Annals of Mathematics, **167** (2008), 53–94

Higher composition laws IV: The parametrization of quintic rings

By Manjul Bhargava

1. Introduction

In the first three parts of this series, we considered quadratic, cubic and quartic rings (i.e., rings free of ranks 2, 3, and 4 over $\mathbb{Z}$) respectively, and found that various algebraic structures involving these rings could be completely parametrized by the integer orbits of an appropriate group representation on a vector space. These orbit results are summarized in Table 1. In particular, the theories behind the parametrizations of quadratic, cubic, and quartic rings, noted in items #2, 9, and 13 of Table 1, were seen to closely parallel the classical developments of the solutions to the quadratic, cubic and quartic equations respectively.

Despite the quintic having been shown to be unsolvable nearly two centuries ago by Abel, it turns out there still remains much to be said regarding the integral theory of the quintic. Although a "solution" naturally still is not possible, we show in this article that it is nevertheless possible to completely parametrize quintic rings; indeed a theory just as complete as in the quadratic, cubic, and quartic cases exists also in the case of the quintic. In fact, we present here a unified theory of ring parametrizations which includes the cases $n = 2$, 3, 4, and 5 simultaneously.

Our strategy to parametrize rings of rank n is as follows. To any order R in a number field of degree n, we give a method of attaching to R a set of n points, $X_R \subset \mathbb{P}^{n-2}(\mathbb{C})$, which is well-defined up to transformations in $\mathrm{GL}_{n-1}(\mathbb{Z})$. We then seek to understand the hypersurfaces in $\mathbb{P}^{n-2}(\mathbb{C})$, defined over $\mathbb{Z}$ and of smallest possible degree, which vanish on all n points of X_R. We find that the hypersurfaces over $\mathbb{Z}$ passing through all n points in X_R correspond in a remarkable way to functions between R and certain *resolvent rings*, a notion we introduced in [1] and [4]. We termed them resolvent rings because they are integral models of the *resolvent fields* studied in the classical literature. In particular, we showed in [4] that for cubic and quartic rings, the resolvent rings turn out to be quadratic and cubic rings respectively. For quintic rings, we will show that the resolvent rings are sextic rings. (For the definitions of quadratic and cubic resolvents, see [4].)

The above program leads to the following results describing how rings of small rank are parametrized. When $n = 3$, one finds that cubic rings are parametrized by integer equivalence classes of binary cubic forms. Specifically, *there is a natural bijection between the* $\mathrm{GL}_2(\mathbb{Z})$*-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*.* We are thus able to recover, from a geometric viewpoint, the celebrated result of Delone-Faddeev [11] and Gan-Gross-Savin [12] parametrizing cubic rings (as reformulated in [4]).

When $n = 4$, analogous geometric and invariant-theoretic principles allow us to show that quartic rings are essentially parametrized by equivalence classes of pairs of ternary quadratic forms. Precisely, *there is a canonical bijection between the* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$*-orbits on the space of pairs of ternary quadratic forms, and the set of isomorphism classes of pairs* (R, S)*, where* R *is a quartic ring and* S *is a cubic resolvent of* R*.* This was the main result of [4].

The above parametrization results were attained in [4] through a close study of the invariant theory of quadratic, cubic, and quartic rings. This invariant theory involved, in particular, many of the central ingredients in the solutions to the quadratic, cubic, and quartic equations. In this article, we reconcile these various invariant-theoretic elements with our new geometric perspective.

The primary focus of this article is, of course, on the theory of quintic rings, and it is here that the interplay between the geometry and invariant theory becomes particularly beautiful. Even though the quintic equation is not solvable, the analogous geometry and invariant theory from the cubic and quartic cases can in fact be completely worked out for the quintic, and one finds that the correct objects parametrizing quintic rings are quadruples of quinary alternating 2-forms. More precisely, our main result is the following:

THEOREM 1. *There is a canonical bijection between the* $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$*-orbits on the space* $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ *of quadruples of* 5×5 *skew-symmetric matrices and the set of isomorphism classes of pairs* (R, S)*, where* R *is a quintic ring and* S *is a sextic resolvent ring of* R*.*

Notice that the enunciation of Theorem 1 is remarkably similar to the cubic and quartic cases cited above. The similarities in fact run much deeper.

A first similarity that must be mentioned regards the justification for the term "parametrization". What made the above results for $n = 3$ and $n = 4$ genuine parametrizations is that every cubic ring and quartic ring actually arises in those correspondences: there exists a binary cubic form corresponding to any given cubic ring, and a pair of ternary quadratic forms to any given quartic ring. Moreover, up to integer equivalence *each maximal ring arises exactly once* in both bijective correspondences.

The identical situation holds for the parametrization of quintic rings in Theorem 1. Given an element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, let us write $R(A)$ for the quintic ring corresponding to A as in Theorem 1, and write $\Gamma = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$. Then we will prove:

THEOREM 2. *Every quintic ring R is of the form $R(A)$ for some element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. If R is a maximal ring, then the element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ with $R = R(A)$ is unique up to Γ-equivalence.*

The implication for sextic resolvents (to be defined) of a quintic ring is that they always exist. This is analogous to the situation with quadratic and cubic resolvents of cubic and quartic rings respectively (cf. [4, Cor. 5]).

COROLLARY 3. *Every quintic ring has at least one sextic resolvent ring. A maximal quintic ring has a unique sextic resolvent ring up to isomorphism.*

A second important similarity among these parametrizations is the method via which they are computed. The forms corresponding to cubic, quartic, or quintic rings in these parametrizations are obtained by determining the most fundamental polynomial mappings relating these rings to their respective resolvent rings. In the cubic and quartic cases, these fundamental mappings are none other than the classical resolvent maps used in the literature in the solutions to the cubic and quartic equations.

More precisely, given a cubic ring R let S denote a *quadratic resolvent* of R as defined in [4], i.e., a quadratic ring having the same discriminant as R. In the case where R and S are orders in a cubic and quadratic number field respectively, the binary cubic form corresponding to (R, S) in the parametrization is obtained as follows. When R and S lie in a fixed algebraic closure of $\mathbb{Q}$, there is a natural, discriminant-preserving map from R to S given by

$$\phi_{3,2}(\alpha) = \frac{\mathrm{Disc}(\alpha) + \sqrt{\mathrm{Disc}(\alpha)}}{2};$$

this may be viewed as an integral model of the classical resolvent map

$$\delta(\alpha) = \sqrt{\mathrm{Disc}(\alpha)} = (\alpha^{(1)} - \alpha^{(2)})(\alpha^{(2)} - \alpha^{(3)})(\alpha^{(3)} - \alpha^{(1)})$$

representing the most fundamental polynomial mapping from a cubic field to its quadratic resolvent field; here $\alpha^{(1)}$, $\alpha^{(2)}$, $\alpha^{(3)}$ denote the conjugates of α in $\bar{\mathbb{Q}}$. The map $\phi_{3,2} : R \to S$ evidently descends to a map $\bar{\phi}_{3,2} : R/\mathbb{Z} \to S/\mathbb{Z}$, and this resulting $\bar{\phi}_{3,2}$ is precisely the binary cubic form associated to the pair (R, S). The remarkable aspect of this parametrization of cubic rings is that a pair (R, S) is completely determined by the binary cubic form $\bar{\phi}_{3,2}$, and conversely, every binary cubic form arises as a $\bar{\phi}_{3,2}$ for some pair of rings (R, S). In sum, $\bar{\phi}_{3,2}$ is the essential map through which the parametrization of cubic rings is computed (entry #9 in Table 1).

Table 1: Summary of Higher Composition Laws

#	Lattice ($V_\mathbb{Z}$)	Group acting ($G_\mathbb{Z}$)	Parametrizes ($\mathcal{C}$)	(k)	(n)	(H)
1.	$\{0\}$	-	Linear rings	0	0	A_0
2.	$\widetilde{\mathbb{Z}}$	$\mathrm{SL}_1(\mathbb{Z})$	Quadratic rings	1	1	A_1
3.	$(\mathrm{Sym}^2\mathbb{Z}^2)^*$ (GAUSS'S LAW)	$\mathrm{SL}_2(\mathbb{Z})$	Ideal classes in quadratic rings	2	3	B_2
4.	$\mathrm{Sym}^3\mathbb{Z}^2$	$\mathrm{SL}_2(\mathbb{Z})$	Order 3 ideal classes in quadratic rings	4	4	G_2
5.	$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$	$\mathrm{SL}_2(\mathbb{Z})^2$	Ideal classes in quadratic rings	4	6	B_3
6.	$\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$	$\mathrm{SL}_2(\mathbb{Z})^3$	Pairs of ideal classes in quadratic rings	4	8	D_4
7.	$\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$	$\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$	Ideal classes in quadratic rings	4	12	D_5
8.	$\wedge^3\mathbb{Z}^6$	$\mathrm{SL}_6(\mathbb{Z})$	Quadratic rings	4	20	E_6
9.	$(\mathrm{Sym}^3\mathbb{Z}^2)^*$	$\mathrm{GL}_2(\mathbb{Z})$	Cubic rings	4	4	G_2
10.	$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$	Order 2 ideal classes in cubic rings	12	12	F_4
11.	$\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})^2$	Ideal classes in cubic rings	12	18	E_6
12.	$\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$	Cubic rings	12	30	E_7
13.	$(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3)^*$	$\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$	Quartic rings	12	12	F_4
14.	$\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$	$\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$	Quintic rings	40	40	E_8

Notation on Table 1. The symbol $\tilde{\mathbb{Z}}$ in #2 denotes the set of elements in $\mathbb{Z}$ congruent to 0 or 1 (mod 4). We use $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ to denote the set of binary quadratic forms with integral coefficients, while $\mathrm{Sym}^2\mathbb{Z}^2$ denotes the sublattice of integral binary quadratic forms whose middle coefficients are even. Similarly, $(\mathrm{Sym}^3\mathbb{Z}^2)^*$ denotes the space of binary cubic forms with integer coefficients, while $\mathrm{Sym}^3\mathbb{Z}^2$ denotes the subset of forms whose middle two coefficients are multiples of 3. The symbol $\otimes$ is used for the usual tensor product; thus, for example, $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ is the space of $2 \times 2 \times 2$ cubical integer matrices, $(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3)^*$ is the space of pairs of ternary quadratic forms with integer coefficients, and $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$ is the space of pairs of integral ternary quadratic forms whose cross terms have even coefficients.

The fourth column of Table 1 gives approximate descriptions of the classes $\mathcal{C}$ of algebraic objects parametrized by the orbit spaces $V_\mathbb{Z}/G_\mathbb{Z}$. In most cases, the algebraic objects listed in the fourth column come equipped with additional structure, such as "resolvent rings" or "balance" conditions; for the precise descriptions of these correspondences, see [2]–[4] and the current article.

The fifth column gives the degree k of the *discriminant* invariant as a polynomial on $V_\mathbb{Z}$, while the sixth column of Table 1 gives the $\mathbb{Z}$-rank n of the lattice $V_\mathbb{Z}$.

Finally, it turns out that each of the correspondences listed in Table 1 is related in a special way to some exceptional Lie group H (see [2, §4] and [3, §4]). These exceptional groups have been listed in the last column of Table 1.

In a similar vein, a *cubic resolvent* of a quartic ring R is a cubic ring S having the same discriminant as R, and which is equipped with a certain natural, discriminant-preserving quadratic map $\phi_{4,3} : R \to S$ (see [4, Sec. 2.3]). In the case where R and S are in fact orders in quartic and cubic number fields respectively (lying in a fixed algebraic closure of $\mathbb{Q}$), this map is none other than the fundamental resolvent map

$$\phi_{4,3}(\alpha) = \alpha^{(1)}\alpha^{(2)} + \alpha^{(3)}\alpha^{(4)}$$

used in the classical literature in the solution to the quartic equation; here $\alpha^{(1)}$, $\alpha^{(2)}$, $\alpha^{(3)}$, $\alpha^{(4)}$ denote the conjugates of α in $\bar{\mathbb{Q}}$. Just as in the cubic case, the map $\phi_{4,3} : R \to S$ descends to a map $\bar{\phi}_{4,3} : R/\mathbb{Z} \to S/\mathbb{Z}$, and this resulting $\bar{\phi}_{4,3}$ is precisely the pair of ternary quadratic forms that corresponds to the pair (R, S) in the parametrization of quartic rings. Again, the remarkable aspect of this parametrization is that the pair (R, S) is completely determined by the corresponding pair of ternary quadratic forms $\bar{\phi}_{4,3}$, and conversely, every pair of ternary quadratic forms arises as a $\bar{\phi}_{4,3}$ for some pair (R, S) consisting of a quartic ring and a cubic resolvent ring. Thus $\bar{\phi}_{4,3}$ forms the fundamental map through which the parametrization of quartic rings is computed, and indeed detailed knowledge of this mapping is what the proof of the parametrization of quartic rings relied on (entry #13 in Table 1).

In the quintic case, the most fundamental map relating a quintic ring (or field) and its sextic resolvent seems to have been missed in the literature. Although various maps relating a quintic field and its sextic resolvent field have been considered in the past, it turns out that all such maps may be realized as higher degree covariants of one special fundamental map $\phi_{5,6}$. This beautiful map is discussed in Section 5, and forms a most crucial ingredient in the proof of Theorem 1 and its corollaries. One reason why the map $\phi_{5,6}$ may have been missed in the past is that it sends a quintic ring R not to its sextic resolvent S, but instead to $\wedge^2 S$. (We actually work more with the dual map $g = \phi_{5,6}^* : \wedge^2 S^* \to R^*$, where R^* and S^* denote the $\mathbb{Z}$-duals of R and S respectively, which turns out to be more convenient.) In perfect analogy with the cubic and quartic cases, this fundamental map $\phi_{5,6}$ is found to descend to a mapping $\bar{\phi}_{5,6} : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$, and this $\bar{\phi}_{5,6}$ may thus be viewed as a quadruple of alternating 2-forms in five variables. Theorem 1 then amounts to the remarkable fact that the pair (R, S) is completely determined by $\bar{\phi}_{5,6}$, and conversely every quadruple of quinary alternating 2-forms arises as the map $\bar{\phi}_{5,6}$ for some pair (R, S) consisting of a quintic ring and a sextic resolvent ring. Thus—analogous to the mappings $\phi_{3,2}$ and $\phi_{4,3}$ in the cubic and quartic cases—$\phi_{5,6}$ (or, equivalently, $g = \phi_{5,6}^*$) is the fundamental mapping through which the parametrization of quintic rings is computed (entry #14 in Table 1).

Finally, the multiplication tables of the rings and resolvent rings corresponding to points in the above spaces—namely the spaces of integral binary

cubic forms, pairs of integral ternary quadratic forms, and quadruples of integral 5×5 skew-symmetric matrices (i.e., items #9, 13, and 14 in Table 1)—may be worked out directly from the point of view of studying sets of n points in $\mathbb{P}^{n-2}$ for $n = 3$, 4 and 5 respectively. We illustrate the case $n = 5$ in this article. The corresponding multiplication tables for $n \leq 4$ were given in [2]–[4].

We observe that each of the group representations given in Table 1 is a $\mathbb{Z}$-form of what is known as a *prehomogeneous vector space*, i.e., a representation having just one Zariski-open orbit over $\mathbb{C}$. This work completes the analysis of orbits over $\mathbb{Z}$ in those prehomogeneous vector spaces corresponding to field extensions, as classified by Wright-Yukie in their important work [15].

The organization of this paper is as follows. In Section 2, we examine the parametrizations of cubic and quartic rings from the geometric point of view described above for general n. We then concentrate strictly on the case of quintic rings, and explain how the space $V_{\mathbb{Z}} = \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ of quadruples of quinary alternating 2-forms arises in this context. The space $V_{\mathbb{Z}}$ has a unique invariant for the action of $\Gamma = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$, which we call the *discriminant*; this invariant is defined in Section 3. In Section 4, given an element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, we use our new geometric perspective to construct a multiplication table for a quintic ring $R = R(A)$ which is found to be naturally associated to A.

In Section 5, we then introduce the notion of a sextic resolvent S for a nondegenerate quintic ring R, and we construct the fundamental mapping g between them alluded to above. We describe the multiplication table for this sextic resolvent ring S in Section 6. The main result, Theorem 1, is then proved in Section 7 in the case of nondegenerate rings. In Section 8, we explain the precise relation between g and Cayley's classical resolvent map $\Phi : R \to S \otimes \mathbb{Q}$ defined by

$$\begin{aligned}\Phi(\alpha) = (\ &\alpha^{(1)}\alpha^{(2)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(3)}\alpha^{(4)} + \alpha^{(4)}\alpha^{(5)} + \alpha^{(5)}\alpha^{(1)} \\ &-\alpha^{(1)}\alpha^{(3)} - \alpha^{(3)}\alpha^{(5)} - \alpha^{(5)}\alpha^{(2)} - \alpha^{(2)}\alpha^{(4)} - \alpha^{(4)}\alpha^{(1)})^2,\end{aligned}$$

which has played a major role in the literature in the solution to the quintic equation whenever it is soluble. Cayley's map is found to be a degree 4 covariant of the map g. In Section 9, we describe an alternative approach to sextic resolvent rings which, in particular, allows for a proof of Theorem 1 in all cases (including those of zero discriminant). In Sections 10 and 11, we study more closely the invariant theory of the space $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, and as a consequence, we prove Theorem 2 and Corollary 3. In Section 12, we examine how conditions such as maximality and prime splitting for quintic rings $R(A)$ manifest themselves as congruence conditions on elements A of $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. This may be useful in future computational applications (see e.g. [6]), and will also play a crucial role for us in obtaining results on the density of discriminants of quintic fields (to appear in [5]).

