

Quartic Rings Associated to Binary Quartic Forms

Melanie Matchett Wood

American Institute of Mathematics, and Department of Mathematics,
and Stanford University, Building 380, Sloan Hall, Stanford, CA 94305,
USA

Correspondence to be sent to: mwood@math.stanford.edu

We give a bijection between binary quartic forms and quartic rings with a monogenic cubic resolvent ring, relating the rings associated to binary quartic forms with Bhargava's cubic resolvent rings. This gives a parametrization of quartic rings with monogenic cubic resolvents. We also give a geometric interpretation of this parametrization.

1 Introduction

Algebraic objects associated to binary forms have long been studied. Dedekind originally associated a quadratic ring and ideal class to every binary quadratic form [8]. In fact, binary quadratic forms exactly parametrize ideal classes of quadratic rings (see [7, Section 5.2, 16], or [24] for a treatment that includes all binary quadratic forms, even the zero form!). In 1940, Delone and Faddeev [12] associated cubic rings to binary cubic forms and found that binary cubic forms exactly parametrize cubic rings (see also [14] for a treatment of all binary cubic forms).

In fact, one can associate an n -ic ring (a ring isomorphic to \mathbb{Z}^n as a \mathbb{Z} module) to a binary n -ic form for any n . (When $n = 2, 3, 4$, we also call an n -ic ring *quadratic*, *cubic*, *quartic*, respectively.) Early work on the rings associated to binary forms was done by Birch and Merriman [4] and Nakagawa [17]. Del Corso et al. [9] determine the splitting of the prime p in such a ring in terms of the factorization of the binary n -ic form modulo p^k . Simon [20] associates an ideal class of the associated ring to a binary n -ic form, and

Received December 20, 2010; Revised March 23, 2011; Accepted March 29, 2011

in [21] he applies this ideal class to study integer solutions to equations of the form $Cy^d = F(x, z)$, where F is a binary form. In [23], it is determined exactly what algebraic structures are parametrized by binary n -ic forms, for all n . This structure is a rank n ring and an ideal class for that ring, such that the action of the ring on the ideal class satisfies a certain exact sequence (which comes naturally from geometry). When $n=2$, the exact sequence condition is vacuous, and when $n=3$ the condition forces the ideal class to be the unit ideal. In this note, we give a different point of view (from [23]) on the algebraic data parametrized by binary quartic forms. We prove the following, which is the main result of this paper.

Theorem 1.1. There is a natural, discriminant preserving bijection between the set of $GL_2(\mathbb{Z})$ -equivalence classes of binary quartic forms and the set of isomorphism classes of pairs (Q, C) where Q is a quartic ring and C is a monogenic cubic resolvent of Q (where isomorphisms are required to preserve the generator of C modulo \mathbb{Z}). \square

In particular, in this paper we construct the bijection of Theorem 1.1 explicitly. For example, the construction of the quartic ring is given in Equation (2). The $GL_2(\mathbb{Z})$ action on binary quartic forms is given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ f(x, y) = f(ax + cy, bx + dy)$. A *monogenic* ring is one that is generated by one element as a \mathbb{Z} -algebra. The above simple criteria for when a quartic ring is associated to a binary quartic form is an application of the notion of the *cubic resolvent* of a quartic ring, which was introduced by Bhargava [1] in his parametrization of quartic rings with their cubic resolvents by pairs of ternary quadratic forms. Theorem 1.1 is used by Bhargava and Shankar [3] in their determination of the average number of 2-torsion elements in the class groups in monogenic maximal cubic orders. Surprisingly, these averages are different than for general maximal cubic orders!

We recall Bhargava’s parametrization of quartic rings and their cubic resolvents here. If we write ternary quadratic forms as matrices, we can give the $GL_3(\mathbb{Z})$ action on pairs of ternary quadratic forms as $(A, B) \mapsto (gAg^t, gBg^t)$ for $g \in GL_3(\mathbb{Z})$. The action of $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ on a pair (A, B) of ternary quadratic forms takes (A, B) to $(aA + bB, cA + dB)$.

Theorem 1.2 ([1, Theorem 1]). There is a natural, discriminant preserving bijection between the set of $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$ -equivalence classes of pairs of ternary quadratic forms and isomorphism classes (Q, C) where Q is a quartic ring and C is a cubic resolvent of Q . \square

Cubic resolvents are integral models of the classical notion of the cubic resolvent field of a quartic field, and they have the same discriminant as their quartic ring. A cubic resolvent C of a quartic ring O comes with a quadratic map from O to C (suppressed from the notation (O, C)), that is, a function $q: O \rightarrow C$ such that for $a \in \mathbb{Z}$, we have $q(ax) = a^2q(x)$, and also such that $q(x+y) - q(x) - q(y)$ is a bilinear form in x and y . When O is a quartic order in a field $\mathbb{Q}(\alpha)$ whose Galois closure has Galois group S_4 or A_4 , then $\mathbb{Q}(\alpha\alpha' + \alpha'\alpha'')$ is the classical cubic resolvent field of $\mathbb{Q}(\alpha)$, where α', α'' , and α''' denote the conjugates of α . In this case, a cubic resolvent ring of O can be defined to be an order C in the cubic resolvent field with the same discriminant as O such that for all $x \in O$, we have $xx' + x'x'' \in C$. The quadratic map from O to C is $x \rightarrow xx' + x'x''$. For other quartic rings O , the definition is a little more subtle (in particular, there is no classical cubic resolvent field) and is given in the Appendix. Every quartic ring has a cubic resolvent ring and quartic maximal orders have a unique cubic resolvent ring [1, Corollary 4]. An isomorphism (O, C) to (O', C') of pairs each consisting of a quartic ring and a cubic resolvent of that quartic ring is given by ring isomorphisms $O \cong O'$ and $C \cong C'$ that commute with the quadratic maps $O \rightarrow C$ and $O' \rightarrow C'$. Note that in Theorem 1.1 the pairs (O, C) also come with a generator of C as a \mathbb{Z} -algebra, and in an isomorphism between (O, C) and (O', C') , the induced map $C/\mathbb{Z} \cong C'/\mathbb{Z}$ must take the chosen generator of C to the chosen generator of C' .

Theorem 1.2 gives a parametrization of all quartic rings with their cubic resolvents. Most cubic rings are not generated by one element as a \mathbb{Z} -algebra, but the special cubic rings which are generated by one element are called monogenic. Our Theorem 1.1 gives a parametrization of quartic rings with monogenic cubic resolvents. Alternatively, Theorem 1.1 can be viewed as answering the question “In the association of quartic rings to binary quartic forms (as in [9, 17, 20, 23]), which quartic rings appear?”

We prove Theorem 1.1 by mapping binary quartic forms to pairs of ternary quadratic forms in a way that respects the constructions on the associated quartic rings (as in [1, 9, 17, 20, 23] respectively). This map is given in Section 2. We then see that the rings associated to binary quartic forms have monogenic cubic resolvents, and then that any quartic ring with a monogenic cubic resolvent is associated to some binary quartic form. We then in Section 3 study how the $\mathrm{GL}_2(\mathbb{Z})$ -action on binary quartic forms changes the associated quartic ring, which allows us to prove our main result (Theorem 1.1) in Section 5, after recording some preliminaries about monogenized cubic rings in Section 4. In Section 6, we explain the results of this paper from a geometric point of view, and discuss analogs in which the integers are replaced by an arbitrary scheme. In Section 7, we see how the $\mathrm{GL}_2(\mathbb{Z})$ invariants of a binary

quartic form are related to the monogenized cubic resolvent ring of the associated quartic ring.

