Quintic rings over Dedekind domains and their sextic resolvents

Evan M. O’Dorney

Abstract

Bhargava parametrized quintic rings over \( \mathbb{Z} \) by quadruples of \( 5 \times 5 \) alternating matrices. We extend the construction to work similarly over any Dedekind domain \( R \). No assumptions are needed on the characteristic of \( R \). The resolvent consists of a pair of locally free modules \( L, M \) with two multilinear maps between them; we can view \( L \) as \( Q/R \), for \( Q \) the quintic ring, and \( M \) as \( S/R \), where \( S \) is a sextic resolvent ring. As in Bhargava’s treatment, any quintic ring has a resolvent ring, and for a maximal ring, the resolvent is unique. We hope that this work will enable the removal of the condition that the characteristic be different from 2 in Bhargava-Shankar-Wang’s proof of Linnik’s conjecture on the asymptotic distribution of discriminants of relative extensions.

Keywords: Quintic ring, Dedekind domain, Resolvent, Higher composition laws

Mathematics Subject Classification: 13F05, 13B02 (Primary), 11E76, 11R21 (Secondary)

1 Introduction

Since their publication in the 2000’s [1–3,5], there has been continual interest in Bhargava’s higher composition laws, that is, parametrizations of number rings and related objects by \( n \)-ary \( d \)-ic forms and similarly explicit objects. Early examples of this, like the Levi–Delone–Gross parametrization of cubic rings by their index forms [8,11,12], now fit into a larger paradigm that include the 14 higher composition laws appearing in Bhargava’s initial series as well as numerous additional examples, such as Wood’s parametrization of 2-torsion in rings parameterized by an odd-degree binary form by \( 2 \times n \times n \) matrices [19]. These higher composition laws have been found very useful, especially in applying the geometry-of-numbers method in arithmetic statistics [4,6].

Although Bhargava’s paper series worked out only the case where the base ring is \( \mathbb{Z} \), it has immediately been clear that his methods work over more general bases. Wood worked out two parametrizations over a general base scheme: the case of Gauss composition of binary quadratic forms, which gave higher composition laws their name [17], and the parametrization of quartic rings, or shall we say fourfold covers [18].

A more modest degree of generalization, in which still a great degree of concreteness can be achieved, is that when the base \( R \) is a Dedekind domain. This includes the case \( R = O_K \)
of the ring of integers of a number field, allowing one to study relative extensions, which have long been of interest in arithmetic statistics [9, 10]. The Dedekind case also includes \( R \) that are fields, DVR’s, or coordinate rings of affine curves, which arise in assorted contexts. Special note must be given to the work of Bhargava, Shankar, and Wang [7], which gives the asymptotic number of relative extensions of degree up to 5 over a global field not of characteristic 2, proving what is commonly called Linnik’s conjecture in those cases. The present work suggests that the last hypothesis can be removed.

In [15], the author adapted Bhargava’s work to parametrize quadratic, cubic, and quartic rings over a Dedekind domain. Among the remaining cases, the parametrization of quintic rings stands out as the most involved of Bhargava’s higher composition laws, and one of great interest:

**Theorem 1.1** (Bhargava [5], Theorems 1 and 2 and Corollary 3) There is a suitable notion of resolvent for quintic rings over \( \mathbb{Z} \) with the following properties:

(a) There is a canonical bijection between the orbits of \( \Gamma = \text{GL}_4(\mathbb{Z}) \times \text{SL}_5(\mathbb{Z}) \) on the space \( \mathbb{Z}^4 \otimes \Lambda^2 \mathbb{Z}^5 \) of quadruples of \( 5 \times 5 \) alternating matrices and the set of isomorphism classes of pairs \((Q, S)\), where \( Q \) is a quintic ring and \( S \) is a sextic resolvent ring of \( Q \).

(b) Every quintic ring \( Q \) has a resolvent, that is, appears in this bijection for some element \( A \in \mathbb{Z}^4 \otimes \Lambda^2 \mathbb{Z}^5 \).

(c) If \( Q \) is a maximal ring, then the resolvent is unique up to isomorphism, and the element \( A \) is unique up to \( \Gamma \)-equivalence.

In this paper, we prove a generalization of these results to the case where the base ring \( \mathbb{Z} \) is replaced by a Dedekind domain. Certain modifications in the method of Bhargava [5] must be made to address the ideal class group of \( R \) and the fact that \( R \) may have characteristic two. Recall that finitely generated, locally free modules \( M \) over a Dedekind domain are characterized by two invariants: the dimension \( n = \dim_K(M \otimes K) \) (where \( K = \text{Frac} R \)) and the Steinitz class, that is, the ideal class \( a \) for which \( \Lambda^n M \cong a \) as \( R \)-modules. The main theorem is notably unchanged in spirit:

**Theorem 1.2** There is a suitable notion of resolvent for quintic rings over a Dedekind domain \( R \) with the following properties:

(a) Let \( a \in \text{Cl}(R) \). Let \( L_a = R^{\oplus 3} \oplus a \) be the lattice over \( R \) of dimension 4 and Steinitz class \( a \). Let \( M_a = R^{\oplus 4} \oplus a^3 \) be the lattice over \( R \) of dimension 5 and Steinitz class \( a^3 \). There is a canonical bijection between:

- the orbits of \( \Gamma_a = \text{GL}(L_a) \times \text{GL}(M_a) \) on the space \( a \otimes L_a \otimes (\Lambda^2 M_a)^a \), whose elements can be viewed as quadruples of \( 5 \times 5 \) alternating matrices whose entries lie in certain powers of \( a \) and
- the isomorphism classes of pairs \( (Q, S) \), where \( Q \) is a quintic ring and \( S \) is a sextic resolvent ring of \( Q \).

(b) Every quintic ring \( Q \) has a resolvent, that is, appears in this bijection for some element \( A \in \mathbb{Z}^4 \otimes \Lambda^2 \mathbb{Z}^5 \).

(c) If \( Q \) is a maximal ring, then the resolvent is unique up to isomorphism, and the element \( A \) is thus unique up to \( \Gamma \)-equivalence.
The remainder of the paper is structured as follows. In Sect. 2, we define a suitable notion of resolvent. In Sects. 3 and 4, we prove Theorem 1.2 by making the passage from resolvents to rings and from rings to resolvents, respectively. In Sect. 5 we touch on the ring structure on the sextic resolvent, which is noticeably absent from our definition. We close with a bound on the number of resolvents of a ring (Sect. 6) and with some examples (Sect. 7).

## 2 Defining resolvents

Let $Q$ be a quintic ring over a Dedekind domain $R$, and let $L = Q/R$. Our first task is to generalize the notion of a sextic resolvent, developed by Bhargava in [5] in the case $R = \mathbb{Z}$.

