Annals of Mathematics, **159** (2004), 1329–1360

Higher composition laws III: The parametrization of quartic rings

By Manjul Bhargava

1. Introduction

In the first two articles of this series, we investigated various higher analogues of Gauss composition, and showed how several algebraic objects involving orders in quadratic and cubic fields could be explicitly parametrized. In particular, a central role in the theory was played by the parametrizations of the quadratic and cubic rings themselves.

These parametrizations are beautiful and easy to state. In the quadratic case, one need only note that a quadratic ring—i.e., any ring that is free of rank 2 as a $\mathbb{Z}$-module—is uniquely specified up to isomorphism by its discriminant; and conversely, given any discriminant D, i.e., any integer congruent to 0 or 1 (mod 4), there is a unique quadratic ring having discriminant D, namely

$$S(D) = \begin{cases} \mathbb{Z}[x]/(x^2) & \text{if } D = 0, \\ \mathbb{Z}\cdot(1,1) + \sqrt{D}(\mathbb{Z}\oplus\mathbb{Z}) & \text{if } D \geq 1 \text{ is a square,} \\ \mathbb{Z}[(D+\sqrt{D})/2] & \text{otherwise.} \end{cases} \tag{1}$$

Thus we may say that *quadratic rings are parametrized by the set* $\mathbb{D} = \{D \in \mathbb{Z} : D \equiv 0 \text{ or } 1 \pmod 4\}$. (For a more detailed discussion of quadratic rings, see [2].)

The cubic case is slightly more complex, in that cubic rings are not parametrized only by their discriminants; indeed, there may sometimes be several cubic orders having the same discriminant. The correct object parametrizing cubic rings—i.e., rings free of rank 3 as $\mathbb{Z}$-modules—was first determined by Delone-Faddeev in their classic 1964 treatise on cubic irrationalities [8]. They showed that cubic rings are in bijective correspondence with $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms, as follows. Given a binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ with $a,b,c,d \in \mathbb{Z}$, one associates to f the ring $R(f)$ having $\mathbb{Z}$-basis $\langle 1, \omega_1, \omega_2\rangle$ and multiplication table

$$\begin{aligned} \omega_1\omega_2 &= -ad, \\ \omega_1^2 &= -ac + b\omega_1 - a\omega_2, \\ \omega_2^2 &= -bd + d\omega_1 - c\omega_2. \end{aligned} \tag{2}$$

One easily verifies that $\mathrm{GL}_2(\mathbb{Z})$-equivalent binary cubic forms yield isomorphic rings, and conversely, that every isomorphism class of ring R can be represented in the form $R(f)$ for a unique binary cubic form f, up to such equivalence. Thus we may say that *isomorphism classes of cubic rings are parametrized by* $\mathrm{GL}_2(\mathbb{Z})$-*equivalence classes of integral binary cubic forms.*

The above parametrizations of quadratic and cubic orders are at once both beautiful and simple, and have enjoyed numerous applications both within this series of articles and elsewhere (see e.g., [7], [8], [9], [10], [13]). It is therefore only natural to ask whether analogous parametrizations might exist for orders in number fields of degree $k > 3$. In this article, we show how such a parametrization can also be achieved for quartic orders (i.e., the case $k = 4$). The problem of parametrizing quintic orders (the case $k = 5$) will be treated in the next article of this series [5].

In classifying quartic rings, a first approach (following the cases $k = 2$ and $k = 3$) might be simply to write out the multiplication laws for a rank 4 ring in terms of an explicit basis, and examine how the structure coefficients transform under changes of basis. However, since the jump in complexity from $k = 3$ to $k = 4$ is so large, this idea goes astray very quickly (yielding a huge mess!), and it becomes necessary to have a new perspective in order to make any further progress.

In Section 2 of this article, we give such a new perspective on the case $k = 3$ in terms of what we call *resolvent rings.* We call them resolvent rings because they are natural integral models of the resolvent fields occurring in the classical literature. The notion of *quadratic resolvent ring*, defined in Section 2.2, immediately yields the Delone-Faddeev parametrization of cubic orders from a purely ring-theoretic viewpoint. Our formulation is slightly different—we prove that *there is a canonical bijection between the set of* $\mathrm{GL}_2(\mathbb{Z})$-*orbits on the space of binary cubic forms and the set of isomorphism classes of pairs* (R, S), *where* R *is a cubic ring and* S *is a quadratic resolvent of* R. Since it turns out that every cubic ring R has a unique quadratic resolvent S up to isomorphism, the information given by S may be dropped if desired, and we recover Delone-Faddeev's result.

Generalizing this perspective of resolvent rings to the case $k = 4$ then suggests that *the analogous objects parametrizing quartic orders should be pairs of ternary quadratic forms, up to integer equivalence.*

Section 3 is dedicated to proving this assertion and its ramifications. Following [2], let us use $(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ to denote the space of pairs of ternary quadratic forms having integer coefficients. Then our main result is:

Theorem 1. *There is a canonical bijection between the set of* $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$-*orbits on the space* $(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ *of pairs of integral ternary quadratic forms and the set of isomorphism classes of pairs* (Q, R), *where* Q *is a quartic ring and* R *is a cubic resolvent ring of* Q.

In coordinate-free language, Theorem 1 states that isomorphism classes of such pairs (Q, R) are in natural bijection with isomorphism classes of quadratic maps $\phi : M \to L$, where M and L are free $\mathbb{Z}$-modules having ranks 3 and 2 respectively. In fact, under this bijection we have that $M = Q/\mathbb{Z}$ and $L = R/\mathbb{Z}$.

In the case that Q is an order in an S_4-quartic field K, we find that R is an order in the usual *cubic resolvent field* of K, which is the subfield of the Galois closure $\bar{K}$ of K fixed by a dihedral subgroup $D_4 \subset S_4$. Furthermore, in this case $\phi : M \to L$ turns out to be none other than the mapping from $Q/\mathbb{Z}$ to $R/\mathbb{Z}$ induced by the resolvent mapping

$$\tilde{\phi}(x) = xx' + x''x''' \tag{3}$$

from Q to R used in the classical solution to the quartic equation, where we have used x, x', x'', x''' to denote the conjugates of x in $\bar{K}$.

Thus quartic rings may also be described naturally through their resolvent rings. However, unlike the case of cubic rings, not every quartic ring has a unique resolvent ring! Thus it becomes important to ask when two elements of $(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ yield the same quartic ring Q in Theorem 1. If $(A, B) \in (\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ is a pair of ternary quadratic forms yielding a quartic ring Q by Theorem 1, and if A is a multiple of n, then we find that the pair $(\frac{1}{n}A, nB) \in (\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ also yields the same quartic ring Q. In fact, with the exception of the trivial quartic ring (i.e., the ring $\mathbb{Z} + \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3$ with all $x_i x_j = 0$), such transformations essentially tell the whole story. Namely, we show that: (a) every nontrivial quartic ring Q occurs in the correspondence of Theorem 1; and (b) two pairs of ternary quadratic forms are associated to the same quartic ring in Theorem 1 if and only if they are related by a transformation in the group $\mathrm{GL}_2^{\pm 1}(\mathbb{Q}) \subset \mathrm{GL}_2(\mathbb{Q})$ consisting of elements having determinant ± 1.

Finally, we show that a pair of ternary quadratic forms (A, B) corresponds to a nontrivial quartic ring in Theorem 1 if and only if A and B are linearly independent over $\mathbb{Q}$. Together these statements give the following:

THEOREM 2. *There is a canonical bijection between isomorphism classes of nontrivial quartic rings and* $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2^{\pm 1}(\mathbb{Q})$*-equivalence classes of pairs* (A, B) *of integral ternary quadratic forms where* A *and* B *are linearly independent over* $\mathbb{Q}$.

There is a third version of the story that is also very useful. If T is a ring, free of rank k over $\mathbb{Z}$ with unit, then it possesses the subring $T_n = \mathbb{Z} + nT$ for any positive integer n. Conversely, any nontrivial ring can be written as T_n for a unique maximal n which we call the *content*, and for a unique ring T, which is then called *primitive* (content 1). This gives a bijection, for any k, between sets

$$\{\text{nontrivial rings of rank } k\} \leftrightarrow \mathbb{N} \times \{\text{primitive rings of rank } k\}.$$

Hence classifying all rings of rank k is equivalent to classifying just those rings that are primitive.

For example, in the case of quadratic rings the content coincides with what is usually called the "conductor". The conductor of a quadratic ring S whose discriminant is $D \in \mathbb{D}$ is simply the largest integer n such that $D/n^2 \in \mathbb{D}$. In particular, a quadratic ring has conductor 1 if and only if its discriminant is *fundamental*; i.e., it is an element of $\mathbb{D}$ that is not a square times any other element of $\mathbb{D}$. Thus, we may say that *isomorphism classes of primitive quadratic rings are parametrized by nonzero elements of $\mathbb{D}$ modulo equivalence under scalar multiplication by $\mathbb{Q}^{\times 2}$*.

In the case of cubic rings, the content of a cubic ring $R = R(f)$ is equal to the content of the corresponding binary cubic form f (in the usual sense, i.e., the greatest common divisor of its coefficients). Indeed, the correspondence $f \leftrightarrow R(f)$ given by (2) implies that

$$R(nf) = \mathbb{Z} + nR(f) = R(f)_n$$

for all f and n, so that a ring corresponding to a cubic form of content n has content at least n, and, conversely, a cubic form corresponding to a cubic ring of content n must be a multiple of n. In particular, primitive cubic rings correspond to primitive binary cubic forms. We may thus say that *isomorphism classes of primitive cubic rings are in canonical bijection with $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Q})$-equivalence classes of nonzero integral binary cubic forms*, where $\mathrm{GL}_1(\mathbb{Q})$ acts on binary cubic forms by scalar multiplication.

The corresponding result for primitive quartic rings is as follows.

THEOREM 3. *There is a canonical bijection between isomorphism classes of primitive quartic rings and $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Q})$-equivalence classes of pairs (A, B) of integral ternary quadratic forms where A and B are linearly independent over $\mathbb{Q}$.*

In coordinate-free terms, Theorem 3 states that primitive quartic rings correspond to pairs (M, V), where M is a free $\mathbb{Z}$-module of rank 3 and V is a two-dimensional rational subspace of the (six-dimensional) vector space of $\mathbb{Q}$-valued quadratic forms on M. Equivalently, primitive quartic rings Q correspond to pairs (M, Λ), where Λ is a maximal two-dimensional lattice of $\mathbb{Z}$-valued quadratic forms on M.

The connection to Theorem 2 is now clear: if $Q_n = \mathbb{Z} + nQ$ is the content n subring associated to a primitive quartic ring Q, then the two-dimensional $\mathbb{Z}$-lattices corresponding to Q_n under the bijection of Theorem 2 are just the index n sublattices of Λ, any two of which have $\mathbb{Z}$-bases related by a rational 2×2 matrix of determinant ± 1. We also now understand Theorem 1 better, because the different cubic resolvents corresponding to the content n subring Q_n are in one-to-one correspondence with the index n sublattices of Λ. This observation has an important consequence on the ring-theoretic side, concerning cubic resolvents:

Corollary 4. *The number of cubic resolvents of a quartic ring depends only on its content n; it is equal to the number $\sum_{d|n} d$ of sublattices of $\mathbb{Z}^2$ having index n.*

In particular, since $\sum_{d|n} d \geq 1$ for all n, cubic resolvent rings always exist for any quartic ring. Moreover, a primitive quartic ring always has a unique cubic resolvent. As a special case of this, we observe that a maximal quartic ring—such as the ring of integers in a quartic number field—will always have a unique, canonically associated cubic resolvent ring. We summarize this discussion as follows.

Corollary 5. *Every quartic ring has a cubic resolvent ring. A primitive quartic ring has a unique cubic resolvent ring up to isomorphism. In particular, every maximal quartic ring has a unique cubic resolvent ring.*

We introduce the notion of resolvent ring in Section 2, and use it to show how pairs of integral ternary quadratic forms are connected to quartic rings. In Section 3, we then investigate the integer orbits on the space of pairs of ternary quadratic forms in detail, and in particular, we establish the bijections of Theorems 1–3 as well as Corollaries 4 and 5. Finally, in Section 4 we investigate how maximality and splitting of primes in quartic rings manifest themselves in terms of pairs of ternary quadratic forms. This may be important in future computational applications (see, e.g., [6]), and will also be crucial for us in obtaining results on the density of discriminants of quartic fields (to appear in [4]).

We note that the relation between pairs of ternary quadratic forms and quartic *fields* has previously been investigated in the important work of Wright-Yukie [15], who showed that nondegenerate rational orbits on the space of pairs of ternary quadratic forms correspond bijectively with étale quartic extensions of $\mathbb{Q}$. As Wright and Yukie point out, rational cubic equations had been studied even earlier as intersections of zeroes of pairs of ternary quadratic forms in the ancient work of Omar Khayyam [12]. Our viewpoint differs from previous work in that we consider pairs of ternary quadratic forms over the integers $\mathbb{Z}$; as we shall see, the integer orbits on the space of pairs of ternary quadratic forms have an extremely rich structure, yielding insights not only into quartic fields, but also into their orders, their "cubic resolvent rings", their collective multiplication tables, their discriminants, local behavior, and much more.