2 Constructions

In this section, we give the constructions of rings from forms mentioned in Section 1, as well as the relationship between binary quartic forms and pairs of ternary quadratic forms that will be the basis of the proof of Theorem 1.1. A *based n -ic ring* is an n -ic ring R , along with a choice of $\zeta_1, \dots, \zeta_{n-1} \in R/\mathbb{Z}$ such that $1, \zeta_1, \dots, \zeta_{n-1}$ is a \mathbb{Z} -module basis of R (which clearly does not depend on the lift of ζ_i to R). If R is an n -ic ring, then for $r \in R$, multiplication by r is a linear transformation on the \mathbb{Z} -module R , and we write $\text{Tr}(r)$ for the trace of that linear transformation. The discriminant of a n -ic ring with \mathbb{Z} -module basis ζ_i is the determinant of the matrix with i, j entry $\text{Tr}(\zeta_i \zeta_j)$ (which is easily seen not to depend on the choice of basis).

2.1 Construction of a ring from a binary form

Given a binary n -ic form, $f = f_0x^n + f_1x^{n-1}y + \dots + f_ny^n$ with $f_i \in \mathbb{Z}$, such that $f_0 \neq 0$, we can form a based n -ic ring R_f as a subring of $\mathbb{Q}(\beta)/(f_0\beta^n + f_1\beta^{n-1} + \dots + f_n)$ with \mathbb{Z} -module basis

$$\begin{aligned} \zeta_0 &= 1, \\ \zeta_1 &= f_0\beta, \\ \zeta_2 &= f_0\beta^2 + f_1\beta, \\ &\vdots \\ \zeta_k &= f_0\beta^k + \dots + f_{k-1}\beta, \\ &\vdots \\ \zeta_{n-1} &= f_0\beta^{n-1} + \dots + f_{n-2}\beta, \end{aligned} \tag{1}$$

as first considered by Birch and Merriman [4]. It is shown that R_f is a ring in [17, Proposition 1.1]. We have the discriminant equality $\text{Disc } R_f = \text{Disc } f$ (see, for example, [19, Proposition 4]). In Section 6, we will recall a less explicit, but more natural geometric construction of R_f that was developed in [23]. In this paper we use this construction when $n = 3, 4$.

Given a binary quartic form, $f = f_0x^4 + f_1x^3y + f_2x^2y^2 + f_3xy^3 + f_4y^4$ with $f_i \in \mathbb{Z}$ and $f_0 \neq 0$, we can work out the multiplication table of R_f explicitly as follows,

letting $\zeta'_3 = \zeta_3 + f_3$:

$$\begin{aligned}
 \zeta_1^2 &= -f_1\zeta_1 + f_0\zeta_2, \\
 \zeta_1\zeta_2 &= -f_2\zeta_1 + f_0\zeta'_3 - f_0f_3, \\
 \zeta_1\zeta'_3 &= -f_0f_4, \\
 \zeta_2\zeta_2 &= -f_3\zeta_1 - f_2\zeta_2 + f_1\zeta'_3 - f_1f_3 - f_0f_4, \\
 \zeta_2\zeta'_3 &= -f_4\zeta_1 - f_1f_4, \\
 (\zeta'_3)^2 &= -f_4\zeta_2 + f_3\zeta'_3 - f_3^2 - f_2f_4.
 \end{aligned}
 \tag{2}$$

Even if $f_0 = 0$, we can use the above multiplication table to construct a based quartic ring R_f from a binary quartic form f . For example, when $f = 0$, we see that $R_f = \mathbb{Z}[\zeta_1, \zeta_2, \zeta'_3]/(\zeta_1, \zeta_2, \zeta'_3)^2$.

Given a binary cubic form, $f = ax^3 + bx^2y + cxy^2 + dy^3$ with $a, b, c, d \in \mathbb{Z}$, we let $\omega = -\zeta_1$ and $\theta = -\zeta_2 - c$ and have the multiplication table for R_f as follows:

$$\begin{aligned}
 \omega\theta &= -ad, \\
 \omega^2 &= -ac + b\omega - a\theta, \\
 \theta^2 &= -bd + d\omega - c\theta.
 \end{aligned}
 \tag{3}$$

Given a based cubic ring C with a \mathbb{Z} -module basis ω, θ for C/\mathbb{Z} , there is a unique choice of lifts of ω and θ to C such that $\omega\theta \in \mathbb{Z}$. Thus a based cubic ring is the same as a cubic ring with choice of \mathbb{Z} -module basis $1, \omega, \theta$ such that $\omega\theta \in \mathbb{Z}$. The construction of R_f from f is equivariant under a $\text{GL}_2(\mathbb{Z})$ action that we specify here. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $\text{GL}_2(\mathbb{Z})$ and $f = F(x, y)$ be a binary cubic form. Then $g \circ f = \frac{1}{ad-bc}F(ax + cy, bx + dy)$. If ω, θ is a basis of C/\mathbb{Z} , then after action by g , the new basis of C/\mathbb{Z} is ω', θ' , where $\begin{bmatrix} \omega' \\ \theta' \end{bmatrix} = g \begin{bmatrix} \omega \\ \theta \end{bmatrix}$. We can now recall the parametrization of cubic rings by binary cubic forms, discovered first by Delone and Faddeev [12] and given more recently and in language closer to ours by Gan et al. [14, Proposition 4.2].

Theorem 2.1 (c.f. [14]). The above construction gives a bijection between based cubic rings and binary cubic forms. The bijection between based cubic rings and binary cubic forms is equivariant for the above $\text{GL}_2(\mathbb{Z})$ actions, giving a bijection between cubic rings and $\text{GL}_2(\mathbb{Z})$ -classes of binary cubic forms. □

2.2 Construction of a quartic ring and cubic resolvent from a pair of ternary quadratic forms

We can represent a pair of ternary quadratic forms by a pair of matrices (A, B) such that

$$A = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \frac{a_{13}}{2} \\ \frac{a_{12}}{2} & a_{22} & \frac{a_{23}}{2} \\ \frac{a_{13}}{2} & \frac{a_{23}}{2} & a_{33} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & \frac{b_{12}}{2} & \frac{b_{13}}{2} \\ \frac{b_{12}}{2} & b_{22} & \frac{b_{23}}{2} \\ \frac{b_{13}}{2} & \frac{b_{23}}{2} & b_{33} \end{pmatrix}$$

with $a_{ij}, b_{ij} \in \mathbb{Z}$. Bhargava [1, Section 3.2] constructed a based quartic ring Q from (A, B) , by giving the multiplication table explicitly in terms of the a_i and b_i . See also Section 6 for a geometric description of this quartic ring that was developed in [22]. We define the *determinant* of the pair (A, B) to be the binary cubic form $4 \text{Det}(Ax - By)$. The based cubic resolvent associated to a pair (A, B) is given by this determinant binary cubic form via Theorem 2.1.

We have a $\text{GL}_3(\mathbb{Z})$ action on pairs of ternary quadratic forms given by $(A, B) \mapsto (gAg^t, gBg^t)$ for $g \in \text{GL}_3(\mathbb{Z})$. The action of $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ on a pair (A, B) of ternary quadratic forms takes (A, B) to $(aA + bB, cA + dB)$. In Bhargava’s construction of a quartic ring Q and cubic resolvent from a pair of ternary quadratic forms, the $\text{GL}_2(\mathbb{Z}) \times \text{GL}_3(\mathbb{Z})$ action on the pair of ternary quadratic forms corresponds to changing the basis of Q and its cubic resolvent, and thus giving the map in Theorem 1.2 (see [1]).