Following the approach of Wood [18] and the author [15], we expect the resolvent to consist of a rank-5 lattice $M$ (originating as $S/R$, where $S$ is a sextic ring) with two elements of some modules derived by multilinear constructions from $L$ and $M$. The orientation map $\theta$, which relates the top exterior powers of $L$ and $M$, is easy to guess. The discriminant of an $R$-algebra $T$ naturally lies in $(\Lambda^\top(T))^{\otimes -2}$. Just as the equality $\text{Disc } Q = \text{Disc } C$ between the discriminants of a quartic ring and its cubic resolvent(s) suggests an identification of the top exterior powers of the two rings, so the relation $\text{Disc } S = (16 \text{Disc } Q)^3$ (Bhargava’s (33) of [5]) linking the discriminants of a quintic ring and its sextic resolvent(s) suggests an isomorphism

$$\theta : \Lambda^5 M \rightarrow (\Lambda^4 L)^{\otimes 3}.$$  

The second piece of data, that which contains the 40 integers that actually parametrize resolvents over $\mathbb{Z}$, is slightly trickier to adapt. Bhargava presents it as a map $\phi$ from $L$ to $\Lambda^2 M$ (equivalently, from $\Lambda^2 M^\ast$ to $L^\ast$), but this does not have the correct properties in our situation. The correct construction, foreshadowed somewhat by the mysterious constant factor in Bhargava’s fundamental resolvent ([(28) in [5]), is to take a map

$$\phi : \Lambda^4 L \otimes L \rightarrow \Lambda^2 M.$$  

Finally, we must find the fundamental relations that link $\phi$ and $\theta$ to the ring structure. Just as Lemma 9 of [3] provided the inspiration for Bhargava’s coordinate-free description of resolvents of a quartic ring ([3], section 3.9), so we begin at Lemma 4(a), which, after eliminating the references to $S_5$-closure, states that

$$\frac{1}{2} \cdot \omega \cdot \left( \begin{array}{c} \text{Pfaff} \left[ \begin{array}{cc} \phi(y) & \phi(x) \\ \phi(x) & \phi(z) \end{array} \right] - \text{Pfaff} \left[ \begin{array}{cc} \phi(y) & \phi(x) \\ \phi(x) & -\phi(z) \end{array} \right] \end{array} \right) = 1 \wedge y \wedge x \wedge z \wedge yz$$  

for a certain generator $\omega$. The Pfaffians are to be interpreted by writing $\phi(x)$, etc., as a $5 \times 5$ alternating matrix with regard to any convenient basis (i.e. viewing it as an alternating bilinear form on $\Lambda^2 M$, once a generator of $\Lambda^4 L$ is fixed). Then we paste together four of these to make a $10 \times 10$ alternating matrix and take the Pfaffian. This is a clever way to manufacture certain degree-5 integer polynomials in the 40 coefficients of $\phi$. To re-express them in a way that is coordinate-free and applicable in characteristic 2, we consider two preliminary multilinear constructions.

### 2.1 The quadratic map

Let $V$ be a 5-dimensional vector space over a field $K$ (which we will soon take to be Frac $R$). We examine the constructions that can be made starting with elements of $\Lambda^2 V$. We have a bilinear map $\wedge : \Lambda^2 V \times \Lambda^2 V \rightarrow \Lambda^4 V$. However, the most fundamental map from $\Lambda^2 V$
to $\Lambda^4 V$ is not the bilinear map $\wedge$ but the quadratic map from which it arises. It is defined by
\[
\left( \sum_{i=1}^{n} v_i \wedge w_i \right) \square = \sum_{1 \leq i < j \leq n} v_i \wedge w_i \wedge v_j \wedge w_j.
\]
(1)

It is not hard to prove that this is well defined. Note that if $\text{char } K \neq 2$, then $\square$ can be described more simply by
\[
\mu \square = \frac{1}{2} \mu \wedge \mu;
\]
if $\text{char } K = 2$, then $\mu \wedge \mu = 0$ yet $\square$ is nonzero. Moreover, the bilinear map $\wedge$ can always be recovered from $\square$ via
\[
\mu \wedge v = (\mu + v)^\square - \mu^\square - v^\square.
\]
(2)

2.2 The contraction $ev$

The second construction takes one element $\mu \in \Lambda^2 V$ and two elements $\alpha, \beta \in \Lambda^4 V$ and outputs an element of a suitable one-dimensional vector space as follows. First, the perfect pairing

$\wedge : \Lambda^4 V \times V \to \Lambda^5 V$

allows us to identify $\alpha$ and $\beta$ as elements of $\Lambda^5 V \otimes V^*$. These have a wedge product

$\alpha \wedge \beta \in \Lambda^2(\Lambda^5 V \otimes V^*) \cong (\Lambda^5 V)^{\otimes 2} \otimes \Lambda^2 V^*$.

We now use the duality between $\Lambda^2 V^*$ and $\Lambda^2 V$, described explicitly by

$$(f \wedge g)(v \wedge w) = fu \cdot gw - fw \cdot gv,$$

to obtain an element

$ev(\mu; \alpha, \beta) \in (\Lambda^5 V)^{\otimes 2}$.

The contraction $ev$ is linear in each of its three arguments, and alternating in the last two.

2.3 The definition

We are now ready to state the definition of a sextic resolvent.

**Definition 2.1** Let $Q$ be a quintic ring over a Dedekind domain $R$, and let $L = Q/R$. A resolvent for $Q$ consists of a rank-5 lattice $M$ and a pair of linear maps

$\phi : \Lambda^4 L \otimes L \to \Lambda^2 M$ and $\theta : \Lambda^5 M \to (\Lambda^4 L)^{\otimes 3}$,

with $\theta$ an isomorphism, satisfying the identity

$\theta^{\otimes 2}[ev(\phi(\lambda_1 x); \phi(\lambda_2 y)^\square, \phi(\lambda_3 z)^\square)] = \lambda_1 \lambda_2 \lambda_3 (x \wedge y \wedge z \wedge yz)$

(3)

where $x, y, z \in L$ and $\lambda_i \in \Lambda^4 L$ are formal variables.

Note that the expression within square brackets lies in $(\Lambda^5 M)^{\otimes 2}$; applying $\theta^{\otimes 2}$, one ends up in $(\Lambda^4 L)^{\otimes 6}$ which is where the right-hand side also resides. It should also be remarked that the product $yz$ is the unique appearance of the ring structure of $Q$; translating the lifts $\tilde{y}, \tilde{z}$ by constants in $R$ simply changes the product $\tilde{y}\tilde{z}$ by multiples of $\tilde{y}, \tilde{z}$, and 1, thereby not changing the product $y \wedge z \wedge yz$. 
3 Resolvent to ring

Our first task is to show that the resolvent maps $\phi$ and $\theta$ uniquely encode the multiplication data of the ring $Q$.

Lemma 3.1 Let $L$ and $M$ be lattices over $R$ of ranks 4 and 5 respectively, and let $\phi : \Lambda^4 L \otimes L \rightarrow \Lambda^3 M$ and $\theta : \Lambda^5 M \rightarrow (\Lambda^4 L)^{\otimes 3}$ be maps. There is a quintic ring $Q$ with a quotient map $Q/R \cong L$, unique up to isomorphism, such that $(M, \phi, \theta)$ is a resolvent of $Q$.

Proof Let $(e_1, e_2, e_3, e_4)$ be a basis for $L$, by which we mean that there is a decomposition $L = a_1 e_1 \oplus \cdots \oplus a_4 e_4$ for some fractional ideals $a_i$ of $R$. (Because the Steinitz class is $a = \prod a_i$, we could take $a_1 = a_2 = a_3 = (1)$ and $a_4 = a$; but we refrain from this choice for the sake of symmetry.) To place a ring structure on the module $Q = L \oplus R$, it is then necessary to choose the coefficients $c_{ij}^k \in a_i a_i^{-1} a_j^{-1}$ such that

$$e_i e_j = \sum_k c_{ij}^k e_k,$$

with the conventions $e_0 = 1$ and $a_0 = 1$. Note that the $c_{ij}^k$ with $i = 0$ or $j = 0$ are already known. Hence the ring structure is given by the 50 coefficients $c_{ij}^k$, $1 \leq i \leq j \leq 4$, $0 \leq k \leq 4$.