2. Resolvent rings and parametrizations

Before introducing the notion of resolvent ring, it is necessary first to understand a formal construction of “Galois closure” at the level of rings, which we call “S_k-closure”. We view this construction as a formal analogue of Galois closure because if R is an order in an S_k-field of degree k, then it turns out that its S_k-closure $\bar{R}$ is an order in the usual Galois closure $\bar{K}$ of K. More generally, the S_k-closure operation gives a way of attaching to any ring R with unit that is free of rank k over $\mathbb{Z}$, a ring $\bar{R}$ with unit that is free of rank $k!$ over $\mathbb{Z}$.

Let us fix some terminology. By a *ring of rank k* we will always mean a commutative ring with unit that is free of rank k over $\mathbb{Z}$. To any such ring R of rank k we may attach the *trace* function $\mathrm{Tr}: R \to \mathbb{Z}$, which assigns to an element $\alpha \in R$ the trace of the endomorphism $m_\alpha : R \xrightarrow{\times\alpha} R$ given by multiplication by α. The *discriminant* $\mathrm{Disc}(R)$ of such a ring R is then defined as the determinant $\det(\mathrm{Tr}(\alpha_i\alpha_j)) \in \mathbb{Z}$, where $\{\alpha_i\}$ is any $\mathbb{Z}$-basis of R.

The discriminants of individual elements in R may also be defined and will play an important role in what follows. Let F_α denote the characteristic polynomial of the linear transformation $m_\alpha : R \to R$ associated to α. Then the *discriminant* $\mathrm{Disc}(\alpha)$ of an element $\alpha \in R$ is defined to be the discriminant of the characteristic polynomial F_α. In particular, if $R = \mathbb{Z}[\alpha]$ for some $\alpha \in R$, then we have $\mathrm{Disc}(R) = \mathrm{Disc}(\alpha)$.

2.1. *The S_k-closure of a ring of rank k.*

Let R be any ring of rank k having nonzero discriminant, and let $R^{\otimes k}$ denote the kth tensor power $R^{\otimes k} = R \otimes_{\mathbb{Z}} R \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} R$ of R. Then $R^{\otimes k}$ is seen to be a ring of rank k^k in which $\mathbb{Z}$ lies naturally as a subring via the mapping $n \mapsto n(1 \otimes 1 \otimes \cdots \otimes 1)$.

Denote by I_R the ideal in $R^{\otimes k}$ generated by all elements of the form

$$(x \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes x \otimes \cdots \otimes 1) + \cdots + (1 \otimes 1 \otimes \cdots \otimes x) \; - \; \mathrm{Tr}(x)$$

for $x \in R$. Let J_R denote the $\mathbb{Z}$-saturation of the ideal I_R; i.e., let

$$J_R = \{r \in R^{\otimes k} : nr \in I_R \text{ for some } n \in \mathbb{Z}\}.$$

With these definitions, it is easy to see that if $\alpha \in R$ satisfies the characteristic equation $F_\alpha(x) = x^k - a_1x^{k-1} + a_2x^{k-2} - \cdots \pm a_k = 0$ with $a_i \in \mathbb{Z}$, then the ith elementary symmetric polynomial in the k elements $\alpha \otimes 1 \otimes \cdots \otimes 1$, $1 \otimes \alpha \otimes \cdots \otimes 1$, $\ldots$, $1 \otimes 1 \otimes \cdots \otimes \alpha$ will be congruent to a_i modulo J_R for all $1 \le i \le k$.

For example, if $k = 2$ and $\alpha \in R$ satisfies $F_\alpha(x) = x^2 - a_1x + a_2 = 0$, then

$$\begin{aligned} 2\,\alpha \otimes \alpha &= (\alpha \otimes 1 + 1 \otimes \alpha)^2 - (\alpha^2 \otimes 1 + 1 \otimes \alpha^2) \\ &\equiv \mathrm{Tr}(\alpha)^2 - \mathrm{Tr}(\alpha^2) = 2a_2 \pmod{I_R} \end{aligned}$$

and hence $\alpha \otimes \alpha \equiv a_2 \pmod{J_R}$. An analogous argument works for all k.

It is therefore natural to make the following definition:

Definition 6. The *S_k-closure* of a ring R of rank k is the ring $\bar{R}$ given by $R^{\otimes k}/J_R$.

This notion of S_k-closure is precisely the formal analogue of "Galois closure" we seek. We may write $\mathrm{Gal}(\bar{R}/\mathbb{Z}) = S_k$, since the symmetric group S_k acts naturally as a group of automorphisms on $\bar{R}$. Furthermore, the subring $\bar{R}^{S_k}$ consisting of all elements fixed by this action is simply $\mathbb{Z}$. Indeed, it is known by the classical theory of polarization that the S_k-invariants of $R^{\otimes k}$ are spanned by elements of the form $x \otimes \cdots \otimes x$ $(x \in R)$, and the latter is simply $N(x)$ modulo J_R. A similar argument shows that we also have $\mathrm{Gal}(\bar{R}/R) = S_{k-1}$, where R naturally embeds into $\bar{R}$ by $x \mapsto x \otimes 1 \otimes \cdots \otimes 1$.

For example, let us consider the case where R is an order in a number field K of degree k such that $\mathrm{Gal}(\bar{K}/\mathbb{Q}) = S_k$. Then $\bar{R}$ is isomorphic to the ring generated by all the Galois conjugates of elements of R in $\bar{K}$, i.e.,

$$\bar{R} = \mathbb{Z}[\{\alpha : \alpha \;\; S_k\text{-conjugate to some element of } R\}].$$

More generally, if R is an order in a number field K of degree k whose associated Galois group has index n in S_k, then the "S_k-closure" of K will be a direct sum of n copies of the Galois closure of K (and hence will have dimension $k!$ over $\mathbb{Q}$), and the S_k-closure of R will be a subring of this having $\mathbb{Z}$-rank $k!$.

In the next two subsections, we use the notion of S_k-closure to attach rings of lower rank to orders in cubic and quartic fields.

2.2. *The quadratic resolvent of a cubic ring.* Given a cubic ring, there is a natural way to associate to R a quadratic ring S, namely the unique quadratic ring S having the same discriminant as R. Since the discriminant $D = \mathrm{Disc}(R)$ of R is necessarily congruent to 0 or 1 modulo 4, the quadratic ring $S(D)$ of discriminant D always exists; we call $S = S(D)$ the *quadratic resolvent ring* of R.

Definition 7. For a cubic ring R, the *quadratic resolvent ring* $S^{\mathrm{res}}(R)$ of R is the unique quadratic ring S such that $\mathrm{Disc}(R) = \mathrm{Disc}(S)$.

Given a cubic ring R, there is a natural map from R to its quadratic resolvent ring S that preserves discriminants. Indeed, for an element $x \in R$, let x, x', x'' denote the S_3-conjugates of x in the S_3-closure $\bar{R}$ of R. Then the element

$$(4) \qquad \tilde{\phi}_{3,2}(x) = \frac{[(x-x')(x'-x'')(x''-x)]^2 + (x-x')(x'-x'')(x''-x)}{2}$$

is contained in some quadratic ring, and $\tilde{\phi}_{3,2}(x)$ has the same discriminant as x. (Notice that the expression (4) is only interesting modulo $\mathbb{Z}$, for $\tilde{\phi}_{3,2}(x)$ could be replaced by any translate by an element of $\mathbb{Z}$ and these same properties would still hold.) Moreover, all the elements $\tilde{\phi}_{3,2}(x)$ may be viewed as lying in a single ring $S^{\mathrm{inv}}(R)$ naturally associated to R, namely the quadratic subring of $\bar{R}\otimes\mathbb{Q}$ defined by

$$S^{\mathrm{inv}}(R) = \mathbb{Z}[\{\tilde{\phi}_{3,2}(x) : x \in R\}]. \tag{5}$$

This ring is quadratic because it is fixed under the natural action of the alternating group on the rank 6 ring $\bar{R}\otimes\mathbb{Q}$. We call $S^{\mathrm{inv}}(R)$ the *quadratic invariant ring* of R.

How is $S^{\mathrm{inv}}(R)$ related to the quadratic resolvent ring $S = S^{\mathrm{res}}(R)$? To answer this question, note that forming $\tilde{\phi}_{3,2}(x)$ for $x \in R$ involves taking a square root of the discriminant of x in $(\bar{R}\otimes\mathbb{Q})^{A_3}$. Since $\mathrm{Disc}(x)$ is equal to $n^2\mathrm{Disc}(R)$ for some integer n, we see that $\tilde{\phi}_{3,2}(x)$ is naturally an element of the quadratic resolvent S for all $x \in R$, so that $S^{\mathrm{inv}}(R)$ is naturally a subring of S. In particular, the map $\tilde{\phi}_{3,2} : R \to S^{\mathrm{inv}}(R)$ may also be viewed as a discriminant-preserving map

$$\tilde{\phi}_{3,2} : R \to S. \tag{6}$$

When does $S^{\mathrm{inv}}(R) = S$? As we shall prove in the next section, the answer is that $S^{\mathrm{inv}}(R) = S$ precisely when R is primitive and $R\otimes\mathbb{Z}_2 \not\cong \mathbb{Z}_2^3$. Thus for "most" cubic rings R, $S^{\mathrm{inv}}(R) = S$.

Let us now examine the implication of our construction for the parametrization of cubic rings. Suppose R is a cubic ring and S is the quadratic resolvent ring of R, and let $\tilde{\phi}_{3,2} : R \to S$ be the mapping defined by (4). Then observe that $\tilde{\phi}_{3,2}(x) = \tilde{\phi}_{3,2}(x + c)$ for any $c \in \mathbb{Z}$; hence, in particular, $\tilde{\phi}_{3,2} : R \to S$ descends to a mapping

$$\phi_{3,2} : R/\mathbb{Z} \to S/\mathbb{Z}. \tag{7}$$

As a map of $\mathbb{Z}$-modules, $\phi_{3,2}$ is seen to be a cubic map from $\mathbb{Z}^2$ to $\mathbb{Z}$, and thus corresponds to an integral binary cubic form, well-defined up to $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z})$-equivalence.

To produce explicitly a binary cubic form corresponding to the cubic ring R as above, we compute the discriminant of $x\omega_1 + y\omega_2 \in R$, where R has $\mathbb{Z}$-basis $\langle 1, \omega_1, \omega_2\rangle$ and multiplication is defined by (2). An explicit calculation shows that

$$\mathrm{Disc}(x\omega_1 + y\omega_2) = D\,(ax^3 + bx^2y + cxy^2 + dy^3)^2.$$

Since $S/\mathbb{Z}$ is generated by $(D+\sqrt{D})/2$, it is clear that the binary cubic form corresponding to the map $\phi_{3,2}$ is given by

$$\frac{\sqrt{\mathrm{Disc}(x\omega_1 + y\omega_2)}/2}{\sqrt{D}/2} = ax^3 + bx^2y + cxy^2 + dy^3.$$

Thus we have obtained a concrete ring-theoretic interpretation of the Delone-Faddeev parametrization of cubic rings.

2.3. *Cubic resolvents of a quartic ring.* Now let Q be a *quartic ring*, i.e., any ring of rank 4. Developing the quartic analogue of the work of the previous section is the key to determining what the corresponding parametrization of quartic rings should be. To accomplish this task, we must in particular determine the correct notions of a cubic resolvent ring R of Q, a cubic invariant ring $R^{\mathrm{inv}}(Q)$ of Q, and a map

$$\tilde{\phi}_{4,3} : Q \to R.$$

As it turns out, the notion of what the cubic resolvent ring R should be is not quite as immediate and clear cut as was the concept of quadratic resolvent ring in the cubic case. Thus, we turn first to the map $\tilde{\phi}_{4,3}$ and to the cubic invariant ring $R^{\mathrm{inv}}(Q)$, which are easier to define.

In analogy with the cubic case of the previous section, we should like $\tilde{\phi}_{4,3}$ to be a polynomial function that associates to any x in a quartic ring a natural element of the same discriminant in a cubic ring. Such a map does indeed exist: if $\bar{Q}$ denotes the S_4-closure of Q, and x, x', x'', x''' denote the conjugates of x in $\bar{Q}$, then $\tilde{\phi}_{4,3}(x)$ is defined by the following well-known expression:

$$\tilde{\phi}_{4,3}(x) = xx' + x''x'''. \tag{8}$$

It is known from the classical theory of solving the quartic that $\tilde{\phi}_{4,3}$ is discriminant-preserving; it is also clear that $\tilde{\phi}_{4,3}(x)$ lies in a cubic ring, having exactly three S_4-conjugates in $\bar{Q}$. In fact, all elements $\tilde{\phi}_{4,3}(x)$ for $x \in Q$ are seen to lie in a single cubic ring, namely, the cubic subring of $\bar{Q}$ fixed under the action of a fixed dihedral subgroup $D_4 \subset S_4$ of order 8. Following the example of the previous section, let us define

$$R^{\mathrm{inv}}(Q) = \mathbb{Z}[\{\tilde{\phi}_{4,3}(x) : x \in Q\}]. \tag{9}$$

We call $R^{\mathrm{inv}}(Q)$ the *cubic invariant ring* of Q. Thus we have a natural, discriminant-preserving map

$$\tilde{\phi}_{4,3} : Q \to R^{\mathrm{inv}}(Q).$$

Let us return to the notion of cubic resolvent of Q. In analogy again with the cubic-quadratic case, we should like to define the cubic resolvent of the quartic ring Q to be a cubic ring R that has the same discriminant as Q and that contains $R^{\mathrm{inv}}(Q)$. However, there may actually be many such rings, and no single one naturally lends itself to being distinguished from the others. Thus we ought to allow any such ring to be called a cubic resolvent ring of Q.