2.3 Construction of a pair of ternary quadratic forms from a binary quartic form

The new construction of this paper is the map

$$\Psi : \{\text{binary quartic forms}\} \longrightarrow \{\text{pairs of ternary quadratic forms}\}.$$

which sends $f = f_0x^4 + f_1x^3y + f_2x^2y^2 + f_3xy^3 + f_4y^4$ to (A_0, B_f) , where

$$A_0 = \begin{pmatrix} 0 & \frac{-1}{2} & 0 \\ \frac{-1}{2} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B_f = \begin{pmatrix} f_4 & 0 & \frac{f_3}{2} \\ 0 & f_0 & \frac{f_1}{2} \\ \frac{f_3}{2} & \frac{f_1}{2} & f_2 \end{pmatrix}.$$

See Section 6.2 for a geometric explanation of why these particular forms arise. One then naturally puts an equivalence on pairs of ternary quadratic forms such that

$(A, B) \sim (A, B + nA)$ for $n \in \mathbb{Z}$, and we can also consider

$$\bar{\Psi} : \{\text{binary quartic forms}\} \longrightarrow \{\text{pairs of ternary quadratic forms}/\sim\},$$

which sends f to $(A_0, B_f + \mathbb{Z}A_0)$. Note that $\bar{\Psi}$ is injective and its image is all classes of pairs (A_0, B) .

We have seen above that the binary quartic form f gives a based quartic ring R_f over \mathbb{Z} , and a pair of ternary quadratic forms gives a based quartic ring Q and a based cubic resolvent C for that quartic ring. The map Ψ may look straightforward, or even arbitrary, but it has been carefully constructed so that Ψ (and also $\bar{\Psi}$) respects the above constructions of based quartic rings and so as to satisfy Theorem 3.1, which says that the map is $\text{GL}_2(\mathbb{Z})$ equivariant.

Lemma 2.2. If a based quartic ring Q is associated to the pair $\Psi(f) = (A_0, B_f)$ or any element of the class $\bar{\Psi}(f) = (A_0, B_f + \mathbb{Z}A_0)$, then $R_f = Q$. □

Proof. We have a basis $\zeta_1, \zeta_2, \zeta_3$ of the quartic ring associated to a binary quartic form as given in Section 2.1. We let $\zeta'_3 = \zeta_3 + f_3$. We let $\alpha_1 = \zeta'_3$ and $\alpha_2 = \zeta_1$ and $\alpha_3 = \zeta_2$. We then see from Equation (2) that the α_i satisfy the multiplication table given in [1, Equations (21) and (23)] for the pair (A_0, B_f) . ■

Note that when we have based rings, it makes sense to talk about equality and not just isomorphism. All of the elements in the class $(A_0, B_f + \mathbb{Z}A_0)$ give the same based quartic ring and the same cubic resolvent, but with different bases for the cubic resolvent.

Since $4 \det(A_0) = -1$, any element of $\bar{\Psi}(f)$ has a based cubic ring given by a cubic form with coefficient -1 of x^3 . In particular, the cubic resolvent ring C associated to $\Psi(f)$ has \mathbb{Z} -module basis $1, \omega, \theta$ with $\omega^2 = -c + b\omega + \theta$ with $b, c \in \mathbb{Z}$, and thus $1, \omega, \omega^2$ is a \mathbb{Z} -module basis of C . A *monogenized cubic ring* is a cubic ring C and an element $\omega \in C/\mathbb{Z}$ such that $C = \mathbb{Z}[\omega]$. An isomorphism of monogenized cubic rings must preserve the chosen element of C/\mathbb{Z} . A *monogenized based cubic ring* is a based cubic ring C with basis $1, \omega, \theta$, such that $1, \omega, \omega^2$ is a \mathbb{Z} -module basis for the ring of the same orientation as $1, \omega, \theta$ (in other words, such that $\theta \in \omega^2 + \omega\mathbb{Z} + \mathbb{Z}$), or equivalently a based cubic ring C that corresponds to a binary cubic form with x^3 coefficient -1 .

Proposition 2.3. Any element of $\bar{\Psi}(f)$ corresponds to a quartic ring with a monogenized based cubic resolvent. □

Corollary 2.4. Any ring R_f from a binary quartic form has a monogenic cubic resolvent. □

We will see that the converse is also true.

Theorem 2.5. If a quartic ring Q has a monogenic resolvent C , then there exist bases of Q and C such that the based pair (Q, C) corresponds to (A_0, B) in the parametrization of quartic rings and cubic resolvents. □

Proof. Recall that $g \in \text{SL}_3(\mathbb{Z})$ acts on A by sending it to gAg^t . There is only one $\text{SL}_3(\mathbb{Z})$ class of ternary quadratic forms with determinant $-\frac{1}{4}$. This is a classical fact from the theory of ternary quadratic forms, see, for example [13, Chapter 5, Theorem 6.3]. Then we can conclude that all such forms are in the $\text{SL}_3(\mathbb{Z})$ class of A_0 . If we have a pair (A, B) corresponding to a quartic ring Q with a monogenic cubic resolvent C , we can choose a monogenized basis of C so that we can assume $\text{Det}(A) = -\frac{1}{4}$. Then we can act by an element $g \in \text{SL}_3(\mathbb{Z})$ so that we obtain $A = A_0$. ■

Corollary 2.6. All quartic rings with monogenic resolvents are the ring R_f constructed from some binary quartic form f . □

In Section 3, we see how the $\text{GL}_2(\mathbb{Z})$ action on binary quartic forms interacts with the construction Ψ .

3 GL Action on Forms

There is a natural (left) $\text{GL}_2(\mathbb{Z})$ action on binary quartic forms. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $\text{GL}_2(\mathbb{Z})$ and $f = F(x, y)$ be a binary quartic form. Then $g \circ f = F(ax + cy, bx + dy)$. Note that this action has a kernel of ± 1 . Recall that the $\text{GL}_3(\mathbb{Z})$ action on pairs of ternary quadratic forms is given by $(A, B) \mapsto (gAg^t, gBg^t)$ for $g \in \text{GL}_3(\mathbb{Z})$.

Theorem 3.1. The map

$$\rho : \text{GL}_2(\mathbb{Z}) \longrightarrow \text{SL}_3(\mathbb{Z}),$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \frac{1}{ad - bc} \begin{pmatrix} d^2 & c^2 & dc \\ b^2 & a^2 & ab \\ 2bd & 2ac & ad + bc \end{pmatrix}$$

is a homomorphism, and gives a $\text{GL}_2(\mathbb{Z})$ action on pairs of ternary quadratic forms for which $\bar{\Psi}$ is equivariant, that is, for $g \in \text{GL}_2(\mathbb{Z})$ we have $\bar{\Psi}(g \circ f) = g\bar{\Psi}(f)$. We have $\text{im}(\rho) \subset \text{Stab}(A_0)$. □

Proof. It is easy to compute that ρ is a homomorphism, and it can also be realized as the representation of $\text{GL}_2(\mathbb{Z})$ on binary quadratic forms (up to a twist by the determinant). We can check the equivariance of $\bar{\psi}$ by computation (which simplifies on generators $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ of $\text{GL}_2(\mathbb{Z})$). Let

$$Y = \begin{pmatrix} d^2 & c^2 & dc \\ b^2 & a^2 & ab \\ 2bd & 2ac & ad + bc \end{pmatrix},$$

and $Y' = \frac{1}{ad-bc}Y$. We can compute formally that $Y' A_0 (Y')^t = A_0$. We can also compute formally that Y gives the correct action on $B + A_0\mathbb{Z}$ exactly; if $\psi(f) = (A_0, B)$ and $\psi(g \circ f) = (A_0, B')$, then $Y(B + A_0\mathbb{Z})Y^t = B' + A_0\mathbb{Z}$. Since $ad - bc = \pm 1$, we have that $Y(B + A_0\mathbb{Z})Y^t = Y'(B + A_0\mathbb{Z})(Y')^t$. ■

The following Lemma is crucial to our main theorem, and is proved in [6, Chapter 13, Lemma 5.2].