Some of these coefficients are immediately determined by the resolvent. For instance, if $\{i, j, k, \ell\}$ is a permutation of $\{1, 2, 3, 4\}$, and $\epsilon = \pm 1$ its sign, then we know

$$c_{ij}^k = -\epsilon c_{\ell\top}^{\epsilon \omega} \cdot e_i \wedge e_j \wedge e_\ell \wedge e_\ell = -\epsilon \omega \cdot \theta^{\otimes 2} \cdot [\text{ev}(\phi(e_i e_\ell); \phi(e_j e_\ell)^{\square})],$$

where $e_\ell = e_1 \wedge e_2 \wedge e_3 \wedge e_4 = \epsilon \cdot e_i \wedge e_j \wedge e_k \wedge e_\ell$ is the generator of $\Lambda^4 L$ induced by the chosen basis and

$$\omega = \theta^* (e_\ell^{\epsilon \omega}) \in (\Lambda^5 M)^{\otimes 2}.$$

This determines the values of all $c_{ij}^k$ where $i, j,$ and $k$ are nonzero and distinct.

Likewise, the following expressions are determined, for $i, j, k, \ell$ distinct:

$$c_{ij}^k = \epsilon c_{\ell\top}^{\epsilon \omega} \cdot e_i \wedge e_j \wedge (e_i + e_k) \wedge e_\ell (e_j + e_\ell) - c_{ij}^k,$$

$$c_{ik}^j - c_{ij}^k = \epsilon c_{\ell\top}^{\epsilon \omega} \cdot e_i \wedge e_k \wedge (e_i + e_k) \wedge e_\ell (e_j + e_\ell) - c_{ik}^j + c_{ij}^k,$$

$$c_{ji}^k - c_{ij}^k = \epsilon c_{\ell\top}^{\epsilon \omega} \cdot e_j \wedge e_i \wedge (e_i + e_j) \wedge (e_i + e_j) (e_i + e_k) - c_{jk}^i + c_{ij}^k + c_{i\ell}^k + c_{i\ell}^j,$$

(5)

The reader familiar with ring parametrizations will recognize the left-hand sides of (4) and (5) as the linear expressions in the $c_{ij}^k$ that are invariant under translations $e_i \mapsto e_i + t_i$ ($t_i \in a_i^{-1}$) of the ring basis elements (see [5, (21)]). If we normalize our basis so that, say, $c_{12}^1 = c_{12}^2 = c_{34}^3 = c_{34}^4 = 0$, then all the $c_{ij}^k$ are now uniquely determined, except for the $c_{ij}^0$. The $c_{ij}^0$ can be computed by comparing the coefficients of $k$ in $(e_i e_j) e_k$ and $e_i (e_j e_k)$ for any $k \neq i$, yielding formula (22) of [5]:

$$c_{ij}^0 = \sum_{r=1}^4 (c_{rk}^0 c_{ri}^0 - c_{rj}^0 c_{rk}^0).$$

The lemma is now reduced to three verifications.

1. That all $c_{ij}^0$ belong to the correct ideals $a_k a_i^{-1} a_j^{-1}$. This is routine.
2. That the \( c^0_{ij} \) are well defined, and more generally that the associative law holds on the ring \( Q = \sum a_i e_i \) that we have just constructed. This is a collection of integer polynomial identities in the 40 free coefficients of \( \phi \) in the chosen basis; as such, it was proved in the course of Bhargava’s parametrization of quintic rings over \( \mathbb{Z} \).

3. That the original maps \( \phi \) and \( \theta \) indeed form a resolvent of \( Q \), i.e. that the identity (3) holds. Since (3) does not directly generalize any result of Bhargava, we here give the outline of a proof. We can assume that \( \lambda_1 = \lambda_2 = \lambda_3 = e_{top} \) and \( x \) is a basis element \( e_i \), since the equation (3) is linear in those variables. We can also assume that each of \( y \) and \( z \) is a basis element or a sum of two different basis elements, since (3) is quadratic in those variables. Now we have a finite set of cases, some of which are the relations (4) and (5). The others will be reduced to them using the following properties of the underlying multilinear operations: 

\[ \square \]

**Lemma 3.2** Let \( V \) be a 5-dimensional vector space, and let \( \mu, \nu, \xi \in \Lambda^2 V \) and \( \alpha \in \Lambda^4 V \). Then

(a) \( \text{ev}(\mu; \mu \wedge \nu, \alpha) = -\text{ev}(\nu; \mu, \alpha) \)

(b) \( \text{ev}(\mu; \mu, \alpha) = 0 \)

(c) \( \text{ev}(\nu; \mu, \mu \wedge \nu) = -\text{ev}(\xi; \mu, \mu \wedge \nu) \).

**Proof** For (a), set \( \mu = u \wedge v + w \wedge x \) and \( v = y \wedge z \) (both sides being linear in \( v \)) and expand. The difference of the two sides is found to be alternating in \( u, v, w, x, y, z \), hence zero, since \( \Lambda^6 V = 0 \). Then (b) follows by setting \( \mu = v \), and (c) by the derivation

\[ \text{ev}(\nu; \mu, \mu \wedge \nu) = -\text{ev}(\nu; \mu \wedge \nu, \mu) = \text{ev}(\nu; \mu \wedge \nu, \mu \wedge \xi) = -\text{ev}(\xi; \mu, \mu \wedge \nu) = -\text{ev}(\xi; \mu, \mu \wedge \nu). \]

\[ \square \]

Now we return to proving

\[ \phi^{\otimes 2} \left[ \text{ev} \left( \phi(e_{top}x); \phi(e_{top}y) \square, \phi(e_{top}z) \square \right) \right] = e_{top}^5(x \wedge y \wedge z \wedge yz) \]  

(6)

for \( x = e_\ell \) and \( y, z \in \{e_i\}_{i \neq \ell} \cup \{e_\ell + e_j\}_{i \neq \ell} \). The cases where \( e_\ell \) does not appear in \( y \) or \( z \) are all subsumed by the definitions (4) and (5), with one exception: the expression for \( c^5_{ii} \) is not visibly symmetric under switching \( k \) and \( \ell \). This can be seen by writing

\[
\begin{align*}
c^5_{ii} &= e_{top}^{-1}(e_\ell \wedge e_\ell \wedge (e_\ell + e_k) \wedge (e_\ell + e_k) - e_\ell \wedge e_\ell \wedge e_\ell \wedge e_\ell) \\
&= e_{top}^{-5} \left( \text{ev}(\phi(e_\ell); \phi(e_\ell) \square, \phi(e_\ell + e_k) \square) - \text{ev}(\phi(e_\ell); \phi(e_\ell) \square, \phi(e_k) \square) \right) \\
&= e_{top}^{-5} \left( \text{ev}(\phi(e_\ell); \phi(e_\ell) \square, \phi(e_\ell) \square) + \phi(e_\ell) \wedge \phi(e_k) + \phi(e_k) \wedge \phi(e_\ell) \\
&- \text{ev}(\phi(e_\ell); \phi(e_\ell) \square, \phi(e_\ell) \square) \right) \\
&= e_{top}^{-5} \left( \text{ev}(\phi(e_\ell; \phi(e_\ell) \square, \phi(e_\ell) \wedge \phi(e_k)) \right)
\end{align*}
\]

and using Lemma 3.2(c). It remains to dispose of the cases where \( e_\ell \) does appear in \( y \) or \( z \). We prove them by induction on the total number of \( e \) terms in \( x, y, \) and \( z \), the base cases being those already shown. Suppose that \( x = e_\ell \) appears in \( x + y = e_\ell + e_k \) (the case where \( x \) appears in \( z \) is symmetric). For brevity let \( \lambda = \phi(e_{top}x), \mu = \phi(e_{top}y), v = \phi(e_{top}z) \). Then
\[ \vartheta^\otimes 2 \left[ \text{ev} \left( \phi(e_{\text{top}} x); \phi(e_{\text{top}} (x + y)); \phi(e_{\text{top}} z) \right) \right] \]
\[ = \vartheta^\otimes 2 \left[ \text{ev} \left( \lambda; (\lambda + \mu)^\square, v^\square \right) \right] \]
\[ = \vartheta^\otimes 2 \left[ \text{ev} \left( \lambda; \lambda^\square + \lambda \wedge \mu + \mu^\square, v^\square \right) \right] \]
\[ = \vartheta^\otimes 2 \left[ -\text{ev} \left( \mu; \lambda^\square, v^\square \right) + \text{ev} \left( \lambda; \mu^\square, v^\square \right) \right] \]
\[ = \epsilon_{\text{top}}^5 (y \wedge x \wedge z \wedge xz + x \wedge y \wedge z \wedge yz) \]
\[ = \epsilon_{\text{top}}^5 (x \wedge (x + y) \wedge z \wedge (x + y)z), \]
where the induction hypothesis applies since \((x, y, z)\) and \((y, x, z)\) both have fewer total \(e\) terms than \((x, x + y, z)\).