Definition 8. Let Q be a quartic ring, and $R^{\mathrm{inv}}(Q)$ its cubic invariant ring. A *cubic resolvent ring* of Q is a cubic ring R such that $\mathrm{Disc}(Q) = \mathrm{Disc}(R)$ and $R \supseteq R^{\mathrm{inv}}(Q)$.

In the next section we will see that every quartic ring has at least one cubic resolvent ring, and moreover, for a primitive quartic ring Q the cubic resolvent is in fact unique (and is simply $R^{\mathrm{inv}}(Q)$). Thus cubic resolvents exist, and given any cubic resolvent R of Q, we may then of course speak of the natural map

$$\tilde{\phi}_{4,3} : Q \to R.$$

Following the cubic case, let us see what implications our construction of cubic resolvents has for the parametrization of quartic rings. Suppose Q is a quartic ring, R is its cubic resolvent ring, and $\tilde{\phi}_{4,3} : Q \to R$ is the natural map as defined by (8). Then observe that for any $c \in \mathbb{Z}$,

$$\tilde{\phi}_{4,3}(x+c) = (x+c)(x'+c) + (x''+c)(x'''+c) = \tilde{\phi}_{4,3}(x) + d$$

for some $d \in \mathbb{Z}$, namely $d = c\,\mathrm{Tr}(x) + 2c^2$. Hence $\tilde{\phi}_{4,3} : Q \to R$ descends naturally to a map

$$\phi_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}. \tag{10}$$

As a map between $\mathbb{Z}$-modules, this map is a quadratic map from $\mathbb{Z}^3$ to $\mathbb{Z}^2$, and thus corresponds to a pair of integral ternary quadratic forms, well-defined up to $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$-equivalence.

As the reader will have noticed, the analogy with the cubic case up to this point is very remarkable, and if it is to continue, it suggests that *isomorphism classes of quartic rings should be parametrized roughly by pairs of integral ternary quadratic forms, up to integer equivalence.*

On the other hand, proving the latter statement, or even just determining the pair of ternary quadratic forms attached to a given quartic ring Q, is not quite as easy as the corresponding calculation was in the cubic case. The difference lies in the fact that, in the case of cubic rings, one could completely describe the quadratic resolvent ring, and so $\phi_{3,2}$ could also be described explicitly. For quartic rings, however, it is difficult to say anything *a priori* about the cubic resolvent ring other than that it is a ring of rank 3 and certain discriminant D; more structural information is not forthcoming without some additional work, which we carry out in Section 3.

Remark 1. The notion of cubic resolvent ring may also be defined without the notion of S_k-closure and cubic invariant ring. If Q is a quartic ring, a *cubic resolvent ring* R is a cubic ring equipped with a degree 2 polynomial map $\phi_{4,3} : Q \to R$, satisfying certain formal properties which make it "look like" $xx' + x''x'''$. Such a definition can be useful when one wishes to extend the results here to situations where the base ring is not $\mathbb{Z}$, or where the quartic rings being considered have discriminant zero. Further details of this approach are described in the Appendix to Section 3.

Remark 2. There are three canonically isomorphic copies of the cubic invariant ring of Q in $\bar{Q}$. The choice of map $\phi_{4,3}$ here thus corresponds simply to a fixed choice of cubic invariant ring in $\bar{Q}$. The other choices are obtained by renumbering the conjugations.

3. Quartic rings and pairs of ternary quadratic forms

Given a quartic ring Q, and a cubic resolvent ring R of Q, we have shown that one may associate to (Q, R) a natural, discriminant-preserving, quadratic map $\phi_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}$. If we choose bases for $Q/\mathbb{Z}$ and $R/\mathbb{Z}$, we may think of this map as a pair (A, B) of integral ternary quadratic forms $A(t_1, t_2, t_3)$ and $B(t_1, t_2, t_3)$. However, even if we are given explicitly a pair of rings (Q, R)—say via their multiplication tables—it is not immediate how to produce explicitly the pair (A, B) of integral ternary quadratic forms corresponding to (Q, R). Hence our strategy is to work the other way around: given a pair (A, B) of integral ternary quadratic forms, we determine the possible structures that the rings Q and R can have.

It is necessary first to understand some of the basic invariant theory of pairs of ternary quadratic forms. This is summarized briefly in Section 3.1. In Sections 3.2–3.5, we gather structural information on the rings Q and R, using only the data (A, B) corresponding to the map (10). This results in a proof of Theorem 1 in cases of nonzero discriminant. In Sections 3.6 and 3.7, we study the integral invariant theory of the space of pairs of ternary quadratic forms, and in particular, we show how the content of a quartic ring Q is related to the number of cubic resolvents of Q. This yields Theorems 2 and 3 and Corollaries 4 and 5, again in cases of nonzero discriminant. Finally, in the Appendix (Section 3.9), we describe a coordinate-free approach to some of the constructions used in this section. This approach allows, in particular, for a proof of Theorems 1–3 and Corollaries 4 and 5 in all cases including those of zero discriminant.

3.1. *The fundamental invariant* Disc(A, B).

In studying a pair (A, B) of ternary quadratic forms representing the map $\phi_{4,3}$ as in (13), we may change the basis of $Q/\mathbb{Z}$ or $R/\mathbb{Z}$ by elements of $\mathrm{GL}_3(\mathbb{Z})$ or $\mathrm{GL}_2(\mathbb{Z})$ respectively. This reflects the fact that the group $G_{\mathbb{Z}} = \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ acts on the space $V_{\mathbb{Z}}$ of pairs (A, B) of integral ternary quadratic forms in a natural way; namely, if $(A, B) \in (\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ is a pair of integral ternary quadratic forms (which we write as a pair of symmetric 3×3 matrices whose diagonal entries are integers and nondiagonal entries are half-integers), then an element $(g_3, g_2) \in G_{\mathbb{Z}}$ operates by sending (A, B) to

$$(g_3, g_2) \cdot (A, B) = (r \cdot g_3 A g_3^t + s \cdot g_3 B g_3^t, t \cdot g_3 A g_3^t + u \cdot g_3 B g_3^t), \tag{11}$$

where we have written g_2 as $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$.

We observe that the representation of $\mathrm{GL}_3(\mathbb{Z})\times\mathrm{GL}_2(\mathbb{Z})$ on $(\mathrm{Sym}^2\mathbb{Z}^3\otimes\mathbb{Z}^2)^*$ has just one polynomial invariant. To see this, notice first that the action of $\mathrm{GL}_3(\mathbb{Z})$ on $V_{\mathbb{Z}}$ has four independent polynomial invariants, namely the coefficients a, b, c, d of the binary cubic form

$$f(x,y) = 4\cdot\mathrm{Det}(Ax+By).$$

Next, $\mathrm{GL}_2(\mathbb{Z})$ acts on the cubic form $f(x,y)$, and it is well-known that this action has exactly one polynomial invariant, namely the discriminant $\mathrm{Disc}(f)$ of f. Thus the unique $\mathrm{GL}_3(\mathbb{Z})\times\mathrm{GL}_2(\mathbb{Z})$-invariant on $(\mathrm{Sym}^2\mathbb{Z}^3\otimes\mathbb{Z}^2)^*$ is $\mathrm{Disc}(4\cdot\mathrm{Det}(Ax+By))$. We call this fundamental invariant the *discriminant* $\mathrm{Disc}(A,B)$ of the pair (A,B). (The factor 4 has been included to insure that any pair of integral ternary quadratic forms has integral discriminant.)

3.2. *How much of the structure of Q is determined by (A,B)?* The only fact we have so far relating the structures of Q, R, and the map $\phi_{4,3}$ is that $\phi_{4,3}$ is discriminant-preserving as a map from Q to R. However, this fact alone yields little information on the nature of Q and R. Thus the following lemma on $\phi_{4,3}$ plays an invaluable role in determining the multiplicative structure of Q.

To state the lemma, we use the notation $\mathrm{Ind}_M(v_1,v_2,\ldots,v_k)$ to denote the (signed) index of the lattice spanned by $v_1,v_2,\ldots,v_k$ in the oriented rank k $\mathbb{Z}$-module M; in other words, $\mathrm{Ind}_M(v_1,v_2,\ldots,v_k)$ is the determinant of the transformation between $v_1,v_2,\ldots,v_k$ and any positively oriented $\mathbb{Z}$-basis of M.

LEMMA 9. *If Q is a quartic ring, and R is a cubic resolvent of Q, then for any $x,y\in Q$,*

$$\mathrm{Ind}_Q(1,x,y,xy) = \pm\,\mathrm{Ind}_R(1,\phi_{4,3}(x),\phi_{4,3}(y)). \tag{12}$$

Proof. Since $\mathrm{Disc}(Q)=\mathrm{Disc}(R)$, the assertion of the lemma is equivalent to the following identity:

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ x & x' & x'' & x''' \\ y & y' & y'' & y''' \\ xy & x'y' & x''y'' & x'''y''' \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ xx'+x''x''' & xx''+x'x''' & xx'''+x'x'' \\ yy'+y''y''' & yy''+y'y''' & yy'''+y'y'' \end{vmatrix}.$$

The identity may be verified by direct calculation. □

The sign in expression (12) of course depends on how Q and R are oriented. To fix the orientations on Q and R once and for all, let $\langle 1,\alpha_1,\alpha_2,\alpha_3\rangle$ and $\langle 1,\omega_1,\omega_2\rangle$ be bases for Q and R respectively such that the map $\phi_{4,3}$ is given by

$$\phi_{4,3}(t_1\bar\alpha_1+t_2\bar\alpha_2+t_3\bar\alpha_3) = B(t_1,t_2,t_3)\bar\omega_1 + A(t_1,t_2,t_3)\bar\omega_2, \tag{13}$$

where $\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3, \bar{\omega}_1, \bar{\omega}_2$ denote the reductions modulo $\mathbb{Z}$ of $\alpha_1, \alpha_2, \alpha_3, \omega_1, \omega_2$ respectively. Then we fix the orientations on Q and R so that $\mathrm{Ind}_Q(1, \alpha_1, \alpha_2, \alpha_3) = \mathrm{Ind}_R(1, \omega_1, \omega_2) = 1$.

We may make one additional assumption about the basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ without any harm. By translating $\alpha_1, \alpha_2, \alpha_3$ by appropriate constants in $\mathbb{Z}$, we may arrange for the coefficients of α_1 and α_2 in $\alpha_1\alpha_2$, together with the coefficient of α_1 in $\alpha_1\alpha_3$, to each equal zero. We call a basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ satisfying the latter conditions a *normal basis* for Q. Similarly, a basis $\langle 1, \omega_1, \omega_2 \rangle$ of R is called normal if the coefficients of ω_1 and ω_2 in $\omega_1\omega_2$ are both equal to zero. If we write out the multiplication laws for Q explicitly as

$$\alpha_i\alpha_j = c_{ij}^0 + \sum_{k=1}^{3} c_{ij}^k \alpha_k \,, \tag{14}$$

where $c_{ij}^k \in \mathbb{Z}$ for all $i, j \in \{1, 2, 3\}$ and $k \in \{0, 1, 2, 3\}$, then the condition that the basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ is normal is equivalent to

$$c_{12}^1 = c_{12}^2 = c_{13}^1 = 0. \tag{15}$$

Similarly, that the basis $\langle 1, \omega_1, \omega_2 \rangle$ of R is normal is equivalent to the multiplication table of R taking the form (2). We choose to normalize bases because bases of $Q/\mathbb{Z}$ (resp. $R/\mathbb{Z}$) then lift uniquely to normal bases of Q (resp. R).

We use Lemma 9 as follows. Let $x = r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3$, $y = s_1\alpha_1 + s_2\alpha_2 + s_3\alpha_3$ be general elements of Q, where $r_i, s_i \in \mathbb{Z}$. Then using (14), we find that

$$xy = c + t_1\alpha_1 + t_2\alpha_2 + t_3\alpha_3,$$

where $c \in \mathbb{Z}$ and

$$t_k = \sum_{1 \le i,j \le 3} c_{ij}^k \, r_i s_j \tag{16}$$

for $k = 1, 2, 3$. It follows that

$$\mathrm{Ind}_Q(1, x, y, xy) = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & r_1 & r_2 & r_3 \\ 0 & s_1 & s_2 & s_3 \\ 0 & t_1 & t_2 & t_3 \end{vmatrix}. \tag{17}$$

The right side of (17) is a polynomial of degree 4 in the variables r_1, r_2, r_3, s_1, s_2, s_3, which we denote by $p(r_1, r_2, r_3, s_1, s_2, s_3)$.