Lemma 3.2. We have $\text{im}(\rho) = \text{Stab}(A_0)$. □

4 Monogenized Cubic Rings

Note that given a monogenized cubic ring, C, ω , there is a unique choice of θ in $C/(\mathbb{Z} \oplus \omega\mathbb{Z})$ that lifts to a monogenized basis of C because of the orientation requirement. We define N to be the subgroup $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ of $\text{GL}_2(\mathbb{Z})$. The action of N on binary cubic forms fixes their x^3 coefficient. Moreover, N acts on the basis of C/\mathbb{Z} of a based cubic ring C and fixes the first basis element. We also have that N acts on pairs of ternary quadratic forms, and fixes the first form in the pair.

Proposition 4.1. We have that N classes of binary cubic forms with x^3 coefficient -1 are in bijection with isomorphism classes of monogenized cubic rings. □

Proof. We have that binary cubic forms with x^3 coefficient -1 are in bijection with based cubic rings in which $1, \omega, \omega^2$ is a basis of the same orientation as the given basis $1, \omega, \theta$. When we pass to N classes of forms, the correspondence is to cubic rings with a choice of $\omega \in C/\mathbb{Z}$ and $\theta \in C/(\mathbb{Z} \oplus \omega\mathbb{Z})$ such that $1, \omega, \omega^2$ is a basis of the same orientation as $1, \omega, \theta$. However, given ω , the only such choice of $\theta \in C/(\mathbb{Z} \oplus \omega\mathbb{Z})$ is $\theta = \omega^2$. ■

5 Main Theorem

In this section, we prove the main theorem of this paper.

Theorem 5.1. There is a bijection between the set of $GL_2(\mathbb{Z})$ -equivalence classes of binary quartic forms and the set of isomorphism classes of pairs (Q, C) where Q is a quartic ring and C is a monogenized cubic resolvent of Q . □

An isomorphism of a pair (Q, C) where C is monogenized, is just an isomorphism of the underlying pair of quartic ring and cubic resolvent such that the isomorphism between cubic rings preserves the chosen generator modulo \mathbb{Z} .

Proof. So far, we have established a bijection

$$\{\text{binary quartic forms}\} \longleftrightarrow \{N \text{ classes of pairs } (A_0, B) \text{ of ternary quadratic forms}\},$$

where A_0 is the fixed form defined in Section 1, and B is any ternary quadratic form. From the parametrization of quartic rings [1], we know that N classes of pairs (A_0, B) of ternary quadratic forms are in bijection with (Q, C) , where Q is a based quartic ring, C is an N class of based cubic resolvent rings, and the resolvent map is given by (A_0, B) . Since $4 \text{Det}(A_0) = -1$, the N class of bases of C exactly corresponds to a monogenization of C . Thus, we have a bijection

$$\{\text{binary quartic forms}\} \longleftrightarrow \left\{ \begin{array}{l} (Q, C), \text{ where } Q \text{ is a based quartic ring,} \\ C \text{ is a monogenized cubic resolvent ring,} \\ \text{and the resolvent map is given by } (A_0, B) \end{array} \right\}.$$

We know that in this map the $GL_2(\mathbb{Z})$ action on binary quartic forms just corresponds to a $SL_3(\mathbb{Z})$ change of basis of Q , and thus gives the same isomorphism class of (Q, C) . Thus, the map from $GL_2(\mathbb{Z})$ classes of binary quartic forms to isomorphism classes of (Q, C) is well defined. We know that the map is surjective by Theorem 2.5. To show it is injective, suppose we have two pairs (Q, C) and (Q', C') of quartic rings with monogenized cubic resolvents. We can choose bases for the quartic rings so that the resolvent maps are given by $(A_0, B + A_0\mathbb{Z})$ and $(A_0, B' + A_0\mathbb{Z})$. If we have an isomorphism of the pairs (Q, C) and (Q', C') , it must come from an element $(g, h) \in GL_2(\mathbb{Z}) \times GL_3(\mathbb{Z})$ with $\det(g)\det(h) = 1$. Since g fixes ω and the orientation of the cubic ring (as both cubic forms have x^3 coefficient -1), it must be an element of N . Then $\det(h) = 1$, and we see that the isomorphism comes from an element of $SL_3(\mathbb{Z})$ that fixes A_0 . By Lemma 3.2, such an element is in the

image of the ρ of Theorem 3.1, and thus $(A_0, B + A_0\mathbb{Z})$ and $(A_0, B' + A_0\mathbb{Z})$ come from the same $\text{GL}_2(\mathbb{Z})$ class of binary quartic forms. ■

A quartic ring might have multiple cubic resolvents, only some of which are monogenic. In our bijection, the quartic ring appears once for each monogenized resolvent. If it has a cubic resolvent monogenic in two different ways, then it will appear for each of those monogenizations of the cubic ring. Also, note that the binary quartic form $-x^3y + bx^2y^2 + cxy^3 + dy^4$ maps to (A_0, B) with determinant $-x^3 + bx^2y + cxy^2 + dy^3$. Thus, every monogenized cubic ring appears as a resolvent of some quartic ring.

6 Geometric Interpretation

We now give a geometric interpretation of Theorem 1.1, which was proved in the last section. This geometric interpretation relies on the geometric constructions of a ring from a binary form and from a pair of ternary quadratic forms from [22, 23], respectively.

6.1 Geometric constructions

Given a binary n -ic form f , we have a map

$$\mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^1}(-n) \xrightarrow{f} \mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^1}$$

of sheaves on $\mathbb{P}_{\mathbb{Z}}^1$. The image of this map defines an ideal sheaf of $\mathbb{P}_{\mathbb{Z}}^1$, corresponding to a subscheme of $\mathbb{P}_{\mathbb{Z}}^1$ that we call S_f , *the scheme cut out by the form f* . The scheme S_f is the scheme of roots of the form f in $\mathbb{P}_{\mathbb{Z}}^1$. We then have a ring $H^0(S_f, \mathcal{O}_{S_f})$ of global functions of the scheme S_f . This construction of a ring from a binary form was given in the case $n=3$ by Deligne in [10] and treated completely for all n in [23]. When f has at least one non-zero coefficient, we have $R_f = H^0(S_f, \mathcal{O}_{S_f})$, which is proved in [23, Theorem 2.4]. (See Section 6.3 or [23, Section 2.4] for a geometric construction that works even when $f=0$.) In other words, the algebraic construction given in Section 2 and this geometric construction of a ring from a binary form agree.

Next we recall the geometric construction, given in [22], of a ring from a pair of ternary quadratic forms. Given a pair (A, B) of ternary quadratic forms, we have a map

$$\mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^2}(-2)^{\oplus 2} \xrightarrow{\begin{bmatrix} A \\ B \end{bmatrix}} \mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^2}$$

of sheaves on $\mathbb{P}_{\mathbb{Z}}^2$. The image of this map defines an ideal sheaf of $\mathbb{P}_{\mathbb{Z}}^2$, corresponding to a subscheme of $\mathbb{P}_{\mathbb{Z}}^2$ that we call $S_{(A,B)}$, *the scheme cut out by the pair (A, B)* . The

scheme S_f is the scheme of common roots of the quadratic forms A and B . We have a ring $H^0(S_{(A,B)}, \mathcal{O}_{S_{(A,B)}})$ of global functions on $S_{(A,B)}$. When A and B have no common non-unit factors in the ring $\mathbb{Z}[x, y, z]$, then this ring agrees with Bhargava’s [1] construction of a quartic ring from (A, B) . This agreement is proved in [22, Theorem 5.1], which also gives a geometric construction of a ring from all pairs (A, B) ; see also the letter [11] from Deligne to Bhargava, which gives a geometric approach to constructing quartic rings from pairs of ternary quadratic forms that is different from the approach in [22].