2. The geometry of ring parametrizations

We begin by recalling some basic terminology. First, let us define *a ring of rank* n to be any commutative ring with unit that is free of rank n as a $\mathbb{Z}$-module. For $n = 2$, 3, 4, 5, and 6, such rings are called *quadratic*, *cubic*, *quartic*, *quintic*, and *sextic* rings respectively. An order in a degree n number field is the prototypical ring of rank n. To any such ring R of rank n we may attach the *trace* function $\mathrm{Tr} : R \to \mathbb{Z}$, which assigns to any element $\alpha \in R$ the trace of the endomorphism $R \xrightarrow{\times\alpha} R$. 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 $\{\alpha_i\}_{i=1}^n$ is any $\mathbb{Z}$-basis of R. Finally, we say that a ring of rank n is *nondegenerate* if its discriminant is nonzero.

In this section, we wish to understand the parametrization of rings of small rank via a natural mapping that associates, to any nondegenerate ring R of rank n, a set X_R of n points in an appropriate projective space.

To this end, let R be any nondegenerate ring of rank n, and fix a $\mathbb{Z}$-basis $\langle \alpha_0 = 1, \alpha_1, \ldots, \alpha_{n-1} \rangle$ of R. Since R is nondegenerate, $K = R \otimes \mathbb{Q}$ is an étale $\mathbb{Q}$-algebra of dimension n, i.e., K is a direct sum of number fields the sum of whose degrees is n. Let $\rho^{(1)}, \ldots, \rho^{(n)}$ denote the distinct $\mathbb{Q}$-algebra homomorphisms from K to $\mathbb{C}$, and for any element $\alpha \in K$, let $\alpha^{(1)}$, $\alpha^{(2)}$, …, $\alpha^{(n)} \in \mathbb{C}$ denote the images of α under the n homomorphisms $\rho^{(1)}, \ldots, \rho^{(n)}$ respectively. For example, in the case that $K \subset \mathbb{C}$ is a field, $\alpha^{(1)}, \ldots, \alpha^{(n)} \in \mathbb{C}$ are simply the conjugates of α over $\mathbb{Q}$.

Let $\langle \alpha_0^*, \alpha_1^*, \ldots, \alpha_{n-1}^* \rangle$ be the dual basis of $\langle \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \rangle$ with respect to the trace pairing on K, i.e., we have $\mathrm{Tr}_{\mathbb{Q}}^K(\alpha_i\alpha_j^*) = \delta_{ij}$ for all $0 \le i, j \le n-1$. For $m \in \{1, 2, \ldots, n\}$, set

$$x_R^{(m)} = \left[\alpha_1^{*(m)} : \cdots : {\alpha_{n-1}^*}^{(m)}\right] \in \mathbb{P}^{n-2}(\mathbb{C}).$$

(Note that α_0^* is not used here.) We thus obtain n points, conjugate to each other over $\mathbb{Q}$ when K is a field, and a set

$$X_R = \left\{x_R^{(1)}, \ldots, x_R^{(n)}\right\}$$

in $\mathbb{P}^{n-2}(\mathbb{C})$ which is now independent of the numbering of the homomorphisms $\rho^{(m)}$.

Alternatively, if $\mathcal{D}$ denotes the $n \times n$ matrix

$$\mathcal{D} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_1^{(n)} \\ \alpha_2^{(1)} & \alpha_2^{(2)} & \cdots & \alpha_2^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1}^{(1)} & \alpha_{n-1}^{(2)} & \cdots & \alpha_{n-1}^{(n)} \end{bmatrix} \tag{1}$$

and $\mathcal{D}_{i,m}$ denotes its (i,m)-th minor, i.e., $(-1)^{i+m}$ times the determinant of the matrix obtained from $\mathcal{D}$ by omitting its ith row and mth column, then we

have $\alpha_i^{*(m)} = \mathcal{D}_{i+1,m}/\det(\mathcal{D})$. Hence we can also write

$$x_R^{(m)} = [\mathcal{D}_{2,m} : \cdots : \mathcal{D}_{n,m}]. \tag{2}$$

Note that the elements $\alpha_i^* \in K$ $(i > 0)$, and hence the points $x_R^{(m)}$, depend only on the basis $\langle \bar{\alpha}_1, \ldots, \bar{\alpha}_{n-1} \rangle$ of $R/\mathbb{Z}$; i.e., changing each α_i to $\alpha_i + m_i$ for $m_i \in \mathbb{Z}$ does not affect α_i^* for $i > 0$. In fact, if we denote by K_0 the traceless elements of K, then the trace gives a nondegenerate pairing $K_0 \times K/\mathbb{Q} \to \mathbb{Q}$ so that $\langle \alpha_1^*, \ldots, \alpha_{n-1}^* \rangle$ is the basis of K_0 dual to the $\mathbb{Q}$-basis $\langle \bar{\alpha}_1, \ldots, \bar{\alpha}_{n-1} \rangle$ of $K/\mathbb{Q}$.

We observe that the points of X_R are in general position in the sense that no $n-1$ of them lie on a hyperplane. Indeed, if say $x^{(1)}$, $x^{(2)}$, …, $x^{(n-1)}$ were on a single hyperplane, then we would have $\det(x^{(1)}, x^{(2)}, \ldots, x^{(n-1)}) = 0$; but a calculation shows that, with the coordinates of the $x^{(i)}$ defined as in (2), $\det(x^{(1)}, x^{(2)}, \ldots, x^{(n-1)}) = \pm(\det \mathcal{D})^{n-2} \neq 0$, since $(\det \mathcal{D})^2 = \mathrm{Disc}(R) \neq 0$.

However, we observe that for any $1 \leq i < j \leq n$, the hyperplane defined by

$$H_{i,j}(t) = \big(\alpha_1^{(i)} - \alpha_1^{(j)}\big)t_1 + \cdots + \big(\alpha_{n-1}^{(i)} - \alpha_{n-1}^{(j)}\big)t_{n-1} = 0, \tag{3}$$

where $[t_1 : \cdots : t_{n-1}]$ are the homogeneous coordinates on $\mathbb{P}^{n-2}$, is seen to pass through $n-2$ of the n points in X_R, namely through all $x^{(k)}$ such that $k \neq i$ and $k \neq j$. This can be seen by replacing the kth column of $\mathcal{D}$ by the difference of its ith and jth columns; this new matrix $\mathcal{D}_{i,j,k}$ evidently has determinant zero. Expanding the determinant of $\mathcal{D}_{i,j,k}$ by minors of the kth column shows that $x^{(k)}$ lies on $H_{i,j}$.

There is a natural family of $n \times n$ skew-symmetric matrices attached to any element $\alpha \in R$ that can be used to describe these hyperplanes as well as certain higher degree hypersurfaces vanishing on various points of X_R. Given any $n \times n$ symmetric matrix $\Lambda = (\lambda_{ij})$, define the $n \times n$ skew-symmetric matrix $M_\Lambda = M_\Lambda(\alpha)$ by

$$\mathrm{M}_\Lambda = (m_{ij}) = \Big(\lambda_{ij}\big(\alpha^{(i)} - \alpha^{(j)}\big)\Big)\,. \tag{4}$$

If we write $\alpha = t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}$, then we may view $M_\Lambda = M_\Lambda(t_1, \ldots, t_{n-1})$ as an $n \times n$ skew-symmetric matrix of linear forms in $t_1, \ldots, t_{n-1}$. If we now allow the variables $t_1, \ldots, t_{n-1}$ to take values in $\mathbb{C}$, then the various sub-Pfaffians[1] of M_Λ give interesting functions on $\mathbb{P}^{n-2}_{\mathbb{C}}$ that vanish on some or all points in $\{x^{(1)}, \ldots, x^{(n)}\}$.

For example, the 2×2 sub-Pfaffians of M_Λ are simply multiples of the linear functionals (3), and they vanish on the $n-2$-sized subsets of $X =$

[1]Recall that the Pfaffian is a canonical square root of the determinant of a skew-symmetric matrix of even size. By sub-Pfaffians, we mean the Pfaffians of principal submatrices of even size.

$\{x^{(1)}, \dots, x^{(n)}\}$. (Note that $\binom{n}{2}$, the number of 2×2 sub-Pfaffians of M_Λ, equals $\binom{n}{n-2}$, the number of $n-2$-sized subsets of X.)

Similarly, the 4×4 sub-Pfaffians (when $n \geq 4$) are seen to yield quadrics that vanish on all of X. In general, the $2m \times 2m$ sub-Pfaffians of M_Λ ($m \geq 2$) yield degree m forms vanishing on X.

The special cases $n = 2, 3, 4$, and 5 give hints as to how orders in small degree number fields—and, more generally, rings of small rank—should be parametrized:

$\underline{n = 2}$: Write $R = \langle 1, \alpha_1 \rangle$. Then

$$M_\Lambda = \begin{bmatrix} 0 & \lambda_{12}\big(\alpha_1^{(1)} - \alpha_1^{(2)}\big) \\ \lambda_{12}\big(\alpha_1^{(2)} - \alpha_1^{(1)}\big) & 0 \end{bmatrix}. \tag{5}$$

The determinant of M_Λ (the square of its Pfaffian) is $\lambda_{12}^2\big(\alpha_1^{(1)} - \alpha_1^{(2)}\big)^2 = \lambda_{12}^2 \mathrm{Disc}(R)$. Setting $\lambda_{12} = 1$ gives $\mathrm{Disc}(R)$, and the correspondence $R \leftrightarrow \mathrm{Disc}(R)$ is precisely how quadratic rings are parametrized. (See [2] for a full treatment.)

$\underline{n = 3}$: Write $R = \langle 1, \alpha_1, \alpha_2 \rangle$. The only relevant sub-Pfaffians of M_Λ are again all 2×2, and are given by the linear forms

$$L_{ij}(t_1, t_2) = \lambda_{ij}\big[\big(\alpha_1^{(i)} - \alpha_1^{(j)}\big)t_1 + \big(\alpha_2^{(i)} - \alpha_2^{(j)}\big)t_2\big] \tag{6}$$

for $(i, j) = (1, 2)$, $(1, 3)$, and $(2, 3)$. This information can be put together by forming their product cubic form

$$f(t_1, t_2) = L_{12}L_{13}L_{23}, \tag{7}$$

and indeed this is the smallest degree form vanishing on all points of X. Choosing Λ so that $\lambda_{12}\lambda_{13}\lambda_{23} = 1/\sqrt{\mathrm{Disc}(R)}$, we obtain precisely the binary cubic form f_R corresponding to R under the Delone-Faddeev parametrization. One checks that $f_R(t_1, t_2)$ is an integral cubic form, and $\mathrm{Disc}(f_R) = \mathrm{Disc}(R)$. (See [3] for a full treatment.)

$\underline{n = 4}$: Let $R = \langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$. We now must consider both the 2×2 and 4×4 sub-Pfaffians of M_Λ. The 2×2 sub-Pfaffians are linear forms that correspond to lines in $\mathbb{P}^2$ passing through pairs of points of $X = \{x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}\}$. The smallest degree form vanishing on all points of X has degree 2, and one such quadratic form is given by the 4×4 Pfaffian of M_Λ, for any fixed choice of Λ. However, for any four points in $\mathbb{P}^2$ in general position, there is a two-dimensional space of quadrics passing through them. Thus to obtain a spanning set for the quadratic forms vanishing on X, we must choose two different Λ's, say Λ and Λ'.

Let $S = \langle 1, \omega, \theta \rangle$ be a cubic resolvent of R in the sense of [4]. Choose Λ so that

$$\lambda_{12}\lambda_{34} = \omega^{(1)}/\sqrt{\mathrm{Disc}(R)},\ \ \lambda_{13}\lambda_{24} = \omega^{(2)}/\sqrt{\mathrm{Disc}(R)},\ \text{and}$$
$$\lambda_{14}\lambda_{23} = \omega^{(3)}/\sqrt{\mathrm{Disc}(R)},$$

and Λ' so that

$$\lambda'_{12}\lambda'_{34} = \theta^{(1)}/\sqrt{\mathrm{Disc}(R)},\ \ \lambda_{13}\lambda_{24} = \theta^{(2)}/\sqrt{\mathrm{Disc}(R)},\ \text{and}$$
$$\lambda'_{14}\lambda'_{23} = \theta^{(3)}/\sqrt{\mathrm{Disc}(R)}.$$

Let A and B denote the quadratic forms $\mathrm{Pfaff}(M_\Lambda)$ and $\mathrm{Pfaff}(M_{\Lambda'})$ respectively. Then (A, B) is precisely the pair of ternary quadratic forms corresponding to R (and S) in the parametrization of quartic rings laid down in [4]. One may check directly that these choices of Λ and Λ' yield integral A and B such that $\mathrm{Disc}(A, B) = \mathrm{Disc}(\mathrm{Det}(Ax - By)) = \mathrm{Disc}(R)$. (For the full theory behind this case, see [4].)

$\underline{\boldsymbol{n = 5}}$: Finally, let $R = \langle 1, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$. We again examine first the 2×2 sub-Pfaffians of M_Λ. There are ten of them, and they correspond to the planes in $\mathbb{P}^3$ going through the various 3-point subsets of $X = \{x^{(1)}, \ldots, x^{(5)}\}$. Next, there are five 4×4 sub-Pfaffians, which for generic[2] choices of Λ are linearly independent; we fix such a Λ. Then the five 4×4 sub-Pfaffians of M_Λ cut out quadric surfaces passing through all five points of X. In fact, for any five points in $\mathbb{P}^3$ in general position, a counting argument shows that there is exactly a five-dimensional family of quaternary quadratic forms vanishing at the five points. Moreover, one finds that the set of common zeros of this five-dimensional family of quadratic forms consists only of these five points. Since all sets of five points in general position in $\mathbb{P}^3_{\mathbb{C}}$ are projectively equivalent, it suffices to check the latter assertion at any desired set of five points in general position in $\mathbb{P}^3_{\mathbb{C}}$.

Now consider the natural left action of the group $\mathrm{GL}_4(\mathbb{C}) \times \mathrm{GL}_5(\mathbb{C})$ on the space $V = \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ of 5×5 skew-symmetric matrices of quaternary linear forms. It is known that this representation is a *prehomogeneous vector space* (see Sato-Kimura [14]), i.e., it posseses a single Zariski-open orbit. This may be seen in an elementary manner as follows. First, note that the action of $\mathrm{GL}_4(\mathbb{C})$ on the orbit of M_Λ in V results in an action of $\mathrm{PGL}_4(\mathbb{C})$ on $\mathbb{P}^3_{\mathbb{C}}$, thereby moving around the set X of five points $x^{(1)}, \ldots, x^{(5)} \in \mathbb{P}^3_{\mathbb{C}}$ where the five 4×4 sub-Pfaffians vanish. Meanwhile, the group $\mathrm{GL}_5(\mathbb{C})$ acts on the vector consisting of the five 4×4 signed sub-Pfaffians by essentially the dual of the standard representation. More precisely, for $v \in V$ define the ith 4×4

[2]More precisely, Λ is "generic" if $F(\Lambda) \neq 0$ for a certain fixed polynomial F in the entries of Λ; see Section 4 for an explicit expression for F.

signed sub-Pfaffian Q_i of v to be $(-1)^{i+1}$ times the Pfaffian of the 4×4 principal submatrix obtained from v by removing its ith row and column. If $g \in \mathrm{GL}_5(\mathbb{C})$, $v \in V$, and Q_1, ..., Q_5 and Q_1', ..., Q_5' denote the 4×4 signed sub-Pfaffians of v and $g \cdot v$ respectively, then we have

$$\begin{bmatrix} Q_1' \\ \vdots \\ Q_5' \end{bmatrix} = (\det g)(g^{-1})^t \begin{bmatrix} Q_1 \\ \vdots \\ Q_5 \end{bmatrix}. \tag{8}$$

Now $\mathrm{PGL}_4(\mathbb{C})$ acts simply transitively on (ordered) sequences $x^{(1)}, \ldots, x^{(5)}$ of five points in general position in $\mathbb{P}^3$, while $\mathrm{SL}_5(\mathbb{C})$ acts simply transitively on bases $\langle Q_1, Q_2, \ldots, Q_5\rangle$ (up to scaling) of the five-dimensional space of quaternary quadratic forms vanishing on $X = \{x^{(1)}, \ldots, x^{(5)}\}$. We conclude that the stabilizer of M_Λ in $\mathrm{GL}_4(\mathbb{C}) \times \mathrm{SL}_5(\mathbb{C})$ is contained in the symmetric group $S_5 = \mathrm{Perm}(X)$, the permutation group of X. Indeed, the only way to send M_Λ to itself via an element of $\mathrm{GL}_4(\mathbb{C}) \times \mathrm{SL}_5(\mathbb{C})$ is to permute the five points in X via an element $\gamma_4 \in \mathrm{SL}_4(\mathbb{C})$; then to apply the unique element $\gamma_5 \in \mathrm{SL}_5(\mathbb{C})$ that returns the basis of 4×4 signed sub-Pfaffians $Q_1, \ldots, Q_5$ to what it was at the outset, up to a possible scaling factor; and finally to multiply by the unique scalar $\gamma_1 \in \mathbb{C}^*$ that returns the quadruple of 5×5 skew-symmetric matrices to its original value M_Λ. Thus the element $(\gamma_1\gamma_4, \gamma_5) \in \mathrm{GL}_4(\mathbb{C}) \times \mathrm{SL}_5(\mathbb{C})$, if it exists, is uniquely determined by the chosen permutation in $\mathrm{Perm}(X)$. It follows that the stabilizer of M_Λ is contained in $S_5 = \mathrm{Perm}(X)$, and a calculation shows that the stabilizer is in fact the full symmetric group S_5. Since the dimension of the group $G(\mathbb{C}) = \mathrm{GL}_4(\mathbb{C}) \times \mathrm{SL}_5(\mathbb{C})$ is $16 + 24 = 40$, as is the dimension of its representation $V = \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$, and since the stabilizer is finite, we conclude that there must be an open orbit for the group action. We call an element $A \in V$ *nondegenerate* if it lies in this open orbit.