Similarly,

$$\mathrm{Ind}_R(1, \phi_{4,3}(x), \phi_{4,3}(y)) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & B(r_1, r_2, r_3) & A(r_1, r_2, r_3) \\ 0 & B(s_1, s_2, s_3) & A(s_1, s_2, s_3) \end{vmatrix}. \tag{18}$$

The right side of (18) is also a polynomial of degree 4 in the variables r_1, r_2, r_3, s_1, s_2, s_3, which we denote by $q(r_1, r_2, r_3, s_1, s_2, s_3)$. (Note that the multiplicative structure of R was not needed for computing the polynomial q.)

By Lemma 9, we conclude that for all integers $r_1, r_2, r_3, s_1, s_2, s_3$,

$$p(r_1, r_2, r_3, s_1, s_2, s_3) = q(r_1, r_2, r_3, s_1, s_2, s_3).$$

As they take equal values at all integer arguments, the polynomials p and q must in fact be identical. Equating coefficients of like terms yields a system of linear equations in the 15 variables c_{ij}^k in terms of the coefficients of the quadratic forms A and B, and this system is easily seen to have a unique solution. Writing out the pair (A, B) of ternary quadratic forms as

$$\begin{aligned} A(x_1, x_2, x_3) &= \sum_{1 \le i \le j \le 3} a_{ij}\, x_i x_j \\ B(x_1, x_2, x_3) &= \sum_{1 \le i \le j \le 3} b_{ij}\, x_i x_j, \end{aligned} \tag{19}$$

and letting $a_{ji} = a_{ij}$ and $b_{ji} = b_{ij}$, define the constants $\lambda_{k\ell}^{ij} = \lambda_{k\ell}^{ij}(A, B)$ by

$$\lambda_{k\ell}^{ij}(A, B) = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{k\ell} & b_{k\ell} \end{vmatrix}; \tag{20}$$

the $\lambda_{k\ell}^{ij}$ thus take up to 15 possible nonzero values up to sign. Then we find that the unique solution to the system $p = q$ is given as follows. For any permutation (i, j, k) of $(1, 2, 3)$, we have

$$\begin{aligned} c_{ii}^i &= \pm\lambda_{ij}^{ik} + C_i, \\ c_{ii}^j &= \pm\lambda_{ik}^{ii}, \\ c_{ij}^i &= \pm\tfrac{1}{2}\lambda_{jj}^{ik} + \tfrac{1}{2}C_j, \\ c_{ij}^k &= \pm\lambda_{ii}^{jj}, \end{aligned} \tag{21}$$

where we have used ± to denote the sign of the permutation (i, j, k) of $(1, 2, 3)$, and where the constants C_i are given by

$$C_1 = \lambda_{11}^{23}, \quad C_2 = -\lambda_{22}^{13}, \quad C_3 = \lambda_{33}^{12}. \tag{22}$$

In particular, the values of the c_{ij}^k (for $k > 0$) are all integral!

Note that the c_{ij}^0 are still undetermined. However, it turns out that the associative law for Q now uniquely determines the c_{ij}^0 from the other c_{ij}^k. Indeed, computing the expressions $(\alpha_i\alpha_j)\alpha_k$ and $\alpha_i(\alpha_j\alpha_k)$ using (14), and then equating the coefficients of α_k, yields the equality

$$c_{ij}^0 = \sum_{r=1}^{3} \bigl(c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k\bigr) \tag{23}$$

for any $k \in \{1,2,3\} \setminus \{j\}$. One easily checks using the explicit values given in (21) that the above expression is independent of k, and that with these values of c_{ij}^0 all relations among the c_{ij}^k implied by the associative law are completely satisfied. Furthermore, the c_{ij}^0 are clearly all integers. Thus we have completely determined the ring structure of $Q = Q(A,B)$ from (A,B); it is given in sum by (14), (21), (22), and (23).

It is also now easy to determine the multiplication structure of $Q(A,B)$ in terms of nonnormalized bases. If a basis element $\alpha_i \in Q$ as above is translated by an integer m_i, then evidently the constant C_i will be translated by $2m_i$. Therefore, the multiplication table of Q in terms of a general basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ is given by (21) and (23), where the C_i are any integer values satisfying

$$C_i \equiv \lambda_{ii}^{jk} \pmod 2. \tag{24}$$

Thus we have obtained a general description of the multiplication table of $Q = Q(A,B)$ in terms of any $\mathbb{Z}$-basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ of Q (not necessarily normalized).

It is interesting to ask what the discriminant of the resulting quartic ring $Q(A,B)$ is in terms of the pair of ternary quadratic forms (A,B). As an explicit calculation shows, the answer is happily that $\mathrm{Disc}(Q(A,B)) = \mathrm{Disc}(A,B)$. We may summarize this discussion as follows:

Proposition 10. *Let* $(A,B) \in (\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ *be a pair of ternary quadratic forms. If* (A,B) *represents the map* $\phi_{4,3}$ *for some pair of rings* (Q,R) *as in equation* (13), *then the quartic ring* $Q = Q(A,B)$ *is uniquely determined by* (A,B). *The multiplication table of* $Q(A,B)$ *is given by* (14), (21), (22), *and* (23), *and* $\mathrm{Disc}(Q(A,B)) = \mathrm{Disc}(A,B)$.

Notice that all the structure coefficients of Q are given in terms of the quantities $\lambda_{k\ell}^{ij}(A,B)$, which are SL_2-invariants on the space of pairs (A,B) of ternary quadratic forms. This should be expected since $\mathrm{SL}_2(\mathbb{Z})$ acts only on the basis of the cubic ring R and does not affect Q nor the chosen basis of Q. We study the SL_2-invariants $\lambda_{k\ell}^{ij}(A,B)$ in more detail in Section 3.7.

3.3. *How much of the structure of R is determined by (A,B)?* Since we have now found that the structure of Q is uniquely determined from the data (A,B), it may come as little surprise that the cubic ring R is also completely determined by (A,B).

In fact, it is easy to guess what R should be. By the Delone-Faddeev parametrization of cubic rings, there is a binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ associated to $R = \langle 1, \omega_1, \omega_2 \rangle$ such that $\mathrm{Disc}(f) = \mathrm{Disc}(R)$ and multiplication in R is as in (2). On the other hand, there is another natural binary cubic form associated to the pair (A,B) of ternary quadratic forms, namely $g(x,y)=a'x^3+b'x^2y+c'xy^2+d'y^3=4\cdot\mathrm{Det}(Ax+By)$, and this cubic form also has the same discriminant as $Q(A,B)$. Thus it is natural to guess that $f=g$, i.e., $a=a',\ b=b',\ c=c',\ d=d'$.

To prove the latter assertion, we may simply use the relation

$$\mathrm{Ind}_Q(1,x,x^2,x^3)=\mathrm{Ind}_R(1,\phi_{4,3}(x),\phi_{4,3}(x)^2), \tag{25}$$

since the multiplicative structure of Q is now in place. Let $x=r_1\alpha_1+r_2\alpha_2+r_3\alpha_3\in Q$. Then

$$\mathrm{Ind}_Q(1,x,x^2,x^3)=p(r_1,r_2,r_3)$$

and

$$\mathrm{Ind}_R(1,\phi_{4,3}(x),\phi_{4,3}(x)^2)=q(r_1,r_2,r_3),$$

where p and q are determinantal expressions similar to (17) and (18), but quite a bit larger and thus best left suppressed. As before, we argue that the polynomials p and q must take the same values for all integer choices of r_1,r_2,r_3, and consequently are identical. Equating coefficients of like terms, we obtain a system of several linear equations in a,b,c,d in terms of the coefficients of A and B. Solving these equations for a,b,c,d, we find that there is a unique solution whenever the image of $\phi_{4,3}$ generates a lattice of rank 2 in $R/\mathbb{Z}$; this occurs, in particular, whenever $\mathrm{Disc}(A,B)\neq 0$. In that case the unique solution is indeed given by $a=a'$, $b=b'$, $c=c'$, $d=d'$. That is,

$$ax^3+bx^2y+cxy^2+dy^3=4\cdot\mathrm{Det}(Ax+By) \tag{26}$$

and hence the structure of R is determined, at least whenever $\mathrm{Disc}(A,B)\neq 0$.

Proposition 11. *Let $(A,B)\in(\mathrm{Sym}^2\mathbb{Z}^3\otimes\mathbb{Z}^2)^*$ be a pair of ternary quadratic forms such that* $\mathrm{Disc}(A,B)\neq 0$. *If (A,B) represents the map $\phi_{4,3}$ for some pair of rings (Q,R) as in equation* (13), *then the ring $R=R(A,B)$ is uniquely determined by (A,B). The multiplication table of $R(A,B)$ is given by* (2) *and* (26), *and* $\mathrm{Disc}(R(A,B))=\mathrm{Disc}(A,B)$.

3.4. *Is R the cubic resolvent of Q*? It remains only to verify that the unique pair (Q,R) of rings we have obtained from (A,B) satisfy the conditions we require of them, namely, that R is a cubic resolvent of Q and that (A,B) describes the map

$$\phi_{4,3}:Q/\mathbb{Z}\to R/\mathbb{Z}.$$

We have already seen that $\mathrm{Disc}(Q)=\mathrm{Disc}(R)$. Hence it suffices just to show: if $F_{w,x,y,z}$ is the characteristic polynomial of a general element $w+x\alpha_1+y\alpha_2+z\alpha_3\in Q$ (acting on Q by multiplication), then there exists a constant $c\in\mathbb{Z}$ such that the characteristic polynomial $G_{w,x,y,z,c}$ of the element

$c+B(x,y,z)\omega_1+A(x,y,z)\omega_2 \in R$ (acting on R by multiplication) is the cubic resolvent of $F_{w,x,y,z}$.*

To prove the latter assertion, we use (14), (21), (22) and (23) to determine the action of $w+x\alpha_1+y\alpha_2+z\alpha_3$ on Q explicitly, allowing us to compute $F_{w,x,y,z}$. Similarly, we use (2) to explicitly compute $G_{w,x,y,z,c}$. These (somewhat lengthy) computations then show that there is a certain polynomial c, in the entries of A and B, such that $G_{w,x,y,z,c}$ is the cubic resolvent of $F_{w,x,y,z}$, as desired.

PROPOSITION 12. *Let* $(A,B) \in (\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ *be a pair of ternary quadratic forms with* $\mathrm{Disc}(A,B) \neq 0$. *Let* $Q(A,B)$ *and* $R(A,B)$ *be the quartic and cubic rings associated to* (A,B) *by Propositions* 10 *and* 11 *respectively. Then the ring* $R(A,B)$ *is a cubic resolvent of* $Q(A,B)$.

3.5. *The fundamental bijection: Remarks on Theorem* 1. The proof of Theorem 1 is now complete, at least in cases of nonzero discriminant. Indeed, the work in Sections 3.2–3.4 makes the bijection of Theorem 1 very precise. Given a quartic ring Q and a cubic resolvent ring R, one obtains a pair (A,B) of ternary quadratic forms from equation (13). Conversely, given a pair (A,B) of ternary quadratic forms, one obtains a quartic ring Q whose multiplication table is given by (14), (21), (22), and (23), and a cubic resolvent ring R of Q whose multiplication laws are given by (2) and (26). Moreover, it is clear from construction that the maps $(Q,R) \to (A,B)$ and $(A,B) \to (Q,R)$ are inverse to each other. This proves Theorem 1. We have also shown:

PROPOSITION 13. *The bijection in Theorem* 1 *is discriminant-preserving. That is, if* (Q,R) *is the pair of rings associated to a pair* (A,B) *of ternary quadratic forms as in Theorem* 1, *then* $\mathrm{Disc}(A,B) = \mathrm{Disc}(Q) = \mathrm{Disc}(R)$.

Notice that the mapping $(A,B) \to (Q,R)$ is described entirely by integer polynomials. Hence the same polynomials can be used to extend this mapping even to cases where (A,B) has zero discriminant. To maintain the bijection of Theorem 1, one need only understand what the appropriate definition of *cubic resolvent ring* is for degenerate quartic rings. The reader interested in more details is referred to the appendix at the end of this section.

As we remarked in the introduction, the cubic resolvent ring associated to a quartic ring is not necessarily unique. This leads to various questions: Does a cubic resolvent always exist for a quartic ring? For which quartic rings is the cubic resolvent ring unique? More generally, given a quartic ring Q, how can

*The cubic resolvent of a quartic polynomial $F(t) = t^4 + pt^3 + qt^2 + rt + s$ is given by the expression $G(t) = t^3 - qt^2 + (pr - 4s)t - (p^2s + 4qs - r^2)$. If the roots of F are denoted $\kappa, \kappa', \kappa'', \kappa'''$, then the roots of G are $\kappa\kappa' + \kappa''\kappa'''$, $\kappa\kappa'' + \kappa'\kappa'''$, $\kappa\kappa''' + \kappa'\kappa''$.

one determine the number of cubic resolvents of Q? To answer these questions, it is necessary to introduce the notion of *content* of a ring, which we discuss in the next section.

3.6. *The content of a ring.* In addition to the discriminant, rings of rank k possess another very important invariant which we call the *content*.