\[ \square \]

### 3.1 Omission of \(\vartheta\)

With our definition, it is natural to wonder what happens when the datum \(\vartheta\) is changed. The answer is simple:

**Proposition 3.3** If \(\vartheta\) is scaled by a unit \(\gamma \in \mathbb{R}^\times\), the corresponding quintic ring is unchanged, up to isomorphism.

**Proof** More strongly, the resolvent itself is unchanged up to isomorphism. Observe that the scalar multiplications \(\gamma^2 : L \rightarrow L\) and \(\gamma^5 : M \rightarrow M\) take one resolvent to the other, thanks to the commutative diagram:

\[ \Lambda^4 L \otimes L \xrightarrow{\phi} \Lambda^2 M \quad \Lambda^5 M \xrightarrow{\gamma^5 \otimes 1} (\Lambda^4 L)^{\otimes 3} \]
\[ (\Lambda^4(y^2))^\otimes \approx \gamma^{10} \] (7)
\[ \Lambda^4(y^2)^\otimes \approx \gamma^{10} \]
\[ \Lambda^4 M \otimes L \xrightarrow{\phi} \Lambda^2 M \quad \Lambda^5 M \xrightarrow{\theta} (\Lambda^4 L)^{\otimes 3} \]
\[ \Lambda^5(y^5)^\otimes \approx \gamma^{25} \] (\Lambda^4(y^2))^\otimes \approx \gamma^{24} \]

\[ \square \]

In spite of this, we retain the datum \(\vartheta\) in our definition of resolvent, as it makes all the resolvent conditions polynomial relations, without an existential quantifier, and eases base change.

**Proof of Theorem 1.2(a):** Let \((L, M, \phi, \theta)\) be a resolvent of Steinitz class \(a\). The modules \(L \cong L_a\) and \(M \cong M_a\) are known up to isomorphism. If isomorphisms are chosen, then \(\phi \in (\Lambda^4 L \otimes L)^{\otimes 2} \Lambda^2 M \cong \alpha^{-1} \otimes L_a \otimes \Lambda^2 M_a\) is realized as an element of the desired lattice, unique up to \(\text{GL}(L) \times \text{GL}(M)\). Conversely, if such a \(\phi\) is given, then due to the redundancy of \(\theta\), we get a resolvent unique up to isomorphism.

\[ \square \]

### 3.2 Compatibility with Bhargava’s definitions

If \(a = (1)\), that is, \(L\) and \(M\) are free over \(R\), the resolvent devolves into the basis representation of \(\phi\). This has 40 independent entries which can be arranged into a quadruple of 5 \(\times\) 5 alternating matrices, representing the values \(\phi(x)\) (as \(x\) runs through a basis of \(L\)) as alternating bilinear forms on \(M^\ast\). The coefficients \(c^L_{ij}\) of the ring we have constructed are certain degree-5 polynomials in these 40 entries which are easily identified with the formulas given in (21) of [5]. Thus our definition of resolvent is compatible with Bhargava’s (Definition 10), which justifies our invocation of his computations in our situation, despite the dissimilarities of the definitions.
4 Constructing resolvents

We now wish to go the other way and prove Theorem 1.2(b): every quintic ring over a Dedekind domain admits at least one resolvent. We begin with the case where $R = K$ is a field.

In the quartic case [3,15], it was the trivial ring $T = K[x,y,z]/(x,y,z)^2$ that had the largest family, all other rings having a unique resolvent. Likewise, here we separate out some of the most degenerate rings, those of the last three types $A_{18}, A_{19}, A_{20}$ in the classification of Mazzola [13, p.292]:

**Definition 4.1** A quintic algebra $Q$ over $K$ is very degenerate if it has subspaces $Q_4 \subseteq Q_3$, of dimension 4 and 3 respectively, such that $Q_4 Q_3 = 0$ (that is, the product of any element of $Q_4$ and any element of $Q_3$ is zero). A quintic algebra $Q$ over $R$ is very degenerate if the corresponding $K$-algebra $Q \otimes_R K$ is.

Let $Q$ be a very degenerate quintic ring over $R$. Upon taking a suitable basis, the multiplication table of $Q$ has the form

|   | $1$ | $\xi_1$ | $\xi_2$ | $\xi_3$ | $\xi_4$ |
|---|-----|-----|-----|-----|-----|
| $1$ | $1$ | $\xi_1$ | $\xi_2$ | $\xi_3$ | $\xi_4$ |
| $\xi_1$ | $\xi_1$ | $c_{11}^1 \xi_1 + c_{12}^1 \xi_2$ | $0$ | $0$ | $0$ |
| $\xi_2$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $\xi_3$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $\xi_4$ | $0$ | $0$ | $0$ | $0$ | $0$ |

(8)

in which at most two of the structure constants $c_{ij}^k$ are nonzero. It is easy to compute from the definition that $Q$ has a family of resolvents of the form

$$A = \begin{pmatrix} 0 & * & * & * & -1 \\ * & 0 & 0 & 0 & 0 \\ 0 & 0 & c_{11}^1 & 0 & 0 \\ 0 & -c_{11}^1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & * & * & 0 \\ * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & * & * & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

with respect to bases for $L_a \cong R \oplus R \oplus a, M_a \cong a \oplus a \oplus a \oplus a \oplus R \oplus R$, where $\ast$ denotes any element of the appropriate ideal. We can therefore ignore very degenerate rings in the sequel.

4.1 Resolvents over a field

**Theorem 4.2** Every not very degenerate quintic $K$-algebra has a unique resolvent up to isomorphism.

**Proof** Let $M$ be a $K$-vector space of dimension 5, and let $\theta : \Lambda^5 M \rightarrow (\Lambda^4 L) \otimes \Lambda^3$ be any isomorphism. So far we have not made any choices. We will first construct the map $\phi^\Box = \phi^\Box(\bullet), a quadratic map from $\Lambda^4 L \otimes L$ to $\Lambda^4 M$. For this purpose we concoct a corollary of (3) that involves only $\phi^\Box$.

**Lemma 4.3** Let $V$ be a 5-dimensional vector space. Let $\mu \in \Lambda^2 V$ and $\alpha, \beta, \gamma, \delta \in \Lambda^4 V$. Then

$$\mu^\Box \wedge \alpha \wedge \beta \wedge \gamma \wedge \delta = \text{ev}(\mu; \alpha, \beta) \text{ev}(\mu; \gamma, \delta) + \text{ev}(\mu; \alpha, \gamma) \text{ev}(\mu; \delta, \beta)$$

$$+ \text{ev}(\mu; \alpha, \delta) \text{ev}(\mu; \beta, \gamma)$$
in $\Lambda^5(\Lambda^4 V) \cong (\Lambda^5 V)^{\otimes 4}$.