In particular, we see now that any element v in $V = \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ in this open orbit possesses 4×4 sub-Pfaffians that intersect in five points in general position in $\mathbb{P}^3$. Conversely, since any five points in $\mathbb{P}^3$ in general position are projectively equivalent, a five-dimensional family of quadrics in $\mathbb{P}^3$ will intersect in five points in general position if and only if the family arises as the span of the five 4×4 sub-Pfaffians of a 5×5 skew-symmetric matrix of quaternary linear forms lying in this open orbit in V. Hence the open orbit of the space $V = \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ of 5×5 skew-symmetric matrices of linear forms in four variables parametrizes the smallest degree hypersurfaces passing through sets X of five points in general position in $\mathbb{P}^3_{\mathbb{C}}$, together with a chosen basis of the (five-dimensional) space of quaternary quadratic forms vanishing on X.

Thus the situation is completely analogous to the previous parametrizations of n points in $\mathbb{P}^{n-2}$ with $n \le 4$, and so we may expect that the integral points of this space, $V_{\mathbb{Z}} = \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, should parametrize quintic rings.

Therefore our goal, following the previous cases, is to find for any nondegenerate quintic ring R an integral element $A \in V_{\mathbb{Z}} = \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ whose 4×4 sub-Pfaffians vanish on $x_R^{(1)}, \ldots, x_R^{(5)}$, and whose discriminant $\mathrm{Disc}(A)$ (to be defined) is equal to $\mathrm{Disc}(R)$. Conversely, we wish to show that the 4×4 sub-Pfaffians of any nondegenerate element $A \in V_{\mathbb{Z}}$ vanish at the five points $x_R^{(1)}$, $\ldots$, $x_R^{(5)} \in \mathbb{P}^3_{\mathbb{C}}$ for some quintic ring R satisfying $\mathrm{Disc}(R) = \mathrm{Disc}(A)$.

This is precisely what is accomplished in the sections that follow. We begin by examining more closely the invariant theory of the action of $\Gamma = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ on $V_{\mathbb{Z}} = \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$.

3. The fundamental Γ-invariant $\mathrm{Disc}(A_1, A_2, A_3, A_4)$

Let us write elements $A \in V_{\mathbb{Z}}$ as quadruples $A = (A_1, A_2, A_3, A_4)$ of 5×5 skew-symmetric matrices over the integers, with the understanding that when we speak of the 4×4 sub-Pfaffians of A, we are referring to the five sub-Pfaffians $Q_1, \ldots, Q_5$ of the single 5×5 skew-symmetric matrix $A_1t_1 + A_2t_2 + A_3t_3 + A_4t_4$.

It is known (see Sato-Kimura [14]) that the action of Γ on $V_{\mathbb{Z}}$ has a single polynomial invariant, which we call the *discriminant* in analogy with our previous terminology in [2]–[4]. This discriminant function has degree 40. As always, we scale the discriminant polynomial $\mathrm{Disc}(\,\cdot\,)$ on $V_{\mathbb{Z}}$ so that it has relatively prime integral coefficients. This only determines $\mathrm{Disc}(\,\cdot\,)$ up to sign, but our choice of sign (and the fact that such a scaling exists) will become clear in the next section, where we construct the discriminant polynomial explicitly. It follows from Sato and Kimura's analysis (and will also follow from our work in Section 4) that an element $A \in V_{\mathbb{Z}}$ is *nondegenerate* precisely when its discriminant is nonzero. We will be primarily interested in the nongedenerate elements of $V_{\mathbb{Z}}$, as they will turn out to correspond to the nondegenerate quintic rings, i.e., those that embed as orders in étale quintic extensions of $\mathbb{Q}$.

4. The multiplication table for quintic rings

Let R be any nondegenerate quintic ring, and let $x^{(1)}, \ldots, x^{(5)}$ be the corresponding points in $\mathbb{P}^3$ as constructed in Section 2. Since up to scaling there is only a single $\mathrm{SL}_5(\mathbb{C})$-orbit of points $A \in V = \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ whose five independent 4×4 sub-Pfaffians vanish on the five points $x^{(1)}, \ldots, x^{(5)}$, the structure coefficients of multiplication in R should also depend, at least up to scaling, only on the SL_5-invariants of the points in this orbit. We therefore wish to construct, and understand the meaning of, the various invariants for the action of $\mathrm{SL}_5(\mathbb{C})$ on V.

First, let us turn to the construction of all the SL_5-invariants, which is quite pretty. Given a point $A = (A_1, A_2, A_3, A_4) \in V$, let M_1, M_2, and M_3

be any three fixed linear combinations of the skew-symmetric 5×5 matrices A_1, A_2, A_3, A_4. Then the Pfaffian of the 10×10 skew-symmetric matrix

$$\begin{bmatrix} M_1 & M_2 \\ M_2 & M_3 \end{bmatrix} \tag{9}$$

is clearly an SL_5-invariant of A, for the action of an element $g \in \mathrm{SL}_5(\mathbb{C})$ on A results in the action of $\left(\begin{smallmatrix} g & \\ & g \end{smallmatrix}\right)$ on the 10×10 skew-symmetric form $\left[\begin{smallmatrix} M_1 & M_2 \\ M_2 & M_3 \end{smallmatrix}\right]$, and hence the value of its Pfaffian does not change. The Pfaffians

$$\mathrm{Pfaff} \begin{bmatrix} M_1 & M_2 \\ M_2 & M_3 \end{bmatrix} \tag{10}$$

are our prototypical SL_5-invariants. In fact, it is not too difficult to show that, over $\mathbb{C}$, all polynomial invariants for $\mathrm{SL}_5(\mathbb{C})$ must be polynomials in these degree 5 Pfaffians! However, we shall not need this fact in what follows, and so we omit the proof.

Next, we would like to understand the meaning of these SL_5-invariants in terms of an appropriate quintic ring R. Let R again be a nondegenerate quintic ring having $\mathbb{Z}$-basis $\langle 1, \alpha_1, \ldots, \alpha_4 \rangle$, let $x^{(1)}, \ldots, x^{(5)}$ be the associated points in $\mathbb{P}^3$ as in Section 2, and denote by $A = (A_1, A_2, A_3, A_4)$ an element of V whose independent 4×4 sub-Pfaffians vanish on $X = \{x^{(1)}, \ldots, x^{(5)}\}$. As remarked earlier, in studying the above SL_5-invariants of A, it suffices to consider the SL_5-invariants of any element $M \in V$ in the same $\mathrm{SL}_5(\mathbb{C})$-orbit of A, or any scalar multiple of such an element. In particular, we may assume that A takes the form $M_\Lambda \in V$ as constructed in Section 2, where $\Lambda = (\lambda_{ij})$ is any generic 5×5 symmetric matrix, to be chosen later.

More precisely, given $\alpha \in R = \langle 1, \alpha_1, \ldots, \alpha_4 \rangle$, denote by $M(\alpha)$ the 5×5 skew-symmetric matrix $\big(\lambda_{ij}(\alpha^{(i)} - \alpha^{(j)})\big)$. Then we have noted in Section 2 that the 4×4 sub-Pfaffians of $M_\Lambda = (M(\alpha_1), \ldots, M(\alpha_4)) \in V$ vanish at the desired points $x_R^{(1)}, \ldots, x_R^{(5)}$. Thus we may consider the SL_5-invariants of M_Λ, which are generated by the Pfaffians $\mathrm{Pfaff} \left[\begin{smallmatrix} M(x) & M(y) \\ M(y) & M(z) \end{smallmatrix}\right]$ for $x, y, z \in R$.

For any 5×5 skew-symmetric matrices X, Y, Z, let us write $\mathrm{Pf}(X, Y, Z) = \mathrm{Pfaff} \left[\begin{smallmatrix} X & Y \\ Y & Z \end{smallmatrix}\right]$, and set

$$P^+(X, Y, Z) = \frac{\mathrm{Pf}(X, Y, Z) + \mathrm{Pf}(X, Y, -Z)}{2}, \tag{11}$$

$$P^-(X, Y, Z) = \frac{\mathrm{Pf}(X, Y, Z) - \mathrm{Pf}(X, Y, -Z)}{-2}. \tag{12}$$

Then one checks that $P^+(X, Y, Z)$ and $P^-(X, Y, Z)$ are primitive integer polynomials in the entries of X, Y, Z having homogeneous degrees 2,1,2 and 1,3,1 respectively. By construction, the integer polynomials $P^\pm(M(x), M(y), M(z))$ for $x, y, z \in R$ are SL_5-invariants of M_Λ.

There is an alternative description of these invariants P^+ and P^- which is also quite appealing. Given a 5×5 skew-symmetric matrix X, let $Q(X)$ denote as before the column vector $[Q_1, \dots, Q_5]^t$ of (signed) 4×4 sub-Pfaffians of X. Then Q is evidently a quadratic form on the vector space of 5×5 skew-symmetric matrices. Let $Q(X, Y)$ denote the corresponding symmetric bilinear form such that $Q(X, X) = 2Q(X)$. Then we have

$$P^+(X, Y, Z) = \quad Q(X)^t \cdot Y \cdot Q(Z), \tag{13}$$

$$P^-(X, Y, Z) = Q(X, Y)^t \cdot Y \cdot Q(Y, Z). \tag{14}$$

More generally, for any 5×5 skew-symmetric matrices U, W, X, Y, Z, we have the SL_5-invariants $P(U, W, X, Y, Z) = Q(U, W)^t \cdot X \cdot Q(Y, Z)$, although it is easy to see that these invariants may also be expressed purely in terms of P^+ (or P^-).

Finally, let $F(\Lambda)$ denote the following integral degree five polynomial in the entries of Λ:

$$F(\Lambda) = \frac{-1}{10} \sum_{i,j,k,\ell,m} \sigma(ijk\ell m) \cdot \lambda_{ij}\lambda_{jk}\lambda_{k\ell}\lambda_{\ell m}\lambda_{mi}, \tag{15}$$

where we have used $\sigma(ijk\ell m)$ to denote the sign of the permutation (i, j, k, ℓ, m) of $(1, 2, 3, 4, 5)$. The polynomial F has a rather natural interpretation in terms of Figure 1 (p. 72), which will play a critical role in the sequel. We observe that Figure 1 shows six of the twelve ways of connecting five points $1, \dots, 5$ by a 5-cycle, the other six being the complements of these graphs in the complete graph on five vertices. The negation of the polynomial $F(\Lambda)$ can be expressed as the sum of twelve terms: six terms of the form $\lambda_{ij}\lambda_{jk}\lambda_{k\ell}\lambda_{\ell m}\lambda_{mi}$, where $(ijklm)$ ranges over the six cycles occurring in Figure 1; and six terms of the form $-\lambda_{ij}\lambda_{jk}\lambda_{k\ell}\lambda_{\ell m}\lambda_{mi}$, where $(ijklm)$ ranges over the complements of these six cycles. (For further details on Figures 1 and 2, see Section 5.2.)

We have the following beautiful identities:

LEMMA 4. *For $x, y, z \in R$, we have*

(a) $P^+(M(x), M(y), M(z))$

$$= F(\Lambda) \cdot \begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ x^{(1)} & x^{(2)} & x^{(3)} & x^{(4)} & x^{(5)} \\ y^{(1)} & y^{(2)} & y^{(3)} & y^{(4)} & y^{(5)} \\ z^{(1)} & z^{(2)} & z^{(3)} & z^{(4)} & z^{(5)} \\ x^{(1)}z^{(1)} & x^{(2)}z^{(2)} & x^{(3)}z^{(3)} & x^{(4)}z^{(4)} & x^{(5)}z^{(5)} \end{vmatrix};$$

(b) $P^-(M(x), M(y), M(z))$

$$= F(\Lambda) \cdot \begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ x^{(1)} & x^{(2)} & x^{(3)} & x^{(4)} & x^{(5)} \\ y^{(1)} & y^{(2)} & y^{(3)} & y^{(4)} & y^{(5)} \\ z^{(1)} & z^{(2)} & z^{(3)} & z^{(4)} & z^{(5)} \\ (y^{(1)})^2 & (y^{(2)})^2 & (y^{(3)})^2 & (y^{(4)})^2 & (y^{(5)})^2 \end{vmatrix}.$$

Proof. Direct multiplication. □

Lemma 4 may be viewed as the quintic analogue of the identities we presented for the quartic case in [4, Lemma 9]. In particular, the lemma allows us to completely regain the multiplicative structure of R from the SL_5-invariants P^+ and P^- of A.

First, we may assume that $\langle 1, \alpha_1, \ldots, \alpha_4 \rangle$ is a *normal* basis for R, by which we mean that $\alpha_1, \ldots, \alpha_4$ have been translated by integers so that the coefficients of α_1 and α_2 in $\alpha_1\alpha_2$ and the coefficients of α_3 and α_4 in $\alpha_3\alpha_4$ are each equal to zero. Now let us write

$$\alpha_i\alpha_j = c_{ij}^0 + \sum_{k=1}^{4} c_{ij}^k \alpha_k \tag{16}$$

for $1 \le i \le j \le 4$. Our normal basis assumption implies that

$$c_{12}^1 = c_{12}^2 = c_{34}^3 = c_{34}^4 = 0. \tag{17}$$

We choose to normalize bases because bases of $R/\mathbb{Z}$ then lift uniquely to normalized bases of R.

We wish to express the structure coefficients c_{ij}^k in terms of the various SL_5-invariants of the quadruple $(M(\alpha_1), \ldots, M(\alpha_4))$ of skew-symmetric 5×5 matrices. For simplicity let us write $A_j = M(\alpha_j)$. Also, for $i, j, k, \ell, m \in \{1, 2, 3, 4\}$, let us use the shorthand

$$\{ijk\ell m\} = Q(A_i, A_j)^t \cdot A_k \cdot Q(A_\ell, A_m) \tag{18}$$

for the various SL_5-invariants of $A = (A_1, A_2, A_3, A_4) \in V$. Note that if $i = j$ or $\ell = m$ then the integral polynomial invariant $\{ijk\ell m\}$ is a multiple of 2; moreover, if both $i = j$ and $\ell = m$ then $\{ijk\ell m\}$ is a multiple of 4.

With this notation, it is easy to see using Lemma 4 that

$$c_{13}^4 = \frac{\{11233\}}{4 \cdot F(\Lambda)\sqrt{\mathrm{Disc}(R)}} \tag{19}$$

while

$$c_{22}^4 = \frac{\{12223\}}{F(\Lambda)\sqrt{\mathrm{Disc}(R)}}; \tag{20}$$

here $\sqrt{\mathrm{Disc}(R)}$ denotes the square root $\det \mathcal{D}$ of $\mathrm{Disc}(R)$, where $\mathcal{D}$ is given as in (1). Thus we see that these c_{ij}^k are defined, as expected, up to an overall scaling factor depending on Λ. In order to render the c_{ij}^k primitive integer polynomials purely in the entries of $A \in V$ (analogous to the cubic and quartic cases), we choose Λ so that $F(\Lambda) = 1/\sqrt{\mathrm{Disc}(R)}$. This gives $c_{13}^4 = \frac{\{11233\}}{4}$ and $c_{22}^4 = \{12223\}$, both now primitive integer polynomials in the entries of A.

In general, we now find that for any permutation (i,j,k,ℓ) of $(1,2,3,4)$, we have

$$\begin{aligned} c_{ij}^k &= \pm\{ii\ell jj\}/4, \\ c_{ii}^j &= \pm\{\ell iiik\}, \\ c_{ij}^j - c_{ik}^k &= \pm\{jk\ell ii\}/2, \\ c_{ii}^i - c_{ij}^j - c_{ik}^k &= \pm\{ij\ell ki\}, \end{aligned} \tag{21}$$

where we have used $\pm$ to denote the sign of the permutation (i,j,k,ℓ) of $(1,2,3,4)$. The normalizing conditions (17) then determine all c_{ij}^k (for $k \neq 0$) as primitive integer polynomials in the entries of A.

The remaining constant coefficients c_{ij}^0 can also now be uniquely expressed as polynomials in the entries of A, using the associative law in R. Indeed, computing the expressions $(\alpha_i\alpha_j)\alpha_k$ and $\alpha_i(\alpha_j\alpha_k)$ using (16), and then equating the coefficients of α_k, yields the equality

$$c_{ij}^0 = \sum_{r=1}^{4} \left(c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k \right) \tag{22}$$

for any $k \in \{1,2,3,4\} \setminus \{i\}$. One checks using the explicit expressions in (21) that the right-hand side of (22) is a polynomial expression in the entries of A that is independent of k. We have thus recovered all structure coefficients of R in terms of the SL_5-invariants $\{ijklm\}$ of the quadruple $(A_1, \ldots, A_4)$ of 5×5 skew-symmetric matrices.

Now suppose $A \in V_{\mathbb{Z}}$ is any element. Then we may naturally attach to A the set $\{c_{ij}^k\}$ of SL_5-invariants of A, where the $c_{ij}^k = c_{ij}^k(A)$ are defined by (17), (21) and (22). With these values of c_{ij}^k, we may then naturally form a ring with $\mathbb{Z}$-basis $\langle 1, \alpha_1, \ldots, \alpha_4 \rangle$ and multiplicative structure given by (16); one checks that all relations among the c_{ij}^k implied by the associative law are satisfied. Hence given any $A \in V_{\mathbb{Z}}$ we obtain in a natural way a corresponding quintic ring with a $\mathbb{Z}$-basis. We denote the resulting ring, whose (normalized) multiplicative structure coefficients c_{ij}^k are given as in (17), (21), and (22), by $R(A) = R_{\mathbb{Z}}(A)$.[3]

[3]More generally, given an element $A \in V_T = T^4 \otimes \wedge^2 T^5$ for any base ring T, we may analogously attach to A a quintic T-algebra $R_T(A)$ via the same relations, since there is a unique ring homomorphism $\mathbb{Z} \to T$ for any ring T. Although our main case of interest here is of course $T = \mathbb{Z}$, we will also have occasions to consider $T = \mathbb{Q}$, $\mathbb{F}_p$, $\mathbb{Q}_p$, $\mathbb{R}$, and $\mathbb{C}$.