Definition 14. Let $\mathcal{R}$ be a ring of rank k. The *content* $\mathrm{ct}(\mathcal{R})$ of $\mathcal{R}$ is defined to be

$$\mathrm{ct}(\mathcal{R}) = \max\{n : \exists\tilde{\mathcal{R}} \text{ of rank } k \text{ such that } \mathcal{R} = \mathbb{Z} + n\tilde{\mathcal{R}}\},$$

if the latter maximum exists; otherwise, the content is said to be ∞.

For example, the quadratic ring $\mathbb{Z}[x]/(x^2)$ of discriminant 0 has content ∞, since it is equal to $\mathbb{Z} + nS_n$, where $S_n = \mathbb{Z}[x_n]/(x_n^2)$ and $x = nx_n$. For other quadratic rings, the content coincides with what is usually called the *conductor.*

It is clear from formulas (14), (21), (22), and (23) that the content of a quartic ring $Q = Q(A,B)$ is equal to the greatest common divisor of the fifteen SL_2-invariants $\lambda_{k\ell}^{ij}(A,B)$. It is thus natural to define the *content* $\mathrm{ct}(A,B)$ of a pair (A,B) of integral ternary quadratic forms to be the content of the corresponding quartic ring, i.e.,

$$\mathrm{ct}(A,B) = \mathrm{ct}(Q(A,B)) = \gcd\{\lambda_{k\ell}^{ij}(A,B)\}.$$

Most "nice" rings have content 1. For example, it is easy to see that any Gorenstein ring $\mathcal{R}$ of rank at least 3 must have content 1; for if $\mathcal{R}$ did not have content 1, then there would exist a prime p such that

$$\mathcal{R}/(p) \cong \mathbb{F}_p[x_1, x_2, \ldots, x_{k-1}]/(x_1, x_2, \ldots, x_{k-1})^2,$$

and the latter is clearly not Gorenstein if $k > 2$. Gan-Gross-Savin [10] have shown that in the rank 3 case, the notions of Gorenstein and content 1 actually coincide. This, however, does not hold true for higher rank, as the non-Gorenstein content 1 ring $\mathbb{Z} \oplus \mathbb{Z}[x,y]/(x^2, xy, y^2)$ illustrates.

Like the discriminant, the content gives important structural information about a ring of rank k. Our motivation for introducing the content arises from its close relation to resolvent rings. We explain this first briefly in the case of cubic rings. Here, the notion of content is exactly what is needed to answer the question posed in Section 2.2: when is the quadratic invariant ring of a cubic ring equal to its quadratic resolvent ring?

THEOREM 15. *Let R be a cubic ring, $S^{\mathrm{inv}}(R)$ the quadratic invariant ring of R, and S the quadratic resolvent ring of R. Then $[S : S^{\mathrm{inv}}(R)] = \epsilon(R)\cdot\mathrm{ct}(R)$, where $\epsilon(R) = 2$ if $R = \mathbb{Z}+\mathrm{ct}(R)\cdot R_1$ with $R_1\otimes\mathbb{Z}_2 \cong \mathbb{Z}_2^3$, and $\epsilon(R) = 1$ otherwise. In particular, $S^{\mathrm{inv}}(R) = S$ if and only if R is primitive and $R \otimes \mathbb{Z}_2 \not\cong \mathbb{Z}_2^3$.*

Proof. We observe that, by definition, the quadratic invariant ring $S^{\text{inv}}(R)$ is the smallest ring containing the image of the mapping $\phi_{3,2} : R \to S$, and any subring of S takes the form $\mathbb{Z} + rS$ for some nonnegative integer r. In the case of $S^{\text{inv}}(R) \subset S$, this number is simply the smallest nonnegative integer r such that $\phi_{3,2}(x)$ is a multiple of r in $S/\mathbb{Z}$ for all $x \in R/\mathbb{Z}$.

However, $\phi_{3,2}$ is given by a binary cubic form, and the greatest common divisor of the values taken by a binary cubic form f is simply $\epsilon(f) \cdot \text{ct}(f)$, where $\text{ct}(f)$ denotes the content of f and $\epsilon(f) = 2$ if $f/\text{ct}(f)$ factors into linear factors (mod 2), and $\epsilon(f) = 1$ otherwise. Now it is easy to check from (2) that $\epsilon(f) = \epsilon(R)$ and $\text{ct}(f) = \text{ct}(R)$. This gives the desired conclusion. □

In Section 3.8 we will show that the analogue of Theorem 15 is true also for quartic rings: $[R : R^{\text{inv}}(Q)] = \text{ct}(Q)$ for any cubic resolvent R of Q, and so the cubic invariant ring $R^{\text{inv}}(Q)$ of a quartic ring Q forms the (unique) cubic resolvent ring if and only if $\text{ct}(Q) = 1$. To prove this result, and its ramifications, it is first necessary to better understand the SL_2-related invariant theory of pairs of ternary quadratic forms. This is carried out in Section 3.7.

3.7. *More on the invariant theory of pairs of ternary quadratic forms.* We observed in Section 3.1 that the polynomial invariants for the action of $\text{SL}_3(\mathbb{C})$ on the space $V_{\mathbb{C}} = \text{Sym}^2\mathbb{C}^3 \otimes \mathbb{C}^2$ of pairs (A, B) of ternary quadratic forms over $\mathbb{C}$ are given by the four coefficients of the binary cubic form $f(x, y) = 4 \cdot \text{Det}(Ax + By) = ax^3 + bx^2y + cxy^2 + dy^3$. Moreover, the unique polynomial invariant for the action of $\text{SL}_3(\mathbb{C}) \times \text{SL}_2(\mathbb{C})$ on $V_{\mathbb{C}}$ is simply $\text{Disc}(A, B) = \text{Disc}(4 \cdot \text{Det}(Ax + By))$.

In this section, we examine more closely the $\text{SL}_2(\mathbb{C})$-invariants on $V_{\mathbb{C}}$, as these are precisely the quantities that determine the structure of the quartic rings corresponding to points in $V_{\mathbb{C}}$. If we write out again the element $(A, B) \in V_{\mathbb{C}}$ in the form (19), then as observed earlier the $\text{SL}_2(\mathbb{C})$-invariants on $V_{\mathbb{C}}$ are given by the 15 numbers $\lambda^{ij}_{k\ell}$ as defined by (20), where $1 \le i \le j \le 3$, $1 \le k \le \ell \le 3$, and $(1, 1) \le (i, j) < (k, \ell) \le (3, 3)$ in lexicographic ordering. However, unlike the case of the four SL_3-invariants a, b, c, d, these 15 SL_2-invariants are not independent, but are related by the fifteen syzygies

$$\lambda^{gh}_{k\ell}(A,B)\,\lambda^{ij}_{mn}(A,B) = \lambda^{gh}_{ij}(A,B)\,\lambda^{k\ell}_{mn}(A,B) + \lambda^{gh}_{mn}(A,B)\,\lambda^{ij}_{k\ell}(A,B), \tag{27}$$

where $(1, 1) \le (g, h) < (i, j) < (k, \ell) < (m, n) \le (3, 3)$ again in lexicographic ordering.[†] The identity (27) is simply a special case of the Plücker relations applied to the four vectors (a_{gh}, b_{gh}), (a_{ij}, b_{ij}), $(a_{k\ell}, b_{k\ell})$, $(a_{mn}, b_{mn}) \in \mathbb{C}^2$.

Conversely, given any set of 15 constants $\{\lambda^{ij}_{k\ell}\}$ satisfying the fifteen relations (27), there is always an $\text{SL}_2(\mathbb{C})$-orbit in $V_{\mathbb{C}}$ possessing these 15 constants

[†] These fifteen syzygies are also not independent, but this does not matter for our purposes.

as the SL_2-invariants. In fact, something stronger is true; namely, if these 15 constants $\lambda_{k\ell}^{ij}$ are actually integers, then there exists an integer point in $V_{\mathbb{C}}$ possessing these 15 constants as the SL_2-invariants. We state this more precisely in the following lemma.

Lemma 16. *For any* 15 *constants* $\lambda_{k\ell}^{ij} \in \mathbb{C}$ *satisfying the relations* (27), *there exists an irreducible* $\mathrm{SL}_2(\mathbb{C})$-*orbit* $W \subset V_{\mathbb{C}}$ *such that*

$$\lambda_{k\ell}^{ij}(W) = \lambda_{k\ell}^{ij} \ \textit{ for all } \ i \leq j, \ \ k \leq \ell, \ \ (i,j) < (k,\ell).$$

If the 15 *constants* $\lambda_{k\ell}^{ij}$ *are not all equal to zero, then* W *is uniquely determined, and if furthermore all the* $\lambda_{k\ell}^{ij}$ *are integers, then the variety* W *contains an integer point* $(A,B) \in V_{\mathbb{Z}}$.

Proof. It is easy to see that all invariants $\lambda_{k\ell}^{ij}(A,B)$ are equal to zero if and only if $\{A,B\}$ spans a zero or one-dimensional space in V. There are of course (infinitely) many such points (A,B), both in $V_{\mathbb{C}}/G_{\mathbb{C}}$ as well as in $V_{\mathbb{Z}}/G_{\mathbb{Z}}$.

We therefore proceed to the case where not all invariants are zero; without loss of generality, we may assume $\lambda_{12}^{11} \neq 0$. Applying the appropriate transformation in $\mathrm{SL}_2(\mathbb{C})$, we may assume then that $a_{11} = 1$, $b_{11} = 0$, $a_{12} = 0$, and $b_{12} = \lambda_{12}^{11} \neq 0$.

With these assumptions, the definition (20) of $\lambda_{k\ell}^{ij}$ for $(i,j) = (1,1)$ and $(1,2)$ immediately implies that $b_{k\ell} = \lambda_{k\ell}^{11}$ for all k,ℓ, and that $a_{k\ell} = \lambda_{k\ell}^{12}/b_{12}$ for all $(k,\ell) \neq (1,1)$. Six of the equations in (20) remain unused, but they, when expanded, now turn out to be equivalent to six of the syzygies in (27). Therefore, if the 15 invariants $\lambda_{k\ell}^{ij}$ are fixed, not all zero, and satisfy the syzygies (27), then there is a unique solution for (A,B) of the above type, and so a unique $\mathrm{SL}_2(\mathbb{C})$-orbit W having the prescribed set of invariants.

Assume now that the 15 constants $\lambda_{k\ell}^{ij}$ are also integral. Then, by the above discussion, the quantities $b_{ij} = \lambda_{ij}^{11}$ are themselves forced to be integers, while the quantities $a_{ij} = \lambda_{ij}^{12}/b_{12}$ are all integer multiples of $1/b_{12}$. Consider the pair of integral forms $(b_{12}A, B) \in V_{\mathbb{Z}}$, whose λ-invariants are all multiples of b_{12}. By the theory of elementary divisors, there exists an $\mathrm{SL}_2(\mathbb{Z})$-transformation (A',B') of $(b_{12}A,B)$ such that A' is a multiple of n_1 and B' is a multiple of n_2, where n_1, n_2 are integers such that $n_1 n_2 = b_{12}$. It follows that $(A'/n_1, B'/n_2) \in V_{\mathbb{Z}}$ is $\mathrm{SL}_2(\mathbb{Q})$-equivalent to (A,B), and is therefore an integer point of W. □

Lemma 16 implies that if the $\lambda_{k\ell}^{ij}$'s are integers satisfying (27), then there exists at least one $G_{\mathbb{Z}}$-orbit on $V_{\mathbb{Z}}$ having those integers as its SL_2-invariants. The next lemma strengthens this, by giving the exact number of $G_{\mathbb{Z}}$-orbits on $V_{\mathbb{Z}}$ having a prescribed set of (integral) SL_2-invariants.

Lemma 17. *Let $\lambda^{ij}_{k\ell} \in \mathbb{Z}$ be any* 15 *integers satisfying the relations* (27), *and let n be their* gcd. *Then the number of $G_{\mathbb{Z}}$-orbits $W_{\mathbb{Z}}$ in $V_{\mathbb{Z}}$ such that*

$$\lambda^{ij}_{k\ell}(W_{\mathbb{Z}}) = \lambda^{ij}_{k\ell} \ \textit{ for all } \ i \le j, \ \ k \le \ell, \ \ (i,j) < (k,\ell)$$

is equal to the number of index n sublattices of $\mathbb{Z}^2$ (*and hence to the sum of the divisors of n*).

Proof. The lemma is true when all the SL$_2$-invariants $\lambda^{ij}_{k\ell}$ are zero (i.e., $n = \infty$), and so we assume the integers $\lambda^{ij}_{k\ell}$ are not all equal to zero.

Clearly, the set of integers $\{\lambda^{ij}_{k\ell}/n\}$ also satisfy the syzygies (27); hence, by Lemma 16, there is exactly one SL$_2(\mathbb{C})$-orbit W in $V_{\mathbb{C}}$ having $\{\lambda^{ij}_{k\ell}/n\}$ as the SL$_2$-invariants, and W contains an integral point (A, B). Let $X \subset \mathrm{Sym}^2\mathbb{C}^3$ denote the two-dimensional $\mathbb{C}$-vector space of ternary quadratic forms spanned by A and B (equivalently, X is the vector space spanned by A_0, B_0 for any point $(A_0, B_0) \in W$), and let $X_{\mathbb{Z}}$ denote the (unique) maximal lattice in X consisting of integral ternary quadratic forms. Since $\gcd\{\lambda^{ij}_{k\ell}(A, B)\} = 1$, it must be that A, B span a maximal integral lattice in X, so A, B actually form a $\mathbb{Z}$-basis for $X_{\mathbb{Z}}$.

