{2}a_{12} & a_{22} & \frac{1}{2}a_{23} \\ \frac{1}{2}a_{13} & \frac{1}{2}a_{23} & a_{33} \end{bmatrix}, \begin{bmatrix} b_{11} & \frac{1}{2}b_{12} & \frac{1}{2}b_{13} \\ \frac{1}{2}b_{12} & b_{22} & \frac{1}{2}b_{23} \\ \frac{1}{2}b_{13} & \frac{1}{2}b_{23} & b_{33} \end{bmatrix}$$

where $a_{ij}, b_{ij} \in \mathbb{Z}$. Some salient examples follow:

- First note that there is a resolvent map of $\mathbb{C}$-algebras from $Q_0 = \mathbb{C}^{\oplus 4}$ to $C_0 = \mathbb{C}^{\oplus 3}$ given by the roots of the equation-solver's resolvent

  $$(x, y, z, w) \mapsto (xy + zw, xz + yw, xw + yz)$$

  or, more accurately, by its reduction modulo $\mathbb{C}$

  $$\phi_0 : (x, y, z, 0) \mapsto (xy - yz, xz - yz, 0),$$

  supplemented of course by the standard identification $\theta_0 : \Lambda^3(Q_0/\mathbb{C}) \to \Lambda^2(C_0/\mathbb{C})$.

  Accordingly, if we have a quartic $\mathbb{Z}$-algebra $Q \subseteq Q_0$ and a cubic $\mathbb{Z}$-algebra $C \subseteq C_0$ on which the restrictions of ϕ_0, θ_0, and θ_0^{-1} are well-defined, then it automatically follows that $C/\mathbb{Z}$ is a resolvent for Q with attached cubic ring structure C.

- As an example, consider the ring

  $$Q = \mathbb{Z} + p(\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}) = \{(a, b, c, d) \in \mathbb{Z}^{\oplus 4} : a \equiv b \equiv c \equiv d \bmod p\}$$

  of content p, for each prime p. The image of ϕ_0 lies in the space $C'/\mathbb{Z}$, where

  $$C' = \mathbb{Z} + p^2 \cdot \mathbb{Z}^{\oplus 3}.$$

  But C' is not a cubic resolvent of S: it has index p^4 in $\mathbb{Z}^{\oplus 3}$, while S has index p^3 in $\mathbb{Z}^{\oplus 4}$, so the restriction of θ_0 cannot possibly be an isomorphism. We must enlarge C' by a factor of p. Note that any subgroup C such that

  $$\mathbb{Z} + p^2 \cdot \mathbb{Z}^{\oplus 3} \subseteq C \subseteq \mathbb{Z} + p \cdot \mathbb{Z}^{\oplus 3}$$

  is a ring, since the product of two elements in $p \cdot \mathbb{Z}^{\oplus 3}$ lies in $p^2 \cdot \mathbb{Z}^{\oplus 3}$. So any ring of the form

  $$C = \mathbb{Z} + p^2 \cdot \mathbb{Z}^{\oplus 3} + \langle ap, bp, 0 \rangle$$

  is a cubic resolvent of Q. Letting $[a : b]$ run over $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ yields the $p+1$ cubic resolvents predicted by Theorem 8.5.

- Note that some of these resolvents are isomorphic under the automorphism group of Q, which is simply S_4 acting by permuting the coordinates. One verifies that S_4 acts through its quotient S_3, which in turn permutes the three distinguished points $0, 1, \infty$ on $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$. Accordingly, if we are using Theorem 8.3 to count quartic rings, the ring Q will appear not $p+1$ times but $\lceil p/6 \rceil + 1$ times (1 time if $p = 2$ or $p = 3$). This is no contradiction with Theorem 8.5, which gives the number of resolvents *as maps out of the given ring* Q.

9 Conclusion and acknowledgements

We have found the Dedekind domain to be a suitable base ring for generalizing the integral parametrizations of algebras and their ideals by Bhargava and his forebears. In each case, ideal decompositions $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ fill the role of $\mathbb{Z}$-bases, and elements of appropriate fractional ideals take the place of integers in the parameter spaces. We have also shown that the notion of "balanced," introduced by Bhargava to describe the ideal triples parametrized by general nondegenerate $2 \times 2 \times 2$ cubes, has some beautiful properties and is worthy of further study. We expect that the methods herein will extend to replicate the other parametrizations in Bhargava's "Higher Composition Laws" series and may shed light on the analytic properties of number fields and orders of low degree over base fields other than $\mathbb{Q}$.

I thank my thesis advisor, Benedict Gross, for many helpful discussions and comments. I thank Melanie Wood for clarifications on the relationships between my work and hers. I thank Arul Shankar for useful discussions, especially for informing me that he and Wood had been interested in the question answered by Corollary 8.7. Finally, I thank Brian Conrad for the suggestion that I work with Prof. Gross.

References

[1] Manjul Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004.

[2] Manjul Bhargava. Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)*, 159(2):865–886, 2004.

[3] Manjul Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3):1329–1360, 2004.

[4] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[5] Manjul Bhargava. Higher composition laws. IV. The parametrization of quintic rings. *Ann. of Math. (2)*, 167(1):53–94, 2008.

[6] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[7] Manjul Bhargava and Ila Varma. The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders. Unpublished. `http://arxiv.org/abs/1401.5875v1`, 2014.

[8] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013.

[9] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree.* Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[10] John Milnor. *Introduction to algebraic K-theory.* Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971. Annals of Mathematics Studies, No. 72.

[11] Bjorn Poonen. The moduli space of commutative algebras of finite rank. *J. Eur. Math. Soc. (JEMS)*, 10(3):817–836, 2008.

[12] Melanie Matchett Wood. Gauss composition over an arbitrary base. *Adv. Math.*, 226(2):1756–1771, 2011.

[13] Melanie Matchett Wood. Parametrizing quartic algebras over an arbitrary base. *Algebra Number Theory*, 5(8):1069–1094, 2011.

[14] Melanie Matchett Wood. Parametrization of ideal classes in rings associated to binary forms. *J. reine angew. Math.*, 689:169–199, 2014.