It is easy to determine the multiplication structure of $R(A)$ for $A \in V_{\mathbb{Z}}$ also in terms of nonnormalized bases. If each basis element $\alpha_i \in R(A)$ is translated by some integer m_i, then the structure constants of the form c_{ij}^j $(j \neq i)$ will be translated by m_i, while c_{ii}^i will be translated by $2m_i$. Thus the expressions on the left side of (21) will remain unchanged. Conversely, it is immediately seen that any integer values assigned to the constants c_{ij}^k satisfying the system (21) must arise by translations of the basis elements α_i by some integers m_i. Therefore, the multiplication table of $R(A)$ in terms of a general basis $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ is given by (16), where the set $\{c_{ij}^k\}$ denotes *any* integer solution to the system of equations (21) and (22). Thus we have obtained a general description of the multiplication table of $R(A)$ in terms of any $\mathbb{Z}$-basis $\langle 1, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ of $R(A)$ (not necessarily normalized).

Since the values of the structure constants of the ring $R(A)$ are given in terms of integer polynomials in the entries of A, the discriminant of the ring $R(A)$ also then becomes a polynomial with integer coefficients in the entries of A. As $\mathrm{Disc}(\mathbb{Z}^5) = 1$, Theorem 17 in Section 11 (with $R = \mathbb{Z}^5$) implies that the polynomial $\mathrm{Disc}(R(A))$ takes the value 1 at some element in $V_{\mathbb{Z}}$, and so in particular this polynomial must have relatively prime coefficients. In addition, the polynomial $\mathrm{Disc}(R(A))$ is evidently Γ-invariant and of degree 40; therefore, we must in fact have $\mathrm{Disc}(A) = \mathrm{Disc}(R(A))$, at least up to sign. We define $\mathrm{Disc}(A) = \mathrm{Disc}(R(A))$. (This naturally fixes the sign of $\mathrm{Disc}(A)$ which was left ambiguous in Section 3.)

We have remarked earlier that the vector space of SL_5-invariants of degree 5 on V is spanned by the various expressions P^+ or P^-. This can be proved, e.g., by computing, via the theory of weights, the number of copies of the trivial representation inside the representation $\mathrm{Sym}^5((\wedge^2\mathbb{C}^5)^{\oplus 4})$ of $\mathrm{SL}_5(\mathbb{C})$; this number turns out to be 36. Meanwhile, one can also check that the vector space of polynomials spanned by the invariants P^+ (or P^-) is 36-dimensional. It follows that the invariants $P^{\pm}$ span all SL_5-invariants of degree 5 on V. On the other hand, a glance at (16) and (17) shows that there are 36 nonzero values among the c_{ij}^k (after normalization) with $k > 0$, and, as these are seen to be linearly independent, they must also span the same 36-dimensional space. Consequently, we may also express the SL_5-invariants of A entirely in terms of the expressions $c_{ij}^k = c_{ij}^k(A)$, whose values are given by (17) and (21).

Now suppose two nondegenerate elements A, A' in $V_{\mathbb{Z}}$ (or even in $V_{\mathbb{C}}$) have the identical SL_5-invariants, i.e., $c_{ij}^k(A) = c_{ij}^k(A')$ for all i, j, k. We claim that A and A' must then in fact be $\mathrm{SL}_5(\mathbb{C})$-equivalent. In other words, for nondegenerate elements of V, the SL_5-invariants determine the $\mathrm{SL}_5(\mathbb{C})$-orbit. To see this, note that an element $\gamma_4 \in \mathrm{GL}_4(\mathbb{C})$ acts on the SL_5-invariants of an element $A \in V$ simply by re-expressing the structure constants c_{ij}^k of the quintic $\mathbb{C}$-algebra $R_{\mathbb{C}}(A)$ with respect to the new γ_4-transformed basis. If such a change-of-basis of $R_{\mathbb{C}}(A)$ preserves the structure constants $c_{ij}^k(A)$,

then it corresponds to a $\mathbb{C}$-algebra automorphism of $R_{\mathbb{C}}(A)$. Since $R_{\mathbb{C}}(A)$ is an étale $\mathbb{C}$-algebra, as $\mathrm{Disc}(R_{\mathbb{C}}(A)) \neq 0$, we have $R_{\mathbb{C}}(A) \cong \mathbb{C}^5$, and it follows that the group of $\mathrm{GL}_4(\mathbb{C})$-transformations of A preserving all SL_5-invariants is isomorphic to $S_5 = \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}^5)$. Now we already know that the stabilizer of A in $\mathrm{GL}_4(\mathbb{C}) \times \mathrm{SL}_5(\mathbb{C})$ is isomorphic to S_5. We conclude that for each $\gamma_4 \in \mathrm{GL}_4(\mathbb{C})$ preserving the SL_5-invariants of A, there must be a unique corresponding element $\gamma_5 \in \mathrm{SL}_5(\mathbb{C})$ such that $(\gamma_4, \gamma_5) \cdot A = A$. In particular, any element A' that is $\mathrm{GL}_4(\mathbb{C}) \times \mathrm{SL}_5(\mathbb{C})$-equivalent to A and also has the same SL_5-invariants as A must in fact lie in the same $\mathrm{SL}_5(\mathbb{C})$-orbit as A, proving the claim.

This has some important geometric consequences for nondegenerate elements $A \in V_{\mathbb{Z}}$. First, if $R = R(A)$, then the five 4×4 sub-Pfaffians of A must vanish at the five associated points $x_R^{(1)}, \ldots, x_R^{(5)} \in \mathbb{P}^3$ as constructed in Section 2. Indeed, we have seen that if A is nondegenerate then the SL_5-invariants of A uniquely determine its $\mathrm{SL}_5(\mathbb{C})$-orbit. Hence A is in the same $\mathrm{GL}_5(\mathbb{C})$-orbit as M_Λ (as constructed in Section 2) where $R = R(A)$ and Λ is any 5×5 symmetric matrix satisfying $F(\Lambda) \neq 0$, and the stated vanishing property follows.

Second, we may also now see that the nondegenerate points $A \in V$ (i.e., those points lying in the open orbit of the representation of $G = \mathrm{GL}_4(\mathbb{C}) \times \mathrm{SL}_5(\mathbb{C})$ on V) are precisely the elements $A \in V$ satisfying $\mathrm{Disc}(A) \neq 0$. Indeed, if $A \in V$ has nonzero discriminant, then the quintic $\mathbb{C}$-algebra $R_{\mathbb{C}}(A)$ also has nonzero discriminant so that the five points $x_R^{(1)}, \ldots, x_R^{(n)}$ where the 4×4 sub-Pfaffians of A vanish lie in general position in $\mathbb{P}^3_{\mathbb{C}}$. Hence A is in the open orbit of V.

In summary, to any element $A = (A_1, A_2, A_3, A_4) \in V_{\mathbb{Z}}$ we have associated a quintic ring $R = R(A)$ over $\mathbb{Z}$, given by (16), (17), (21), and (22), such that $\mathrm{Disc}(A) = \mathrm{Disc}(R)$. Furthermore, in the case that A (equivalently, R) is nondegenerate, we also have the geometric property that the five 4×4 sub-Pfaffians of A vanish at the five associated points $x_R^{(1)}, \ldots, x_R^{(5)} \in \mathbb{P}^3$.

In Section 11, we will prove that every nondegenerate quintic ring R in fact arises as $R(A)$ for some $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. But what is the meaning of the integers that occur as the entries of the matrices $A_1, \ldots, A_4$? And what is the meaning of the five quadratic mappings that arise as the five 4×4 sub-Pfaffians of A? A theory of the space $V_{\mathbb{Z}}$ could not be complete without understanding what the very entries of the A_i mean in terms of the corresponding quintic ring $R(A)$. In [4] we answered the analogous questions for cubic and quartic rings by developing a theory of *resolvent rings* (quadratic resolvent rings in the case of cubic rings, and cubic resolvent rings in the case of quartic rings). Carrying out the analogous program for quintic rings yields the notion of *sextic* resolvent rings, to which we turn next.

5. Sextic resolvents of a quintic ring

The theory of sextic resolvents is very beautiful, and involves heavily the combinatorics of the numbers 5 and 6.

5.1. *The S_5-closure of a ring of rank 5.* To begin, we recall briefly the notion of S_k-closure of a ring. Let R be a ring of rank k with nonzero discriminant. Then the S_k-closure of R, denoted $\bar{R}$, is defined to be $R^{\otimes k}/I_R$, where I_R is the $\mathbb{Z}$-closure of the ideal in $R^{\otimes k}$ generated by all elements in $R^{\otimes k}$ of the form

$$(x \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes x \otimes \cdots \otimes 1) + \cdots + (1 \otimes 1 \otimes \cdots \otimes x) \\ - \mathrm{Tr}_{\mathbb{Z}}^{R}(x)(1 \otimes 1 \otimes \cdots \otimes 1)$$

for $x \in R$. (The $\mathbb{Z}$-closure of an ideal J in a ring R' is the set of all elements $x \in R'$ such that $nx \in J$ for some $n \in \mathbb{Z}$.)

When R is a quintic ring of nonzero discriminant, the S_k-closure construction yields a ring $\bar{R}$ of rank 120, and the group S_5 acts naturally as a group of automorphisms of $\bar{R}$ via permutation of the tensor factors. Thus the ring $\bar{R}$ may be viewed as an integral model of "Galois closure". The ring R embeds naturally into $\bar{R}$ in five different (conjugate) ways, via the maps $x \to x \otimes 1 \otimes \cdots \otimes 1$, ..., $x \to 1 \otimes 1 \otimes \cdots \otimes x$ respectively. We denote the images of these maps by $R^{(1)}$, ..., $R^{(5)}$ respectively, and identify R with $R^{(1)}$. The group S_5 acts on the five rings $R^{(i)}$ in the standard way, and the stabilizer of $R^{(i)}$ in S_5 is denoted by $S_4^{(i)}$.

The notion of sextic resolvent arises due to the existence of six fundamental index 6 subgroups $M^{(1)}, \ldots, M^{(6)}$ in S_5, called the *metacyclic* subgroups. Each of these subgroups is generated by a 5-cycle and a 4-cycle. For consistency with the sections that follow, we set $M^{(1)} = \langle (12345), (2354) \rangle$, $M^{(2)} = \langle (13254), (3245) \rangle$, while $M^{(2+i)}$ $(1 \le i \le 4)$ is obtained by conjugating $M^{(2)}$ by the 5-cycle $(12345)^i$. These six metacyclic groups form a set of conjugate subgroups.

For simplicity, we shall write $M = M^{(1)}$. The ring $\bar{R}^M$ fixed pointwise by the action of M is evidently a ring of rank 6 (i.e., a *sextic* ring), which we call the *sextic invariant ring* and denote $S^{\mathrm{inv}}(R)$. We will be looking for the sextic resolvent ring of R inside the sextic $\mathbb{Q}$-algebra $S^{\mathrm{inv}}(R) \otimes \mathbb{Q}$. In order to define it more precisely, we need to understand the combinatorics of M more closely.

5.2. *Six pentagons and a hexagon.* The complete graph on five vertices contains twelve 5-cycles. The symmetric group S_5 acts naturally on this set of twelve 5-cycles, and under this action, the unique S_5-orbit of twelve elements splits up into two A_5-orbits consisting of six elements each. One such A_5-orbit of 5-cycles is illustrated in Figure 1, while the other A_5-orbit can be obtained simply by taking the graph complements of the 5-cycles shown in Figure 1.

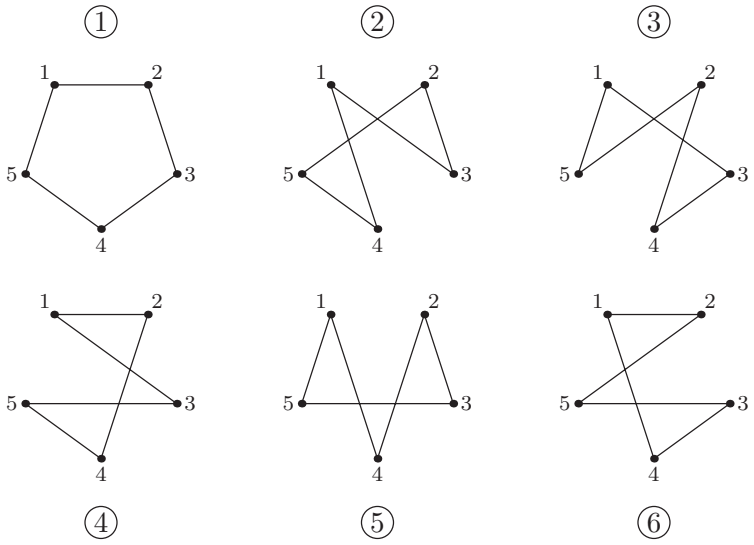

Figure 1: Six pentagons.

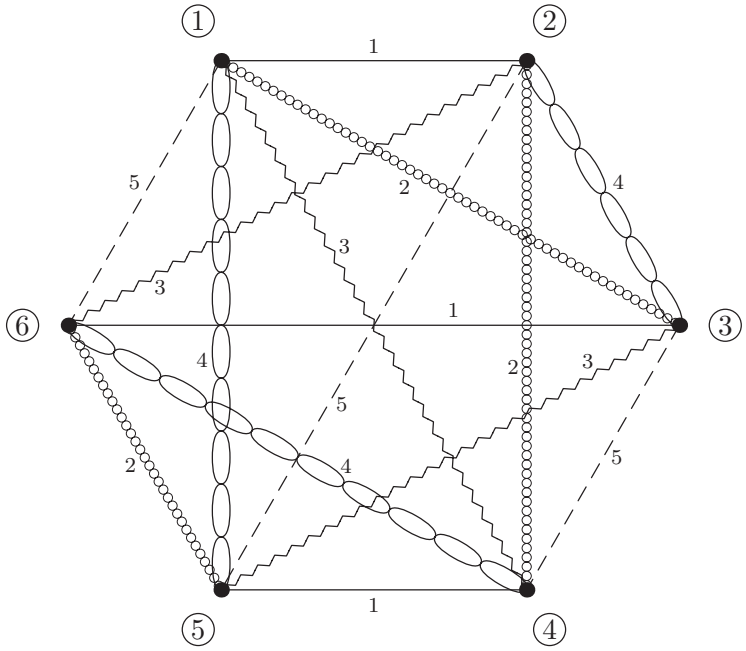

Figure 2: A hexagon.

Together these two A_5-orbits, viewed as six pairs of complementary graphs, yield the six ways of partitioning the complete graph on five vertices into pairs of 5-cycles. The subgroup $M^{(i)}$ of Section 5.1 may be viewed as the set of all elements in S_5 which map the 5-cycle in Figure 1ⓘ to either itself *or* its complement.

We observe that any two 5-cycles in Figure 1 share exactly two common edges; moreover, these two edges always involve four distinct vertices, so that there is exactly one vertex that neither edge passes through. For example, the 5-cycles labelled ① and ② in Figure 1 share precisely the edges $\overline{2\ 3}$ and $\overline{4\ 5}$ and thus involve the four distinct vertices 2, 3, 4 and 5. Vertex 1 does not arise. Hence in Figure 2, we label the edge connecting ① and ② by the number "1". In general, the edge connecting ⓘ and ⓙ in Figure 2 is labelled by the number of the unique vertex that does not lie on a common edge of the cycles labelled ⓘ and ⓙ in Figure 1. In this way, we obtain in Figure 2 a complete graph on six vertices whose 15 edges are labelled by numbers in the set $\{1, 2, \ldots, 5\}$, and where each of the 5 numbers occurs as the label of an edge exactly 3 times. Thus, for example, "1" occurs as the label on the three disjoint edges (①,②), (③,⑥), and (④,⑤). It is interesting to note that the process of obtaining Figure 2 from Figure 1 is completely reversible; i.e., up to taking the graph complements of ①,...,⑥, the 5-cycles labelled ①,...,⑥ in Figure 1 are completely determined by the labellings in Figure 2. In particular, the natural action of S_5 on the six elements ①,...,⑥ is completely determined by Figure 2.

In sum, the elements of $\{①, ②, ③, ④, ⑤, ⑥\}$ correspond to certain 5-cycles on the set $\{1, 2, 3, 4, 5\}$ (Fig. 1), while the elements of $\{1, 2, 3, 4, 5\}$ correspond to certain disjoint triples of pairs of elements in $\{①, ②, ③, ④, ⑤, ⑥\}$ (Fig. 2). These "dual" correspondences between the sets $\{1, 2, 3, 4, 5\}$ and $\{①, ②, ③, ④, ⑤, ⑥\}$ will play a central role in understanding the relationship between quintic rings and their sextic resolvents.

5.3. *The fundamental resolvent maps.* As indicated in [4], to develop the notion of a resolvent ring it is first necessary to have the correct notion of *resolvent map*. Although it turns out that many direct polynomial/tensorial maps exist between a quintic ring R and its sextic resolvent $S \subset S^{\mathrm{inv}}(R) \otimes \mathbb{Q}$ (to be defined), they are all of relatively high degree and considering them can give rise to unnecessary complications. The key insight is to note that the most basic and fundamental maps in fact involve the $\mathbb{Z}$-duals R^* and S^* of R and S respectively.