Define $W_{\mathbb{Z}}$ by

$$W_{\mathbb{Z}} = \{(A, B) : \{A, B\} \text{ spans } X_{\mathbb{Z}} \text{ as a } \mathbb{Z}\text{-module}\}.$$

Then $W_{\mathbb{Z}} \subset W$, $W_{\mathbb{Z}}$ forms a single SL$_2(\mathbb{Z})$-orbit, and any integral point $(A, B) \in W$ must lie in $W_{\mathbb{Z}}$. Hence $W_{\mathbb{Z}}$ is the unique SL$_2(\mathbb{Z})$-orbit in $V_{\mathbb{Z}}$ having $\lambda^{ij}_{k\ell}/n$ as the SL$_2$-invariants.

Similarly, if $W'_{\mathbb{Z}}$ is an SL$_2(\mathbb{Z})$-orbit in $V_{\mathbb{Z}}$ having SL$_2$-invariants $\lambda^{ij}_{k\ell}$, then for any $(A', B') \in W'_{\mathbb{Z}}$, A', B' span a lattice L in $X_{\mathbb{Z}}$, and we may define $W'_{\mathbb{Z}}$ by

$$W'_{\mathbb{Z}} = \{(A, B) : \{A, B\} \text{ spans } L \text{ as a } \mathbb{Z}\text{-module}\}. \tag{28}$$

Moreover, $\gcd\{\lambda^{ij}_{k\ell}(A, B)\} = n$ implies that this sublattice L has index n in $X_{\mathbb{Z}}$. Conversely, given any index n sublattice L of $X_{\mathbb{Z}}$, let $W'_{\mathbb{Z}}$ be defined by (28). Then $W'_{\mathbb{Z}}$ is an SL$_2(\mathbb{Z})$-orbit with the desired invariants. Thus the SL$_2(\mathbb{Z})$-orbits in $V_{\mathbb{Z}}$ having SL$_2$-invariants $\lambda^{ij}_{k\ell}$ are in one-to-one correspondence with the index n sublattices of $X_{\mathbb{Z}} \cong \mathbb{Z}^2$. This implies the lemma. □

3.8. *Isolating Q*: *Remarks on Theorems* 2 *and* 3. Given a quartic ring Q, and given the structure coefficients of Q with respect to a normal basis $\langle 1, \alpha_1, \alpha_2, \alpha_3\rangle$ of Q, the relations (21), (22), and (23) completely determine the values of the 15 constants $\lambda^{ij}_{k\ell}$. Indeed, equation (21) shows that only the coefficients c^k_{ij} for $k > 0$ are needed in order to determine the values of $\lambda^{ij}_{k\ell}$. The associative law in Q then does two things. First, as we have observed earlier, it implies that the values of the constant coefficients c^0_{ij} must then be as given in (23). Second, it implies that the syzygies (27) must hold among the $\lambda^{ij}_{k\ell}$. By Lemma 16, it follows that there exists an integer orbit $\bar{x} \in V_{\mathbb{Z}}/G_{\mathbb{Z}}$ such that $Q(\bar{x}) = Q$ and $\mathrm{Disc}(Q(\bar{x})) = \mathrm{Disc}(x)$, and Lemma 17 gives the number of such orbits. In conjunction with Theorem 1, this proves Theorems 2 and 3 and Corollaries 4 and 5.

We may also now prove the analogue of Theorem 15 for quartic rings:

Corollary 18. *Let Q be a quartic ring, $R^{\mathrm{inv}}(Q)$ the cubic invariant ring of Q, and R any cubic resolvent ring of Q. Then $[R : R^{\mathrm{inv}}(Q)] = \mathrm{ct}(Q)$. In particular, $R^{\mathrm{inv}}(Q) = R$ if and only if Q is primitive.*

Proof. Let (A, B) denote any pair of ternary quadratic forms corresponding to (Q, R) as in Theorem 1. If $\mathrm{ct}(A, B) = \mathrm{ct}(Q) = 1$, then the six vectors $(a_{ij}, b_{ij}) \in \mathbb{Z}^2$ for $1 \leq i, j \leq 3$ generate all of $\mathbb{Z}^2$. It follows that the $\mathbb{Z}$-module generated by $\phi_{4,3}(\bar{\alpha})$, for $\bar{\alpha} \in Q/\mathbb{Z}$, is all of $R/\mathbb{Z}$. Hence, if Q is primitive, then $R^{\mathrm{inv}}(Q) = R$.

Suppose now that $\mathrm{ct}(A, B) = \mathrm{ct}(Q) = n > 1$. Let Q' be the quartic ring such that $Q = \mathbb{Z} + nQ'$. Since Q' is primitive, $R' = R^{\mathrm{inv}}(Q')$ is the (unique) cubic resolvent of Q'. Furthermore, because the discriminant of a quartic ring is equal to the discriminant of any of its cubic resolvents, we must have $[R' : R] = [Q' : Q] = n^3$. Finally, since $\phi_{4,3}$ is quadratic, it is clear that $R^{\mathrm{inv}}(Q) = \mathbb{Z} + n^2 R'$, and therefore we have $[R' : R^{\mathrm{inv}}(Q)] = n^4$. It follows that $[R : R^{\mathrm{inv}}(Q)] = [R' : R^{\mathrm{inv}}(Q)]/[R' : R] = n^4/n^3 = n$, as desired. □

Note that the proof of Corollary 18 implies that for a quartic order Q, the $\mathbb{Z}$-*module* in $\bar{Q}$ generated by 1 and $\tilde{\phi}_{4,3}(\alpha)$ $(\alpha \in Q)$ is in fact always a ring, namely, it is the cubic invariant ring $R^{\mathrm{inv}}(Q)$ as defined by (9).

3.9. *Appendix*: *An alternative description of cubic resolvents.* In this appendix, we describe an alternative definition of a cubic resolvent ring of a quartic ring which does not use the notion of S_k-closure. This definition is especially useful for quartic rings of zero discriminant, and allows for an immediate proof of Theorem 1 in all cases. It also allows one to use base rings other than $\mathbb{Z}$, such as $\mathbb{Z}_p$ or $\mathbb{F}_p$. In the case of $\mathbb{F}_p$, discriminant zero rings are particularly important as they frequently arise as reductions modulo p of orders in a number field.

The idea is to view a cubic resolvent ring of a quartic ring Q as a cubic ring R equipped with a quadratic map $\phi : Q/\mathbb{Z} \to R/\mathbb{Z}$ (called the *resolvent mapping*) which satisfies all properties of the "$xx' + x''x'''$ map" (i.e., the "$\phi_{4,3}$ map") that were crucial for us in Sections 2.3 and 3.2–3.4. To isolate the necessary properties, we examine the identities (12) and (25), as these are the identities that were needed to obtain multiplication structures on Q and R respectively.

Let us first consider the identity (12). To choose the positive sign in this identity, it was necessary for us to assign compatible orientations on Q and R. This may be viewed as a choice of isomorphism $\tilde{\xi} : \wedge^4 Q \to \wedge^3 R$, or equivalently, as an isomorphism $\xi : \wedge^3(Q/\mathbb{Z}) \to \wedge^2(R/\mathbb{Z})$. Equation (12) then states that we have, for any $x, y \in Q$, the identity

$$\xi(x \wedge y \wedge xy) = \phi(x) \wedge \phi(y). \tag{29}$$

As was proven in Section 3.2, this identity suffices to determine the multiplication structure on Q from the data ϕ.

Next, we consider equation (25), which states that

$$\xi(x \wedge x^2 \wedge x^3) = \phi(x) \wedge \phi(x)^2. \tag{30}$$

As noted in Section 3.3, this identity is enough to determine the structure on R, provided that the cubic invariant ring $\mathbb{Z}[\phi(x) : x \in Q]$ is actually a cubic ring. For Q having discriminant zero, however, this is not always the case. Nevertheless, the canonical multiplication structure on R obtained from (25) in cases of nonzero discriminant can naturally be extended by Zariski closure to a canonical multiplication structure on R in all cases, including those of discriminant zero. Namely, if ϕ is represented by a pair of ternary quadratic forms (A, B) as in (13), then R should be the cubic ring $R(f)$ given by the Delone-Faddeev correspondence, where f is as before the binary cubic form $f(x, y) = \mathrm{Disc}(Ax + By) = 4 \cdot \mathrm{Det}(Ax + By)$.

This description of R may be expressed in coordinate-free language as follows. A quadratic map $\phi : Q/\mathbb{Z} \to R/\mathbb{Z}$ is equivalent to a linear map $\mathrm{Sym}^2(Q/\mathbb{Z}) \to R/\mathbb{Z}$, and so may be viewed as an element

$$\phi \in \mathrm{Sym}^2(Q/\mathbb{Z})^* \otimes R/\mathbb{Z}. \tag{31}$$

Now an element $\mathrm{Sym}^2(Q/\mathbb{Z})^*$ is a quadratic form on $Q/\mathbb{Z}$, and so one can take its discriminant $\mathrm{Disc} = 4 \cdot \mathrm{Det}$ in the usual sense. Therefore, we may apply the map $\mathrm{disc} = \mathrm{Disc} \otimes \mathrm{id}$ to (31) and we obtain

$$\mathrm{disc} \circ \phi \in \wedge^3(Q/\mathbb{Z})^{\otimes -2} \otimes R/\mathbb{Z}. \tag{32}$$

Next, there is a natural bilinear skew-symmetric pairing $(\ ,\ ) : R/\mathbb{Z} \otimes R/\mathbb{Z} \to \wedge^2(R/\mathbb{Z}) \cong \mathbb{Z}$ given by $(x, y) = x \wedge y$, yielding a natural isomorphism $\iota : R/\mathbb{Z} \xrightarrow{\sim} \wedge^2\,(R/\mathbb{Z}) \otimes (R/\mathbb{Z})^*$. Since $\wedge^3(Q/\mathbb{Z})^*$ is isomorphic to $\wedge^2(R/\mathbb{Z})^*$ via the map ξ^{*-1}, we may apply $\eta = \xi^{*-1} \otimes \xi^{*-1} \otimes \iota$ to (32) to obtain

$$\eta \circ \mathrm{disc} \circ \phi \in \wedge^2(R/\mathbb{Z})^* \otimes (R/\mathbb{Z})^*. \tag{33}$$

Finally, because of the alternating pairing $(\ ,\ )$ on $R/\mathbb{Z}$, the spaces $R/\mathbb{Z}$ and $(R/\mathbb{Z})^*$ may be naturally identified up to sign. Therefore, $\wedge^2(R/\mathbb{Z})$ and $\wedge^2(R/\mathbb{Z})^*$ are canonically isomorphic, with no issues of sign, and so we may view the element in (33) as a map

$$\eta \circ \mathrm{disc} \circ \phi : R/\mathbb{Z} \to \wedge^2(R/\mathbb{Z}).$$

We write $\eta \circ \mathrm{disc} \circ \phi = \mathrm{Disc}(\phi)$. In this notation, the requirement that R correspond to ϕ under the Delone-Faddeev correspondence amounts to the identity

$$[\,\mathrm{Disc}(\phi)\,](z) = z \wedge z^2, \tag{34}$$

for any $z \in R$. It follows from Delone and Faddeev's theorem that the above identity determines the ring R from the data ϕ.

The following definition thus isolates the essential properties of the classical resolvent mapping $\phi_{4,3}(x) = xx' + x''x'''$ that were needed during the course of the proof of Theorem 1.

Definition 19. Let Q be a quartic ring, R a cubic ring, and $\xi : \wedge^3(Q/\mathbb{Z}) \to \wedge^2(R/\mathbb{Z})$ an isomorphism. Then we call a quadratic map $\phi : Q/\mathbb{Z} \to R/\mathbb{Z}$ a *resolvent mapping* if (a) the identity (29) holds for all $x, y \in Q$; and (b) the binary cubic form associated to R under the Delone-Faddeev correspondence is $\mathrm{Disc}(\phi)$ (that is, the identity (34) holds for all $z \in R$).

It is clear from the work of Sections 3.2–3.4 that the above definition agrees with the classical resolvent mapping $\phi_{4,3}$ in the case that Q lies in a quartic field and R lies in the cubic resolvent field.

We may now define a general notion of cubic resolvent ring:

Definition 20. Let Q be a quartic ring. A *cubic resolvent ring* of Q is a cubic ring R equipped with an isomorphism $\xi : \wedge^3(Q/\mathbb{Z}) \to \wedge^2(R/\mathbb{Z})$ and a resolvent mapping $\phi : Q/\mathbb{Z} \to R/\mathbb{Z}$.

With these definitions, Theorem 1 immediately extends also to cases of zero discriminant, and our remarks on the proof of Theorem 1 (Section 3.5, first paragraph) hold true without any change.

Remark. Professor Deligne has recently remarked to me that, with the latter formulation of cubic resolvent ring, it should be possible to extend Theorem 1 to locally-free quartic algebras over an arbitrary base ring. We hope that this interesting possibility will be considered in future work.

