A. C. Kable and A. Yukie
Nagoya Math. J.
Vol. 173 (2004), 163–203

A CONSTRUCTION OF QUINTIC RINGS

ANTHONY C. KABLE AND AKIHIKO YUKIE

Abstract. We construct a discriminant-preserving map from the set of orbits in the space of quadruples of quinary alternating forms over the integers to the set of isomorphism classes of quintic rings. This map may be regarded as an analogue of the famous map from the set of equivalence classes of integral binary cubic forms to the set of isomorphism classes of cubic rings and may be expected to have similar applications. We show that the ring of integers of every quintic number field lies in the image of the map. These results have been used to establish an upper bound on the number of quintic number fields with bounded discriminant.

§1. Introduction

To set the stage, we shall first remind the reader of the work of Delone and Fadeev. In [9], these authors began with an integral binary cubic form f and showed how to construct from it a based cubic ring R_f over $\mathbb{Z}$. (Here, as below, an *n-tic ring over $\mathbb{Z}$* is a commutative $\mathbb{Z}$-algebra that is free of rank n as a $\mathbb{Z}$-module. A ring is *based* if it is equipped with a distinguished basis containing 1.) They showed that the isomorphism class of R_f as a ring depends only upon the $\mathrm{GL}(2,\mathbb{Z})$-equivalence class of f and that the map $[f] \mapsto [R_f]$ from the set of equivalence classes of non-singular forms to the set of isomorphism classes of separable cubic rings is bijective. Moreover, they showed that their map is discriminant-preserving, where the discriminant of f is understood in the sense of invariant theory and that of R_f in the sense of ring theory. It is also (probably more) well known that Gauss constructed a correspondence between the set of equivalence

Received October 10, 2002.

Revised November 14, 2002.

2000 Mathematics Subject Classification: Primary 11R04; Secondary 11R21, 15A72, 14L30.

The first author was partially supported by a Dean's Incentive Grant, College of Arts and Sciences, Oklahoma State University.

The second author was partially supported by Grant-in-Aid for Scientific Research (No. 12440002), The Ministry of Education, Culture, Sports, Science and Technology, Japan.

classes of primitive integral binary quadratic forms and the narrow ideal class groups of orders of quadratic fields.

The spaces of binary quadratic and cubic forms are examples of what we call prehomogeneous vector spaces and there has been work on orbits of prehomogeneous vector spaces. For the general notion of prehomogeneous vector spaces, the reader should see [21] or [34]. We shall give the definition of prehomogeneous vector spaces in the case of irreducible representations in Section 4 (see Definition 1).

In [32], orbits of eight prehomogeneous vector spaces over fields were considered and the interpretations of orbits of these prehomogeneous vector spaces were given. As far as integral orbits are concerned, besides classical works, [15] was the first work that was carried out in the context of prehomogeneous vector spaces. In [15], integral orbits in one of the smaller examples identified in [32] were considered. Bhargava [2] considered integral orbits of several important cases. One of the cases Bhargava considered was the space of pairs of ternary quadratic forms. This case is one of the cases considered in [32] and orbits over fields correspond to quartic extensions of the ground field. In [2], Bhargava constructed a bijective map from the set of integral orbits of this prehomogeneous vector space to the set of triples (R, C, f) where R is a quartic ring, C is its resolvent ring (this notion of the resolvent ring is due to him) and f is a certain quadratic map from R to C. If one only considers R, this gives a map from the set of integral orbits of pairs of ternary quadratic forms to the set of quartic rings, thus giving an analogue of Delone and Fadeev's map. He also showed that this map is surjective and determined the orders of the fibers. Note that even though the correspondence between integral orbits and the set of triples (R, C, f) is bijective, the correspondence between integral orbits and the set of R (up to isomorphism) is not bijective.

The original Delone-Fadeev map has had various applications. Perhaps the most celebrated of these is the determination, by Davenport and Heilbronn [7], [8], of the density of cubic number fields. The Delone-Fadeev correspondence made it possible to study this question by understanding the integral orbits in the space of binary cubic forms, where all the machinery of reduction theory could be applied, and then transferring this understanding to the set of cubic rings. A quite different and much more recent application of the cubic Delone-Fadeev correspondence has been its use in [12] to establish a theory of Fourier coefficients for a class of quaternionic modular forms on the group G_2.

Even though we are mainly interested in orbits of prehomogeneous vector spaces, we shall consider a slightly more general pair (G, V) where G is a reductive algebraic group and V is a representation of G in this introduction to discuss the background. In order to formulate the properties of Delone and Fadeev's map, we require an invariant-theoretic discriminant on V to play the role of the discriminant of a binary cubic form. Fortunately, there is indeed a general invariant-theoretic definition of a discriminant. The idea may be traced back to Cayley, at least when G is a product of general linear groups and V is a tensor product of standard representations (see [4], where the discriminant is called the hyperdeterminant), but Cayley's language might prove obscure to a modern reader and various discriminants appear in his work under various names. The theory has recently been developed by Gelfand, Kapranov and Zelevinsky [11] in a far more general setting than we are currently considering. Fortunately, one may consult the important article of Knop and Menzel [22], which contains a wealth of information about discriminants of representations, including a simple criterion for a discriminant to exist. We shall call (G, V) *discriminantal* if it has a discriminant in the sense of [22]. We may then say that Delone and Fadeev's map is an example of a map $v \mapsto R_v$ from the space of a discriminantal representation to a set of based rings such that the ring-theoretic discriminant of R_v is equal to the invariant-theoretic discriminant of v and the isomorphism class of R_v depends only on the G-orbit of v.

In general we call a map from the set of integral orbits of a prehomogeneous vector space to the set of isomorphism classes of rings of some kind an *orbit-ring map.* When there is an orbit-ring map $v \mapsto R_v$ under discussion, we shall refer to its domain as the *parameter space.* If the group and the representation are defined over a ring Z and the rings R_v are Z-algebras, then we shall say that the orbit-ring map is *over* Z.

If an irreducible representation (G, V) is prehomogeneous then all relatively invariant polynomials on V are multiples of powers of a single polynomial. If (G, V) is discriminantal then it follows that this polynomial must be the discriminant in the sense of [22]. The prehomogeneous representation studied in this paper is discriminantal and so its fundamental relatively invariant polynomial is also its discriminant. This kind of terminology was used in [15] and [2] instead of the more usual terminology of relatively invariant polynomials.

Among the eight examples considered in [32], two were classical and six were new, at least in this form. This list included the space of pairs of ternary quadratic forms, parameterizing quartic algebras over the ground field and the space of quadruples of quinary alternating forms, parameterizing quintic algebras over the ground field even though the ring structures were not given directly. The correspondences in [32] were carried out in two ways, via geometry and via Galois cohomology. It is also natural to attempt to use invariant-theoretic methods to construct orbit-ring maps and this method was used in Section 2 of [31] to construct an orbit-ring map over a field with parameter space the space of trivectors on seven-dimensional affine space, parameterizing Cayley algebras over the field. In [2], Bhargava constructed orbit-ring maps for several cases and identified additional structures on the ring side, necessary to render the maps bijective. He also applied his results, in the spirit of Davenport-Heilbronn, to obtain a density theorem for symmetric totally real quartic number fields, with a more explicit constant than that previously announced by Cohen, Diaz y Diaz and Olivier [5] for all quartic number fields, thus confirming a conjecture of the second author [33]. Of all the results in [2], the one that is most relevant to us here is the construction of an orbit-ring map over the integers with parameter space the space of pairs of ternary quadratic forms, parameterizing quartic rings. (In fact, Bhargava's result is more precise in the sense that he introduces the notion of a cubic resolvent ring of a quartic ring and is thus able to make his map bijective.) The technique used to construct this map is similar to that originally used by Delone and Fadeev, with several additional complications. In [2], Bhargava also conjectures the existence of several other orbit-ring maps over the integers, refining those given in [32] over fields.

It may be helpful to be more explicit in the case of the space of trivectors on seven-dimensional affine space since the construction given in [31] may be viewed as a prototype for what we do here. Let $G = \mathrm{GL}(7)$ and let W denote the standard representation of G on seven-dimensional affine space. Then G acts on $V = \bigwedge^3 W$ and we seek to construct a Cayley algebra R_v from a point $v \in V$. To do so, let k be the underlying field and define $R_v = k \oplus W^*$ as k-vector spaces. The identity of the Cayley algebra R_v is $(1, 0) \in R_v$. The product operation on W^* may be identified with a pair of tensors, one in $W \otimes_k W \otimes_k W^*$, giving the W^* part of the product, and one in $W \otimes_k W$, giving the k part of the product. These spaces of tensors are located inside the polynomial algebra of V by constructing equivariant polynomial maps from V to each of them. The multiplication on $W^* \subset R_v$ is then specified by the images of v under these two maps. Even though the consideration was over fields in [31], the construction in [31] can be made integral with a proper normalization.

Now that we have sketched the development of the theory of orbit-ring maps up to this point, we are ready to state our main result, which is an amalgam of specializations of Theorems 1 and 4.

Theorem. *There is an orbit-ring map from the space of quadruples of quinary alternating forms over $\mathbb{Z}$ to the set of based quintic rings over $\mathbb{Z}$. The image of this map contains the maximal order in every quintic number field.*

As we have already mentioned, the existence of an orbit-ring map over the integers for quintic rings with parameter space the space of quadruples of quinary alternating forms is suggested by one of the examples in [32]. After we had completed and begun to circulate preprints of this paper, Bhargava [3] announced that he had proved a result similar to the above theorem. Since his announcement does not contain a detailed statement of his theorem nor any indication of the proof, we cannot currently assess the relationship between our work and his. If his work on quartic rings is any guide, then it seems likely that our methods differ somewhat. In any case, our ultimate goal is the estimate on quintic discriminants stated below.