**Proof** Write the general $\mu$ as $u \wedge v + w \wedge x$ ($u, v, w, x \in V$) and expand. \hfill \Box

Motivated by this, we define for any quintic ring $Q$ the pentaquadratic form

$$F(a, b, c, d, e) = (a \wedge b \wedge c \wedge bc)(a \wedge d \wedge e \wedge de)$$

$$+ (a \wedge b \wedge d \wedge bd)(a \wedge e \wedge c \wedge ec)$$

$$+ (a \wedge b \wedge e \wedge be)(a \wedge c \wedge d \wedge cd)$$

from $L^5$ to $(\Lambda^4 L)^{\otimes 2}$, or equivalently from $(\Lambda^4 L \otimes L)^5$ to $(\Lambda^4 L)^{\otimes 12}$. We get that for any resolvent $(M, \phi, \theta)$ of $Q$,

$$\phi^{\otimes 4}(\phi(a) \square \wedge \phi(b) \square \wedge \phi(c) \square \wedge \phi(d) \square \wedge \phi(e) \square) = F(a, b, c, d, e)$$

We claim the following:

**Lemma 4.4** $F$ is identically zero if and only if $Q$ is very degenerate.

**Proof** We prove that the property of being very degenerate is invariant under base-changing to the algebraic closure $\bar{K}$ of $K$; then the lemma can be proved by checking the finitely many quintic algebras over an algebraically closed field (see Mazzola [13] and Poonen [16]). Let $\bar{Q} = Q \otimes_K \bar{K}$ be the corresponding $\bar{K}$-algebra. Clearly if $Q$ is very degenerate, so is $\bar{Q}$, so assume that $\bar{Q}$ is very degenerate.

First look at the reduced $Q_{\red}$, $\bar{Q}_{\red}$ formed by quotienting out by the nilpotents. Since $\bar{Q}$ is very degenerate, $\bar{Q}_{\red}$ is isomorphic to either $\bar{K}$ or $\bar{K} \times \bar{K}$, the latter case occurring when

$$\bar{Q} \cong \bar{K} \times \bar{K}[\epsilon_1, \epsilon_2, \epsilon_3]/(\epsilon_1, \epsilon_2, \epsilon_3)^2.$$  \hfill (11)

**Case 1.** If $\bar{Q}_{\red} \cong \bar{K}$, then $Q_{\red}$ must be a field, and its degree must divide 5: so $Q_{\red} = Q$ or $Q_{\red} \cong K$. If $Q_{\red} = Q$, then $\bar{Q}$ is either totally split or (in the purely inseparable case, which occurs only in characteristic 5) $\bar{Q} \cong \bar{K}[\epsilon]/(\epsilon^5)$, which is not a very degenerate ring. If $Q_{\red} \cong K$, then there is a distinguished section $s : L \hookrightarrow Q$, namely the isomorphism onto the 4-dimensional subspace of nilpotents. The condition that $Q$ be very degenerate can be stated as saying that the multiplication tensor

$$\text{mult} \in L^* \otimes L^* \otimes L$$

$$\text{mult}(x, y) = s(x)s(y) \mod K$$

has rank 1, that is, is an elementary tensor. This is a condition invariant under base change (incidentally, it is given by an intersection of quadrics which are the coefficients of $F$).

**Case 2.** If $\bar{Q}_{\red} \cong \bar{K} \times \bar{K}$, then we have (11). As the rank-1 idempotent is unique, $Q \cong K \times Q'$ must also split as a product of factors of the correct degrees. Then $Q$ is very degenerate if and only if $Q'$ is the trivial ring, that is, all the entries of its multiplication table are 0, and this too is invariant under base change. \hfill \Box

**Proof of Theorem 4.2** Picking $a_1, \ldots, a_5 \in \Lambda^4 L \otimes L$ such that $F(a_1, a_2, a_3, a_4, a_5) = f_0 \neq 0$, we get that the five vectors $v_i = \phi(a_i) \square$ must form a basis such that

$$\phi^{\otimes 4}(v_1 \wedge v_2 \wedge v_3 \wedge v_4 \wedge v_5) = f_0.$$
Any such basis is as good as any other: they are all related by elements of SL($\Lambda^4 M$), which is canonically isomorphic to SL($M$). Once the $v_i$ are fixed, there is at most one candidate for the map $\phi$ up to SL($M$)-equivalence, namely

$$\phi(a) = \frac{1}{f_0} \sum_{i=1}^{5} F(a_1, \ldots, a_i, \ldots, a_5) v_i \quad (12)$$

Then the relations

$$\text{ev}(\phi(x); \phi(a_1), \phi(a_j)) = x \wedge a_i \wedge a_j a_i$$

for $1 \leq i < j \leq 5$, determine the map $\phi$ uniquely. So the resolvent map $\phi$, if it exists, is unique. It remains to verify the resolvent relations, which are finite in number since the $a_i$ in (12) can be chosen from the finite set $\{e_1, e_2, e_3, e_4, e_1 + e_2, e_1 + e_3, \ldots, e_3 + e_4\}$ for any basis $\{e_1, e_2, e_3, e_4\}$ of $\Lambda^4 L \otimes L$. It remains to prove that the $(M, \phi, \theta)$ we have hereby constructed is actually a resolvent; this is a collection of integer polynomial identities, not in a family of free variables as in the previous lemma, but in the coefficients $c_{ij}^k$ of the given ring $Q$, which are restricted by the associative law. To prove these identities, it is enough to change base to the algebraic closure $\bar{K}$ and exhibit a resolvent for each of the finitely many quintic $\bar{K}$-algebras found in the classification of Mazzola and Poonen. For $\bar{K}^{\overline{Q^5}}$, the unique nondegenerate quintic $\bar{K}$-algebra, the resolvent is shown in Example 7.1. This takes care of all the $Q$ which are limits of étale algebras in the variety of based algebras (which is true for all $Q$ in characteristic 0, as Mazzola observes, and is most likely true in characteristic $p$). \qed

### 4.2 Resolvents over a Dedekind domain

We now want to endow our resolvents with integral structure.

**Proof** Let $Q$ be a quintic ring over a Dedekind domain $R$. We will assume that $Q$ is not very degenerate and hence that the corresponding $K$-algebra $Q_K = Q \otimes_R K$ has a unique resolvent $(M_K, \phi, \theta)$. Resolvents of $Q$ are now in bijection with lattices $M$ in the vector space $M_K$ such that

$$\phi(\Lambda^4 L \otimes L) \subseteq \Lambda^2 M \quad (13)$$

$$\theta(\Lambda^5 M) \subseteq (\Lambda^4 L)^{\otimes 3}. \quad (14)$$

For any resolvent $M$, note that we must have

$$M^* \cong \Lambda^4 M \otimes (M^*)^{\otimes -1} \cong \left(\phi(\Lambda^4 L \otimes L)\right)^{\otimes -1}. \quad (15)$$

Here $\left(\phi(\Lambda^4 L \otimes L)\right)^{\otimes -1}$ means the closure of the image of the quadratic map $\phi$ under addition and $O_K$-multiplication. Since $Q$ is not very degenerate, the right-hand side is a lattice of full rank and we may take its dual, which we denote by $M_0$. Then any resolvent is contained in $M_0$. Condition (13) is vacuous for $M = M_0$, since

$$\phi(\lambda x)(\phi(\lambda' y)) = \theta^{\otimes 2}((\lambda' \lambda''(x \wedge y \wedge z)) \in (\theta(\Lambda^2 L))^{\otimes 2}$$

for all $\lambda', \lambda'' \in \Lambda^3 L$ and $y, z \in L$. On the other hand, condition (14) is generally not satisfied by $M = M_0$; indeed, one readily finds that $\theta^{-1}((\Lambda^4 L)^{\otimes 3}) \subseteq \Lambda^5 M_0$ using (10).