When A and B generate a two-dimensional subspace of ternary quadratic forms over \mathbb{Q} and every \mathbb{Z}/p (call this *nice*), then it makes sense to talk about the $\mathbb{P}_{\mathbb{Z}}^1$ (pencil) of conics through A and B (see [18, I.6.2:Example 1, II.6.4:Example 1] for an introduction to the idea of a pencil of conics). Recall that the cubic resolvent ring associated to (A, B) is the cubic ring associated to the binary cubic form $4 \text{Det}(Ax - By)$. A conic given by a symmetric matrix A is singular in a fiber if and only if $4 \text{Det}(A)$ is 0 in that fiber. To form the matrix A from the conic, we must use $\frac{1}{2}$, but then $D = 4 \text{Det}(A)$ is a polynomial with integer coefficients in the coefficients of the form defining the conic. Even in characteristic 2, the polynomial D gives the exact condition for singularity. This is the form that cuts out the singular locus of the pencil of conics through A and B (originally described in Deligne’s letter [11] to Bhargava). So when $4 \text{Det}(Ax - By) \in \mathbb{Z}[x, y]$ is not 0, the cubic resolvent ring will be given by the regular functions on the subscheme of singular conics in the $\mathbb{P}_{\mathbb{Z}}^1$ of conics through A and B .

6.2 Geometric relationship between forms

We have a map $\mathbb{P}_{\mathbb{Z}}^1 \rightarrow \mathbb{P}_{\mathbb{Z}}^2$ given by anticanonical embedding of the projective line, or $[u : v] \mapsto [v^2 : u^2 : uv]$. Note that A_0 gives a quadratic form on $\mathbb{P}_{\mathbb{Z}}^2$, and the scheme cut out by this form is the rational normal curve specified above. If we have a pair (A_0, B) (with B not a multiple of A_0), then the conic given by A_0 in the pencil is not singular in any fiber. Thus, the associated cubic resolvent ring is given by the ring of regular functions of a closed subscheme of $\mathbb{P}_{\mathbb{Z}}^1 \setminus \{A_0\} \cong \mathbb{A}_{\mathbb{Z}}^1$, and thus is monogenic.

We can see from the parametrization of cubic rings (Theorem 4) that whenever a cubic ring is monogenic, in its realization as the global functions of a subscheme of $\mathbb{P}_{\mathbb{Z}}^1$, that subscheme actually sits inside an $\mathbb{A}_{\mathbb{Z}}^1 \subset \mathbb{P}_{\mathbb{Z}}^1$. Thus, if the cubic resolvent ring associated to a nice (as above) pair (A, B) is monogenic, then that means that the subscheme of singular conics in the $\mathbb{P}_{\mathbb{Z}}^1$ of conics through A and B is disjoint from some particular conic defined over \mathbb{Z} , and we can change basis of the pencil so that it is disjoint from A . This means that A is non-singular. From the fact that there is only one $\text{SL}_3(\mathbb{Z})$ class of

ternary quadratic forms with determinant $-\frac{1}{4}$, we know that up to $\mathrm{GL}_3(\mathbb{Z})$ change of basis on $\mathbb{P}_{\mathbb{Z}}^2$, the only such conic is the one cut out by $\pm A_0$. So we see that pairs (A_0, B) correspond to pairs of quartic rings and cubic resolvents such that the resolvents are monogenic.

Moreover, if we have a pair (A_0, B) , we can pull B back to a form on the $\mathbb{P}_{\mathbb{Z}}^1$ cut out by A_0 to obtain a binary quartic form (and we obtain the same binary quartic form with any element of $B + A_0\mathbb{Z}$). We can easily compute that every binary quartic form arises this way. In particular, if $B = b_{11}x^2 + b_{12}xy + b_{13}xz + b_{22}y^2 + b_{23}yz + b_{33}z^2$, we see it pulls back to the form $b_{11}v^4 + b_{12}u^2v^2 + b_{13}uw^3 + b_{22}u^4 + b_{23}u^3v + b_{33}u^2v^2$ (exactly inverse to the map Ψ defined in the introduction). The elements of $\mathrm{GL}_3(\mathbb{Z})$ that fix the $\mathbb{P}_{\mathbb{Z}}^1$ cut out by A_0 setwise restrict to elements of $\mathrm{GL}_2(\mathbb{Z})$ acting on that $\mathbb{P}_{\mathbb{Z}}^1$. This allows us to see the correspondence of the $\mathrm{GL}_2(\mathbb{Z})$ action on $\mathbb{P}_{\mathbb{Z}}^1$ and an action on $\mathbb{P}_{\mathbb{Z}}^2$ which fixes the rational normal curve.

If we have a primitive binary quartic form f , then the scheme S_f cut out by the form is Spec of the associated ring [23, Theorem 2.9]. The ideal class of R_f associated to the form f (as constructed in [23]) is the line bundle $\mathcal{O}(1)$ pulled back from $\mathbb{P}_{\mathbb{Z}}^1$ to S_f and gives a map of S_f into $\mathbb{P}_{\mathbb{Z}}^1$. The scheme S_f is also a subscheme of $\mathbb{P}_{\mathbb{Z}}^2$ cut out by (A_0, B_f) . We can see the relationship here between the ideal and the monogenic cubic resolvent. The ideal gives a map of S_f to $\mathbb{P}_{\mathbb{Z}}^1$, and then by composing with the rational normal curve map into $\mathbb{P}_{\mathbb{Z}}^2$ we see from the above story that the cubic resolvent is monogenic. Conversely, a monogenic cubic resolvent gives a smooth conic on which our degree four subscheme lies (as in the above story), and pulling back $\mathcal{O}(1)$ from this conic (which is isomorphic to $\mathbb{P}_{\mathbb{Z}}^1$) gives the ideal associated to the binary quartic form.

6.3 Analogs over an arbitrary base

In the construction of a quartic ring from a binary quartic form with \mathbb{Z} coefficients, one can replace \mathbb{Z} with an arbitrary scheme S . An *binary quartic form* over S is a triple (V, L, f) , in which V and L are vector bundles on S of ranks 2 and 1, respectively, and $f \in H^0(S, \mathrm{Sym}^4 U \otimes L)$. A *double ternary quadratic form* over S (analogous to a pair of ternary quadratic forms) is a quadruple (W, U, p, ϕ) , in which W and U are vector bundles on S of ranks 3 and 2, respectively, $p \in H^0(S, \mathrm{Sym}^2 W \otimes U)$, and an isomorphism (called an orientation) $\wedge^3 W \otimes \wedge^2 U \xrightarrow{\sim} \mathcal{O}_S$.

From either a binary quartic form or double ternary quadratic forms over S one can construct a quartic \mathcal{O}_S -algebra (an \mathcal{O}_S -algebra which is a locally free rank 4 \mathcal{O}_S -module), or equivalently, a degree 4 cover of S . If we let π denote the map $\mathbb{P}(V) \rightarrow S$

(or, respectively, $\mathbb{P}(W) \rightarrow S$) and K the Koszul complex of f (respectively p), then the quartic algebra R_f (respectively R_p) is given by $H^0 R\pi_* K$, with the algebra structure being inherited from the multiplication on the Koszul complex. More details on these constructions are given in [23, Section 3, 22, Section 4].