The great complexity of the parameter space of the quintic orbit-ring map means that we are currently unable to deduce the precise density of symmetric quintic number fields. However, we are able to derive upper bounds. Let $N_5(X)$ denote the number of quintic number fields whose discriminant does not exceed X in absolute value. There is an old conjecture that $N_5(X) \sim c_5 X$ for some constant c_5 (see [25, Unsolved Problem 7]). As far as we are aware, the best previously known upper bound in this direction is $N_5(X) \ll X^{7/4}$, due to W. Schmidt [29]. In [18] we improve on this as follows:

Theorem. *For any $\epsilon > 0$ there is a constant C_ϵ such that $N_5(X) \leq C_\epsilon X^{1+\epsilon}$ for all $X > 0$.*

The proof of this theorem combines the main theorem of this paper with a convergence result for an incomplete zeta integral associated with the space of quadruples of quinary alternating forms, proved in [18]. This paper and [18] are inseparable companions and each depends on the other; ideally, they should be read together.

It is now time to describe our approach and the content and purpose of the sections to follow. We shall do this in some detail because, although the minutiae of the argument are often complex, the overall structure is rather simple and we wish to make this clear.

Our first task is the construction of the orbit-ring map for quintic rings. Although we have only considered quintic rings over $\mathbb{Z}$ above, the natural setting for the construction is more general and there seems to be no reason to impose unnecessary restrictions. In what follows, we shall take a principal ideal domain Z of characteristic zero as the ground ring. The field of fractions of Z will be denoted by Q. We already suspect that the space V of quadruples of quinary alternating forms under the action of $G = \mathrm{GL}(4) \times \mathrm{GL}(5)$ is an appropriate parameter space and this provides a starting point. If R is a quintic ring over Z then we may split R as $R = Z \cdot 1 \oplus M$, where M is a rank four Z-module, and all the essential information about the ring structure of R is contained in the map $M \otimes_Z M \to M$ given by multiplication followed by projection to M. One way to associate a ring R_v to a point $v \in V_Z$ is to find a way to construct from v a rank four Z-module M and a suitable map $M \otimes_Z M \to M$. Since the isomorphism class of R_v is to depend only on the G_Z-orbit of v, this association should be equivariant with respect to some homomorphism $G_Z \to \mathrm{GL}(M)$. When it is phrased in this way, the problem of constructing an orbit-ring map may be recognized as a problem of classical invariant theory.

Let $\mathrm{Aff}(4)_Z$ denote rank four affine space over Z and $\mathrm{Aff}(4)^*_Z$ denote its dual. It is harmless to standardize M by identifying it either with $\mathrm{Aff}(4)_Z$ or $\mathrm{Aff}(4)^*_Z$ (to exclude the second possibility at this stage would be prejudicial). Thus we seek an equivariant polynomial map of the form

$$V \longrightarrow \chi \otimes \mathrm{Aff}(4)^* \otimes \mathrm{Aff}(4)^* \otimes \mathrm{Aff}(4)$$

or

$$V \longrightarrow \chi \otimes \mathrm{Aff}(4) \otimes \mathrm{Aff}(4) \otimes \mathrm{Aff}(4)^*,$$

where χ denotes a character of G. It emerges that, up to twists (which increase the degree), there is precisely one map of each kind. The reader may consult [16] for results that reduce this assertion to a routine calculation. The fundamental map of the first kind is given by polynomials of degree fifteen and the fundamental map of the second kind is given by polynomials of degree five. Of these two, only the second satisfies the necessary requirements to arise from the multiplication operation on a quintic ring. Thus we see that the correct choice is to identify M with $\mathrm{Aff}(4)^*_Z$ and that, once this is done, our invariant theory problem has a unique solution. In this way, we may build a quintic ring structure on $Z \oplus \mathrm{Aff}(4)^*_Z$ from a point $v \in V_Z$ in an equivariant fashion.

If we were working over a field, then this would be the end of the construction, but as it is there is an additional complication. There is no non-zero equivariant map $V \to \chi \otimes \mathrm{Aff}(4)$ and, as a consequence of this, the trace of every element of $\mathrm{Aff}(4)^*_Z$ under the ring structure just constructed on $Z \oplus \mathrm{Aff}(4)^*_Z$ is zero. However, most quintic rings do not admit a splitting with this property. In order to solve this problem, we observe that in every quintic ring R there is an order $R[5] = Z \cdot 1 + 5R$ that does admit such a splitting. The ring we have just constructed is $R[5]$ and we wish to recover R. This is an elementary problem of ring theory and, by solving it, we finish the construction. So our construction is to go through $R[5]$ to R. In [2], the construction was made using special bases of quartic rings and yielded the quartic ring directly. Our construction requires two steps, but does not use any special choice of basis and hence is fully equivariant. In the proof of the upper bound in [18], we shall need to prove that the construction in this paper is compatible with the geometric construction in [32]. For that purpose it is essential that the construction be fully equivariant. We have decided to include the self-contained proof of the compatibility statement in [18], rather than in the present paper.

The details of the construction just described are carried out in Sections 2–5. In Section 2, we review for later use the most basic notions of tensor invariant theory. Section 3 starts with a review of some basic facts from the theory of rings of finite rank, including the connection between the multiplication law on R and the map $M \otimes_Z M \to M$ used above. In Proposition 1, we give the solution to the problem of recognizing that a ring of rank n has the form $R[n]$ for some ring R. The section concludes by describing a slight generalization of the discriminant of a Z-lattice in a Q-algebra. This discriminant will play an essential role later on. The salient features of the parameter space V are reviewed in Section 4. Finally, the construction of the orbit-ring map for quintic rings is carried out in Section 5, following the path that we have already described.

After the construction of the orbit-ring map is complete, our next task is to show that the ring of integers in every quintic number field lies in the image of the map. We do this in two steps. The first is to prove a result to the effect that if the ring $R[N] = Z\cdot 1 + NR$ lies in the image of the orbit-ring map then so does the ring R. Actually, the result we prove is slightly weaker than this, but the distinction is not conceptually important. For obvious reasons, we refer to this result as the division theorem (Theorem 2). The proof of this theorem is, unfortunately, rather intricate, but the idea is simple. We choose a point $v \in V_Z$ such that v maps to the ring $R[N]$. All the components of the first restricted structure tensor of $R[N]$ with respect to a suitable restricted basis are divisible by N and our aim is to modify v so as to remove this common factor. We choose a prime factor p of N; it suffices to modify v so as to divide the components of the first restricted structure tensor by p. To do this, we consider the reduction $\bar{v}$ of v modulo p. This is a point of V_K, where $K = Z/pZ$, and we apply the theory of alternating forms over a field to bring $\bar{v}$ into a relatively simple shape. Then, by using the fact that the first restricted structure tensor associated to $\bar{v}$ is identically zero modulo p, we obtain enough divisibility conditions on the entries of v so as to be able to effect the division by p. The proof of the division theorem occupies the whole of Section 6.

The division theorem reduces the problem of showing that a quintic ring R lies in the image of the orbit-ring map to the problem of showing that the order $R[N]$ lies in the image for some N. In Section 7, this is done when R is the maximal order in a quintic number field. Given the results of [32] and the division theorem, the proof is a fairly simple matter.

§2. A notational primer

In this work we shall have to consider relatively equivariant polynomial maps between various representations. In order to construct and describe these maps, it will be convenient to use the notational apparatus and some of the elementary results from tensor invariant theory, for which [13] is an excellent modern reference. The purpose of this section is to establish our conventions regarding this notation. Although this material is standard, we hope that a brief discussion will render our exposition more self-contained.

For any $n \geq 1$ let $\mathrm{Aff}(n)$ denote n-dimensional affine space, regarded as a variety over $\mathbb{Z}$. By a *tensor* we shall mean an element of a space of the form

$$\mathrm{Aff}(n_1) \otimes \cdots \otimes \mathrm{Aff}(n_r) \otimes \mathrm{Aff}(m_1)^* \otimes \cdots \otimes \mathrm{Aff}(m_s)^*. \tag{1}$$

Since $\mathrm{Aff}(n)$ and $\mathrm{Aff}(n)^*$ are equipped with canonical bases, a tensor has canonical coordinates. We shall use subscripts to index coordinates corresponding to factors of the form $\mathrm{Aff}(n)$ and superscripts to index coordinates corresponding to factors of the form $\mathrm{Aff}(n)^*$. Thus the canonical coordinates of a tensor A in the above space would be written as

$$A^{j_1 j_2 \cdots j_s}_{i_1 i_2 \cdots i_r},$$

with $1 \le i_p \le n_p$ and $1 \le j_q \le m_q$. We shall refer to n_p as the *valence* of the subscript i_p and similarly with superscripts. We shall also refer to the canonical coordinates as components of the tensor A.

The tensors we consider will usually have indices of two different valences and we use different alphabets to distinguish them. In later sections, but not in this one, it will be understood that roman indices have valence four and that greek indices have valence five.