The classification of resolvents is now reduced to a local problem. Any $M$ determines a family of resolvents $(M_p, \phi, \theta)$ of the quintic algebras $Q_p$ over the DVR’s $R_p \subseteq K$, and
conversely an arbitrary choice of resolvents $M_p$ of the $R_p$ can be glued together to form the resolvent $M = \bigcap_p M_p$. The choice $M_p = M_{0,p} = M_0 \otimes R_p$ is forced for all but finitely many primes $p$, namely those dividing the ideal
\[
c = [\Lambda^5M_0 : \theta^{-1}((\Lambda^4L)^{\otimes 3})] = [(\Lambda^4L)^{\otimes 2} : \{F(a, b, c, d, e) : a, b, c, d, e \in L\}].
\] (15)

Therefore, for the remainder of the proof, we assume that $R = R_p$ is a DVR. We adapt the method of proof of Bhargava [5], Lemmas 13--15.

We first prove that for some $n \geq 0$, the module $\pi^nL$, which corresponds to the ring $R + \pi^nQ$, has a resolvent. Let $M_1$ be any lattice of the correct index $c$ in $M_0$. With respect to any bases of $L$ and $M_0$, the map $\phi$ is represented by a box $A = (A_1, A_2, A_3, A_4)$ whose entries are in $K$. If we pass from $L$ to $\pi^5L$ and from $M_1$ to $\pi^{12}M_1$, the discriminant condition remains satisfied and the entries are multiplied by $\pi$. Performing this operation enough times, the entries become integral.

We now attempt to lower the exponent $n$ for which $\pi^nL$ has a resolvent $M$ until it becomes zero.

First, the quadratic map $\phi^{(2)} : L \to \Lambda^4V \cong \Lambda^5V \otimes V^*$ is determined by its values at the ten vectors $e_1, \ldots, e_4, e_1 + e_2, \ldots, e_2 + e_3$, where the $e_i$ form a basis of $L$. Wedging any five of them yields a vector in $\Lambda^5(\Lambda^4V) \cong (\Lambda^5V)^{\otimes 4}$; these are the fundamental invariants of $5$. Being invariant under $\text{SL}(V)$, they are quadratic polynomials in the fundamental invariants for the action of $\text{SL}(V)$ on boxes $A$, namely the ring coefficients $c_i^{(k)}$. Of interest to us is that these polynomials have coefficients in $\mathbb{Z}$. Since $L$ defines a ring, the $c_i^{(k)}$ of $\pi^n$ are divisible by $\pi^n$ and the determinantal invariants are divisible by $\pi^{2n}$, that is, lie in $\Lambda^5(M)^{\otimes 4}$.

Let $A = (A_1, A_2, A_3, A_4)$ be the $4 \times 5 \times 5$ box, with entries in $R$, corresponding to $\pi^{2n}L$ and its resolvent $M$. Since the determinantal invariants are all linearly dependent mod $\pi$, the image of $\phi = \pi^{2n}\phi^{(2)}$ lies in a sublattice of $M_1$ of index $\pi$; that is, with respect to a suitable basis, the upper $4 \times 4$ submatrices of the $A_i$ and their $R$-linear combinations are all singular modulo $\pi$. As explained in the proof of Lemma 15 in [5], it is possible to change bases further so that these submatrices are either all $0$ mod $\pi$ or have one of the forms
\[
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{bmatrix}, \quad
\begin{bmatrix}
0 & 0 & c_1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{bmatrix}, \quad
\begin{bmatrix}
0 & 0 & 0 & c_2 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{bmatrix}.
\] (16)

If the submatrices are zero or of the form (16) modulo $\pi$, we use the fact that the lower right $3 \times 3$ submatrices of each matrix in $A$ is divisible by $p$ to derive that $\pi^{n-1}L$ has the resolvent
\[
M' = \pi^{-3} \langle \mu_1, \pi\mu_2, \pi\mu_3, \pi\mu_4, \mu_5 \rangle
\]
where $\langle \mu_i \rangle$ is the basis of $M$ in which $A$ has been written. In the case (17), from $p \mid c_{23}^4 = \text{ev}(\phi(e_1)\phi(e_2)\phi(e_3)\pi(e_3)\pi(e_3)^3)$ we get that the $(4, 5)$ entry of $A_1$ is zero mod $p$. Symmetrically
we get the same for $A_2$ and $A_3$, and also for $A_4$ since replacing $A_2$ by $A_2 + A_4$ does not change the situation. So the entire fourth rows and fourth columns of $A$ are divisible by $p$, so $\pi^{n-2}M$ has the resolvent

$$M' = \pi^{-5} \langle \mu_1, \mu_2, \mu_3, \pi \mu_4, \mu_5 \rangle.$$ 

Thus, as long as $n > 0$, we can lower $n$. In the case that $n$ becomes negative, we can raise it back to 0 by the method of proof of Lemma 13 of [5].

In the special case that $c$ is the unit ideal, $M_0$ is the only resolvent. This occurs in one important instance, highlighted in Theorem 1.2(c).

**Lemma 4.5** If $Q$ is a maximal quintic ring, that is, is not contained in any strictly larger quintic ring, then the ideal $c$ in (15) is the unit ideal, implying that $Q$ has a unique resolvent.

**Proof** Suppose that $c$ were not the unit ideal, so there is a prime $p$ such that $pF(a, b, c, d, e)$ for all $a, b, c, d, e \in L$. We will prove that $Q$ is not maximal at $p$. It is convenient to localize and assume that $R = R_p$ is a DVR with uniformizer $\pi$.

Note that $Q/pQ$, a quintic algebra over $R/p$, has its associated pentaquadric form $F$ identically zero, so by Lemma 4.4, it is very degenerate. So $Q$ has an $R$-basis $(1, x, \epsilon_1, \epsilon_2, \epsilon_3)$ such that $(x, \epsilon_1, \epsilon_2, \epsilon_3)(\epsilon_1, \epsilon_2, \epsilon_3) \subseteq pR$. We claim that the lattice $Q'$ with basis $(1, x, \pi^{-1} \epsilon_1, \pi^{-1} \epsilon_2, \pi^{-1} \epsilon_3)$ either is a quintic ring or is contained in a quintic ring, showing that $Q$ is not maximal.

Set $M = \langle \pi, x, \epsilon_1, \epsilon_2, \epsilon_3 \rangle$ and $N = \langle \pi, \pi x, \epsilon_1, \epsilon_2, \epsilon_3 \rangle$. Then $Q \supseteq M \supseteq N \supseteq \pi Q$ and $MN \subseteq \pi Q$. Consider, for any $i, j \in \{1, 2, 3\}$, the multiplication maps

$$\begin{align*}
Q/N &\twoheadrightarrow N/\pi Q \twoheadrightarrow \pi Q/\pi N \twoheadrightarrow \pi N/\pi^2 Q \\
\langle 1, x \rangle &\twoheadrightarrow \langle \epsilon_1, \epsilon_2, \epsilon_3 \rangle \twoheadrightarrow \langle \pi, \pi x \rangle \twoheadrightarrow \langle \pi \epsilon_1, \pi \epsilon_2, \pi \epsilon_3 \rangle.
\end{align*}$$

These are all linear maps of $R/p$-vector spaces. Denote by $f$ the composition of the left two maps and by $g$ the composition of the right two. Write $f(1) = \pi (a + bx)$, where $a, b \in R/p$. Then $g(\epsilon_i) = a \pi \epsilon_i$, since $x \epsilon_i \in \pi Q$. Thus $g$ is given in the bases above by the scalar matrix $a$. But $g$ has rank at most 2, since it factors through the two-dimensional space $\pi Q/\pi N$; hence $a = 0$. So $N^2 \subseteq \pi M$.