Given a binary quartic form f over S which is a *non-zero-divisor* (everywhere locally on S), then f determines a proper subscheme S_f of $\mathbb{P}(V)$, of generic relative dimension 0 over each irreducible component of S , and the associated quartic algebra R_f is $\pi_* \mathcal{O}_{S_f}$ (see [23, Section 3]). Moreover, if for every $s \in S$, we have that f is not identically zero in the fiber over s , then $S_f \rightarrow S$ has relative dimension 0 and is the degree 4 cover associated to f . This is because $S_f \rightarrow S$ is quasi-finite and projective, and thus finite and affine by [15, Book 4, Chapter 18, Section 12].

The most geometric analogs of the work in this paper concern Gorenstein quartic algebras, and now we will see which binary quartic forms give Gorenstein quartic algebras.

Proposition 6.1. Given a binary quartic form f over S , the following are equivalent:

1. for every $s \in S$, we have that f is not identically zero in the fiber over s ;
2. $\text{Spec } R_f \rightarrow S$ is Gorenstein. □

Proof. If for every $s \in S$, we have that f is not identically zero in the fiber over s , then $\text{Spec } R_f = S_f$, which is a complete intersection and thus Gorenstein. Conversely, suppose $\text{Spec } R_f \rightarrow S$ is Gorenstein but that f is zero in the fiber over s . Then, we have a simple computation that $R_f \otimes_{\mathcal{O}_s} k(s) = k(s)[x, y, z]/(x, y, z)^2$ (cf. Equation (2)), which is not Gorenstein, a contradiction. ■

The next proposition shows that for Gorenstein quartic covers, coming from a binary quartic form is equivalent to being a closed subscheme of a \mathbb{P}^1 -bundle.

Proposition 6.2. Given a quartic algebra R over a scheme S , we have that the following are equivalent:

1. there exists a binary quartic form f such that $R \cong R_f$ and $\text{Spec } R \rightarrow S$ is Gorenstein;
2. $\text{Spec } R \rightarrow S$ factors through a \mathbb{P}^1 bundle $X \rightarrow S$ such that $\text{Spec } R \rightarrow X$ is a closed immersion. □

Proof. For an \mathcal{O}_S -vector bundle W , let W^* denote the dual $\mathcal{H}om(W, \mathcal{O}_S)$. The fact that (1) implies (2) is clear from the above. If we have $\text{Spec } R \subset \mathbb{P}(V)$ (as S schemes), where V is a vector bundle of rank 2 on S , then locally on S , we have that $\text{Spec } R_f$ is cut out by a degree 4 equation, determined up to a unit on S . Thus, we have a line bundle L on S and $L \subset \pi_*\mathcal{O}(4)_{\mathbb{P}(V)}$ is the line bundle of sections vanishing on $\text{Spec } R_f$. This gives a map $L \rightarrow \text{Sym}^4 V$, or equivalently, a section of $H^0(\text{Sym}^4 V \otimes L^*)$, which is a binary quartic form f . Then from the above we see that R is the quartic algebra associated to f , and that $\text{Spec } R \rightarrow S$ is Gorenstein, showing that (2) implies (1). \blacksquare

One can also define cubic resolvents of quartic algebras over S analogously to Definition A.3 (see [22, Section 1.1]). For convenience, by way of the work of Wood [22] that establishes a correspondence between double ternary quartic forms and quartic algebras with cubic resolvents analogous to Theorem 1.2, we work as follows. A double ternary quadratic form has a determinant binary cubic form $\text{Det}(p)$ (see [22, Section 3]), which locally agrees with the above construction $4 \text{Det}(Ax - By)$. If a double ternary quadratic form p has an associated quartic algebra R_p , we call the cubic algebra associated to $\text{Det}(p)$ (via the same construction as a quartic algebra from a binary quartic form) a *cubic resolvent* of R_p .

Now we will see that a quartic algebra from a binary quartic form has a cubic resolvent that is a closed subscheme of (the total space of a) line bundle. This is the analog over S of monogenicity over \mathbb{Z} .

Proposition 6.3. If R is a quartic algebra over S satisfying the conditions of Proposition 6.2, then R has a Gorenstein cubic resolvent C such that $\text{Spec } C$ is a closed sub-scheme of the total space of a line bundle over S . \square

Proof. Assuming (2) of Proposition 6.2, we have $\text{Spec } R \subset \mathbb{P}(V)$, and an associated binary quartic form $f \in H^0(\text{Sym}^4 V \otimes L^*)$. The idea of this proof is that we will produce a double ternary quadratic form that has associated quartic algebra R . In this way, we will produce a cubic resolvent of R , and see that it has the desired property. To produce a double ternary quadratic form that has associated quartic algebra R , we will embed R into a \mathbb{P}^2 -bundle over S and then use the pencil of conics vanishing on R as our double ternary quadratic form. One technical difficulty is that we must produce an orientation for our double ternary quadratic form. We handle this by first constructing the most natural candidate for a double ternary quadratic form, measuring the line bundle that

obstructs it from having an orientation, and then twisting things appropriately by that line bundle.

The section f naturally gives a map $g: L \rightarrow \text{Sym}^4 V$. Let $M \subset \text{Sym}^2 \text{Sym}^2 V$ be the pre-image of $\text{im}(g)$ in the natural map $\text{Sym}^2 \text{Sym}^2 V \rightarrow \text{Sym}^4 V$. It is easy to see, by working locally, that M is a rank 2 vector bundle over S . Moreover, the forms in M are the forms of $\text{Sym}^2 \text{Sym}^2 V$ that vanish on $\text{Spec } R$ in the composite map $\text{Spec } R \subset \mathbb{P}(V) \subset \mathbb{P}(\text{Sym}^2 V)$. So M gives a pencil on conics in $\mathbb{P}(\text{Sym}^2 V)$ that cut out $\text{Spec } R$ as a closed subscheme. However, M may not allow the orientation isomorphism required to be a double ternary quadratic form. We have a line bundle $P := \wedge^3(\text{Sym}^2 V) \otimes \wedge^2 M^*$, that measures the failure of M to allow this orientation isomorphism.

We now twist by P to construct a double ternary quadratic form from the pencil of conics determined by M . We have a map $h: L \otimes P^2 \rightarrow \text{Sym}^4 V \otimes P^2$ induced from the map g above. Let $N \subset \text{Sym}^2((\text{Sym}^2 V) \otimes P)$ be the pre-image of $\text{im}(h)$ in the natural map $\text{Sym}^2((\text{Sym}^2 V) \otimes P) \rightarrow \text{Sym}^4 V \otimes P^2$. We have $N \cong M \otimes P^2$.

The map $N \subset \text{Sym}^2((\text{Sym}^2 V) \otimes P)$ gives a section $p \in H^0(S, \text{Sym}^2((\text{Sym}^2 V) \otimes P) \otimes N^*)$ and thus a double ternary quadratic form $((\text{Sym}^2 V) \otimes P, N^*, p, \phi)$, where ϕ is the natural map $\wedge^3((\text{Sym}^2 V) \otimes P) \otimes \wedge^2 N^* \cong \wedge^3(\text{Sym}^2 V) \otimes P^{\otimes 3} \otimes \wedge^2 M^* \otimes P^{\otimes -4} \cong \mathcal{O}_S$. Note that ϕ exists because our twist by P was exactly the twist necessary to give the isomorphism ϕ .