It will be convenient to employ a variation of the summation convention in certain formulas. According to this convention, summation takes place over any index that appears in a term both as a subscript and as a superscript. A formula containing a summation sign without a specified set of summation indices is to be interpreted using this convention. Thus, the expression

$$\sum A^{ij}_{kl} B^{pk}_{iq}$$

means

$$\sum_{i,k} A^{ij}_{kl} B^{pk}_{iq}.$$

The group

$$\mathrm{GL}(n_1) \times \cdots \times \mathrm{GL}(n_r) \times \mathrm{GL}(m_1) \times \cdots \times \mathrm{GL}(m_s) \tag{2}$$

acts on the space (1) and we want to express this action in canonical coordinates. An element $g \in \mathrm{GL}(n)$ will be written as $g = (g^j_i)$. If g is identified with an n-by-n matrix then i is the row index and j is the column index. The inverse of g will be written as $g^{-1} = (\bar{g}^j_i)$. We note that $(gh)^j_i = \sum g^k_i h^j_k$. If A is an element of (1) and $g = (g(1), \ldots, g(r), h(1), \ldots, h(s))$ is an element of (2), then let $\widehat{A} = gA$. In canonical coordinates, we have

$$\widehat{A}^{l_1 l_2 \cdots l_s}_{k_1 k_2 \cdots k_r} = \sum A^{j_1 j_2 \cdots j_s}_{i_1 i_2 \cdots i_r} g(1)^{i_1}_{k_1} \cdots g(r)^{i_r}_{k_r} \overline{h(1)}^{l_1}_{j_1} \cdots \overline{h(s)}^{l_s}_{j_s}. \tag{3}$$

The discussion of the previous paragraph may also be applied to the action of subgroups of (2) on (1). In our applications of this formalism, the ranks of the modules will all be either 4 or 5 and we shall consider tensors under the action of GL(4) × GL(5) embedded diagonally into (2). This brings us closer to the standard setting of tensor invariant theory, where all the modules are of the same rank n and the group is $\mathrm{GL}(n)$ acting simultaneously on all the factors in (1). In context, there should be no ambiguity.

We shall make frequent use of three special tensors. The Kronecker delta $\boldsymbol{\delta}$ of rank n is the tensor in $\mathrm{Aff}(n) \otimes \mathrm{Aff}(n)^*$ whose canonical coordinates are

$$\boldsymbol{\delta}^i_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

The fully alternating contravariant tensor of rank n, denoted by $\boldsymbol{\varepsilon}$, is the element of $\bigl(\mathrm{Aff}(n)^*\bigr)^{\otimes n}$ whose canonical coordinates are

$$\boldsymbol{\varepsilon}^{i_1 \cdots i_n} = \begin{cases} 1 & \text{if } (i_1, \ldots, i_n) \text{ is an even rearrangement of } (1, \ldots, n), \\ -1 & \text{if } (i_1, \ldots, i_n) \text{ is an odd rearrangement of } (1, \ldots, n), \\ 0 & \text{otherwise}, \end{cases}$$

and the fully alternating covariant tensor of rank n, also denoted by $\boldsymbol{\varepsilon}$, is the element of $\mathrm{Aff}(n)^{\otimes n}$ whose canonical coordinates are defined similarly. The fundamental property of $\boldsymbol{\varepsilon}$ is expressed by the equations

$$\sum \boldsymbol{\varepsilon}^{i_1 \cdots i_n} g^{j_1}_{i_1} \cdots g^{j_n}_{i_n} = \det(g) \boldsymbol{\varepsilon}^{j_1 \cdots j_n} \tag{4}$$

and

$$\sum \boldsymbol{\varepsilon}_{j_1 \cdots j_n} g^{j_1}_{i_1} \cdots g^{j_n}_{i_n} = \det(g) \boldsymbol{\varepsilon}_{i_1 \cdots i_n} \tag{5}$$

for $g \in \mathrm{GL}(n)$. It is also useful to observe the identity

$$\det(g) \sum \boldsymbol{\varepsilon}^{j_1 \cdots j_{n-1} c} \bar{g}^b_c = \sum \boldsymbol{\varepsilon}^{i_1 \cdots i_{n-1} b} g^{j_1}_{i_1} g^{j_2}_{i_2} \cdots g^{j_{n-1}}_{i_{n-1}}, \tag{6}$$

which expresses the classical relationship between the adjoint and the inverse of $g \in \mathrm{GL}(n)$.

So far we have restricted our discussion to tensors on affine space, where there is a canonical basis and hence canonical coordinates. There is a second point of view on tensors that we shall require in Section 3. Suppose that Z is a commutative ring with 1 and that $N_1, \ldots, N_r$ and $M_1, \ldots, M_s$ are free Z-modules of ranks $n_1, \ldots, n_r$ and $m_1, \ldots, m_s$. We may extend the notion of a tensor to include elements of the space

$$N_1 \otimes_Z \cdots \otimes_Z N_r \otimes_Z M_1^* \otimes_Z \cdots \otimes_Z M_s^*, \tag{7}$$

where M_q^* denotes $\mathrm{Hom}_Z(M_q, Z)$. There are non-canonical isomorphisms $N_p \cong \mathrm{Aff}(n_p)_Z$ and $M_q^* \cong \mathrm{Aff}(m_q)_Z^*$ and thus we may non-canonically identify an element of (7) with an element of (1) and hence assign it coordinates. From this point of view, (3) expresses the relationship between two sets of coordinates for a single tensor A in (7). We shall occasionally blur the distinction between a tensor in (7) and its components with respect to some specified choice of bases. This harmless abuse of terminology is akin to the so-called abstract index notation sometimes used in differential geometry and is similarly convenient.

§3. Generalities on rings and modules

Let Z be a principal ideal domain of characteristic zero and Q be its field of fractions. We shall regard $\mathbb{Z}$ as embedded in Z. A *ring of rank* n is an associative commutative Z-algebra R such that, considered as a Z-module via the Z-algebra structure, R is free of rank n. If we wish to emphasize Z then we shall refer to a ring of rank n *over* Z. The case $n = 2$ is somewhat anomalous and so we shall always require that $n \geq 3$.

Let R be a ring of rank n. The identity $1 \in R$ is indivisible and consequently it is possible to find an ordered basis of R of the form $1, v_1, \ldots, v_{n-1}$. We call such an ordered basis a *restricted basis* of R. Let $1, v_1, \ldots, v_{n-1}$ be a restricted basis of R and $1^*, v_1^*, \ldots, v_{n-1}^*$ be its dual basis. Let M be the submodule of R generated by $\{v_1, \ldots, v_{n-1}\}$. The multiplication operation on R determines and is determined by two maps $C : M \otimes_Z M \to M$ and $D : M \otimes_Z M \to Z$ such that

$$rs = D(r \otimes s) \cdot 1 + C(r \otimes s)$$

for $r, s \in M$. We may regard C as a tensor in the space $M^* \otimes_Z M^* \otimes_Z M$ and D as a tensor in the space $M^* \otimes_Z M^*$. We call C and D the *first* and *second restricted structure tensors* of R with respect to the given restricted basis.

In order to introduce the components of these tensors, we identify $v_1, \ldots, v_{n-1}$ with the standard ordered basis of $\mathrm{Aff}(n-1)_Z^*$. It may seem strange that we take the dual space here, but this is the most convenient choice. After making this identification, C is identified with a tensor in $\mathrm{Aff}(n-1)_Z \otimes_Z \mathrm{Aff}(n-1)_Z \otimes_Z \mathrm{Aff}(n-1)_Z^*$ and D is identified with a tensor in $\mathrm{Aff}(n-1)_Z \otimes_Z \mathrm{Aff}(n-1)_Z$. The components of these tensors are $C_{ij}^k = v_k^*(v_i v_j)$ and $D_{ij} = 1^*(v_i v_j)$ for $1 \leq i, j, k \leq n-1$.

We may recover the ring R, up to isomorphism, from the components C_{ij}^k and D_{ij}. To do this, we introduce a Z-bilinear multiplication on the Z-module $R' = Z \oplus \mathrm{Aff}(n-1)_Z^*$ such that $(1,0)$ is a multiplicative identity and

$$(0, e_i^*)(0, e_j^*) = \Big(D_{ij}, \sum_k C_{ij}^k e_k^*\Big) \tag{8}$$

for $1 \leq i, j \leq n-1$. The resulting ring R' is isomorphic to the original ring R. It is important to observe that the isomorphism class of the ring R' depends only on the tensors C and D. Thus, if $g \in \mathrm{GL}(n)_Z$ and

$$\begin{aligned} \widehat{C}_{ij}^k &= \sum C_{ab}^c g_i^a g_j^b \bar{g}_c^k, \\ \widehat{D}_{ij} &= \sum D_{ab} g_i^a g_j^b, \end{aligned}$$

then the ring R'' constructed as above from $\widehat{C}$ and $\widehat{D}$ is isomorphic to the ring R' constructed from C and D. Indeed, the Z-linear map $f : R'' \to R'$ given by $f(1,0) = (1,0)$ and $f(0, e_i^*) = \big(0, \sum_a g_i^a e_a^*\big)$ is an isomorphism. We shall use this observation frequently in what follows.

Lemma 1. *The first and second restricted structure tensors of a ring of rank n with respect to any restricted basis satisfy the identities*

$$C_{ij}^k = C_{ji}^k, \tag{9}$$

$$D_{ij} = D_{ji}, \tag{10}$$

$$\sum_r D_{ir} C_{jk}^r = \sum_s D_{js} C_{ik}^s, \tag{11}$$

$$\sum_r C_{ij}^r C_{rk}^l + \delta_k^l D_{ij} = \sum_s C_{jk}^s C_{si}^l + \delta_i^l D_{jk}. \tag{12}$$

Conversely, if C and D are tensors satisfying these identities then they are the first and second restricted structure tensors of a ring of rank n.

Proof. The first two identities follow from the commutativity of multiplication and the second two from the associativity of multiplication. Conversely, suppose that we have tensors C and D satisfying these identities. Then we may create a ring R' from them as explained in the paragraph containing (8). This ring has C and D as its first and second restricted structure tensors. □

The first part of the following lemma was observed by Delone and Fadeev when $n = 3$ (Equation (2), Section 15 in [9]) and extended to $n = 4$ by Bhargava [2].