4. Maximality, prime splitting, and local densities

An important class of rings on which Theorem 1 gives a bijective correspondence are the maximal orders in quartic number fields. These, of course, are the quartic rings of greatest interest to algebraic number theorists. We therefore wish to understand those pairs (A, B) of integral ternary quadratic forms that correspond to maximal orders in quartic fields, and moreover, to understand the splitting behavior of primes in those fields in terms of the corresponding pairs (A, B).

This is the goal of Sections 4.1 and 4.2. In particular, we determine the p-adic density of the set of all $(A, B) \in V$ corresponding to maximal quartic rings $Q(A, B)$, and we similarly determine the p-adic density of all (A, B) such that $Q(A, B)$ has any one of the various types of prime-splitting behavior at p. These results may be useful in future computational applications (see e.g., [6]), and they also play a very important role in determining the density of discriminants of quartic fields (see [4]).

4.1. *Local behavior.* In this section, we consider pairs (A, B) of ternary quadratic forms over the p-adic ring $\mathbb{Z}_p$ and over its residue field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Let (A, B) be an element of $V_{\mathbb{Z}}$ (resp. of $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$). Over the residue field $\mathbb{F}_p$, (A, B) determines two conics in $\mathbb{P}^2_{\mathbb{F}_p}$, which, aside from certain degenerate cases, intersect each other in exactly four points (counting multiplicities). For such nondegenerate pairs (A, B), define the symbol $((A, B), p)$ by putting

$$((A, B), p) = (f_1^{e_1} f_2^{e_2} \cdots), \tag{35}$$

where the f_i's indicate the degrees of the residue fields at the points of intersection, and the e_i's indicate the respective multiplicities. There are thus eleven possible values for the symbol $((A, B), p)$, namely, (1111), (112), (13), (22), (4), $(1^2 11)$, $(1^2 2)$, $(1^2 1^2)$, (2^2), $(1^3 1)$, and (1^4). (As is customary, we suppress exponents that are equal to one.)

It is clear that if two points x, y in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) are equivalent under a transformation in $\mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{GL}_2(\mathbb{Z}_p)$, $\mathrm{GL}_2(\mathbb{F}_p)$), then $(x, p) = (y, p)$. By $T_p(1111), T_p(112)$, etc., let us denote the set of x such that $(x, p) = (1111)$, $(x, p) = (112)$, etc.

By the definition of $Q(A, B)$, the ring structure of the quotient ring $Q(A, B)/(p)$ depends only on the $\mathrm{GL}_2(\mathbb{F}_p)$-orbit of the pair (A, B) modulo p; thus the symbol $((A, B), p)$ should indicate something about the structure of the ring $Q(A, B)$ when reduced modulo p. In fact, a direct calculation shows that

$$(A, B) \in T_p(f_1^{e_1} f_2^{e_2} \cdots) \tag{36}$$

if and only if

$$Q(A, B)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \cdots, \tag{37}$$

except in the case $T_p(1^4)$, where the ring $Q(A, B)/(p)$ might take other forms, namely $\mathbb{F}_2[x, y]/(x^2, xy + y^2)$, $\mathbb{F}_p[x, y]/(x^2, y^2)$, or $\mathbb{F}_p[x, y]/(xy, x^2 + ny^2)$, where n denotes a quadratic nonresidue modulo p. It is therefore natural to partition $T_p(1^4)$ into two further sets: $T_p^{(1)}(1^4)$, consisting of the pairs (A, B) such that $Q(A, B)/(p) \cong \mathbb{F}_p[t]/(t^4)$; and $T_p^{(2)}(1^4)$, consisting of the remaining elements of $T_p(1^4)$. Geometrically, $T_p^{(1)}(1^4)$ consists of pairs (A, B) where the two conics $A = 0$ and $B = 0$ intersect in exactly one point and at least one of $A = 0$

or $B=0$ is irreducible over $\bar{\mathbb{F}}_p$, while $T_p^{(2)}(1^4)$ consists of pairs (A,B) where $A=0$ and $B=0$ are reducible conics passing through a single common point.

For any set S in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) that is definable by congruence conditions, denote by $\mu(S)=\mu_p(S)$ the p-adic density of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure μ on V so that $\mu(V_{\mathbb{Z}_p})=1$. The following lemma gives the p-adic densities of the sets $T_p(\cdot)$.

Lemma 21.

$$\begin{aligned}
\mu(T_p(1111)) &= \tfrac{1}{24}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(112)) &= \tfrac{1}{4}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(13)) &= \tfrac{1}{3}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(22)) &= \tfrac{1}{8}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(4)) &= \tfrac{1}{4}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(1^211)) &= \tfrac{1}{2}\,(p-1)^3\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(1^22)) &= \tfrac{1}{2}\,(p-1)^3\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(1^21^2)) &= \tfrac{1}{2}\,(p-1)^2\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(2^2)) &= \tfrac{1}{2}\,(p-1)^3\,p^4\,(p+1)\,\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p(1^31)) &= (p-1)^3\,p^3\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p^{(1)}(1^4)) &= (p-1)^3\,p^2\,(p+1)^2\,(p^2+p+1)\,/\,p^{12},\\
\mu(T_p^{(2)}(1^4)) &= (p-1)^2\,p^3\,(p+1)\,\,(p^2+p+1)\,/\,p^{12}.
\end{aligned}$$

Proof. Since the criteria for membership of (A,B) in a $T_p(\cdot)$ depend only on the residue class of (A,B) modulo p, it suffices to consider the situation over $\mathbb{F}_p$.

We examine first $\mu(T_p(1111))$. The number of unordered quadruples of points in $\mathbb{P}^2_{\mathbb{F}_p}$, no three of which are collinear, is

$$\frac{1}{24}(p^2+p+1)(p^2+p)(p^2)(p^2-2p+1).$$

Furthermore, given such a quadruple of points, there is a two-dimensional vector space of conics passing through those four points; that is, there are $(p^2-1)(p^2-p)$ ordered pairs (A,B) of ternary quadratic forms over $\mathbb{F}_p$ having those four points as common zeros. Since the total number of pairs of ternary quadratic forms over $\mathbb{F}_p$ is p^{12}, it follows that

$$\begin{aligned}
&\mu(T_p(1111))\\
&\qquad = \tfrac{1}{24}\left[(p^2+p+1)(p^2+p)(p^2)(p^2-2p+1)\right]\cdot\left[(p^2-1)(p^2-p)\right]/\,p^{12},
\end{aligned}$$

as given by the lemma.

Let us next consider $\mu(T_p(1^22))$. The number of unordered conjugate pairs of points P_1, P_2 in $\mathbb{P}^2_{\mathbb{F}_{p^2}} \setminus \mathbb{P}^2_{\mathbb{F}_p}$ is $\frac{1}{2}(p^4+p^2+1-p^2-p-1) = \frac{1}{2}(p^4-p)$. Furthermore, the number of points P_3 in $\mathbb{P}^2_{\mathbb{F}_p}$ not lying on the line through P_1 and P_2 is p^2, and the number of possible tangent lines ℓ through such a point P_3 is $p+1$. As before, given the data P_1, P_2, P_3, ℓ, there will be a two-dimensional vector space of conics that pass through P_1, P_2, P_3 and that are tangent to ℓ at P_3. Thus we obtain

$$\mu(T_p(1^22)) = \tfrac{1}{2}\left[(p^4-p)(p^2)(p+1)\right] \cdot \left[(p^2-1)(p^2-p)\right] / \, p^{12}$$

as in the lemma.

Let us consider next $T_p^{(1)}(1^4)$. Note that (A,B) is contained in $T_p^{(1)}(1^4)$ only if there is a linear combination C of A and B such that $C=0$ is a double line and, moreover, $A=0$ and $B=0$ are tangent to this double line at the same point P. The number of choices for this double line ℓ is p^2+p+1, and the number of choices for the point P on ℓ is then $p+1$. There is a four-dimensional vector space of conics passing through P and tangent to ℓ at P, and the number of two-dimensional subspaces that contain the element C is p^2+p+1. Of these p^2+p+1 two-dimensional spaces, $p+1$ correspond to pencils of reducible conics containing the common component ℓ, while an additional p consist solely of reducible conics passing through the point P with multiplicity two (hence instead giving elements of $T_p^{(2)}(1^4)$). The p^2-p two-dimensional spaces that remain are the ones that contribute to $T_p^{(1)}(1^4)$, and so we have

$$\mu(T_p^{(1)}(1^4)) = \left[(p^2+p+1)(p+1)(p^2-p)\right] \cdot \left[(p^2-1)(p^2-p)\right] / \, p^{12}$$

as in the lemma.

The other parts may be handled with essentially identical arguments. □

It can be seen by a direct calculation that a pair (A,B) has nonzero discriminant modulo p if and only if it is in $T_p(1111), T_p(112), T_p(13), T_p(22)$, or $T_p(4)$ (i.e., if and only if $A=0$ and $B=0$ intersect in four distinct points as conics over $\bar{\mathbb{F}}_p$). Note that these are the cases with positive asymptotic density as $p \to \infty$.

4.2. *Maximal quartic rings.* A quartic ring having nonzero discriminant is said to be *maximal* if it is not a subring of any other quartic ring. In this section, we determine necessary and sufficient conditions on $(A,B) \in V_{\mathbb{Z}}$ for $Q(A,B)$ to be a maximal quartic ring.

By the theory of algebraic numbers, a maximal ring R of nonzero discriminant is a direct sum of Dedekind domains. In particular, a prime p factorizes uniquely in Q as a product of prime ideals of Q. If $p = P_1^{e_1}P_2^{e_2}\cdots$ is the factorization of p into prime ideals of $Q(A,B)$, where $Q/P_i \cong \mathbb{F}_{p^{f_i}}$, we define the symbol (Q,p) by setting

$$(Q,p)=(f_1^{e_1}f_2^{e_2}\cdots). \tag{38}$$

Suppose now $(A,B)\in V_{\mathbb{Z}}$ is such that $Q(A,B)$ is maximal. If $(Q,p)=(f_1^{e_1}f_2^{e_2}\cdots)$, then clearly

$$Q(A,B)/(p)\cong\mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1})\oplus\mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2})\oplus\cdots, \tag{39}$$

so that by (36), $(A,B)\in T_p(f_1^{e_1}f_2^{e_2}\cdots)$. Therefore, if the ring $Q(A,B)$ is maximal for an element $(A,B)\in V_{\mathbb{Z}}$, then (A,B) is contained in one of the $T_p(\cdot)$'s as defined in the previous section (with the exception of $T_p^{(2)}(1^4)$), and we have

$$((A,B),p)=(Q(A,B),p). \tag{40}$$

Now a quartic ring Q is maximal if and only if for all primes p, the ring Q is maximal at p, i.e., $Q\otimes\mathbb{Z}_p$ is not contained in any other quartic $\mathbb{Z}_p$-algebra. Since a quartic ring Q with discriminant prime to p is necessarily maximal at p, $Q(A,B)$ is automatically maximal at p for any (A,B) in $T_p(1111), T_p(112), T_p(13), T_p(4)$, or $T_p(22)$.

In order to understand the other $T_p(\cdot)$'s with regard to maximality, we require the following lemma.

Lemma 22. *If Q is any quartic ring that is not maximal at p, then there exists a $\mathbb{Z}$-basis $1,\alpha_1,\alpha_2,\alpha_3$ of Q such that at least one of the following is true*:

(i) $\mathbb{Z}+\mathbb{Z}\cdot(\alpha_1/p)+\mathbb{Z}\cdot\alpha_2+\mathbb{Z}\cdot\alpha_3$ *forms a ring*;

(ii) $\mathbb{Z}+\mathbb{Z}\cdot(\alpha_1/p)+\mathbb{Z}\cdot(\alpha_2/p)+\mathbb{Z}\cdot\alpha_3$ *forms a ring*;

(iii) $\mathbb{Z}+\mathbb{Z}\cdot(\alpha_1/p)+\mathbb{Z}\cdot(\alpha_2/p)+\mathbb{Z}\cdot(\alpha_3/p)$ *forms a ring.*

Proof. Since Q is not maximal at p, there exists a quartic ring Q' containing Q such that p divides the index of Q in Q'. By the theory of elementary divisors, there exist positive integers n_1,n_2,n_3 and a basis $\langle\alpha_1,\alpha_2,\alpha_3\rangle$ of Q such that

$$Q'=\mathbb{Z}+\mathbb{Z}(\alpha_1/n_1)+\mathbb{Z}(\alpha_2/n_2)+\mathbb{Z}(\alpha_3/n_3) \tag{41}$$

and $n_3\mid n_2\mid n_1$. Note that $p\mid n_1$. If $n_1=p$, then we are done. Hence we assume that n_1/p is an integer greater than 1.

Let the multiplicative structure of Q with respect to the basis $\langle\alpha_1,\alpha_2,\alpha_3\rangle$ be given by (14). That the right side of (41) is a ring then translates into the following congruence conditions on the structure coefficients:

$$n_kc_{ij}^k\equiv 0 \pmod{n_in_j}, \tag{42}$$

for all $i,j,k\in\{1,2,3\}$.

Suppose $\ell \neq p$ is a prime dividing n_1. Then removal of all factors of ℓ in the prime factorizations of n_1, n_2, n_3 maintains the truth of the congruences (42), and the new Q' as defined by (41) remains a ring. Hence we may assume that $\ell \nmid n_1, n_2, n_3$ for all primes $\ell \neq p$.