We have $\mathbb{P}(V) \subset \mathbb{P}(\text{Sym}^2 V) \cong \mathbb{P}(\text{Sym}^2 V \otimes P)$, cut out by the kernel of the map $\text{Sym}^2((\text{Sym}^2 V) \otimes P) \rightarrow \text{Sym}^4 V \otimes P^2$. By the same argument as in Section 6.1, the cubic resolvent C associated to p is the cubic algebra associated to the binary cubic form c cutting out the singular conics in the pencil of conics through $\text{Spec } R \subset \mathbb{P}(\text{Sym}^2 V \otimes P)$. Since $\mathbb{P}(V)$ is a smooth conic in this pencil, we see that c is non-zero in each fiber over S , and thus the cubic resolvent is Gorenstein and $\text{Spec } C$ is cut out by c in the pencil of conics through $\text{Spec } R$ (by the same argument as in Proposition 6.1). Moreover, since $\mathbb{P}(V)$ is a smooth conic, we see that $\text{Spec } C$ is a closed subscheme not only in the \mathbb{P}^1 bundle of conics, but in the line bundle constructed by removing $\mathbb{P}(V)$ from the pencil. ■

We have a partial converse to Proposition 6.3.

Proposition 6.4. If R is a Gorenstein quartic algebra over an integral scheme S , and R has a Gorenstein cubic resolvent C such that $\text{Spec } C$ is a closed sub- S -scheme of the total space of a line bundle over S , then $\text{Spec } R \rightarrow S$ factors through a (smooth) conic bundle $X \rightarrow S$ such that $\text{Spec } R \rightarrow X$ is a closed immersion. □

Proof. Let (W, U, p, ϕ) be a double ternary quadratic form giving R and C . Since R is Gorenstein, we can deduce that p cuts out $\text{Spec } R$ in $\mathbb{P}(W)$ (by a computation showing all forms over an algebraically closed field not cutting out a relative dimension 0 S -scheme give non-Gorenstein algebras). Since $C \rightarrow S$ is Gorenstein, C (as an S -scheme) has a unique (up to isomorphism) closed immersion in a \mathbb{P}^1 bundle over S by [5, Theorem 1.3]. Since $\text{Spec } C$ is a closed sub- S -scheme of the total space of a line bundle over S , completing that line bundle to a \mathbb{P}^1 -bundle gives such a closed immersion.

Also, $\text{Spec } C$ is the singular locus in the pencil of conics through $\text{Spec } R$, which gives a closed immersion of $\text{Spec } C$ into a \mathbb{P}^1 -bundle (the pencil of conics). Thus, in this closed immersion $\text{Spec } C$ must sit inside a line bundle in the \mathbb{P}^1 bundle. The difference between the line bundle and the \mathbb{P}^1 -bundle gives a section of S into the \mathbb{P}^1 -bundle (the pencil of conics). This section corresponds to a conic bundle over S through $\text{Spec } R$, but since it has no intersection with $\text{Spec } C$, it is a smooth conic bundle. ■

Over a general scheme S , a conic bundle is not necessary a \mathbb{P}^1 -bundle, and thus Proposition 6.4 does not give a full converse to Proposition 6.3. Over \mathbb{Z} , of course, there is a unique (smooth) conic bundle, which is a \mathbb{P}^1 -bundle and we have a full converse. Also, the explicit argument given for Theorem 1.1 works for all quartic algebras, whereas the geometric arguments given above are restricted to Gorenstein quartic algebras. (When one tries to extend to the non-Gorenstein locus by the hypercohomology construction of the quartic algebras, one recovers essentially the explicit argument given in the first part of this paper.) The recent results on class groups of monogenic cubic rings [3] are not restricted by any Gorenstein condition, and thus over \mathbb{Z} it is convenient to have the complete statement of Theorem 1.1.

7 $\text{GL}_2(\mathbb{Z})$ Invariants of Binary Quartic Forms and Cubic Resolvent Rings

We have a canonical map Ψ' which sends $f = f_0x^4 + f_1x^3y + f_2x^2y^2 + f_3xy^3 + f_4y^4$ to

$$\left(A_0, \begin{pmatrix} f_4 & \frac{f_2}{6} & \frac{f_3}{2} \\ \frac{f_2}{6} & f_0 & \frac{f_1}{2} \\ \frac{f_3}{2} & \frac{f_1}{2} & \frac{2f_2}{3} \end{pmatrix} \right),$$

which is equivariant with respect to the $\text{GL}_2(\mathbb{Z})$ action on the binary quartic forms and the $\text{GL}_2(\mathbb{Z})$ action on pairs of ternary quadratic forms given in Theorem 3.1. Our previous

map Ψ was equivariant only as a map to N classes of pairs of ternary quadratic forms. However, Ψ was defined over \mathbb{Z} , and Ψ' requires the use of $\frac{1}{3}$.

The determinant binary cubic of any element in the image of Ψ' has x^3y coefficient 0. If $3 \mid f_2$, then $\Psi'(f)$ has integral coefficients and its determinant is the unique binary cubic form to give a basis $1, \omega, \theta$ such that $\omega\theta \in \mathbb{Z}$ and $\omega^2 - \theta \in \mathbb{Z}$, where ω is the generator of the resolvent cubic associated to the form f . If $3 \nmid f_2$, then there is no basis $1, \omega, \theta$ of the monogenized resolvent cubic C, ω such that $\omega\theta \in \mathbb{Z}$ and $\omega^2 - \theta \in \mathbb{Z}$.

We define $N_{1/3}$ to be the group of matrices of the form $\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$, where $n \in \frac{1}{3}\mathbb{Z}$.

Proposition 7.1. The map from N classes of monogenic binary cubic forms to $N_{1/3}$ classes of binary cubic forms is injective. □

Proof. Consider the action of $\begin{pmatrix} 1 & \\ k/3 & 1 \end{pmatrix}$ (where $k \in \mathbb{Z}$) on the form $-x^3 + bx^2y + cxy^2 + dy^3$. The new coefficient of y^3 is $d - \frac{ck}{3} + \frac{bk^2}{9} - \frac{k^2}{27}$, which is only an integer if k is divisible by 3. ■

The determinant of $\Psi'(f)$ is

$$-x^3 + \frac{I}{3}xy^2 - \frac{J}{27}y^3,$$

where I and J are generators for the $SL_2(\mathbb{Z})$ invariants of binary quartic forms, given by

$$\frac{I}{3} = 4f_0f_4 - f_1f_3 + \frac{1}{3}f_2^2 \quad \text{and} \quad \frac{-J}{27} = \frac{-8}{3}f_0f_2f_4 + \frac{2}{27}f_2^3 + f_0f_3^2 + f_4f_1^2 - \frac{1}{3}f_1f_2f_3.$$

Given a binary quartic form, we have an associated quartic ring and a monogenized cubic resolvent C with generator ω . We can thus give the monogenized cubic resolvent canonically by saying it corresponds to the N class of binary cubic forms over \mathbb{Z} in the $N_{1/3}$ class of $-x^3 + \frac{I}{3}xy^2 - \frac{J}{27}y^3$.

Let r be a root of $-x^3 + \frac{I}{3}x - \frac{J}{27}$. Then there is only one \mathbb{Z} coset of algebraic integers in $r + \frac{1}{3}\mathbb{Z}$, and it is $\omega + \mathbb{Z}$. So, we have found a description for ω in terms of the $GL_2(\mathbb{Z})$ invariants of the binary quartic form. (Note that even if $-x^3 + \frac{I}{3}x - \frac{J}{27}$ is reducible, we can still make sense of r as an element of $\mathbb{Q}(r)/(-r^3 + \frac{I}{3}r - \frac{J}{27})$ and there is only one \mathbb{Z} coset in $r + \frac{1}{3}\mathbb{Z}$ whose elements generate algebras that are finitely generated \mathbb{Z} -modules.)