Lemma 2. *Let R be a ring of rank n over Z and $1, v_1, \ldots, v_{n-1}$ a restricted basis for R. The first restricted structure tensor of R with respect to this basis determines the second. If Z_0 is a subring of Z and $C_{ij}^k \in Z_0$ for all i, j and k then $D_{ij} \in Z_0$ for all i and j. If, in addition, $\sum_j C_{ij}^j = 0$ then $D_{ij} = \frac{1}{n-2} \sum_{r,s} C_{ir}^s C_{sj}^r$.*

Proof. Choose i, j between 1 and $n - 1$. Since $n - 1 \geq 2$, we may choose l between 1 and $n - 1$ such that $l \neq i$ and set $k = l$. With these choices, (12) gives a formula for D_{ij} in terms of C. This formula only involves sums and products of various components of C and, from this, the second claim follows. If $\sum_j C_{ij}^j = 0$ then the given expression for D follows by contracting (12) with respect to i and l. □

It follows from this lemma that two rings of rank n that have the same first restricted structure tensor with respect to some choices of restricted bases are isomorphic.

We next recall some facts about the trace form and discriminants. Assume that R is a ring of rank n. Then to each $u \in R$ is associated a linear map $L_u : R \to R$ given by $L_u(v) = uv$ and we define $\operatorname{tr} : R \to Z$ by $\operatorname{tr}(u) = \operatorname{tr}(L_u)$. This construction gives rise to a bilinear form $(u, v) \mapsto \operatorname{tr}(uv)$, the *trace form* of R. If N is any Z-submodule of R of rank n then the *discriminant of N* is the discriminant of the restriction of the trace form to N. We shall denote the discriminant of N by $\operatorname{Disc}(N)$. This discriminant is well-defined as an element of the set $Z/(Z^\times)^2$ and equalities involving discriminants must be understood to take place in this coset space.

Lemma 3. *Suppose that R is a ring of rank n and that the first restricted structure tensor of R satisfies $\sum_j C_{ij}^j = 0$. Then* $\operatorname{Disc}(R) = n^n \det(D)$.

Proof. Choose a restricted basis $1, v_1, \ldots, v_{n-1}$ of R. The condition $\sum_j C_{ij}^j = 0$ is equivalent to $\operatorname{tr}(v_i) = 0$. Thus $\operatorname{tr}(v_i v_j) = nD_{ij}$ for all i and j and it follows that the matrix of the trace form with respect to the given restricted basis is

$$\begin{pmatrix} n & 0 \\ 0 & nD \end{pmatrix}.$$

The determinant of this is $n^n \det(D)$. ∎

Let R be a ring of rank n and $a \in Z \setminus \{0\}$. We define $R[a] = Z \cdot 1 + aR$. Then $R[a]$ is an order in R and $\mathrm{Disc}(R[a]) = \mathrm{Disc}(R)a^{2n-2}$.

Lemma 4. *If R and R' are rings of rank n and $R[n] \cong R'[n]$ then $R \cong R'$.*

Proof. The trace of every element of the ring $R[n]$ is divisible by n. If we let M be the set of elements in $R[n]$ whose trace is zero then it follows that $R[n] = Z \cdot 1 \oplus M$. Let $\tilde{v}_1, \ldots, \tilde{v}_{n-1}$ be an ordered basis for M. Then there are elements $v_1, \ldots, v_{n-1} \in R$ such that $\tilde{v}_i = nv_i - t_i 1$ where $t_i = \mathrm{tr}(v_i)$. Moreover, $1, v_1, \ldots, v_{n-1}$ is a restricted basis for R. If $\widetilde{C}$ is the first restricted structure tensor of $R[n]$ with respect to $1, \tilde{v}_1, \ldots, \tilde{v}_{n-1}$ and C is the first restricted structure tensor of R with respect to $1, v_1, \ldots, v_{n-1}$ then

$$\widetilde{C}^k_{ij} = -t_i \boldsymbol{\delta}^k_j - t_j \boldsymbol{\delta}^k_i + nC^k_{ij}.$$

The congruence class of t_i modulo n can therefore be recovered from $\widetilde{C}$ and, once representatives of the appropriate congruence classes are chosen, we can then solve for C. Replacing t_i by $t_i + ns_i$ changes C^k_{ij} into $C^k_{ij} + s_i \boldsymbol{\delta}^k_j + s_j \boldsymbol{\delta}^k_i$. This amounts to replacing the restricted basis $1, v_1, \ldots, v_{n-1}$ by the restricted basis $1, v_1 + s_1 1, \ldots, v_{n-1} + s_{n-1} 1$. Thus the isomorphism class of R is determined by that of $R[n]$. ∎

Proposition 1. *Suppose that $\widetilde{R}$ is a ring of rank n and that $\widetilde{R}$ has a restricted basis $1, \tilde{v}_1, \ldots, \tilde{v}_{n-1}$ such that the corresponding first restricted structure tensor satisfies*

$$\widetilde{C}^k_{ij} \equiv 0 \ (n) \quad \textit{whenever } k \notin \{i, j\} \tag{13}$$

$$\widetilde{C}^j_{ij} \equiv \widetilde{C}^k_{ik} \ (n) \quad \textit{whenever } i \notin \{j, k\} \tag{14}$$

$$\sum_j \widetilde{C}^j_{ij} \equiv 0 \ (n) \quad \textit{for all } i. \tag{15}$$

Then there is a ring R of rank n such that $\widetilde{R} \cong R[n]$.

Proof. According to (14), it is possible to choose $t_1, \ldots, t_{n-1} \in Z$ such that $t_i \equiv -\widetilde{C}^j_{ij} \ (n)$ whenever $j \neq i$. We shall establish the congruence

$$\widetilde{D}_{ij} - \sum_r \widetilde{C}^r_{ij} t_r - t_i t_j \equiv 0 \ (n^2) \tag{16}$$

for these integers. This will require several steps. First, by combining (15) with the congruences for the t_i, we find that $\widetilde{C}^i_{ii} \equiv -2t_i\ (n)$ for all i.

Secondly, observe that (16) is either true for all possible choices of $t_1, \ldots, t_{n-1}$ or false for all of them. Indeed, if we take the difference between the left hand side of (16) for $t_1, \ldots, t_{n-1}$ and for $t_1 + ns_1, \ldots, t_{n-1} + ns_{n-1}$, we obtain

$$n\Big[\sum_r \widetilde{C}^r_{ij} s_r + s_i t_j + s_j t_i\Big]. \tag{17}$$

All the terms in the sum such that $r \notin \{i, j\}$ are divisible by n by (13) and so (17) is congruent modulo n^2 to $n\big[\widetilde{C}^i_{ij} s_i + \widetilde{C}^j_{ij} s_j + s_i t_j + s_j t_i\big]$, if $i \neq j$, and to $n\big[\widetilde{C}^i_{ii} s_i + 2 s_i t_i\big]$, if $i = j$. In either case, the expression in square brackets is divisible by n and the observation is established. It follows that it suffices to establish (16) for any particular choice of $t_1, \ldots, t_{n-1}$.

It will be convenient to assume henceforth that $n \geq 4$. When $n = 3$ the congruence may be verified by a slight variation of the following argument. We do not require this case and so we do not take the space to record the variant. Since $(n-1) \geq 3$, we may choose some $k \notin \{i, j\}$. We shall verify (16) for the specific choices $t_a = -\widetilde{C}^k_{ak}$ for $a \neq k$ and $t_k = -\widetilde{C}^i_{ik}$. Making the choice $l = k$ in (12), we obtain

$$\widetilde{D}_{ij} = \sum_s \widetilde{C}^s_{jk} \widetilde{C}^k_{si} - \sum_r \widetilde{C}^r_{ij} \widetilde{C}^k_{rk}. \tag{18}$$

In the first sum, all terms are divisible by n^2 except possibly those with $s = j$ and $s = k$. Consequently, these terms may be discarded from the sum modulo n^2. Also, $t_r = -\widetilde{C}^k_{rk}$ for $r \neq k$, $t_i = -\widetilde{C}^k_{ik}$ and $t_j = -\widetilde{C}^k_{jk}$. Thus

$$\widetilde{D}_{ij} \equiv \widetilde{C}^j_{jk} \widetilde{C}^k_{ij} + t_i t_j + \sum_{r \neq k} \widetilde{C}^r_{ij} t_r - \widetilde{C}^k_{ij} \widetilde{C}^k_{kk}\ (n^2). \tag{19}$$

This gives

$$\widetilde{D}_{ij} - \sum_r \widetilde{C}^r_{ij} t_r - t_i t_j \equiv \widetilde{C}^k_{ij}\big[\widetilde{C}^j_{jk} - t_k - \widetilde{C}^k_{kk}\big]\ (n^2) \tag{20}$$

and the factor in square brackets is congruent to $-t_k - t_k + 2t_k = 0$ modulo n. Since n divides $\widetilde{C}^k_{ij}$, (16) is established.