If R is a nondegenerate quintic ring, then we may explicitly realize R^* as a sublattice of $R \otimes \mathbb{Q}$ via the trace pairing $\langle x, y \rangle_R = \mathrm{Tr}^R_{\mathbb{Z}}(xy)$. Let $\langle \alpha_0^*, \alpha_1^*, \ldots, \alpha_4^* \rangle$ denote the dual basis of $\langle \alpha_0 = 1, \alpha_1, \ldots, \alpha_4 \rangle$ with respect to this pairing. As noted in Section 2, we have the formula $\alpha_i^* = \mathcal{D}_{i+1,1}/(\det \mathcal{D})$. Similarly, we may embed S^* as a lattice in $(\bar{R} \otimes \mathbb{Q})^M$ via the pairing $\langle x, y \rangle_S = \mathrm{Tr}^S_{\mathbb{Z}}(xy)$. Expres-

sions for the basis $\langle \beta_0^*, \beta_1^*, \dots, \beta_5^* \rangle$ of S^* dual to the basis $\langle \beta_0 = 1, \beta_1, \dots, \beta_5 \rangle$ of S may be given in an analogous manner.

The fundamental resolvent map is then a trilinear alternating mapping $f : S \times S \times S \to R^*$, given as follows. For $s \in S$, let $s^{(1)}, s^{(2)}, \dots, s^{(6)}$ denote the conjugates of s in $\bar{R} \otimes \mathbb{Q}$, labelled so that they are stabilized by $M^{(1)}, M^{(2)}, \dots, M^{(6)}$ respectively; then for any $x, y, z \in S$, define $f(x, y, z) \in R^*$ by

$$f(x,y,z) = \frac{1}{16 \cdot \mathrm{Disc}(R)} \begin{vmatrix} x^{(1)} - x^{(2)} & x^{(3)} - x^{(6)} & x^{(4)} - x^{(5)} \\ y^{(1)} - y^{(2)} & y^{(3)} - y^{(6)} & y^{(4)} - y^{(5)} \\ z^{(1)} - z^{(2)} & z^{(3)} - z^{(6)} & z^{(4)} - z^{(5)} \end{vmatrix}. \tag{23}$$

(The reasons behind the scaling factor $1/(16 \cdot \mathrm{Disc}(R))$ will become evident shortly.) One checks using Figures 1 and 2 that the value of the determinant in (23) does not change under the action of $S_4^{(1)} \subset S_5$. Hence $f(x, y, z)$ lies in $R^* \otimes \mathbb{Q} \subset \bar{R} \otimes \mathbb{Q}$. Our first requirement for S to be a sextic resolvent ring is that the image of f on $S \times S \times S$ lies not just in $R^* \otimes \mathbb{Q}$, but in R^* itself. That is, f is an alternating trilinear mapping from $S \times S \times S$ to R^*. (Note that f also naturally descends to a mapping $\bar{f} : S/\mathbb{Z} \times S/\mathbb{Z} \times S/\mathbb{Z} \to R^*$.)

Being fixed by $S_4^{(1)}$, the map $f(x, y, z)$ has five S_5-conjugate mappings $f^{(1)}(x, y, z) = f(x, y, z)$, $f^{(2)}(x, y, z), \dots, f^{(5)}(x, y, z)$ whose images lie in ${R^{(1)}}^* = R^*$, ${R^{(2)}}^*, \dots, {R^{(5)}}^*$ respectively. The mapping $f^{(k)}(x, y, z)$ can be obtained by applying the cycle (23456) $k - 1$ times to the superscript indices occurring in (23); for example, we have

$$f^{(2)}(x,y,z) = \frac{1}{16 \cdot \mathrm{Disc}(R)} \begin{vmatrix} x^{(1)} - x^{(3)} & x^{(4)} - x^{(2)} & x^{(5)} - x^{(6)} \\ y^{(1)} - y^{(3)} & y^{(4)} - y^{(2)} & y^{(5)} - y^{(6)} \\ z^{(1)} - z^{(3)} & z^{(4)} - z^{(2)} & z^{(5)} - z^{(6)} \end{vmatrix}. \tag{24}$$

Note that the pairs of superscripts occurring in the entries of the latter determinant correspond precisely to the edges labelled "2" in Figure 2.

An important observation regarding f is that, since

$$f^{(1)}(x,y,z) + f^{(2)}(x,y,z) + \cdots + f^{(5)}(x,y,z) = 0,$$

the image of f lies not only in R^*, but in fact lies in the distinguished four-dimensional sublattice $\widetilde{R} \subset R^*$ defined by

$$\widetilde{R} = \{x \in R^* : \langle 1, x \rangle_R = 0\} = \mathbb{Z}\alpha_1^* + \mathbb{Z}\alpha_2^* + \mathbb{Z}\alpha_3^* + \mathbb{Z}\alpha_4^*. \tag{25}$$

Indeed, $\widetilde{R}$ is canonically dual to the $\mathbb{Z}$-module $R/\mathbb{Z}$ via the trace pairing $\langle\ ,\ \rangle_R$. It follows that we may write

$$f(\beta_k, \beta_\ell, \beta_m) = a_{1k\ell m}^* \alpha_1^* + a_{2k\ell m}^* \alpha_2^* + a_{3k\ell m}^* \alpha_3^* + a_{4k\ell m}^* \alpha_4^* \tag{26}$$

for some set of forty integers $\{a_{rk\ell m}^*\}_{\substack{1 \le r \le 4 \\ 1 \le k < \ell < m \le 5}}$.

These forty integers naturally comprise a quadruple of quinary alternating 3-forms, i.e., an element of $\mathbb{Z}^4 \otimes \wedge^3\mathbb{Z}^5$. To obtain instead an element of $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, as considered in Sections 2–4, we observe that a trilinear alternating mapping $\bar{f} : S/\mathbb{Z} \times S/\mathbb{Z} \times S/\mathbb{Z} \to \widetilde{R}$ is equivalent to a bilinear alternating map $g : \widetilde{S} \times \widetilde{S} \to \widetilde{R}$, where

$$\widetilde{S} = \{x \in S^* : \langle 1, x\rangle_S = 0\} = \mathbb{Z}\beta_1^* + \mathbb{Z}\beta_2^* + \ldots + \mathbb{Z}\beta_5^* \tag{27}$$

is the $\mathbb{Z}$-module canonically dual to $S/\mathbb{Z}$ via the pairing $\langle\ ,\ \rangle_S$. It is possible to determine an explicit expression for g. For $w \in \widetilde{S}$, let $w^{(1)}, w^{(2)}, \ldots, w^{(6)}$ denote the S_5-conjugates of w in $\bar{R} \otimes \mathbb{Q}$, labelled again so that they are stabilized by $M^{(1)}, M^{(2)}, \ldots, M^{(6)}$ respectively. Then we find

$$g(u,v) \;=\; \frac{\sqrt{\mathrm{Disc}(S)}}{48 \cdot \mathrm{Disc}(R)} \cdot \begin{vmatrix} 1 & 1 & 1 \\ u^{(1)} + u^{(2)} & u^{(3)} + u^{(6)} & u^{(4)} + u^{(5)} \\ v^{(1)} + v^{(2)} & v^{(3)} + v^{(6)} & v^{(4)} + v^{(5)} \end{vmatrix} \tag{28}$$

where $\sqrt{\mathrm{Disc}(S)}$ is defined analogously to $\sqrt{\mathrm{Disc}(R)}$, namely, as $\det[(\beta_i^{(m)})_{\substack{0 \le i \le 5 \\ 1 \le m \le 6}}]$.

If we now write

$$g(\beta_i^*, \beta_j^*) = a_{1ij}\alpha_1^* + a_{2ij}\alpha_2^* + a_{3ij}\alpha_3^* + a_{4ij}\alpha_4^*\,, \tag{29}$$

then the set of forty integers $A = \{a_{rij}\}_{\substack{1 \le r \le 4 \\ 1 \le i < j \le 5}}$ gives the element of $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ we desired.

Now recall that in Section 4, we described a natural method of creating a quintic ring $R(A)$ from any element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. Our second and final requirement for S to be a sextic resolvent of R is that, for the element $A = \{a_{rij}\} \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ defined by (28) and (29), we should have $R(A) = R$; i.e., if R has structure coefficients $\{c_{ij}^k\}$ with respect to its basis $1, \alpha_1, \ldots, \alpha_4$, then we should have $c_{ij}^k(A) = c_{ij}^k$ for all i, j, k.

Given S and A as above, to see that the equality $R(A) = R$ holds it suffices to prove that A satisfies the following two conditions: 1) $\mathrm{Disc}(A) = \mathrm{Disc}(R)$, and 2) the 4×4 sub-Pfaffians of A vanish on $x_R^{(1)}, x_R^{(2)}, \ldots x_R^{(5)}$. Indeed, if condition 2) is satisfied, then by the work in Section 4, we see that $c_{ij}^k(A) = \lambda c_{ij}^k$ for all i, j, k, for some nonzero constant $\lambda \in \mathbb{Q}$. Condition 1) then gives $\mathrm{Disc}(A) = \mathrm{Disc}(R(A)) = \lambda^8\mathrm{Disc}(R)$, and thus $\lambda = \pm 1$. A calculation using the explicit expressions (29) and (21) for A and $c_{ij}^k(A)$, respectively, shows that λ is positive or negative in accordance with whether the chosen bases of R and S are *similarly* or *oppositely oriented*, i.e., whether the ratio $\sqrt{\mathrm{Disc}(S)}/\sqrt{\mathrm{Disc}(R)}$ is positive or negative. We henceforth always choose our bases of R and S to be similarly oriented. Provided that A is expressed in terms of similarly oriented bases for R and S, then conditions 1) and 2) imply $\lambda = 1$ and thus $R(A) = R$.

It remains now to check conditions 1) and 2). The second condition is satisfied delightfully automatically. Since A is defined over $\mathbb{Q}$, it suffices to

check only that the 4×4 sub-Pfaffians of A vanish on $x_R^{(1)}$. Noting that $x_R^{(1)} = [\alpha_1^* : \alpha_2^*: \alpha_3^*: \alpha_4^*]$, we see from (29) that this is equivalent to the vanishing of the 4×4 sub-Pfaffians of the 5×5 skew-symmetric matrix $G = (g(\beta_i^*, \beta_j^*))_{1 \le i,j \le 5}$. Using the expression (28) for $g(u,v)$, one verifies easily that $g(u,v)g(x,y) - g(u,x)g(v,y) + g(u,y)g(v,x) = 0$, and this gives the desired conclusion.

Condition 1) above amounts to a discriminant condition on S. Let us first determine how the discriminants of A, R, and S are related. If we solve for the coefficients a_{rij} in (29), we see that

$$a_{rij} = \langle \alpha_r, g(\beta_i^*, \beta_j^*) \rangle_R = \mathrm{Tr}\big(\alpha_r \cdot g(\beta_i^*, \beta_j^*)\big) \tag{30}$$

for all r, i, j, where we have used "Tr" to denote the trace from $R \otimes \mathbb{Q}$ to $\mathbb{Q}$; i.e., we have

$$a_{rij} = \alpha_r^{(1)} g^{(1)}(\beta_i^*, \beta_j^*) + \cdots + \alpha_r^{(5)} g^{(5)}(\beta_i^*, \beta_j^*) \tag{31}$$

where $g^{(1)}, \ldots, g^{(5)}$ denote the S_5-conjugates of $g = g^{(1)}$ respectively. Using formula (31) for the entries of A, we may work out the beautiful relation

$$\mathrm{Disc}(A) = \frac{\mathrm{Disc}(S)^{12}}{16^{36} \cdot \mathrm{Disc}(R)^{35}}\,. \tag{32}$$

Condition 1) above is thus equivalent to the condition that

$$\mathrm{Disc}(S) = \big(16 \cdot \mathrm{Disc}(R)\big)^3\,. \tag{33}$$

We have at last arrived at the definition of a sextic resolvent of a quintic ring.

Definition 5. Let R be a quintic ring of nonzero discriminant, and let $\bar{R}$ denote its S_5–closure. A *sextic resolvent* of R is a rank 6 sublattice $S \subset \bar{R}^M \otimes \mathbb{Q}$ such that $\mathrm{Disc}(S) = (16 \cdot \mathrm{Disc}(R))^3$, and such that any one of the following (equivalent) conditions holds:

- $f(x,y,z) \in \widetilde{R} \quad \forall x, y, z \in S$;
- $g(u,v) \in \widetilde{R} \quad \forall u, v \in \widetilde{S}$;
- $\mathrm{Tr}(\alpha \cdot f(x,y,z)) \in \mathbb{Z} \quad \forall \alpha \in R$ and $x, y, z \in S$.
- $\mathrm{Tr}(\alpha \cdot g(u,v)) \in \mathbb{Z} \quad \forall \alpha \in R$ and $u, v \in \widetilde{S}$.

It is evident from (23)–(30) that the four conditions are equivalent to each other. Note that Definition 5 only insists that the sextic resolvent S is a sublattice in $\bar{R}^{M^{(1)}}$ with the desired properties; it does not insist on any ring structure!

However, just as in the quadratic and cubic cases we find that a ring structure on S in fact follows automatically from its other properties! We have the following:

PROPOSITION 6. *Any sextic resolvent lattice of a quintic ring is also a ring.*

Hence we may refer to a sextic resolvent of a quintic ring R as a *sextic resolvent ring* of R. Proposition 6 is proved in the next section.

6. The multiplication table for sextic resolvent rings

Just as the multiplication table for the quintic ring $R(A)$ was given in terms of the SL_5-invariants of the element $A \in V_{\mathbb{Z}}$, the structure constants for a putative ring structure on the sextic resolvent lattice $S(A)$ of $R(A)$ must similarly be given in terms of the SL_4-invariants of $A \in V_{\mathbb{Z}}$. This is because the group $\mathrm{SL}_4(\mathbb{Z})$ acts only on the basis of the quintic ring $R(A)$ and does not affect the sextic resolvent lattice $S(A)$ nor the chosen basis of $S(A)$.

The prototypical SL_4-invariants on the space $V_{\mathbb{Z}} = \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ are the degree 4 polynomials in the entries of $A = (a_{rij}) \in V$ given by

$$\delta(i_1, j_1; i_2, j_2; i_3, j_3; i_4, j_4) = \begin{vmatrix} a_{1i_1j_1} & a_{2i_1j_1} & a_{3i_1j_1} & a_{4i_1j_1} \\ a_{1i_2j_2} & a_{2i_2j_2} & a_{3i_2j_2} & a_{4i_2j_2} \\ a_{1i_3j_3} & a_{2i_3j_3} & a_{3i_3j_3} & a_{4i_3j_3} \\ a_{1i_4j_4} & a_{2i_4j_4} & a_{3i_4j_4} & a_{4i_4j_4} \end{vmatrix}.$$

By the fundamental theorem of invariant theory, these polynomials generate all polynomial SL_4-invariants on V.

Now let us write the potential ring structure on $S = S(A) = \langle 1, \beta_1, \ldots, \beta_5 \rangle$ in the form

$$\beta_i\beta_j = d_{ij}^0 + \sum_{k=1}^{5} d_{ij}^k \beta_k \tag{34}$$

for some constants $d_{ij}^k \in \mathbb{Z}$. Then from the equality $\mathrm{Disc}(S) = (16 \cdot \mathrm{Disc}(A))^3$, we see that if the structure constants d_{ij}^k ($k \neq 0$) are polynomials in the entries of A, then they must be of degree 12. Thus the polynomials d_{ij}^k ($k \neq 0$), if they exist, must be degree 3 polynomials in the fundamental SL_4-invariants δ. Furthermore, the putative polynomials d_{ij}^k must transform appropriately under the action of SL_5, i.e., precisely as the structure coefficients of a sextic ring would.

Keeping these constraints in mind, we define invariants $D_{ij}^k = D_{ij}^k(A)$ for $A \in V_{\mathbb{Z}}$ by

(35)
$$D_{ij}^k = \frac{1}{2304} \sum_{\substack{k_n \ (n=2,3,4) \\ \ell_n, k'_n, \ell'_n, k''_n, \ell''_n \ (n=1,\dots,4)}} \Big[\sigma(i\ell'_1\ell'_2k'_3\ell'_3)\,\sigma(j\ell''_1\ell''_2k''_3\ell''_3)\,\sigma(k'_1\ell_1\ell_2k_3\ell_3)\,\sigma(k''_1k'_2k'_4\ell'_4\ell''_4)\,\sigma(k_2k''_2k_4k''_4\ell_4)$$
$$\cdot\,\delta(k,\ell_1;k_2,\ell_2;k_3,\ell_3;k_4,\ell_4)\cdot\delta(k'_1,\ell'_1;k'_2,\ell'_2;k'_3,\ell'_3;k'_4,\ell'_4)\cdot\delta(k''_1,\ell''_1;k''_2,\ell''_2;k''_3,\ell''_3;k''_4,\ell''_4)\Big],$$

where we have again used $\sigma(n_1 \dots n_5)$ to denote the sign of the permutation $(n_1, \dots, n_5)$ of $(1, \dots, 5)$. As in the case of quintic rings, to specify the ring structure on S it suffices to specify the values of d_{ij}^k, d_{ii}^j, $d_{ij}^j - d_{ik}^k$, and $d_{ii}^i - d_{ij}^j - d_{ik}^k$. Let

(36)
$$\begin{aligned} d_{ij}^k &= D_{ij}^k, \\ d_{ii}^j &= D_{ii}^j, \\ d_{ij}^j - d_{ik}^k &= D_{ij}^j - D_{ik}^k, \\ d_{ii}^i - d_{ij}^j - d_{ik}^k &= D_{ii}^i - D_{ij}^j - D_{ik}^k. \end{aligned}$$

One checks that although the D_{ij}^k are not necessarily all integer polynomials, the expressions on the right-hand side of (36) are in fact integer polynomials!