Now consider the following multiplication maps:

$$\begin{align*}
Q/M &\twoheadrightarrow N/\pi Q \twoheadrightarrow \pi M/\pi N \twoheadrightarrow \pi^2 Q/\pi^2 M \twoheadrightarrow \pi^2 N/\pi^3 Q \\
\langle 1 \rangle &\twoheadrightarrow \langle \epsilon_1, \epsilon_2, \epsilon_3 \rangle \twoheadrightarrow \langle \pi x \rangle \twoheadrightarrow \langle \pi^2 \rangle \twoheadrightarrow \langle \pi^2 \epsilon_1, \pi^2 \epsilon_2, \pi^2 \epsilon_3 \rangle.
\end{align*}$$

Similarly to the previous argument, the composition of the first three maps must be zero, or else the composition of the last three would be a nonzero scalar. Since the images of the first map (as $i$ varies) span $N/\pi Q$, the composition of the middle two maps is always zero. Since $j$ and $k$ can vary independently and $\pi M/\pi N$ is one-dimensional, there are two cases:

(a) The second map is always zero, that is, $N^2 \subseteq \pi N$. This implies that $\pi^{-1}N$ is a quintic ring, as desired.
(b) The third map is always zero, that is, $MN \subseteq \pi M$. We get that $\pi^{-1}\epsilon_i$ is integral over $R$ (look at the characteristic polynomial of its action on $M$), so $R[\pi^{-1}\epsilon_1, \pi^{-1}\epsilon_2, \pi^{-1}\epsilon_3]$ is finitely generated and thus a quintic ring, as desired. □

Note that, in this proof, if the resolvent is not unique, then the extension $Q' \supseteq Q$ has $(R/p)^3 \subseteq Q'/Q$. So the following stronger theorem holds:

\textbf{Theorem 4.6} If $Q$ is a quintic ring such that the $R/p$-vector space of congruence classes in $\pi^{-1}Q/Q$ whose elements are integral over $R$ has dimension at most 2, for each prime $p$, then $Q$ has a unique resolvent.

5 The sextic ring

Given any resolvent $(L, M, \phi, \theta)$, the rank-6 lattice $S = M \oplus R$ also picks up a canonical ring structure, whose structure coefficients $a_{ij}^k$ are integer polynomials in the coefficients of $\phi$ of degree 12 (for $k \neq 0$) and 24 (for $k = 0$). As the construction given by Bhargava in [5], Section 6 works without change over a Dedekind domain, we will not spell out the details. We have the equation

$$\text{Disc } S = (16 \text{ Disc } Q)^3$$

from (33) of [5]. (These discriminants are to be interpreted as specifying both the Steinitz class and the discriminant ideal; see [15] for details.)

It is natural to ask whether the sextic resolvent ring is always an order in the sextic resolvent $K$-algebra, generated by classical methods from the theory of solving equations. For instance, if $Q$ is an order in $K^5$, is $S$ an order in $K^6$? We leave out the case where $\text{char } K = 2$, where (18) shows that $S$ is always degenerate.

\textbf{Theorem 5.1} Assume that $\text{char } K \neq 2$. Consider the familiar bijection between $n$-ic rings that are étale (that is, have nonzero discriminant) and maps $\text{Gal}(\bar{K}/K) \to S_n$ to the symmetric group (see for instance Milne [14, Theorem 7.29]). Let $Q$ be a quintic ring and $S$ its sextic resolvent. Then the maps $\psi_Q, \psi_S$ associated to the étale $K$-algebras $Q \otimes_R K$ and $S \otimes_R K$ are related by the commutative diagram

$$\begin{array}{ccc}
\text{Gal}(\bar{K}/K) & \xrightarrow{\psi_Q} & S_5 \\
\downarrow & & \downarrow \iota_{5,6} \\
S_5 & \xrightarrow{\psi_S} & S_6
\end{array}$$

where $\iota_{5,6} : S_5 \to S_6$ is the exceptional embedding (given by composing the obvious injection with the famous outer automorphism of $S_6$).

\textbf{Proof} We may assume $R = K$ is a field. The proof consists of the following steps:

- Check that the resolvent of $Z^5$ is an order of index 64 in $Z^6$ (Example 7.1).
- Deduce that the resolvent of $\hat{K}^5$ is $\hat{K}^6$.
- Analyze how the $S_n$-actions on $\hat{K}^n$ interact with the resolvent. We find that for each $\sigma \in S_5$,

$$\sigma : \hat{K}^5 \to \hat{K}^5, \quad \iota_{5,6} \sigma : \hat{K}^6 \to \hat{K}^6$$

act by permutation.
• By the standard description of the Galois parametrization (see Milne [14, p. 107]),

\[ Q = \{ x \in \bar{K}^5 : gx = \psi_Q(g)x \quad \forall g \in \text{Gal}(\bar{K}/K) \}, \]

where \( g \) acts componentwise on \( \bar{K}^5 \), but \( \psi_Q(g) \) acts by permutation. Consider the sextic algebra associated to \( \iota_{5,6} \circ \psi_Q \):

\[ S' = \{ x \in \bar{K}^6 : gx = \iota_{5,6}(\psi_Q(g))x \quad \forall g \in \text{Gal}(\bar{K}/K) \}. \]

By the preceding considerations, \( \phi \) and \( \theta \) restrict to maps making \( S' \) a resolvent for \( Q \). Because \( Q \) is nondegenerate over a field, the resolvent \( S' = S \) is unique, so \( \psi_S = \iota_{5,6} \circ \psi_Q \) as desired.

\[ \Box \]

6 Finiteness of the number of resolvents

It is natural to wonder, if the resolvent of a quintic ring is not unique, how close to being unique it is. For the quartic case, a beautifully simple formula was given in [3] and extended to the Dedekind case in [15]: the number of (numerical) resolvents is the sum of the absolute norms of the content. In the quintic case, things do not appear to be so simple. However, we have finiteness and an upper bound that is theoretically effective.

**Theorem 6.1** Let \( Q \) be a not very degenerate quintic ring. Then \( Q \) has at most

\[ \prod_{p \text{ prime}, \ p | c} \left( \frac{N(p)^5 - 1}{N(p) - 1} \right)^{v_p(c)} \]

resolvents, provided that the absolute norms \( N(p) = |R/p| \) are finite. In particular, a not very degenerate quintic ring over the ring of integers of a number field has finitely many resolvents.