Now define

$$R = \Big\{\alpha_0 + \sum_r \alpha_r \tilde{v}_r \in Q \otimes_Z \widetilde{R} \;\Big|\; n\alpha_1, \ldots, n\alpha_{n-1} \in Z,\ \alpha_0 - \sum_r t_r \alpha_r \in Z\Big\}.$$

Then R is a Z-submodule of $Q \otimes_Z \widetilde{R}$ of rank n with basis $1, v_1, \ldots, v_{n-1}$ where $v_i = \frac{1}{n}(t_i + \tilde{v}_i)$. Also, $\widetilde{R} = R[n]$. The only thing that remains to be verified is that R is a subring of $Q \otimes_Z \widetilde{R}$. This amounts to checking that R is closed under multiplication and for this it is sufficient to show that $v_i v_j \in R$ for all i and j. For definiteness, we assume that $i \neq j$; the other case is almost identical. We have

$$v_i v_j = \frac{1}{n^2}(\widetilde{D}_{ij} + t_i t_j) + \frac{1}{n^2}(t_j + \widetilde{C}^i_{ij})\tilde{v}_i + \frac{1}{n^2}(t_i + \widetilde{C}^j_{ij})\tilde{v}_j + \frac{1}{n^2} \sum_{r \notin \{i,j\}} \widetilde{C}^r_{ij} \tilde{v}_r.$$

The first $n-1$ conditions required for this to be an element of R follow from (13) and the congruences $t_i \equiv -\widetilde{C}^j_{ij}\ (n)$ and $t_j \equiv -\widetilde{C}^i_{ij}\ (n)$. The last condition reduces to (16). □

The following observation will prove a useful complement to Proposition 1.

LEMMA 5. *Let K be a commutative ring with* 1 *and V a free K-module of rank $n-1$ with $n \geq 3$. Suppose that $n = 0$ in K, that $A \in V \otimes_K V \otimes_K V^*$ and that the components of A with respect to some basis of V satisfy the conditions*

$$A^k_{ij} = A^k_{ji}, \tag{21}$$

$$A^k_{ij} = 0 \quad \textit{whenever } k \notin \{i, j\}, \tag{22}$$

$$A^j_{ij} = A^k_{ik} \quad \textit{whenever } i \notin \{j, k\}, \tag{23}$$

$$\sum_j A^j_{ij} = 0. \tag{24}$$

Then the components of A with respect to any basis satisfy the same conditions.

Proof. It is well-known that symmetry conditions such as (21) are invariant under change of basis. Condition (24) expresses the vanishing of the vector $B_i = \sum_j A^j_{ij}$ and so it is automatically true with respect to all bases if it is true with respect to one. The other two conditions are not tensorial in nature and so we must verify directly that they are preserved under change of basis.

Suppose that the matrix (h^j_i) expresses the change of basis from a basis such that the conditions hold to a second basis and that $(\bar{h}^j_i)$ is the inverse matrix. Let $\widehat{A}_{ij}^{k}$ be the components of A with respect to the second basis. Then

$$\widehat{A}_{ij}^{k} = \sum_{a,b,c} A_{ab}^{c}\, h_i^a\, h_j^b\, \bar{h}_c^k. \tag{25}$$

We may choose $u_1, \ldots, u_{n-1} \in K$ such that $u_i = A_{ij}^{j}$ whenever $i \neq j$, by Condition (23). According to Condition (24), we have $(n-2)u_i + A_{ii}^{i} = 0$ for all i. By the assumption that $n = 0$ in K, this implies that $A_{ii}^{i} = 2u_i$ for all i. Thus, making use of Conditions (21) and (22),

$$\widehat{A}_{ij}^{k} = \sum_{a \neq b} u_b\, h_i^a\, h_j^b\, \bar{h}_a^k + \sum_{b \neq a} u_a\, h_i^a\, h_j^b\, \bar{h}_b^k + 2 \sum_{a} u_a\, h_i^a\, h_j^a\, \bar{h}_a^k. \tag{26}$$

Now, $\sum_l h_i^l \bar{h}_l^j = \boldsymbol{\delta}_i^j$ and so this equation yields

$$\widehat{A}_{ij}^{k} = \boldsymbol{\delta}_i^k \sum_{b} u_b\, h_j^b + \boldsymbol{\delta}_j^k \sum_{a} u_a\, h_i^a. \tag{27}$$

This expression makes it clear that Conditions (22) and (23) hold with respect to the new basis. □

As a last point of terminology, we shall refer to a ring of rank five as a *quintic ring.*

§4. Review of the parameter space

In this section we give a brief review of the salient properties of the space of quadruples of quinary alternating forms. This remarkable space has been investigated from various perspectives by a number of authors. For example, in [21] and [26] it is studied over $\mathbb{C}$ from the point of view of invariant theory. The space appears as the abelianization of the unipotent radical of a certain maximal parabolic subgroup of a reductive group of type E_8 under the conjugation action of the Levi component. For this reason, it arises when the representation theory of E_8 is investigated. The referee has been kind enough to bring to our attention several articles in which the space of quadruples of quinary alternating forms plays a significant role in the representation theory of E_8 over a finite field. The most approachable of these is [19], but the referee has also noted that the same space appears in Lusztig's theory of character sheaves [14], [23]. The list could be extended to include studies involving representation theory over p-adic fields, as well as other applications, but perhaps the reader will already grant the point that the space is significant and of wide interest.

For the sake of the reader we briefly recall the definition of prehomogeneous vector spaces. Since we are mainly interested in the space of quadruples of quinary alternating forms, we restrict ourselves to irreducible representations. For the definition of more general prehomogeneous vector spaces, the reader should see [21].

Let G be a connected reductive group and V an irreducible representation of G.

Definition 1. The pair (G, V) is called a *prehomogeneous vector space* if

(1) there exists a Zariski open G-orbit in V and

(2) there exists a non-constant polynomial $P(x) \in k[V]$ and a rational character $\chi(g)$ of G such that $P(gx) = \chi(g)P(x)$ for all $g \in G$ and $x \in V$.

Any polynomial $P(x)$ in the above definition is called a relatively invariant polynomial.

In [32], the space of quadruples of quinary alternating forms is considered over an arbitrary field and this reference is a convenient source for the facts that we require. Note that in [32], there was an assumption on the characteristic of the field, but it was pointed out later in [17] that such an assumption is unnecessary. Let $V = \mathrm{Aff}(4) \otimes \bigwedge^2 \mathrm{Aff}(5)$ and $G = \mathrm{GL}(4) \times \mathrm{GL}(5)$. Then G acts on V and it is well known that the pair (G, V) is a prehomogeneous vector space. It easily follows from the criterion of [22] that this representation is discriminantal. In light of the definition of a discriminant, the same conclusion can also be drawn from a glance at the table of orbits in (G, V) and their duals given in [26].

Let $f_1, \dots, f_4$ be the standard basis of $\mathrm{Aff}(4)$ and $e_1, \dots, e_5$ be the standard basis of $\mathrm{Aff}(5)$. We introduce canonical coordinates $x_{i\alpha\beta}$ on V dual to the basis

$$\{f_i \otimes (e_\alpha \wedge e_\beta) \mid 1 \le i \le 4,\ 1 \le \alpha < \beta \le 5\}$$

and extend the notation by setting $x_{i\alpha\alpha} = 0$ and $x_{i\beta\alpha} = -x_{i\alpha\beta}$. Since G acts on V, it also acts on V^* and it is important to note that x thus extended is tensorial with respect to this action. That is, if $(h, g) \in G$ then

$$(h, g)x_{i\alpha\beta} = \sum x_{j\gamma\delta}\, h_i^j\, g_\alpha^\gamma\, g_\beta^\delta. \tag{28}$$

There is a second model of the space (G, V) that will be useful in Section 6. Here we identify the elements of V with 1-by-4 row vectors of 5-by-5 alternating matrices. The action of G on V in this model may be written as

$$(h, g)[M_1, \ldots, M_4] = [gM_1{}^t g, \ldots, gM_4{}^t g]\,{}^t h.$$

Define

$$\begin{aligned} w_1 &= f_1 \otimes (e_1 \wedge e_2), \\ w_2 &= f_2 \otimes (e_3 \wedge e_4), \\ w_3 &= f_3 \otimes (e_1 \wedge e_5 + e_3 \wedge e_5), \\ w_4 &= f_4 \otimes (-e_1 \wedge e_2 + e_1 \wedge e_4 + e_2 \wedge e_4 + e_2 \wedge e_5 - e_4 \wedge e_5), \end{aligned}$$

and

$$w = w_1 + w_2 + w_3 + w_4.$$

Suppose that k is a field and that $v \in V_k$. We call v *generic* if the orbit of v is Zariski open. It is shown in [32] that the point $w \in V$ is *universally generic*, in the sense that w is generic in V_k for any field k.

Let $P \in \mathbb{Z}[V]$ be a non-constant relatively invariant polynomial of minimal degree. We assume, as we may, that P is primitive so that P reduces to a non-zero polynomial in $\mathbb{F}_p[V]$ for all primes p. If p is a prime factor of the integer $P(w)$ then $w \in V_{\mathbb{F}_p}$ lies in the hypersurface defined by the equation $P = 0$ and this contradicts the fact that w is universally generic. Thus $P(w)$ is free of prime factors and so $P(w) = \pm 1$. By changing the sign if necessary, we may assume that $P(w) = 1$. It is known that the polynomial P has degree 40 and satisfies $P(gv) = \omega^2(g)P(v)$, where $\omega(g_1, g_2) = \det(g_1)^5 \det(g_2)^8$. As a by-product of the construction carried out in Section 5, we shall find a convenient way to evaluate $P(v)$ for any $v \in V$. This method of computing P was originally given in [1], although the description of it to be found there is superficially quite different from ours. The Zariski open set in V defined by the condition $P \neq 0$ will be denoted by V^{ss}.

§5. Construction of the orbit-ring map

Our goal in this section is to construct an orbit-ring map for quintic rings over Z with V as the parameter space. That is, we seek to associate to each point $v \in V_Z$ a based quintic ring R_v over Z. This ring will be constructed via its structure tensors in such a way that the isomorphism class of R_v as a ring will depend only upon the G_Z-orbit of v.