Now let R be any nondegenerate quintic ring with $\mathbb{Z}$-basis $\langle 1, \alpha_1, \dots, \alpha_4\rangle$, let S be a sextic resolvent of R having (similarly oriented) $\mathbb{Z}$-basis $\langle 1, \beta_1, \dots \beta_5\rangle$, and let $A = (a_{rij}) \in V_{\mathbb{Z}}$ be defined as in (30). For $x_1, \dots, x_6 \in S$, let $\mathrm{Ind}_S(x_1, x_2, x_3, x_4, x_5, x_6)$ denote the (signed) index of the lattice spanned by $x_1, x_2, \dots, x_6$ inside that spanned by $1, \beta_1, \dots, \beta_5$; i.e., $\mathrm{Ind}_S(x_1, x_2, x_3, x_4, x_5, x_6)$ denotes the determinant of the linear transformation taking $1, \beta_1, \dots, \beta_5$ to $x_1, x_2, \dots, x_6$. Then we have the following analogue of Lemma 4 for the sextic resolvent lattice S, stated in terms of its chosen basis:

Lemma 7. *For any permutation (i, j, k, ℓ, m) of $(1, 2, 3, 4, 5)$, we have*

$$\begin{aligned} D_{ij}^k &= \pm\mathrm{Ind}_S(1,\ \beta_i,\ \beta_j, \beta_i\beta_j,\ \beta_\ell,\ \beta_m), \\ D_{ii}^j &= \pm\mathrm{Ind}_S(1,\ \beta_i,\ \beta_i^2,\ \beta_k,\ \beta_\ell,\ \beta_m), \\ D_{ij}^j - D_{ik}^k &= \pm\big[\mathrm{Ind}_S(1,\ \beta_i, \beta_i\beta_j,\ \beta_k,\ \beta_\ell,\ \beta_m) \\ &\qquad -\mathrm{Ind}_S(1,\ \beta_i,\ \beta_j, \beta_i\beta_k,\ \beta_\ell,\ \beta_m)\big], \\ D_{ii}^i - D_{ij}^j - D_{ik}^k &= \pm\big[\mathrm{Ind}_S(1,\ \beta_i^2,\ \beta_j,\ \beta_k,\ \beta_\ell,\ \beta_m) \\ &\qquad -\mathrm{Ind}_S(1,\ \beta_i, \beta_i\beta_j,\ \beta_k,\ \beta_\ell,\ \beta_m) \\ &\qquad -\mathrm{Ind}_S(1,\ \beta_i,\ \beta_j, \beta_i\beta_k,\ \beta_\ell,\ \beta_m)\big], \end{aligned}$$

where we use $\pm$ to denote the sign of the permutation (i, j, k, ℓ, m) of $(1, 2, 3, 4, 5)$.

Proof. We simply expand both sides using (31) and (35). □

The identities of Lemma 7 immediately imply that the multiplicative structure of S is indeed given as in (34), where the values of the structure constants d_{ij}^k ($k \neq 0$) are as in (36). To insure a unique integer solution for the d_{ij}^k (for $k > 0$), we can choose to normalize bases as in the quintic case; e.g., we may translate the β_i by integers so that the coefficients of β_1 and β_2 in $\beta_1\beta_2$ are zero, as are the coefficients of β_3 and β_4 in $\beta_3\beta_4$ and the coefficient of β_4 in $\beta_4\beta_5$. That is, we may assume

$$d_{12}^1 = d_{12}^2 = d_{34}^3 = d_{34}^4 = d_{45}^4 = 0. \tag{37}$$

The remaining constant coefficients d_{ij}^0 are then determined by the associative law, just as in the cubic, quartic, and quintic cases. Namely, by computing the expressions $(\beta_i\beta_j)\beta_k$ and $\beta_i(\beta_j\beta_k)$ using (34), and then equating the coefficients of β_k, we obtain

$$d_{ij}^0 = \sum_{r=1}^{5} \left(d_{jk}^r d_{ri}^k - d_{ij}^r d_{rk}^k \right) \tag{38}$$

for any $k \in \{1,2,3,4,5\} \setminus \{i\}$. One checks using the explicit expressions given in (36) and (37) that the above expression is independent of k, and that with these values of d_{ij}^0 all relations among the d_{ij}^k implied by the associative law are satisfied. We denote the resulting ring, whose multiplicative structure coefficients $d_{ij}^k = d_{ij}^k(A)$ are given as in (35), (36), (37), and (38), by $S(A)$.

In particular, we have proven Proposition 6.

7. The main theorem

Given a nondegenerate quintic ring R and a sextic resolvent ring S of R, with similarly oriented $\mathbb{Z}$-bases for R and S, we have shown in Section 5 how to create an element $A \in V_{\mathbb{Z}}$ such that the following three properties hold: 1) $\mathrm{Disc}(A) = \mathrm{Disc}(R)$; 2) the 4×4 sub-Pfaffians of A vanish on the five points associated to R in $\mathbb{P}^3$; and 3) A describes the fundamental resolvent map $g : \wedge^2 \widetilde{S} \to \widetilde{R}$.

Conversely, suppose we are given a nondegenerate element $A \in V_{\mathbb{Z}}$. Then we may create a quintic ring $R = R(A)$ with properties 1) and 2) explicitly using formulas (16), (17), (21), and (22). Furthermore, as $R = R(A)$ is nondegenerate, the algebra $\bar{R}^M \otimes \mathbb{Q}$ has dimension 6 over $\mathbb{Q}$. Let S' be any lattice in $\bar{R}^M \otimes \mathbb{Q}$ such that $\mathbb{Q} \cap S' = \mathbb{Z}$ and $\mathrm{Disc}(S') = (16 \cdot \mathrm{Disc}(R))^3$. Let $1, \alpha_1, \ldots, \alpha_4$ and $1, \beta_1, \ldots, \beta_5$ be similarly oriented $\mathbb{Z}$-bases for R and S' respectively. Then we have seen that the element $A' \in V_{\mathbb{Q}}$ defined by (30) describes the map $g : \wedge^2 \widetilde{S}' \to \widetilde{R} \otimes \mathbb{Q}$.

Now by construction, A is $\mathrm{SL}_5(\mathbb{C})$-equivalent to A', since A and A' possess the same SL_5-invariants. They must in fact be $\mathrm{SL}_5(\mathbb{Q})$-equivalent, for if $\gamma \in$

$\mathrm{SL}_5(\mathbb{C})$ takes A' to A, then $(\gamma^{-1})^t$ must take Q' to Q, where $Q' = [Q'_1, \dots, Q'_5]^t$ and $Q = [Q_1, \dots, Q_5]^t$ denote the vectors of 4×4 signed sub-Pfaffians of A' and A respectively. Now the Q_i and the Q'_i each span the same five-dimensional *rational* vector space of quaternary quadratic forms, namely those rational quaternary quadratic forms that vanish on the set $X_R = \{x^{(1)}, \dots, x^{(5)}\}$. We conclude that $\gamma \in \mathrm{SL}_5(\mathbb{Q})$. Let S be the lattice in $\bar{R}^M \otimes \mathbb{Q}$ spanned by 1 and $(\gamma^{-1})^t\beta_1, \dots, (\gamma^{-1})^t\beta_5$. Then A describes the map $g : \wedge^2\widetilde{S} \to \widetilde{R}$; it follows that S is the desired sextic resolvent ring of $R = R(A)$ corresponding to A. The multiplication structure of S can be recovered from (34), (35), (36), (37), and (38).

Finally, it is clear from the above constructions that the maps $(R, S) \mapsto A$ and $A \mapsto (R, S)$ are inverse to each other. We have thus completed the proof of the following theorem.

THEOREM 8. *There is a natural bijection between the set of nondegenerate* $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$*-equivalence classes of elements* $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ *and the set of isomorphism classes of pairs* (R, S)*, where* R *is a nondegenerate quintic ring and* S *is a sextic resolvent ring of* R*. Under this bijection, we have* $\mathrm{Disc}(A) = \mathrm{Disc}(R) = \frac{1}{16}\mathrm{Disc}(S)^{1/3}$.

Of course, the theorem remains true if $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ is replaced by $\mathbb{Z}^4 \otimes \wedge^3\mathbb{Z}^5$; in this case, the element $A^* = (a^*_{rk\ell m}) \in \mathbb{Z}^4 \otimes \wedge^3\mathbb{Z}^5$ corresponding to a pair (R, S) is given by (26) or via the more direct formula

$$\begin{aligned} a^*_{rk\ell m} &= \mathrm{Tr}\big(\alpha_r \cdot f(\beta_k, \beta_\ell, \beta_m)\big) \\ &= \alpha_r^{(1)} f^{(1)}(\beta_k, \beta_\ell, \beta_m) + \cdots + \alpha_r^{(5)} f^{(5)}(\beta_k, \beta_\ell, \beta_m). \end{aligned} \tag{39}$$

8. Pfaffians and the classical resolvent map

In the previous section, we have proven that an element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ corresponds to the most fundamental mapping

$$g : \widetilde{S} \otimes \widetilde{S} \to \widetilde{R}$$

relating the quintic ring $R = R(A)$ and its sextic resolvent S. However, there are many other beautiful polynomial mappings relating the rings R and S, and any such mapping may be understood in terms of higher covariants of A.

In particular, we may consider the classical resolvent map

$$\psi : R \to \widetilde{S} \otimes \mathbb{Q}$$

defined by

$$\begin{aligned} \psi(\alpha) = \frac{1}{\sqrt{\mathrm{Disc}(R)}}\big(\ &\alpha^{(1)}\alpha^{(2)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(3)}\alpha^{(4)} + \alpha^{(4)}\alpha^{(5)} + \alpha^{(5)}\alpha^{(1)} \\ &- \alpha^{(1)}\alpha^{(3)} - \alpha^{(3)}\alpha^{(5)} - \alpha^{(5)}\alpha^{(2)} - \alpha^{(2)}\alpha^{(4)} - \alpha^{(4)}\alpha^{(1)}\big). \end{aligned} \tag{40}$$

This map was first introduced by Cayley [9], and has since served as one of the primary tools in the solution of the quintic equation (whenever soluble) and in the study of icosahedral and S_5-extensions of $\mathbb{Q}$; see for example [8]. The relation between ψ and the graph ① in Figure 1 is evident: the rule for the determination of the sign of $\alpha^{(i)}\alpha^{(j)}$ in $\psi(\alpha)$ is that terms associated with adjacent edges take a positive sign, while those with nonadjacent edges take a negative sign.

To see that the image of ψ is in $S^* \otimes \mathbb{Q}$, we need only observe that ψ is fixed by the elements of $M^{(1)}$. Since in addition $\mathrm{Tr}(\psi(\alpha)) = 0$, it follows that the image of ψ lies in $\widetilde{S} \otimes \mathbb{Q}$. We show below that, remarkably, the image of ψ lies not only in $\widetilde{S} \otimes \mathbb{Q}$, but in $\widetilde{S}$ itself. Moreover, we have $\psi(x + c) = \psi(x)$ for any $c \in \mathbb{Z}$; hence ψ actually descends to a map

$$\bar{\psi} : R/\mathbb{Z} \to \widetilde{S}.$$

Thus we may view $\bar{\psi}$ as a quadratic function from $\mathbb{Z}^4$ to $\mathbb{Z}^5$, or, equivalently, as a quintuple $Q' = (Q'_1, Q'_2, \ldots, Q'_5)$ of quaternary quadratic forms. Now as A represents the "fundamental" map g relating R and S, the quintuple Q' should be some natural $\mathrm{SL}_4 \times \mathrm{SL}_5$-covariant function of A. Which covariant? We find that, up to a constant factor, Q' is none other than the degree 2 covariant $Q = (Q_1, Q_2, \ldots, Q_5)$ consisting of the five 4×4 sub-Pfaffians of A! More precisely, we have:

THEOREM 9. *Let A be any nondegenerate element of $V_\mathbb{Z}$, and let (R, S) denote the pair of quintic and sextic rings corresponding to A via Theorem* 8. *Then the classical resolvent map ψ of Cayley maps R to $\widetilde{S}$, and this mapping $\psi : R \to \widetilde{S}$ is exactly given, in terms of the associated bases for R and $\widetilde{S}$, by four times the quintuple $(Q_1, Q_2, \ldots, Q_5)$ of 4×4 sub-Pfaffians of A.*

Proof. To prove Theorem 9, we appeal directly to the formula (30) for the entries a_{rij} of A in terms of the bases $\langle 1, \alpha_1, \ldots, \alpha_4\rangle$ and $\langle 1, \beta_1, \ldots, \beta_5\rangle$ for R and S respectively. In terms of these expressions for a_{rij} and the expression (28) for g, we compute the k-th 4×4 sub-Pfaffian Q_k of A to be

(41)
$$Q_k(t_1, t_2, t_3, t_4) = \frac{1}{4}\left(\psi^{(1)}\left(\sum_{i=1}^{4} t_i\alpha_i\right) \cdot \beta_k^{(1)} + \cdots + \psi^{(6)}\left(\sum_{i=1}^{4} t_i\alpha_i\right) \cdot \beta_k^{(6)}\right),$$

where $\psi^{(1)}, \ldots, \psi^{(6)}$ denote the six A_5-conjguate mappings of $\psi = \psi^{(1)}$ taking R to $\widetilde{S}^{(1)} \otimes \mathbb{Q}$, …, $\widetilde{S}^{(6)} \otimes \mathbb{Q}$ respectively. It follows from (41) that for $t = (t_1, t_2, t_3, t_4) \in \mathbb{Z}^4$ and $\alpha(t) = t_1\alpha_1 + \cdots + t_4\alpha_4 \in R/\mathbb{Z}$, we have

$$\psi(\alpha(t)) = 4Q_1(t)\tilde{\beta}_1 + \cdots + 4Q_5(t)\tilde{\beta}_5. \tag{42}$$

Therefore the quintuple $4\,Q$ of quaternary quadratic forms represents the classical resolvent map ψ, and ψ maps R into $\widetilde{S}$. □

Thus for all $n = 2, 3, 4, 5$, the spaces of smallest degree hypersurfaces passing through the points X_R correspond to the natural maps between R and S used in the classical solutions to the n-tic equation! However, in the case $n = 5$, we see that there is an additional subtlety in that this classical resolvent map is not the most fundamental map relating R and S. In the cases of $n = 3$ and $n = 4$, it was the most fundamental map, but in the case $n = 5$ the smallest polynomial map relating R and S is the map $g : \widetilde{S} \otimes \widetilde{S} \to \widetilde{R}$. Indeed, ψ is a degree 2 covariant polynomial in g. The more basic map g seems to have been missed in the classical literature, perhaps because it is an alternating map, and because it is most naturally defined as a map between the dual rings.

Finally, we remark that other higher degree maps involving R, S, $\widetilde{R}$, and $\widetilde{S}$ also exist, and they can similarly be understood by examining the higher degree tensor covariants of $g \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$.

9. An alternative description of sextic resolvents

We have seen that a sextic resolvent ring S of a nondegenerate quintic ring R, and its associated resolvent map $\phi_{5,6} : R \to \wedge^2 S$, possess, and indeed are characterized by, a number of remarkable geometric, Galois-theoretic, and invariant-theoretic properties. The purpose of this section is to give an alternative, more minimalist definition of a sextic resolvent ring that in particular does not use the notion of S_k-closure. Such a definition—though at the surface less informative—is especially useful for 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 $\mathbb{F}_p$, rings having zero discriminant are particularly important as they frequently arise as reductions modulo p of orders in a number field.

The idea is to view a sextic resolvent ring of a quintic ring R as a sextic ring S together with a special $\mathbb{Z}$-linear map $\phi : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$ (called a *sextic resolvent map*) which satisfies all properties of the $\phi_{5,6}$ map that were crucial for us in Sections 2–8. Of these, the truly essential properties were the identities (21) and (35)–(36) which were needed to recover the multiplicative structures on the rings R and S respectively.

More precisely, for any map $\phi : L_4 \to \wedge^2 L_5$, where L_4 and L_5 are free $\mathbb{Z}$-modules of rank 4 and 5 respectively, we have given in Sections 4 and 6 a method of attaching to ϕ a quintic ring $R(\phi)$ and a sextic ring $S(\phi)$, with natural $\mathbb{Z}$-module isomorphisms $R(\phi)/\mathbb{Z} \cong L_4$ and $S(\phi)/\mathbb{Z} \cong L_5$. In particular, if $\phi_{5,6} : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$ is the $\mathbb{Z}$-linear map induced by the fundamental Galois-theoretic map $g : \wedge^2 S^* \to R^*$, where R is a nondegenerate quintic ring and S is a sextic resolvent of R, then we obtain natural ring identifications "$R(\phi_{5,6}) = R$" and "$S(\phi_{5,6}) = S$". That is, if $\mathbb{Z}$-bases are chosen for $R/\mathbb{Z}$ and $S/\mathbb{Z}$, then with respect to these bases we have $c^k_{ij}(\phi_{5,6}) = c^k_{ij}$ and $d^k_{ij}(\phi_{5,6}) = d^k_{ij}$

for all i, j, k, where c_{ij}^k and d_{ij}^k denote the normalized multiplicative structure constants of R and S respectively. It is clear from construction that these conditions $R(\phi_{5,6}) = R$ and $S(\phi_{5,6}) = S$ are independent of the choice of $\mathbb{Z}$-bases.

For any quintic ring R and sextic ring S, we define a $\mathbb{Z}$-linear map $\phi : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$ to be a *sextic resolvent map* if $R(\phi) = R$ and $S(\phi) = S$. A *sextic resolvent* of a quintic ring R is then any sextic ring S equipped with a sextic resolvent map $\phi : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$.

Definition 10. Let R be a quintic ring and S a sextic ring. We call a $\mathbb{Z}$-linear map $\phi : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$ a *sextic resolvent mapping* if $R(\phi) = R$ and $S(\phi) = S$.