**Proof** Since all resolvents have index \( c \) in \( M_0 \), it suffices to bound the number of sublattices of index \( c \) in a fixed lattice \( M_0 \). By localization we may reduce to the case \( c = p^n \), where \( p \) is prime. Now a fixed lattice \( M \) has \( (N(p)^5 - 1)/(N(p) - 1) \) sublattices of index \( p \), the kernels of the nonzero linear functionals \( \ell : M/pM \to R/p \mod \text{scaling} \). A sublattice \( M_n \) of index \( p^n \) has a filtration \( M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \) where the quotients are \( R/p; \) given \( M_i \), there are at most \( (N(p)^5 - 1)/(N(p) - 1) \) possibilities for \( M_{i+1} \), giving the claimed bound.

\[ \Box \]

7 Examples

**Example 7.1** The most fundamental example of a sextic resolvent is as follows. Let \( Q = R^{\oplus 5} \), with basis \( e_1, e_2, \ldots, e_5 \), and let \( M = R^5 \) with basis \( f_1, \ldots, f_5 \). Then the map

\[ \phi(e_i) = f_i \wedge (f_i-1 + f_{i+1}) \]

(indices mod 5), supplemented by the orientation \( \theta(f_{\top}) = e_{\top}^3 \) induced by these bases, is verified to be a resolvent for \( Q \) (indeed the unique one, as \( Q \) is maximal). The automorphism group \( S_5 \) of \( Q \) acts on \( M \) by the 5-dimensional irreducible representation obtained (in characteristic not 2) by restricting to the image of the exceptional embedding \( \iota_{5,6} \) the standard representation of \( S_6 \), permuting the six vectors

\[ f_{i-2} - f_{i-1} + f_i - f_{i+1} + f_{i+2} \quad (1 \leq i \leq 5) \quad \text{and} \quad f_1 + f_2 + f_3 + f_4 + f_5. \]
The corresponding ring structure $S$ produced in Sect. 5 is none other than the ring $S = \mathbb{Z} \otimes \mathbb{Z} R$, where
\[
S_{\mathbb{Z}} = \{ (x_1; x_2; x_3; x_4; x_5; x_6) \in \mathbb{Z}^6 : x_i \equiv x_j \mod 2 \ \forall i, j; \text{ and } \sum x_i \equiv 2x_1 \mod 4 \}.
\]

**Example 7.2** Consider the subring $Q = \{ x_1 e_1 + \cdots + x_5 e_5 \in \mathbb{Z}^{\oplus 5} : x_1 \equiv x_2 \equiv x_3 \equiv x_4 \mod p \}$.

Over $K$, this is a special case of the preceding example, so the $K$-resolvent $M_K$ and the associated maps $\phi$ and $\theta$ are forced. But the bounding module $M_0$ of Sect. 4.2 is no longer a resolvent, as can be seen by observing that $Q/pQ \equiv \mathbb{F}_p[t, e_1, e_2, e_3]/(\langle t^2 - t e_0, e_1 \rangle)$ is very degenerate. We have $L = (pe_1, pe_2, pe_3, e_5)$ and thus $\Lambda^4L = \langle p^3e_{\text{top}} \rangle$. One computes that
\[
M_0 = \{ p(f_1 + f_3), p^2f_2, p^2f_3, p^2f_4, pf_5 \},
\]
and thus
\[
\epsilon = [\Lambda^5M_0 : \phi^{-1}((\Lambda^4L)^{\otimes 3})] = [(p^3e_{\text{top}}) : (p^3f_{\text{top}})] = p.
\]

Consequently a resolvent of $Q$ is a submodule $M$ of index $p$ in $M_0$ having the property that $\phi(\Lambda^4L \otimes L) \subseteq \Lambda^2M$. Writing $M$ as the kernel of some linear functional $\ell : M_0/pM_0 \rightarrow \mathbb{F}_p$, the condition is that $\ell$ lies in the kernel of each of the alternating bilinear forms obtained by reducing $\phi(x) \in \Lambda^2M_0 \mod p$ for all $x \in \Lambda^4L \otimes L$). Let
\[
f'_i = p(f_1 + f_4), f'_2 = p^2f_2, f'_3 = p^2f_3, f'_4 = p^2f_4, f'_5 = pf_5
\]
be the basis elements of $M_0$ listed above. We compute
\[
\begin{align*}
\phi(p^4e_{\text{top}} e_1) &= (pf'_1 - f'_4) \wedge (pf'_2 + f'_3) \\
\phi(p^4e_{\text{top}} e_2) &= f'_2 \wedge (pf'_1 - f'_4 + f'_3) \\
\phi(p^4e_{\text{top}} e_3) &= f'_3 \wedge (pf'_2 + f'_4) \\
\phi(p^3e_{\text{top}} e_5) &= f'_5 \wedge (pf'_1).
\end{align*}
\]

So, letting $\bar{f}'_i$ denote the basis vector of $M_0/pM_0$ corresponding to $f'_i$ and $\bar{f}'^*_i$ the corresponding vector of the dual basis, we have
\[
\ell \in \ker(\bar{f}'_2 \wedge \bar{f}'_3) \cap \ker(\bar{f}'_3 \wedge \bar{f}'_4) \cap \ker(\bar{f}'_5 \wedge \bar{f}'_4) = \langle \bar{f}'^*_i \rangle.
\]

Since $\ell$ can take any value in the last-named vector space, up to scaling, we get $p + 1$ resolvents.

**Example 7.3** The ring
\[
Q = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}[x, y]/(x, y)^2
\]
is a curious example of Theorem 4.6. Although $Q$ is infinitely far from being maximal $(\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}[n^{-1}x, n^{-1}y]/(n^{-2}(x, y)^2)$ is a quintic extension ring for any $n > 0$), the extensions are only in two directions, as it were, and the resolvent is accordingly unique.
Data availability This project has no associated data.

Received: 24 December 2021 Accepted: 3 June 2022 Published online: 7 July 2022

References

1. Bhargava, M.: Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. Ann. Math. (2) 159(1), 217–250 (2004)
2. Bhargava, M.: Higher composition laws. II. On cubic analogues of Gauss composition. Ann. Math. (2) 159(2), 865–886 (2004)
3. Bhargava, M.: Higher composition laws. III. The parametrization of quartic rings. Ann. Math. (2) 159(3), 1329–1360 (2004)
4. Bhargava, M.: The density of discriminants of quartic rings and fields. Ann. Math. (2) 162(2), 1031–1063 (2005)
5. Bhargava, M.: Higher composition laws. IV. The parametrization of quintic rings. Ann. Math. (2) 167(1), 53–94 (2008)
6. Bhargava, M.: The density of discriminants of quintic rings and fields. Ann. Math. (2) 172(3), 1559–1591 (2010)
7. Bhargava, M., Shankar, A., Wang, X. Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces (2015)
8. Delone, B.N., Faddeev, D.K.: The Theory of Irrationalities of the Third Degree. Translations of Mathematical Monographs, vol. 10. American Mathematical Society, Providence, RI (1964)
9. Dummit, E.P.: Counting $G$-extensions by discriminant. Math. Res. Lett. 25(4), 1151–1172 (2018)
10. Ellenberg, J.S., Venkatesh, A.: The number of extensions of a number field with fixed degree and bounded discriminant. Ann. Math. (2) 163(2), 723–741 (2006)
11. Gan, W.T., Gross, B., Savin, G.: Fourier coefficients of modular forms on $G_2$. Duke Math. J. 115(1), 105–169 (2002)
12. Levi, F.W.: Kubische Zahlkörper und binäre kubische Formenklassen [Cubic number fields and cubic form classes]. Leipz. Ber. 66, 26–37 (1914)
13. Mazza, G.: Generic finite schemes and Hochschild cocycles. Comment. Math. Helv. 55(2), 267–293 (1980)
14. Milne, J.S.: Fields and Galois Theory (v=4.30) (2012). Available at www.jmilne.org/math/
15. O’Dorney, E.M.: Rings of small rank over a Dedekind domain and their ideals. Res. Math. Sci. 3(8) (2016)
16. Poonen, B.: Isomorphism types of commutative algebras of finite rank over an algebraically closed field. In Computational Arithmetic Geometry, volume 463 of Contemp. Math., pp. 111–120. Amer. Math. Soc., Providence, RI (2008)
17. Wood, M.M.: Gauss composition over an arbitrary base. Adv. Math. 226(2), 1756–1771 (2011)
18. Wood, M.M.: Parametrizing quartic algebras over an arbitrary base. Algebra Number Theory 5(8), 1069–1094 (2011)
19. Wood, M.M.: Parametrization of ideal classes in rings associated to binary forms. J. Reine Angew. Math. 689, 169–199 (2014)

Publisher’s Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.