In terms of the canonical coordinates $x_{i\alpha\beta}$ on V, we define $C^l_{jk}(x)$ to be

(29)
$$\frac{1}{32}\sum \varepsilon^{\alpha_1\beta_1\alpha_4\beta_4\alpha_3}\varepsilon^{\beta_3\alpha_2\beta_2\alpha_5\beta_5}\varepsilon^{i_3i_4i_5l}x_{j\alpha_1\beta_1}x_{k\alpha_2\beta_2}x_{i_3\alpha_3\beta_3}x_{i_4\alpha_4\beta_4}x_{i_5\alpha_5\beta_5}.$$

Each $C^l_{jk}(x)$ is an element of the ring $\mathbb{Q}[V]$. The collection $C^l_{jk}(x)$ defines a relatively equivariant polynomial map from V to the space

$$\mathrm{Aff}(4)^*\otimes\mathrm{Aff}(4)\otimes\mathrm{Aff}(4).$$

This follows from general principles of tensor invariant theory and is made precise in the following lemma.

LEMMA 6. *We have $C^l_{jk}(x)=C^l_{kj}(x)$. Furthermore, if $(h,g)\in G$ then*

$$C^l_{jk}\big((h,g)x\big)=\det(h)\det(g)^2\sum C^c_{ab}(x)\,h^a_j\,h^b_k\,\bar{h}^l_c.$$

Proof. The first assertion follows on rearranging the sums in the definition of C^l_{jk} according to the recipe $(\alpha_1,\beta_1)\leftrightarrow(\alpha_2,\beta_2)$, $(\alpha_4,\beta_4)\leftrightarrow(\alpha_5,\beta_5)$, $\alpha_3\leftrightarrow\beta_3$, $i_4\leftrightarrow i_5$. The second follows at once from (4), (6) and (28). □

It follows from the first assertion of Lemma 6 that the collection $C^l_{jk}(x)$ actually defines a relatively equivariant polynomial map from V into the space

$$\mathrm{Aff}(4)^*\otimes\mathrm{sym}^2(\mathrm{Aff}(4)).$$

LEMMA 7. *We have $C^l_{jk}(x)\in\mathbb{Z}[V]$ for all j, k and l.*

Proof. The proof of this lemma will rely in part on symbolic computation using [30]. To keep the computation as manageable as possible, we begin by making some reductions. The group generated by the commuting involutions $\alpha_m\leftrightarrow\beta_m$, $m\in\{1,2,4,5\}$ acts with trivial isotropy subgroups on the set of indices leading to each particular monomial in $C^l_{jk}(x)$. This makes it clear that $2C^l_{jk}(x)\in\mathbb{Z}[V]$ and that

(30) $$2C^l_{jk}(x)\equiv\sum x_{j\alpha_1\beta_1}x_{k\alpha_2\beta_2}x_{i_3\alpha_3\beta_3}x_{i_4\alpha_4\beta_4}x_{i_5\alpha_5\beta_5}\pmod 2,$$

where the sum is over all sets of indices satisfying the conditions

$$\begin{aligned}&\{\alpha_1,\beta_1,\alpha_4,\beta_4,\alpha_3\}=\{\beta_3,\alpha_2,\beta_2,\alpha_5,\beta_5\}=\{1,2,3,4,5\},\\&\{i_3,i_4,i_5,l\}=\{1,2,3,4\},\\&\alpha_1<\beta_1,\ \alpha_2<\beta_2,\ \alpha_4<\beta_4,\ \alpha_5<\beta_5.\end{aligned}$$

It remains to show that the coefficient of each monomial on the right-hand side of (30) is even. If $j=k$ then the involution described in the proof of Lemma 6 also acts without fixed points on the set of indices leading to each particular monomial and the claim follows. Thus we may assume that $j\neq k$. Renumbering the indices in the set $\{1,2,3,4\}$ has no effect on the claim and so it suffices to consider the two cases $(j,k,l)=(1,2,1)$ and $(j,k,l)=(1,2,4)$. This may easily be done using [30]. ∎

Lemma 8. *The value of $C(w)$ is*

$$C^1(w)=\begin{pmatrix}3&-1&-1&-1\\-1&0&0&0\\-1&0&0&0\\-1&0&0&0\end{pmatrix},\quad C^2(w)=\begin{pmatrix}0&-1&0&0\\-1&3&-1&-1\\0&-1&0&0\\0&-1&0&0\end{pmatrix},$$
$$C^3(w)=\begin{pmatrix}0&0&-1&0\\0&0&-1&0\\-1&-1&3&-1\\0&0&-1&0\end{pmatrix},\quad C^4(w)=\begin{pmatrix}0&0&0&-1\\0&0&0&-1\\0&0&0&-1\\-1&-1&-1&3\end{pmatrix}.$$

Proof. This is a routine numerical computation using the value of w given in Section 4. ∎

Lemma 9. *We have $\sum C^k_{jk}(x)=0$ for all j.*

Proof. It suffices to verify this identity after extending the ground ring to an algebraically closed field K. Since each $C^l_{jk}(x)$ lies in $\mathbb{Z}[V]$, $\sum C^k_{jk}(x)$ is a regular function on V_K and so it suffices to show that this sum vanishes on the orbit of w under G_K. But the sum does vanish at w itself, by Lemma 8, and the identity follows from Lemma 6. ∎

In accordance with Lemma 2, we now define a tensor D in terms of C by

$$D_{ij}(x)=\frac{1}{3}\sum C^s_{ir}(x)C^r_{sj}(x). \tag{31}$$

Lemmas 2, 7 and 11 imply that $D_{ij}(x) \in \mathbb{Z}[V]$ for all i and j. To see this, apply Lemma 2 with $Z = \mathbb{Q}(V)$ and $Z_0 = \mathbb{Z}[V]$; the other two lemmas verify the hypotheses necessary to do so. The transformation law

$$D_{ij}\big((h,g)x\big) = \det(h)^2 \det(g)^4 \sum D_{ab}(x) h_i^a h_j^b \tag{32}$$

for $(h,g) \in G$ follows easily from Lemma 6.

Lemma 10. *The value of $D(w)$ is*

$$D(w) = \begin{pmatrix} 4 & -1 & -1 & -1 \\ -1 & 4 & -1 & -1 \\ -1 & -1 & 4 & -1 \\ -1 & -1 & -1 & 4 \end{pmatrix}.$$

Proof. A computation using Lemma 8. □

Lemma 11. *For each $v \in V_Z$, the tensor $C_{ij}^k(v)$ is the first restricted structure tensor of a quintic ring over Z.*

Proof. The identities that C and D must satisfy in order to be the first and second restricted structure tensors of a quintic ring are given in Lemma 1. These identities are tensorial and so they hold at all points of an orbit if they hold at one. They are also identities between regular functions on V and so they hold if they hold on the orbit of w over an algebraically closed field. Thus it suffices to check that the identities hold at w.

In order to verify this without undue computation, we give a quintic ring over $\mathbb{Z}$ whose first and second restricted structure tensors are C and D evaluated at w. Since $\mathbb{Z}$ is embedded in Z and the structure tensors are unchanged upon extension of the base, this will complete the proof. In $R = \mathbb{Z}^{\oplus 5}$, consider the submodule $\widetilde{R}$ generated by the elements

$$\begin{aligned} 1 &= (1,1,1,1,1), \\ f_1 &= (4,-1,-1,-1,-1), \\ f_2 &= (-1,4,-1,-1,-1), \\ f_3 &= (-1,-1,4,-1,-1), \\ f_4 &= (-1,-1,-1,4,-1). \end{aligned}$$

It is easy to check that $\{1, f_1, \ldots, f_4\}$ is linearly independent and so $\widetilde{R}$ is a free $\mathbb{Z}$-module of rank 5. Moreover, $f_i^2 = 4 + 3f_i$ and $f_i f_j = -1 - f_i - f_j$

for $i \neq j$. Thus $\widetilde{R}$ is a quintic $\mathbb{Z}$-algebra having first and second restricted structure tensors C and D evaluated at w.

Now we know that C and D satisfy the relevant identities, there is a based quintic algebra over Q having $C_{ij}^k(v)$ and $D_{ij}(v)$ as its first and second restricted structure tensors. But $C_{ij}^k(v) \in Z$ for all i, j and k, by Lemma 7, and so $D_{ij}(v) \in Z$ for all i and j, by the remark following Lemma 2. It follows that $C_{ij}^k(v)$ is actually the first restricted structure tensor of a based quintic ring over Z, as required. □

Lemma 12. *In the ring $\mathbb{Z}[V]$, we have*

$$\begin{aligned} &C_{jk}^l(x) \equiv 0 \pmod 5 \quad \textit{whenever } l \notin \{j,k\}, \\ &C_{jk}^k(x) \equiv C_{jl}^l(x) \pmod 5 \ \textit{whenever } j \notin \{k,l\}. \end{aligned}$$

Proof. Let K be the algebraic closure of the finite field $\mathbb{F}_5$. We may regard each $C_{jk}^l(x)$ as an element of $K[V]$ by reduction modulo 5 and it suffices to show that this reduction satisfies the conditions

$$\begin{aligned} &C_{jk}^l(x) = 0 \quad \text{whenever } l \notin \{j,k\}, \\ &C_{jk}^k(x) = C_{jl}^l(x) \quad \text{whenever } j \notin \{k,l\}, \end{aligned}$$

since K is infinite. These are identities of regular functions on V_K and K is algebraically closed and so it suffices to establish that they hold on the orbit of w under G_K. Note that these conditions do hold at w itself. In fact, all the conditions enumerated in Lemma 5 are satisfied by C evaluated at w. By the lemma, it follows that these conditions must hold at all points of the orbit of w. □

For $v \in V_Z$, we let $\widetilde{R}_v$ denote the based quintic ring with first reduced structure tensor equal to $C_{ij}^k(v)$ and second reduced structure tensor equal to $D_{ij}(v)$. This ring may be constructed concretely as described in Section 3.