Definition 11. Let R be a quintic ring. A *sextic resolvent ring* of R is a sextic ring S equipped with a sextic resolvent mapping $\phi : R/\mathbb{Z} \to \wedge^2(S/\mathbb{Z})$.

It follows from the work in Sections 2–8 that, in the nondegenerate case, the above definitions agree with those given in more Galois-theoretic language in Section 5. With these definitions, Theorem 8 immediately extends also to cases where the discriminant is zero.

It would be interesting to formulate the conditions $R(\phi) = R$ and $S(\phi) = S$ in a more coordinate-free manner, as was described for the parametrizations of cubic and quartic rings in [4]. In particular, such a formulation would likely be useful in extending Theorem 1 to locally free quintic and sextic algebras over an arbitrary base. We hope that this possibility will be considered in future work.

10. More on the invariant theory of quadruples of alternating 2-forms, and the existence of sextic resolvents

In this section, we examine more closely the SL_5-invariant theory of the space of quadruples of alternating 2-forms of rank 5. As noted in Section 4, the smallest degree SL_5-invariants on $V_{\mathbb{Z}}$ are in degree 5, and these invariants are linearly spanned by the polynomials $P^{\pm}$, or equivalently, by the 36 linearly independent polynomials $c_{ij}^k(A)$ $(k \geq 1)$ as given in (17) and (21).

The associative law, which allowed us to solve unambiguously for the constant coefficients $c_{ij}^0(A)$ of the ring $R(A)$, implies that these 36 invariants $c_{ij}^k(A)$ for $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ are not algebraically independent, but satisfy certain syzygies. Indeed, the associative law on $R(A)$ is equivalent to

(43)

$$\sum_{r=1}^{4} c_{ik}^r c_{rj}^{\ell} = \sum_{r=1}^{4} c_{jk}^r c_{ri}^{\ell} \text{ for all } i, j, k, \ell \in \{1, 2, 3, 4\} \text{ with } i \neq \ell \text{ and } j \neq \ell; \text{ and}$$

$$(44)\quad \sum_{r=1}^{4}(c_{ik}^r c_{rj}^k - c_{ij}^r c_{rk}^k)$$
$$= \sum_{r=1}^{4}(c_{i\ell}^r c_{rj}^\ell - c_{ij}^r c_{r\ell}^\ell) \text{ for all } i,j,k,\ell \in \{1,2,3,4\} \text{ with } j \neq k \text{ and } j \neq \ell.$$

Do the 36 SL_5-invariants satisfy any other relations, besides those obtainable from (43) and (44) via algebraic operations? The answer is no. The reason for this is that, up to isomorphism, there are only finitely many quintic algebras over $\mathbb{C}$ and it is easy to check that every such algebra arises as $R(A)$ for some $A \in V_{\mathbb{Z}}$. Hence there can be no other polynomial relations among the SL_5-invariants $c_{ij}^k(A)$ other than those contained in the radical of the ideal generated by the associative law relations (43) and (44). In particular, the possible values of the SL_5-invariants $\{c_{ij}^k(A)\}$ for $A \in V$ coincide precisely with the possible values $\{c_{ij}^k\}$ of (normalized) multiplicative structure coefficients of quintic algebras over $\mathbb{C}$.

Our next question concerns fields of definition. Suppose we have a quintic algebra $R = \langle 1, \alpha_1, \ldots, \alpha_4\rangle$ over $\mathbb{Q}$, with structure coefficients given by the set of rational numbers $\{c_{ij}^k\}$. We know then that there exists a complex point $A \in V$ with $c_{ij}^k(A) = c_{ij}^k$ for all i,j,k. Does there actually exist a rational point $A \in V_{\mathbb{Q}}$ with this property?

The answer is yes. If R is étale over $\mathbb{Q}$, then we may construct such an A as follows. Let $\bar{R}$ denote the S_5-closure of R, and let S denote the sextic algebra over $\mathbb{Q}$ fixed by the metacyclic group $M^{(1)}$. Let $\langle 1, \beta_1, \ldots, \beta_5\rangle$ be a $\mathbb{Q}$-basis of S such that $\mathrm{Disc}(1,\beta_1,\ldots,\beta_5) = (16 \cdot \mathrm{Disc}(1,\alpha_1,\ldots,\alpha_4))^3$. Then the element $A = (a_{rij}) \in \mathbb{Q}^4 \otimes \wedge^2\mathbb{Q}^5$ defined by (30) satisfies $c_{ij}^k(A) = c_{ij}^k$ for all r,i,j, as desired.

The case of nonétale quintic algebras R over $\mathbb{Q}$ can also be handled in a similar manner, via a case-by-case analysis of the various (but finitely many) types of quintic algebras over $\mathbb{Q}$; we omit the proof.

Finally, we would like to consider the analogous question over $\mathbb{Z}$. This is answered by the following theorem.

THEOREM 12. *Suppose the constants $\{c_{ij}^k\}$ arise as the SL_5-invariants of some element in $V = \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$, where all the values of c_{ij}^k are integers. Then there exists an integer point $A \in V_{\mathbb{Z}}$ such that $c_{ij}^k(A) = c_{ij}^k$ for all i,j,k.*

We prove the theorem in three steps. Our first lemma shows that it suffices to prove the theorem in the case where the c_{ij}^k are relatively prime.

LEMMA 13. *If the set of constants $\{c_{ij}^k\}$ arises as the system of SL_5-invariants of an element in $V_{\mathbb{Z}}$, then so does the set of constants $\{nc_{ij}^k\}$, where n is any integer.*

Proof. Let $A = (A_1, A_2, A_3, A_4) \in V_{\mathbb{Z}}$ be an element with $c_{ij}^k(A) = c_{ij}^k$ for all i, j, k. Furthermore, suppose there exist linearly independent integral column vectors $v, w \in \mathbb{Z}^5$ such that $v^t A_r w = 0$ for all $r \in \{1, 2, 3, 4\}$. By a change of basis in $\mathrm{SL}_5(\mathbb{Z})$, then, we may assume that the $(1, 2)$ entry (say) of A_r is zero for all $r \in \{1, 2, 3, 4\}$.

Let $A' = (A'_1, A'_2, A'_3, A'_4) \in V_{\mathbb{Z}}$ be the element A with all entries multiplied by n. Since the SL_5-invariants $c_{ij}^k(A)$ are of degree 5, it is clear that $c_{ij}^k(A') = n^5 c_{ij}^k(A)$ for all i, j, k. Now since the (1,2) entry of A'_r vanishes for all $r \in \{1, 2, 3, 4\}$, it is in particular divisible by n^2. We may therefore divide the first and second rows and columns of A'_r by n, for all $r = 1, 2, 3, 4$, to obtain an integral element $A'' \in V_{\mathbb{Z}}$. From the Pfaffian description (11) of the invariants $P^{\pm}$, it is evident that $c_{ij}^k(A'') = n^{-4} c_{ij}^k(A')$ (since the relevant 10×10 Pfaffians have four rows and four columns divided by n). The quadruple A'' therefore satisfies $c_{ij}^k(A'') = n c_{ij}^k(A)$ as required by the lemma.

To complete the proof of the lemma we must show only that there exists a pair v, w of linearly independent integral column vectors as above with $v^t A_r w = 0$ for all $r \in \{1, 2, 3, 4\}$. Such a pair v, w may be constructed as follows. Let v^t be an arbitrary integral nonzero row vector in the left kernel of A_1. Such a vector exists because A_1 is a 5×5 skew-symmetric matrix and hence has rank at most 4. Now for each $r \in \{2, 3, 4\}$, the row vector $v^t A_r$, being of rank at most 1, has a right kernel of dimension at least 4. The intersection W of the right kernels of $v^t A_r$, for $r \in \{1, 2, 3\}$, therefore has dimension at least 2. In particular, there exists an integral vector $w \in W$ that is independent of v, and such a w will evidently satisfy $v^t A_r w = 0$ for all $r \in \{1, 2, 3, 4\}$. This is the desired conclusion. □

LEMMA 14. *Suppose the constants $\{c_{ij}^k\}$ arise as the SL_5-invariants of some element in $V = \mathbb{C}^4 \otimes \wedge^2 \mathbb{C}^5$, where all the values of c_{ij}^k are integers. Then there exists an integer point $A \in V_{\mathbb{Z}}$ and a positive integer n such that $c_{ij}^k(A) = n c_{ij}^k$ for all i, j, k.*

Proof. As noted earlier, there exists some element $A' \in V_{\mathbb{Q}}$ with $c_{ij}^k(A') = c_{ij}^k$ for all i, j, k. Furthermore, there exists an integer $s > 0$ such that $A = sA' \in V_{\mathbb{Z}}$. This value of A, with $n = s^5$, satisfies the requirements of the lemma. □

Theorem 12 will be proved once the following lemma is established. The lemma states that the value of n in Lemma 14 can always be lowered. In particular, it may be lowered until it reaches 1; together with Lemma 13, this implies the theorem.

LEMMA 15. *Let $A \in V_{\mathbb{Z}} = \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ be an element with $c_{ij}^k(A) = n c_{ij}^k$, for some integers c_{ij}^k and n with $n > 1$. Then there exists an integer point $A' \in V_{\mathbb{Z}}$ and a positive integer $n' < n$ satisfying $c_{ij}^k(A') = n' c_{ij}^k$ for all i, j, k.*

Proof. We begin by observing that, to prove the lemma for one $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, it suffices to prove the lemma for any A_0 in the same Γ-orbit as A. More precisely, if $A_0 \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ is an element for which $A_0 = \gamma A$ for some $\gamma \in \Gamma$, and if we locate an $A_0' \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ with $c_{ij}^k(A_0') = (n'/n)c_{ij}^k(A_0)$ for all i, j, k, then $\gamma^{-1}A_0'$ will be an A' satisfying $c_{ij}^k(A') = n'c_{ij}^k$ for all i, j, k, as desired. Below, this observation will allow us to mold A into more convenient shapes in $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, thereby simplifying calculations.

The key to our proof is the quintuple of quaternary quadratic forms $Q = (Q_1, Q_2, \ldots, Q_5)$ given by the five signed 4×4 sub-Pfaffians of A. As observed in Section 2, the action of $\mathrm{SL}_5(\mathbb{Z})$ on A results in an action of $\mathrm{SL}_5(\mathbb{Z})$ on Q as in (8). We may use the resulting action on Q to produce some handy SL_5-invariant polynomials as follows. Notice that each quadratic form Q_i consists of 10 coefficients. Taking any subset of 5 such coefficients from Q_1, and the corresponding coefficients from each of the other Q_i, yields a 5×5 matrix whose determinant is clearly an SL_5-invariant. This construction evidently yields $\binom{10}{5} = 252$ such invariants. Being invariant under the action of SL_5, these determinantal expressions must be algebraically dependent on the c_{ij}^k (which form a complete set of SL_5-invariants), and indeed one finds that each of these 252 invariants is a degree 2 integer polynomial in the c_{ij}^k.

Now let p be any prime dividing n. Since all the c_{ij}^k are multiples of p, the 252 determinantal invariants must actually be multiples of p^2. It follows, by the theory of elementary divisors, that we may apply a transformation $\mathrm{SL}_5(\mathbb{Z})$ to A so that either 1) both Q_1 and Q_5 become multiples of p, or 2) Q_5 becomes a multiple of p^2.

Having applied such a transformation, we may assume that at least one of the conditions 1) or 2) holds. Either way, we have that Q_5 is a multiple of p; i.e., the top left 4×4 sub-Pfaffian of M is a multiple of p for any 5×5 matrix in the $\mathbb{Z}$-linear span of A_1, A_2, A_3, A_4.

Observe that the condition that Q_5 be a multiple of p remains true even if we apply an element of $\mathrm{SL}_4(\mathbb{Z}) = \mathrm{SL}_4(\mathbb{Z}) \times \{e\}$ (considered as a subgroup of $\mathrm{SL}_5(\mathbb{Z})$) to the element A; we are therefore free to apply elements of $\mathrm{SL}_4(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z}) \subset \Gamma$ to further transform A. Let us write $\mathrm{SL}_4(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z}) \subset \Gamma = \mathrm{SL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ as $\mathrm{SL}_4^{(1)}(\mathbb{Z}) \times \mathrm{SL}_4^{(2)}(\mathbb{Z})$ to distinguish the two factors of SL_4.

Let B_1, B_2, B_3, B_4 denote the top left 4×4 submatrices of A_1, A_2, A_3, A_4 respectively, considered modulo p so that the entries of B_i lie in $\mathbb{F}_p$. The above-mentioned action of $\mathrm{SL}_4^{(1)}(\mathbb{Z}) \times \mathrm{SL}_4^{(2)}(\mathbb{Z}) \subset \Gamma$ on A reduces to an action of $\mathrm{SL}_4(\mathbb{F}_p) \times \mathrm{SL}_4(\mathbb{F}_p)$ on $B = (B_1, B_2, B_3, B_4)$. We use this action to simplify B, with the understanding that any such transformation of B will be lifted to a transformation γ of A with $\gamma \in \mathrm{SL}_4^{(1)}(\mathbb{Z}) \times \mathrm{SL}_4^{(2)}(\mathbb{Z})$. This will enable us to mold A into a particularly simple shape modulo p.

First, since $\det(B_i) = 0$ in $\mathbb{F}_p$, the rank of each B_i is either 0 or 2. If each B_i is the zero matrix, then we are done: we simply multiply the last row and column of each A_i by p, and then divide each A_i by p. The resulting $A' \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ evidently satisfies $c_{ij}^k(A') = (n/p^3)c_{ij}^k$, and so we may let $n' = n/p^3$.

Thus we may assume some B_i has rank 2, and without loss of generality $i = 1$. By an appropriate transformation in $\mathrm{SL}_4^{(2)}(\mathbb{Z})$, we may further assume that $B_1 = \left[\begin{smallmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$. Using transformations in $\mathrm{SL}_4^{(1)}(\mathbb{Z})$, we can then clear out the (1,2) entries of B_2, B_3, B_4. Moreover, with this value of B_1, the expression $\mathrm{Pfaff}(B_1 + B_i) - \mathrm{Pfaff}(B_i)$, for $i > 1$, is computed to be equal to simply the (3,4) entry of B_i. Therefore, the (3,4) entry of every B_i is equal to 0 too, and hence $B = (B_1, B_2, B_3, B_4)$ takes the form

(45)
$$\left(\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & & \\ 0 & 0 & & R \\ & & 0 & 0 \\ & -R & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & & \\ 0 & 0 & & S \\ & & 0 & 0 \\ & -S & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & & \\ 0 & 0 & & T \\ & & 0 & 0 \\ & -T & 0 & 0 \end{bmatrix}\right)$$

for some triple of 2×2 matrices (R, S, T). Now since the Pfaffians of B_2, B_3, and B_4 are the determinants of R, S, and T respectively, we see that each of R, S, T must have rank ≤ 1. In fact, since any linear combination of B_2, B_3, B_4 has vanishing Pfaffian, the linear span of R, S, T must contain only matrices of rank ≤ 1. It follows that, by an appropriate change of basis, the entries of R, S, T either lie all in the first row or all in the first column, and hence B is either of the form

(46)
$$\left(\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & c_1 & 0 \\ 0 & 0 & 0 & 0 \\ -c_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & c_2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -c_2 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}\right)$$

for some $c_1, c_2 \in \{0, 1\}$, or of the form

(47)
$$\left(\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}\right).$$

If B is of the form (46), then the central 3×3 matrix of every A_i is a multiple of p. Thus, we may multiply the first and last rows and columns of each A_i by p, and then divide each A_i by p. The resulting $A' \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ is integral, and satisfies $c_{ij}^k(A') = (n/p)c_{ij}^k$; we may let $n' = n/p$.

It remains to consider the case where B is of the form (47). Thus, we assume that the top left 4×4 submatrix of A_i is congruent to B_i modulo p,

with B_i as in (47), and let x_i denote the $(4,5)$ entry of A_i for $i = 1,2,3,4$. Then a calculation modulo p shows that we have $P^-(A_1, A_2, A_3) \equiv -x_2^2$. As the latter SL_5-invariant must be a multiple of p, we conclude that x_2 is a multiple of p. Similarly, $P^-(A_1, A_2, A_3 + A_4) \equiv -(x_2 + x_4)^2$, so that x_4 is a multiple of p. Examining similarly $P^-(A_3, A_1, A_2)$ and $P^-(A_2, A_3, A_1)$, we see that x_1 and x_3 are also multiples of p. Thus the fourth rows and columns of A_i vanish modulo p for $i = 1,2,3,4$. We may therefore divide the fourth row and column of each A_i by p to obtain an integral $A' \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. It is evident that $c_{ij}^k(A') = (n/p^2)c_{ij}^k$, and so we may let $n' = n/p^2$. This completes the proof. □

Lemmas 13, 14, and 15 together prove Theorem 12. Next, let us return to the main case of interest in Theorem 12, namely when the constants $c_{ij}^k(A)$ give the structure coefficients of a *maximal* quintic ring, i.e., a quintic ring that is not a subring of any other quintic ring. In that case, we have the following stronger result:

Lemma 16. *Suppose the constants $\{c_{ij}^k\}$ form the structure coefficients of a maximal quintic ring R. Then the element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ with $c_{ij}^k(A) = c_{ij}^k$ for all i,j,k, as constructed in Theorem* 12, *is unique up to* $\mathrm{SL}_5(\mathbb{Z})$*-equivalence.*

Proof. Let $A, A' \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ be any elements with $c_{ij}^k(A) = c_{ij}^k(A') = c_{ij}^k$ for all i,j,k; such A, A' are guaranteed to exist by Theorem 12. We wish to show that A and A' must in fact be $\mathrm{SL}_5(\mathbb{Z})$-equivalent. To this end, let $Q = (Q_1, \ldots, Q_5)$ and $Q' = (Q'_1, \ldots, Q'_5)$ be the associated quintuples of quaternary quadratic forms given by the 4×4 signed sub-Pfaffians of A and A' respectively. The proof of Theorem 12 implies that for any p, if the 252 determinantal SL_5-invariants of Q are all multiples of p, then either a) $\gcd\{c_{ij}^k\} \geq p$, or b) there is a transformation $\gamma \in \Gamma$ such that the vector consisting of the top left 4×4 submatrices of A_1, A_2, A_3, A_4 takes the form (47) modulo p. Condition (a) evidently contradicts the maximality of R, since if all structure constants c_{ij}^k are multiples of p then there is a ring $R' \supset R$ such that $R = \mathbb{Z} + pR'$. Similarly, condition (b) contradicts the maximality of R: if some A_i, say A_1, has a nonzero (4,5) entry, then by subtracting multiples of A_1 from the other A_j we can clear out, modulo p, the (4,5) entries of all the A_j $(j \neq 1)$; now multiply A_1 by p, and then divide the fourth row and column of each A_j $(j = 1,2,3,4)$ by p. We obtain an element $A' \in V_\mathbb{Z}$ in the same $\mathbb{Q}$-orbit as A with $\mathrm{Disc}(A') = \mathrm{Disc}(A)/p^6$, and so $R(A)$ cannot be maximal. (In fact, by examining the structure coefficients of $R(A)$ and $R(A')$, we see that if we write $R(A) = \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3 + \mathbb{Z}\alpha_4$ and $R(A') = \mathbb{Z} + \mathbb{Z}\alpha'_1 + \mathbb{Z}\alpha'_2 + \mathbb{Z}\alpha'_3 + \mathbb{Z}\alpha'_4$, then $\alpha_1 = \alpha'_1$ and $\alpha_j = p\,\alpha'_j$ for $j = 2,3,4$, implying $R'/R \cong (\mathbb{Z}/p\mathbb{Z})^3$.)