Appendix: Cubic Resolvents

Let Q be a quartic ring. The following definition is an important step in constructing the cubic resolvent of a general quartic ring, and was first given in [1, Definition 6], though see [2] for a more thorough treatment.

Definition A.1. The S_4 -closure of Q , denoted \bar{Q} , is the ring $Q^{\otimes 4}/J_Q$, where J_Q is the \mathbb{Z} -saturation of the ideal I_Q generated by all the elements of the form

$$x \otimes 1 \otimes 1 \otimes 1 + 1 \otimes x \otimes 1 \otimes 1 + 1 \otimes 1 \otimes x \otimes 1 + 1 \otimes 1 \otimes 1 \otimes x$$

for $x \in Q$ (that is, $J_Q = \{r \in Q^{\otimes 4} \mid nr \in I_Q \text{ for some } n \in \mathbb{Z}\}$). \square

The idea is that $1 \otimes x \otimes 1 \otimes 1, 1 \otimes 1 \otimes x \otimes 1, 1 \otimes 1 \otimes 1 \otimes x$ act as formal conjugates of $x \otimes 1 \otimes 1 \otimes 1$. We then consider the cubic invariant ring of Q , that is

$$R^{\text{inv}}(Q) := \mathbb{Z}[\{x \otimes x \otimes 1 \otimes 1 + 1 \otimes 1 \otimes x \otimes x \mid x \in Q\}] \subset \bar{Q}.$$

Now we can give the definition of a cubic resolvent ring as given in [1, Definition 8].

Definition A.2. If Q is a quartic ring with non-zero discriminant, a *cubic resolvent ring* C of Q is any cubic ring with $R^{\text{inv}}(Q)$ as a subring such that $\text{disc}(C) = \text{disc}(Q)$. Then $x \mapsto x \otimes x \otimes 1 \otimes 1 + 1 \otimes 1 \otimes x \otimes x$ gives a quadratic map from Q to C . \square

We also give the following alternative definition [1, Definition 20] which works for all quartic rings, and is easier to use in practice in some cases.

Definition A.3. Given a quartic ring Q , a *cubic resolvent* C of Q is

- a cubic ring C ;
- a quadratic map $\phi : Q/\mathbb{Z} \rightarrow C/\mathbb{Z}$; and
- an isomorphism $\delta : \wedge^4 Q \cong \wedge^3 C$ (or equivalently $\bar{\delta} : \wedge^3 Q/\mathbb{Z} \cong \wedge^2 C/\mathbb{Z}$)

such that

1. for all $x, y \in Q$, we have $\delta(1 \wedge x \wedge y \wedge xy) = 1 \wedge \phi(x) \wedge \phi(y)$;

2. the binary cubic form in $\text{Sym}^3(C/\mathbb{Z})^* \otimes \wedge^2(C/\mathbb{Z})$ corresponding to C is $\text{Det}(\phi)$. \square

Acknowledgements

The author would like to thank Manjul Bhargava for asking the questions that inspired this research, guidance along the way, and helpful feedback both on the ideas and the exposition in this paper. The author would also like to thank the referee for several suggestions that improved the paper.

Funding

Part of this work was supported by an NSF Graduate Fellowship, an NDSEG Fellowship, an AAUW Dissertation Fellowship, and a Josephine De Kármán Fellowship. Part of this work was done while the author was supported by an American Institute of Mathematics Five-Year Fellowship and National Science Foundation grant DMS-1001083.

References

- [1] Bhargava, M. "Higher composition laws. III. The parametrization of quartic rings." *Annals of Mathematics* (2) 159, no. 3 (2004): 1329–60.
- [2] Bhargava, M. and M. Satriano. "On a notion of 'Galois closure' for extensions of rings." (2010): preprint arXiv:1006.2562.
- [3] Bhargava, M. and A. Shankar. "Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves." (2010): preprint arXiv:1006.1002v2.
- [4] Birch, B. J. and J. R. Merriman. "Finiteness theorems for binary forms with given discriminant." *Proceedings of the London Mathematical Society* (3) 24 (1972): 385–94.
- [5] Casnati, G. and T. Ekedahl. "Covers of algebraic varieties. I. A general structure theorem, covers of degree 3,4 and Enriques surfaces." *Journal of Algebraic Geometry* 5, no. 3 (1996): 439–60.
- [6] Cassels, J. W. S. *Rational Quadratic Forms*. London: Academic Press, 1978.
- [7] Cohen, H. *A Course in Computational Algebraic Number Theory*. Berlin: Springer, 1993.
- [8] Dedekind, R. Supplement X in P.G.L. Dirichlet. *Vorlesungen über Zahlentheorie*, 2nd ed. Vieweg, 1871.
- [9] Del Corso, I., R. Dvornicich, and D. Simon. "Decomposition of primes in non-maximal orders." *Acta Arithmetica* 120, no. 3 (2005): 231–44.
- [10] Deligne, P. Letter to W. T. Gan, B. Gross and G. Savin, November 13, 2000.
- [11] Deligne, P. Letter to M. Bhargava, March 5, 2004.
- [12] Delone, B. N. and D. K. Faddeev. *The Theory of Irrationalities of the Third Degree*. Providence, RI: American Mathematical Society, 1964. (translation of B. N. Delone and D. K. Faddeev,

- Theory of Irrationalities of Third Degree, Acad. Sci. URSS. Trav. Inst. Math. Stekloff, 11 (1940).)
- [13] Flath, D. E. *Introduction to Number Theory*. New York: Wiley, 1989.
 - [14] Gan, W. T., B. Gross, and G. Savin. "Fourier coefficients of modular forms on G_2 ." *Duke Mathematical Journal* 115, no. 1 (2002): 105–69.
 - [15] Grothendieck, A. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV." *Institut de Hautes Etudes Scientifiques Publications Mathématiques*. no.32 (1967): 361.
 - [16] Kneser, M. "Composition of binary quadratic forms." *Journal of Number Theory* 15, no. 3 (1982): 406–13.
 - [17] Nakagawa, J. "Binary forms and orders of algebraic number fields." *Inventiones Mathematicae* 97, no. 2 (1989): 219–35.
 - [18] Shafarevich, I. R. *Basic Algebraic Geometry. 1*, 2nd ed. Translated from the 1988 Russian edition and with notes by Miles Reid. Berlin: Springer, 1994.
 - [19] Simon, D. "The index of nonmonic polynomials." *Indagationes Mathematicae (N.S.)* 12, no. 4 (2001): 505–17.
 - [20] Simon, D. "La classe invariante d'une forme binaire." *Comptes Rendus Mathématique. Académie des Sciences* 336, no. 1 (2003): 7–10.
 - [21] Simon, D. "A 'class group' obstruction for the equation $Cy^d = F(x, z)$." *Journal de Théorie des Nombres de Bordeaux* 20, no. 3 (2008): 811–28.
 - [22] Wood, M. M. "Parametrizing quartic algebras over an arbitrary base." *Algebra and Number Theory*, 2010: preprint arXiv:1007.5503v1.
 - [23] Wood, M. M. "Rings and ideal parametrized by binary n -ic forms." *Journal of London Mathematical Society* (2) 83 (2011): 208–31.
 - [24] Wood, M. M. "Gauss composition over an arbitrary base." *Advances in Mathematics* 226 (2011): 1756–71.