Now, if $p \nmid n_2, n_3$ but $p^2 \mid n_1$, then it is easy to see that replacing (n_1, n_2, n_3) by $(n_1/p, n_2, n_3)$ maintains the truth of the congruences (42), so that Q' as defined by (41) is again a ring. Similarly, if $p \nmid n_3$, but $p^2 \mid n_2$, then we may replace (n_1, n_2, n_3) by $(n_1/p, n_2/p, n_3)$, and if $p^2 \mid n_3$, then we may replace (n_1, n_2, n_3) by $(n_1/p, n_2/p, n_3/p)$. Thus by a finite sequence of such moves we arrive at $n_1 = p$, the desired conclusion. □

For an $(A, B) \in V_{\mathbb{Z}}$, using the multiplication laws of $Q(A, B)$ as given in (14), (21), (22), and (23), we may translate the conditions itemized in Lemma 22 into the following conditions respectively on the λ-invariants of (A, B):

(i) $\lambda_{22}^{11}, \lambda_{23}^{11}, \lambda_{33}^{11}, \lambda_{13}^{12}$ are multiples of p, and $\lambda_{12}^{11}, \lambda_{13}^{11}$ are multiples of p^2,

(ii) $\lambda_{13}^{11}, \lambda_{23}^{11}, \lambda_{13}^{12}, \lambda_{23}^{12}, \lambda_{22}^{13}, \lambda_{23}^{22}$ are all multiples of p, and $\lambda_{12}^{11}, \lambda_{22}^{11}, \lambda_{22}^{12}$ are multiples of p^2,

(iii) all the $\lambda_{k\ell}^{ij}$'s are multiples of p.

Recall that condition (iii) is equivalent to A, B spanning a rank zero or one space over $\mathbb{F}_p$. In particular, an element (A, B) satisfying (iii) will not lie in any of the $T_p(\cdot)$'s.

Let us therefore assume that we are not in case (iii), so that A, B span a two-dimensional space of conics over $\mathbb{F}_p$. Then condition (i) occurs if and only if $a_{11} \equiv b_{11} \equiv 0 \pmod{p}$ and the vectors $(a_{11}/p, a_{12}, a_{13})$ and $(b_{11}/p, b_{12}, b_{13})$ are linearly dependent (mod p). By a transformation in $\mathrm{GL}_2(\mathbb{Z})$, we may then assume in sum that

$$a_{11} \equiv b_{12} \equiv b_{13} \equiv 0 \pmod{p}, \text{ and } b_{11} \equiv 0 \pmod{p^2}. \tag{43}$$

In particular, we see that $(1, 0, 0)$ is an intersection point of multiplicity at least two when A, B are viewed as two conics in $\mathbb{P}^2_{\bar{\mathbb{F}}_p}$. It follows that if such an element (A, B) is in a $T_p(\cdot)$, it must be in one of $T_p(1^2 11), T_p(1^2 2), T_p(1^2 1^2)$, $T_p(1^3 1)$, or $T_p(1^4)$.

Similarly, one observes that condition (ii) occurs if and only if at least one of the following two conditions holds:

(a) The top left 2×2 blocks of A and B are zero (mod p).

(b) After a $\mathrm{GL}_2(\mathbb{Z})$-transformation, the top left 2×2 block of B is zero (mod p^2), and $b_{13} \equiv b_{23} \equiv 0 \pmod{p}$.

Subcase (a) implies that $A=0$ and $B=0$ share a common component in $\mathbb{P}^2_{\mathbb{F}_p}$, and this situation will not arise for an (A,B) in a $T_p(\cdot)$. Subcase (b) implies that $B=0$ is a double line in $\mathbb{P}^2_{\mathbb{F}_p}$. If (A,B) is in a $T_p(\cdot)$, then it is clear that a double line will lie in the span of A and B (mod p) if and only if (A,B) is in $T_p(1^21^2)$, $T_p(2^2)$, or $T_p(1^4)$. (These are the so-called "over-ramified" cases; their significance will be discussed in more detail in [4].)

Thus, if we have an (A,B) in some $T_p(\cdot)$ such that $Q(A,B)$ is not maximal at p, then after a suitable transformation in $\mathrm{GL}_2(\mathbb{Z})\times\mathrm{SL}_3(\mathbb{Z})$, the element (A,B) will satisfy condition (i) (i.e., equation (43)) or condition (ii)(b). These observations suffice to determine which elements of the various $T_p(\cdot)$'s correspond to maximal quartic rings.

Let us use $U_p(\cdot)$ to denote the subset of elements $(A,B)\in T_p(\cdot)$ for which $Q(A,B)$ is maximal at p. To determine whether an element $(A,B)\in T_p(\cdot)$ is in $U_p(\cdot)$, we simply transform that element into one satisfying the conditions (i) or (ii)(b) above modulo p—and then check whether it satisfies the necessary conditions modulo p^2.

For example, if (A,B) is an element of $T_p(1^211)$, $T_p(1^22)$, or $T_p(1^31)$, then it can be brought into the form

$$a_{11}\equiv b_{12}\equiv b_{13}\equiv 0 \pmod p, \text{ and } b_{11}\equiv 0 \pmod p$$

by sending the unique multiple point of intersection of $A=0$ and $B=0$ in $\mathbb{P}^2_{\mathbb{F}_p}$ to the point $(1,0,0)\in\mathbb{P}^2_{\mathbb{F}_p}$ via a transformation in $\mathrm{SL}_3(\mathbb{Z})$. One may then use a $\mathrm{GL}_2(\mathbb{Z})$ transformation to insure that, modulo p, the conic $B=0$ is a product of two lines each of which passes through $(1,0,0)$. Of all $(A,B)\in T_p(1^211)$, $T_p(1^22)$, or $T_p(1^31)$ rendered in such a form, a proportion of $1/p$ actually satisfies (43). Since we have observed that such an (A,B) cannot satisfy condition (ii), we have $\mu(U_p(1^211))=\frac{p-1}{p}\mu(T_p(1^211))$, $\mu(U_p(1^22))=\frac{p-1}{p}\mu(T_p(1^22))$, and $\mu(U_p(1^31))=\frac{p-1}{p}\mu(T_p(1^31))$.

Similarly, if $(A,B)\in T_p(2^2)$, then (A,B) cannot satisfy condition (i), since there is no rational intersection point of $A=0$ and $B=0$ in $\mathbb{P}^2_{\mathbb{F}_p}$ of multiplicity at least two. However, the $\mathrm{GL}_2(\mathbb{Z})$-span of A and B will contain a double line, so that by applying a transformation in $\mathrm{GL}_3(\mathbb{Z})\times\mathrm{GL}_2(\mathbb{Z})$, we may assume that (A,B) satisfies

$$b_{11}\equiv b_{12}\equiv b_{13}\equiv b_{22}\equiv b_{23}\equiv 0 \pmod p. \tag{44}$$

Now such an (A,B) can be $GL_2(\mathbb{Z})$-transformed to satisfy condition (ii)(b) if and only if the vectors (a_{11},a_{12},a_{22}) and $(b_{11}/p,b_{12}/p,b_{22}/p)$ are linearly dependent (mod p). The first vector (a_{11},a_{12},a_{22}) will be nonzero, for otherwise $A=0$ and $B=0$ would contain a common component modulo p. Therefore, the probability that $(b_{11}/p,b_{12}/p,b_{22}/p)$ is a multiple of (a_{11},a_{12},a_{22}) modulo p is $p/p^3=1/p^2$. It follows that $\mu(U_p(2^2))=\frac{p^2-1}{p^2}\mu(T_p(2^2))$.

An element (A, B) in any one of the remaining cases—namely, $T_p(1^21^2)$ or $T_p(1^4)$—can be transformed to satisfy condition (i) or condition (ii)(b) modulo p. In fact, one can transform such an (A, B) so that it satisfies both conditions modulo p simultaneously. There will be a $\mathrm{GL}_2(\mathbb{Z})$-transformation that makes $B = 0$ a double line in $\mathbb{P}^2_{\mathbb{F}_p}$, and one can then use a $\mathrm{GL}_3(\mathbb{Z})$-transformation to move this line to $(*, *, 0) \subset \mathbb{P}^2_{\mathbb{F}_p}$ and also to move one of the multiple intersection points of $A = 0$ and $B = 0$ in $\mathbb{P}^2_{\mathbb{F}_p}$ to $(1, 0, 0)$. After such transformations, condition (i) evidently subsumes condition (ii)(b), so that we need not consider (ii)(b). Therefore, just as with the cases (1^211), (1^22), and (1^31), we have $\mu(U_p(1^4)) = \frac{p-1}{p}\mu(T_p^{(1)}(1^4))$. As for $T_p(1^21^2)$, since there are not one but two rational double intersection points in $\mathbb{P}^2_{\mathbb{F}_p}$ for an element $(A, B) \in T_p(1^21^2)$, and since each of these two intersection points must satisfy the same maximality condition, we conclude that $\mu(U_p(1^21^2)) = \left(\frac{p-1}{p}\right)^2\mu(T_p(1^21^2))$.

Finally, we have already remarked that $T_p(\cdot) = U_p(\cdot)$ in the case of the splitting types (1111), (112), (13), (22), and (4). We have therefore proven the following:

Lemma 23.

$$\begin{aligned}
\mu(U_p(1111)) &= \tfrac{1}{24}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(112)) &= \tfrac{1}{4}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(13)) &= \tfrac{1}{3}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(22)) &= \tfrac{1}{8}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(4)) &= \tfrac{1}{4}\,(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(1^211)) &= \tfrac{1}{2}\,(p-1)^4\,p^3\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(1^22)) &= \tfrac{1}{2}\,(p-1)^4\,p^3\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(1^21^2)) &= \tfrac{1}{2}\,(p-1)^4\,p^2\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(2^2)) &= \tfrac{1}{2}\,(p-1)^4\,p^2\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(1^31)) &= (p-1)^4\,p^2\,(p+1)^2\,(p^2+p+1)/\,p^{12},\\
\mu(U_p(1^4)) &= (p-1)^4\,p\,\ (p+1)^2\,(p^2+p+1)/\,p^{12}.
\end{aligned}$$

Let $\mathcal{U}_p$ denote the union of the eleven $U_p(\cdot)$'s in $V_{\mathbb{Z}}$, as described above. Then Lemma 23 implies that

$$\mu(\mathcal{U}_p) = (p-1)^4\,p\,(p+1)^2\,(p^2+p+1)(p^3+p^2+2p+1)/\,p^{12}. \tag{45}$$

Regarding maximality, we have shown:

Theorem 24. *Let $(A, B) \in V_{\mathbb{Z}}$. Then $Q(A, B)$ is a maximal ring if and only if $(A, B) \in \mathcal{U}_p$ for all primes p. The p-adic density of $\mathcal{U}_p$ in $V_{\mathbb{Z}}$ is given by* (45).

The preceding density results will play an important role in obtaining the density of discriminants of quartic rings and fields (see [4]).

Acknowledgments. This article is based on Chapter 4 of the author's Ph.D. thesis [1] at Princeton University. I am extremely grateful to my advisor Professor A. Wiles and to Professor P. Sarnak for all their enthusiasm, encouragement, and guidance during this work. I am also very thankful to Professors P. Deligne, B. Gross, H. W. Lenstra, J-P. Serre, and especially D. Zagier for their kind correspondence and numerous helpful comments on earlier versions of this manuscript.

I extend my gratitude to the Hertz Foundation for funding this work, and to the Clay Mathematics Institute for their subsequent support.

Clay Mathematics Institute, Cambridge, MA
Princeton University, Princeton, NJ
E-mail address: bhargava@math.princeton.edu

References

[1] M. Bhargava, *Higher Composition Laws*, Ph.D. thesis, Princeton University, June 2001.

[2] ———, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Ann. of Math.* **159** (2004), no. 1, 217–250.

[3] ———, Higher composition laws II: On cubic analogues of Gauss composition, *Ann. of Math.* **159** (2004), no. 2, 865–886.

[4] ———, The density of discriminants of quartic rings and fields, *Ann. of Math.*, to appear.

[5] ———, Higher composition laws IV: The parametrization of quintic rings, *Ann. of Math.*, to appear.

[6] ———, Gauss composition and generalizations, *Lecture Notes in Computer Science* **2369**, June 2002, 1–8.

[7] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), 405–420.

[8] B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, *Translations of Mathematical Monographs* **10**, A.M.S., Providence, RI, 1964.

[9] P. G. L. Dirichlet, *Zahlentheorie*, 4th. edition, Vieweg Brunswick, 1894.

[10] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115** (2002), 105–169.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[12] O. Khayyam, *Maqalat fi al-Jabr wa al-Muqabila*, 1079.

[13] J. Nakagawa, On the relations among the class numbers of binary cubic forms, *Invent. Math.* **134** (1998), 101–138.

[14] M. Sato and T. Kimura, A classification of irreducible prehomogeneous vector spaces and their relative invariants, *Nagoya Math. J.* **65** (1977), 1–155.

[15] D. J. Wright and A. Yukie, Prehomogeneous vector spaces and field extensions, *Invent. Math.* **110** (1992), 283–314.

(Received February 29, 2004)