Theorem 1. *For each $v \in V_Z$ there is a quintic ring R_v such that $\widetilde{R}_v \cong R_v[5]$. The isomorphism class of R_v as a ring depends only on the G_Z-orbit of v. Furthermore,* $\mathrm{Disc}(R_v) = P(v)$ *for all $v \in V_Z$.*

Proof. It follows from Lemma 6 that the isomorphism class of the ring $\widetilde{R}_v$ depends only on the orbit of v. We have verified all the conditions necessary to apply Proposition 1 to $\widetilde{R}_v$. Thus there is a ring R_v such that

$\widetilde{R}_v \cong R_v[5]$. By Lemma 4, the isomorphism class of R_v is determined by that of $\widetilde{R}_v$ and hence by the orbit of v. By Lemma 3 and the remark following it, we have $5^3 \operatorname{Disc}(R_v) = \det(D(v))$. This identity allows us to regard $\operatorname{Disc}(R_v)$ as a polynomial function on V_Z. (This is possible essentially because the discriminant of a *based* ring is unambiguous.) By Lemma 10, $\det(D(w)) = 5^3$ and consequently $\operatorname{Disc}(R_w) = 1$. The transformation law (32) for D shows that $v \mapsto \operatorname{Disc}(R_v)$ is a relatively invariant polynomial on V with the same character as P. Since they also have the same value at w, it follows that $\operatorname{Disc}(R_v) = P(v)$. □

For later use, it will be convenient to observe that $R_w \cong Z^5$. This follows from the proof of Lemma 11 and the construction of R_v just described. Also, we shall allow ourselves to refer to the map from $G_Z \backslash V_Z$ to the set of isomorphism classes of quintic rings over Z induced by the orbit-ring map by the same name.

§6. A division theorem

The purpose of this section is to prove a result to the effect that if the image of the orbit-ring map constructed in Section 5 contains a principal order inside the ring R then the image contains R itself. We refer to this result as the division theorem. Actually, we only require a slightly weaker statement, which is also easier to prove and so we content ourselves with this. The precise enunciation is given below.

In order to prepare for the proof, we must first discuss the classification of pairs of quinary alternating forms over an arbitrary field K. A definitive and beautiful treatment of pairs of alternating forms over an arbitrary field was given by R. Scharlau in [28]. In fact, he reduced the classification problem for such pairs to the classification problem for pairs of rectangular matrices under simultaneous row and column operations. The solution to this problem is given by the celebrated Kronecker-Weierstrass Theorem, which has been considered over arbitrary fields by several authorities, including Dieudonné [10]. We recommend [6] for a clear statement of the theorem.

Let K be a field. In the terminology of [28], a *Kronecker module* is a quadruple (U, W, α, β) consisting of two K-vector spaces U and W and two K-linear maps $\alpha, \beta : U \to W$. If $\gamma : U \to W$ is any linear map then we may create an alternating form on $U \oplus W^*$ by setting

$$\langle (u_1, \lambda_1), (u_2, \lambda_2) \rangle_\gamma = \lambda_2\bigl(\gamma(u_1)\bigr) - \lambda_1\bigl(\gamma(u_2)\bigr)$$

and, in this way, a Kronecker module gives rise to a pair of alternating forms on the same space. It is proved in [28] that every pair of alternating forms is equivalent to a pair constructed in this way. The dual of the Kronecker module $X = (U, W, \alpha, \beta)$ is the Kronecker module $X^* = (W^*, U^*, \alpha^*, \beta^*)$. There is also an obvious notion of the direct sum of Kronecker modules. It is shown in [28] that two Kronecker modules X and Y give rise to equivalent pairs of alternating forms if and only if $X \oplus X^* \cong Y \oplus Y^*$.

Call a square matrix $A = (a_i^j)$ with entries in K *skew-symmetric* if $a_i^i = 0$ and $a_i^j = -a_j^i$ for all i and j. Let $\mathcal{A}(n)_K$ denote the space of n-by-n skew-symmetric matrices over K. The group $\mathrm{GL}(n)_K$ acts on $\mathcal{A}(n)_K$ by $g \cdot A = gA\,{}^t g$ and on $\mathcal{A}(n)_K \oplus \mathcal{A}(n)_K$ diagonally. Let

$$M_0 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad N_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$M_1(c) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & -c & 0 \end{pmatrix}, \qquad N_1(d) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & d \\ 0 & 0 & 0 & -d & 0 \end{pmatrix}$$

for $c, d \in K$.

LEMMA 13. *Let K be a field and $(A, B) \in \mathcal{A}(5)_K \oplus \mathcal{A}(5)_K$. If the intersection of the nullspaces of A and B is $\{0\}$ then (A, B) is equivalent under the action of $\mathrm{SL}(5)_K$ either to (M_0, N_0) or to $(M_1(c), N_1(1))$ for some $c \in K$ or to $(M_1(1), N_1(0))$.*

Proof. We begin by considering equivalence under $\mathrm{GL}(5)_K$. We shall refine to $\mathrm{SL}(5)_K$ equivalence at the end. Suppose that $(A, B) \in \mathcal{A}(5)_K \oplus \mathcal{A}(5)_K$ is a pair of alternating matrices and let $X = (U, W, \alpha, \beta)$ be a Kronecker module that gives rise to this pair by the procedure explained above. If any of the indecomposable summands of X has the form $(U', \{0\}, 0, 0)$ or $(\{0\}, W', 0, 0)$, then the matrices A and B will have a common non-zero null vector. Assume now that this is not the case. Since $\dim(U) + \dim(W) = 5$, it follows that X can have at most two indecomposable summands. If X

and Y are two Kronecker modules, then they lead to equivalent pairs of alternating matrices if and only if $X \oplus X^* \cong Y \oplus Y^*$. It follows from this that we may assume that in each indecomposable summand of X, the dimension of the first space is greater than or equal to that of the second.

Suppose first that X is indecomposable. By inspection of the list of indecomposable modules given by the Kronecker-Weierstrass Theorem (see Theorem 34.40 of [6]), recalling the assumption made in the previous paragraph, we see that X must be isomorphic to $(K^3, K^2, \alpha, \beta)$, where, with respect to the standard bases,

$$\alpha = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \beta = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Let e_1, e_2, e_3 be the standard ordered basis of K^3, f_1, f_2 be the standard ordered basis of K^2 and f_1^*, f_2^* be its dual basis. It is easy to verify that, with respect to the ordered basis

$$(0, -f_2^*),\ (0, -f_1^*),\ (e_1, 0),\ (e_2, 0),\ (e_3, 0)$$

of $K^3 \oplus (K^2)^*$, the matrices of the forms $\langle\,\cdot\,,\,\cdot\,\rangle_\alpha$ and $\langle\,\cdot\,,\,\cdot\,\rangle_\beta$ are M_0 and N_0, respectively.

Now suppose that X has two indecomposable summands. Given the reductions and assumptions made above, they must be isomorphic to $(K^2, K, \alpha_1, \beta_1)$ and $(K, K, \alpha_2, \beta_2)$. There is only one isomorphism class of indecomposable Kronecker modules of the form $(K^2, K, \alpha_1, \beta_1)$ and it is realized by taking

$$\alpha_1 = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad \beta_1 = \begin{bmatrix} 0 & 1 \end{bmatrix}.$$

Let e_1, e_2 be the standard ordered basis of K^2, F be the standard ordered basis of K and f^* be its dual. With respect to the ordered basis $(0, -f^*)$, $(e_2, 0)$, $(e_1, 0)$ of $K^2 \oplus K^*$, the alternating forms corresponding to α_1 and β_1 have matrices

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

respectively. All the isomorphism classes of non-zero Kronecker modules having the form $(K, K, \alpha_2, \beta_2)$ may be represented by taking

$$\alpha_2 = \begin{bmatrix} c \end{bmatrix}, \quad \beta_2 = \begin{bmatrix} 1 \end{bmatrix}$$

for each $c \in K$ and

$$\alpha_2 = \begin{bmatrix} 1 \end{bmatrix}, \quad \beta_2 = \begin{bmatrix} 0 \end{bmatrix}.$$

These Kronecker modules lead, respectively, to the pairs of alternating matrices

$$\begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

The block sum of the pairs of alternating matrices just described leads to the pairs $(M_1(c), N_1(1))$ for $c \in K$ and $(M_1(1), N_1(0))$.

This completes the first part of the proof. Now we must show that the equivalence classes are unchanged if we restrict to equivalence under $\mathrm{SL}(5)_K$. In order to do this, all that is necessary is to exhibit an element of the stabilizer of each pair with any given determinant. For $t \in K^\times$, let

$$\nu_1(t) = \mathrm{diag}(t^{-1}, t^{-1}, t, t, t),$$
$$\nu_2(t) = \mathrm{diag}(t^{-1}, t, t, t^{-1}, t).$$

Then $\det(\nu_1(t)) = \det(\nu_2(t)) = t$, $\nu_1(t)$ stabilizes the pair (M_0, N_0) and $\nu_2(t)$ stabilizes the pairs $(M_1(c), N_1(1))$ and $(M_1(1), N_1(0))$. $\square$

We note that the pair $(M_1(1), N_1(0))$ is equivalent to the pair $(N_1(1), M_1(0))$. Since we shall eventually be interested in unordered pairs, this observation reduces us from three cases to two.