We conclude that the 252 determinantal invariants of Q must be relatively prime. That is, if $X_\mathbb{Z}$ denotes the $\mathbb{Z}$-module of quaternary quadratic forms spanned by $Q_1, \ldots, Q_5$, then $X_\mathbb{Z}$ must be the maximal integral lattice

in the five-dimensional complex vector space $X_{\mathbb{C}} = X_{\mathbb{Z}} \otimes \mathbb{C}$ of quaternary quadratic forms. By the identical reasoning, if $X'_{\mathbb{Z}}$ is the $\mathbb{Z}$-module of quaternary quadratic forms spanned by $Q'_1, \ldots, Q'_5$, then $X'_{\mathbb{Z}}$ must be the maximal integral lattice inside the five-dimensional $\mathbb{C}$-vector space $X'_{\mathbb{C}} = X'_{\mathbb{Z}} \otimes \mathbb{C}$.

Now since A and A' share the same SL_5-invariants, $A' = \gamma A$ for some $\gamma \in \mathrm{SL}_5(\mathbb{C})$. It follows that $Q' = Q\gamma^{-1}$, which implies $X_{\mathbb{C}} = X'_{\mathbb{C}}$. Moreover, since $X_{\mathbb{Z}}$ and $X'_{\mathbb{Z}}$ are maximal integral lattices in the same $\mathbb{C}$-vector space $X_{\mathbb{C}}$ of quaternary quadratic forms, we conclude that $X_{\mathbb{Z}} = X'_{\mathbb{Z}}$. Finally, because γ acts as a transformation of $X_{\mathbb{C}}$ which preserves the integral lattice $X_{\mathbb{Z}}$, we have $\gamma \in \mathrm{SL}_5(\mathbb{Z})$. This is the desired conclusion. □

Note that, by Theorem 12, $R(A)$ is a maximal quintic ring for an element $A \in V_{\mathbb{Z}}$ precisely when A is a *minimal integral model*, that is, when A has the smallest (nonzero) discriminant among all integral elements in its $\mathbb{Q}$-orbit. Lemma 16 thus states that any nondegenerate element $A \in V_{\mathbb{Q}}$ has a *unique* minimal integral model up to Γ-equivalence.

11. Isolating R

We may rephrase the preceding invariant theory in terms of quintic rings:

THEOREM 17. *Every quintic ring R is of the form $R(A)$ for some $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. Moreover, if R is maximal then the element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ with $R = R(A)$ is unique up to Γ-equivalence.*

COROLLARY 18. *Every quintic ring has at least one sextic resolvent ring.*

COROLLARY 19. *The sextic resolvent ring of a maximal quintic ring is unique up to isomorphism.*

Thus the situation is in complete parallel with the cubic and quartic cases [4].

Corollary 19 states that a maximal quintic ring always has a unique, canonically associated sextic resolvent ring. In fact, the proof of Lemma 16 shows that this property holds for an even larger class of quintic rings: if R is any nondegenerate quintic ring contained in a maximal ring R' such that the finite abelian group R'/R has p-rank less than 3 for all primes p, then R has a unique sextic resolvent ring up to isomorphism.

Analogous to Corollary 4 of [4], which gives the precise number of cubic resolvents of any given quartic ring, it would be interesting to have an exact counting formula for the number of sextic resolvents of an arbitrary quintic ring. We are not sure on which invariants of the quintic ring this number depends. (In the quartic case, it depended only on the *content* of the ring; see [4, §3.7].)

12. Maximality, prime splitting, and local densities

As remarked in the previous section, an important class of rings on which Theorem 1 (or Theorem 8) yields a one-to-one correspondence are the *maximal* quintic rings. These, of course, are the quintic rings of greatest interest to algebraic number theorists. We therefore wish to understand how maximality of quintic rings, and prime splitting and ramification in maximal quintic rings, manifest themselves in terms of the corresponding quadruples of integral quinary alternating 2-forms. An understanding of these phenomena will, e.g., be very useful in [5] (see also [6]).

Noting that maximality and prime splitting are local conditions, in this section we consider elements in the spaces of quadruples of quinary alternating 2-forms over the integers $\mathbb{Z}$, the p-adic ring $\mathbb{Z}_p$, and over the residue field $\mathbb{Z}/p\mathbb{Z}$. We denote these spaces by $V_{\mathbb{Z}} = \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, $V_{\mathbb{Z}_p} = \mathbb{Z}_p^4 \otimes \wedge^2\mathbb{Z}_p^5$, and $V_{\mathbb{F}_p} = \mathbb{F}_p^4 \otimes \wedge^2\mathbb{F}_p^5$.

Let A be an element of $V_{\mathbb{Z}}$ (resp. of $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$). Then over the residue field $\mathbb{F}_p$, the element A determines a quintic $\mathbb{F}_p$-algebra $R(A)/(p) = R_{\mathbb{F}_p}(A)$ given by the multiplication recipe in (16), (21), and (22) taken modulo p. Let us define the splitting symbol (A, p) by

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

whenever $R(A)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \cdots$. There are thus 17 possible values for the symbol (A, p), namely, (11111), (1112), (122), (113), (23), (14), (5), ($1^2$111), ($1^2$12), ($1^2$3), ($1^2$1^{2}1), ($2^2$1), ($1^3$11), ($1^3$2), ($1^3$1^2), ($1^4$1), and (1^5). (As is customary, we suppress exponents that are equal to one, and omit all factors for which the exponent is zero.)

The symbol (A, p) has a natural geometric interpretation. Namely, suppose $(A, p) = (f_1^{e_1} f_2^{e_2} \cdots)$ for some $A \in V_{\mathbb{F}_p}$. Then one can show that the sub-Pfaffians of A intersect in exactly five points (counting multiplicities) in $\mathbb{P}^3_{\overline{\mathbb{F}}_p}$. Moreover, the residue field degrees over $\mathbb{F}_p$ at the points of intersection are given by the f_i, while their respective multiplicities are given by the e_i.

Let $G = \mathrm{GL}_4 \times \mathrm{SL}_5$. It is clear that if two elements A, A' in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) are equivalent under a transformation in $G(\mathbb{Z})$ (resp. $G(\mathbb{Z}_p)$, $G(\mathbb{F}_p)$), then $(A, p) = (A', p)$. For any of the seventeen values σ of the splitting symbol, let $T_p(\sigma)$ denote the set of A such that $(A, p) = \sigma$. We observe that such an element A has nonzero discriminant modulo p if and only if it is in $T_p(11111)$, $T_p(1112)$, $T_p(122)$, $T_p(113)$, $T_p(23)$, $T_p(14)$, or $T_p(5)$ (i.e., if and only if the five quadrics in $\mathbb{P}^3$ determined by A intersect in five distinct points over $\overline{\mathbb{F}}_p$).

A nondegenerate quintic ring is said to be *maximal* if it is not a subring of any other quintic 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 R as a product of prime ideals of R. If $p =$

$P_1^{e_1}P_2^{e_2}\cdots$ is the factorization of p into prime ideals of $R(A)$, where $R/P_i \cong \mathbb{F}_{p^{f_i}}$, define the symbol (R,p) by setting

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

Suppose now $A \in V_{\mathbb{Z}}$ is such that $R(A)$ is maximal. If $(R,p) = (f_1^{e_1} f_2^{e_2} \cdots)$, then clearly $R(A)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \cdots$, so that $A \in T_p(f_1^{e_1} f_2^{e_2} \cdots)$. Therefore, if the ring $R(A)$ is maximal for an element $A \in V_{\mathbb{Z}}$, then A is contained in one of the $T_p(\cdot)$'s, and

$$(A,p) = (R(A),p).$$

A quintic ring R is maximal if and only if the $\mathbb{Z}_p$-algebra $R_p = R \otimes \mathbb{Z}_p$ is maximal for every p, in the sense that R_p is not contained in any other quintic $\mathbb{Z}_p$-algebra over $\mathbb{Z}_p$. For each splitting symbol σ, denote by $U_p(\sigma) \subset V_{\mathbb{Z}}$ the subset of elements in $T_p(\sigma)$ corresponding to quintic rings that are maximal at p. Then since a quintic ring R with discriminant prime to p is necessarily maximal at p, $R(A)$ is automatically maximal at p for any A in $T_p(11111)$, $T_p(1112)$, $T_p(122)$, $T_p(113)$, $T_p(23)$, $T_p(14)$, or $T_p(5)$, and hence $T_p(\sigma) = U_p(\sigma)$ for any of these seven values of σ. For other values of σ, the set $U_p(\sigma)$ is not simply defined by conditions modulo p, though it is defined as a set via conditions modulo a sufficiently high power of p.

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 determines the p-adic densities of the sets $U_p(\cdot)$, and is the analogue of Lemma 23 of [4].

LEMMA 20. *We have*

$$\begin{aligned}
\mu(U_p(11111)) &= \tfrac{1}{120}(p-1)^8 p^{16}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1112)) &= \tfrac{1}{12}(p-1)^8 p^{16}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(122)) &= \tfrac{1}{8}(p-1)^8 p^{16}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(113)) &= \tfrac{1}{6}(p-1)^8 p^{16}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(23)) &= \tfrac{1}{6}(p-1)^8 p^{16}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(14)) &= \tfrac{1}{4}(p-1)^8 p^{16}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(5)) &= \tfrac{1}{5}(p-1)^8 p^{16}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^2111)) &= \tfrac{1}{6}(p-1)^8 p^{15}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^212)) &= \tfrac{1}{2}(p-1)^8 p^{15}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^23)) &= \tfrac{1}{3}(p-1)^8 p^{15}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^21^21)) &= \tfrac{1}{2}(p-1)^8 p^{14}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(2^21)) &= \tfrac{1}{2}(p-1)^8 p^{14}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^311)) &= \tfrac{1}{2}(p-1)^8 p^{14}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^32)) &= \tfrac{1}{2}(p-1)^8 p^{14}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^31^2)) &= (p-1)^8 p^{13}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^41)) &= (p-1)^8 p^{13}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}\\
\mu(U_p(1^5)) &= (p-1)^8 p^{12}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{40}
\end{aligned}$$

Proof. The proof of Theorem 17, with $\mathbb{Z}_p$ in place of $\mathbb{Z}$, shows that for any maximal quintic $\mathbb{Z}_p$-algebra R there is a unique element $A \in V_{\mathbb{Z}_p}$ up to $G(\mathbb{Z}_p)$-equivalence satisfying $R_{\mathbb{Z}_p}(A) = R$. Moreover, the automorphism group of such a maximal quintic $\mathbb{Z}_p$-algebra R is simply the size of the stabilizer in $G(\mathbb{Z}_p)$ of the corresponding element $A \in V_{\mathbb{Z}_p}$.

We normalize Haar measure dg on the p-adic group $G(\mathbb{Z}_p)$ so that $\int_{g\in G(\mathbb{Z}_p)} dg = \#G(\mathbb{F}_p)$. Since $|\mathrm{Disc}(x)|_p^{-1} \cdot dx$ is a $G(\mathbb{Q}_p)$-invariant measure on $V_{\mathbb{Z}_p}$, we must have for any maximal quintic $\mathbb{Z}_p$-algebra $R = R(A_0)$ that

$$\int_{\substack{x\in V_{\mathbb{Z}_p}\\ R(x)=R}} dx = c \cdot \int_{g\in G(\mathbb{Z}_p)/\mathrm{Stab}(A_0)} |\mathrm{Disc}(gA_0)|_p \cdot dg = c \cdot \frac{|\mathrm{Disc}(R)|_p \cdot \#G(\mathbb{F}_p)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(R)},$$

for some constant c. A Jacobian calculation using an indeterminate A_0 satisfying $\mathrm{Disc}(A_0) \neq 0$ shows that $c = 1$, independent of A_0.

We thus obtain, for any splitting symbol σ, that

$$\mu(U_p(\sigma)) \;=\; \int_{x\in U_p(\sigma)} dx \;=\; \#G(\mathbb{F}_p) \cdot \sum_{\{R\,:\,(R,p)=\sigma\}} \frac{|\mathrm{Disc}(R)|_p}{\#\mathrm{Aut}_{\mathbb{Z}_p}(R)},$$

where the sum is over isomorphism classes of maximal $\mathbb{Z}_p$-algebras R satisfying $(R,p) = \sigma$. The latter sum can be computed using a "mass formula" for étale $\mathbb{Q}_p$-extensions having a given splitting type σ (see [7, Prop. 1]), and we obtain

$$\mu(U_p(\sigma)) \;=\; \int_{x\in U_p(\sigma)} dx \;=\; \#G(\mathbb{F}_p) \cdot \frac{|\mathrm{Disc}(\sigma)|_p}{\#\mathrm{Aut}(\sigma)},$$

where $\mathrm{Disc}_p(\sigma)$ for $\sigma = (f_1^{e_1} f_2^{e_2} \cdots)$ is defined to be $p^{\sum_i f_i(e_i-1)}$, and $\#\mathrm{Aut}(\sigma)$ is defined to be the product of all the f_i times the number of permutations of the factors $f_i^{e_i}$ that preserve the symbol σ. For example, for $\sigma = (1^2 1^2 1)$, we have $\mathrm{Disc}_p(\sigma) = p^2$ and $\mathrm{Aut}(\sigma) = (1\cdot 1\cdot 1)\cdot 2 = 2$.

Computing $\#\mathrm{Aut}(\sigma)$ for each of the 17 values of σ, and noting that

$$\#G(\mathbb{F}_p) = (p-1)^8\, p^{16}\, (p+1)^4\, (p^2+1)^2\, (p^2+p+1)^2\, (p^4+p^3+p^2+p+1)\,/\,p^{40},$$

yields the lemma. □

Let $\mathcal{U}_p$ denote the union of the seventeen $U_p(\cdot)$'s in $V_{\mathbb{Z}}$. Then Lemma 20 implies that

$$\begin{aligned}(48)\quad \mu(\mathcal{U}_p) = (p-1)^8\, p^{12}\, (p+1)^4\, (p^2+1)^2\, (p^2+p+1)^2 \\ \cdot (p^4+p^3+p^2+p+1)\, (p^4+p^3+2p^2+2p+1)\,/\,p^{40}\end{aligned}$$

Regarding maximality, we have shown:

Theorem 21. *Let $A \in V_{\mathbb{Z}}$. Then $R(A)$ is a maximal ring if and only if $A \in \mathcal{U}_p$ for all primes p. The p-adic density of $\mathcal{U}_p$ in $V_{\mathbb{Z}}$ is given by* (48).

The preceding density results will play a critical role in understanding the density of discriminants of quintic rings and fields (see [5]).

Acknowledgments. This article is based on the methods of the author's Ph.D. thesis [1] at Princeton University. A preliminary summary and announcement of the results presented in this article appeared in [6].

I am extremely grateful to my advisor A. Wiles and to P. Sarnak for all their enthusiasm, encouragement, and guidance during this work. I am also very thankful to P. Deligne, B. Gross, H. Lenstra, J-P. Serre, and especially D. Zagier and M. Wood for numerous helpful comments and kind correspondence regarding earlier versions of this manuscript.

I thank E. Olszewski and W. Palenstijn for their invaluable help in typsetting the text and graphics in this manuscript. Last but not least, I wish to extend my gratitude to the Hertz Foundation for funding this work and to the Clay Mathematics Institute and the Packard Foundation for their subsequent support.

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), 217–250.

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

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

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

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

[7] ———, Mass formulae for local fields, and conjectures on the density of number field discriminants, *Internat. Math. Research Notices* (2007), Vol. 2007, Article ID rnm052, 20 pages.

[8] J. Buhler, *Artin's Conjecture for Icosohedral Representations*, Lecture Notes in Mathematics, Vol. 654, Springer-Verlag, New York, 1978.

[9] A. Cayley, On a new auxiliary equation in the theory of equations of the fifth order, *Philosophical Transactions of the Royal Society of London* **CLI** (1861), 263–276.

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

[11] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[12] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115** (2002), no. 1, 105–169.

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

[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 August 21, 2003)