In what follows, we let $H = \mathrm{SL}(4) \times \mathrm{SL}(5)$. The reason for introducing this subgroup is that, if p is a prime in Z and $K = Z/pZ$ then the reduction map $H_Z \to H_K$ is surjective. The analogous statement concerning G would, of course, be false. Consider a point $v = (A_1, \ldots, A_4) \in \mathcal{A}(5)_K^4$. By making use of the action of the first factor in H_K on $\mathcal{A}(5)_K^4$, we may replace the first two matrices by any two independent linear combinations of all four matrices. (This is a consequence of the fact that any two independent vectors in K^4 are the first two columns of a 4-by-4 unimodular matrix.) Thus, if there are independent vectors $(a_1, \ldots, a_4)$ and $(b_1, \ldots, b_4)$ in K^4 such that $a_1 A_1 + \cdots + a_4 A_4$ and $b_1 A_1 + \cdots + b_4 A_4$ do not have a common null vector, then we may apply Lemma 13 to find a point in the H_K-orbit of v such that the first two matrices are equal to one of the canonical pairs identified in the lemma. This leaves us to consider the case where all such pairs of linear combinations do have a common null vector. The content of the next two lemmas is that, in this situation, either all four matrices have a common non-zero null vector or v is equivalent under H_K to a point having the very restricted form described in Lemma 15. Before we embark on the proofs, it may be helpful to point out that if $(a_1, \dots, a_4)$ and $(b_1, \dots, b_4)$ in K^4 are linearly dependent then $a_1A_1 + \cdots + a_4A_4$ and $b_1A_1 + \cdots + b_4A_4$ always have a common non-zero null vector. This is because they are both multiples of a single skew-symmetric matrix and the rank of such a matrix is always even.

Lemma 14. *Let $(A_1, A_2, A_3, A_4) \in \mathcal{A}(5)^4_K$ and suppose that, for any vectors $(a_1, \dots, a_4)$ and $(b_1, \dots, b_4)$ in K^4, the matrices $a_1A_1 + \cdots + a_4A_4$ and $b_1A_1 + \cdots + b_4A_4$ have a common non-zero null vector. Then either $A_1, \dots, A_4$ have a common non-zero null vector or $(A_1, \dots, A_4)$ is equivalent under the action of G_K to the quadruple $(B_1, \dots, B_4)$ with*

$$B_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

Proof. Let us assume that $A_1, \dots, A_4$ do not have a common non-zero null vector. We must show that the quadruple $(A_1, \dots, A_4)$ is equivalent to the quadruple $(B_1, \dots, B_4)$ under the action of G_K. Note that the action of G_K preserves the assumption on the non-existence of a common null vector.

The assumption implies that $A_1, \dots, A_4$ are not all zero and hence one of them has positive rank. Since they are alternating matrices, their ranks are even. Suppose that A_1 has rank four. Then there is a non-zero null vector, x, of A_1 and x is unique up to multiplication by a non-zero scalar. The hypotheses imply that the pair A_1, A_2 has a common non-zero null vector and hence $A_2x = 0$. Similarly, $A_3x = 0$ and $A_4x = 0$. This contradicts our assumption and it follows that the rank of A_1 is less than or equal to two. Under the action of G_K, we may replace A_1 by any combination of $A_1, \dots, A_4$, provided only that one of the coefficients in the combination is non-zero. It follows that, for any vector $(a_1, \ldots, a_4) \in K^4$, the matrix $a_1A_1 + \cdots + a_4A_4$ has rank at most two.

By replacing A_1 by some combination of $A_1, \ldots, A_4$, we may assume that the rank of A_1 is exactly two. Consider the pair (A_1, A_2) under the action of $\mathrm{GL}(5)_K$. Note that, for any $(a_1, a_2) \in K^2$, the matrix $a_1A_1 + a_2A_2$ has rank at most two and that A_1, A_2 have a common non-zero null vector. After making a change of basis, we may assume that A_1 and A_2 take the form

$$A_1 = \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} C_2 & 0 \\ 0 & 0 \end{pmatrix},$$

where $(C_1, C_2) \in \mathcal{A}(4)^2_K$. The stabilizer of the common non-zero null vector inside $\mathrm{GL}(5)_K$ contains a subgroup isomorphic to $\mathrm{GL}(4)_K$ and this subgroup acts in the standard way on the pair (C_1, C_2). Thus we may proceed to apply the classification theory to this pair. Let (U, W, α, β) be the Kronecker module that gives rise to the pair (C_1, C_2). The only indecomposable Kronecker modules of the correct dimensions are isomorphic to $(K^2, K^2, \alpha, \beta)$, where either α or β is the identity map. But then either C_1 or C_2 would have rank four and this is not allowed. Thus the Kronecker module is decomposable. We use again the fact that two Kronecker modules X and Y give rise to equivalent pairs of alternating forms if and only if $X \oplus X^* \cong Y \oplus Y^*$. In light of this, the pair (C_1, C_2) must be equivalent to the pair that arises from one of the Kronecker modules enumerated below.

(1) $(K^2, K, [1\ 0], [0\ 1]) \oplus (K, \{0\}, 0, 0)$

(2) $(K, K, [c], [1]) \oplus (K, K, [d], [1])$

(3) $(K, K, [c], [1]) \oplus (K, K, [1], [0])$

(4) $(K, K, [1], [0]) \oplus (K, K, [d], [1])$

(5) $(K, K, [1], [0]) \oplus (K, K, [1], [0])$

(6) $(K, K, [c], [1]) \oplus (K, \{0\}, 0, 0) \oplus (K, \{0\}, 0, 0)$

(7) $(K, K, [1], [0]) \oplus (K, \{0\}, 0, 0) \oplus (K, \{0\}, 0, 0)$

However, (2) is ruled out because the rank of C_2 would be four, (3) is ruled out because either C_1 would have rank four, if $c \neq 0$, or $C_1 + C_2$ would have rank four if $c = 0$, and (4) and (5) are ruled out for similar reasons. Thus only (1), (6) and (7) actually yield apparently allowable pairs (C_1, C_2).

We continue the analysis of the situation of the previous paragraph. We first note that all the allowable Kronecker modules (1), (6) and (7) have a trivial summand. It follows that if $(A_1, A_2) \in \mathcal{A}(5)_K^2$, the rank of A_1 is two and the rank of $a_1A_1 + a_2A_2$ is at most two for any $(a_1, a_2) \in K^2$, then the common nullspace of A_1 and A_2 is at least two-dimensional. We shall use this remark several times below. Its first application is to rule out cases (6) and (7). In both these cases, A_1 and A_2 are proportional and so, after applying a suitable element of G_K, we may assume that $A_2 = 0$. This done, let N be the nullspace of A_1, $N_{13} \subset N$ be the common nullspace of A_1 and A_3 and $N_{14} \subset N$ be the common nullspace of A_1 and A_4. Since A_1 has rank two, $\dim(N) = 3$. The pairs (A_1, A_3) and (A_1, A_4) have the properties mentioned in the remark and so $\dim(N_{13}) \geq 2$ and $\dim(N_{14}) \geq 2$. Thus $\dim(N_{13} \cap N_{14}) \geq 1$ and so A_1, A_3 and A_4 have a common non-zero null vector. Because $A_2 = 0$, this is also a null vector of A_2 and this contradicts our supposition that $A_1, \ldots, A_4$ do not share a common non-zero null vector. It follows that only case (1) is possible and thus that (A_1, A_2) is equivalent to (B_1, B_2) under $\mathrm{GL}(5)_K$. We henceforth assume that $A_1 = B_1$ and $A_2 = B_2$.

Before proceeding, we observe a consequence of the argument of the last two paragraphs, namely that any three of $A_1, \ldots, A_4$ have a common non-zero null vector. For if all three have rank zero then the conclusion follows at once, whereas if one of them has rank two then we may use it in place of A_1 in the above argument to reach the required conclusion.

Let $e_1, \ldots, e_5$ be the standard ordered basis of K^5. The common nullspace of A_1 and A_2 is the space spanned by e_4, e_5. By the observation of the previous paragraph, A_1, A_2 and A_3 have a common non-zero null vector. Acting on A_3 by the stabilizer of the pair (A_1, A_2) inside $\mathrm{GL}(5)_K$, we may assume that e_5 is a common null vector and hence that A_3 takes the form

$$A_3 = \begin{pmatrix} C_3 & 0 \\ 0 & 0 \end{pmatrix},$$

where $C_3 \in \mathcal{A}(4)_K$. By adding multiples of A_1 and A_2 to A_3, we may further assume that C_3 takes the form

$$C_3 = \begin{pmatrix} 0 & 0 & 0 & x_{14} \\ 0 & 0 & x_{23} & x_{24} \\ 0 & -x_{23} & 0 & x_{34} \\ -x_{14} & -x_{24} & -x_{34} & 0 \end{pmatrix}.$$

Now, the common nullspace of A_1 and A_3 is at least two-dimensional, by the remark made above, and hence some non-zero linear combination of e_3 and

e_4 is a null vector of A_3. This implies that $x_{34} = 0$. Similarly, the common nullspace of A_2 and A_3 is at least two-dimensional and hence some non-zero linear combination of e_2 and e_4 is a null vector of A_3. This implies that $x_{24} = 0$. Let N be the nullspace of A_1, $N_{123} \subset N$ be the common nullspace of A_1, A_2 and A_3 and $N_{14} \subset N$ be the common nullspace of A_1 and A_4. Suppose that $x_{14} = 0$. Then $e_4, e_5 \in N_{123}$ and so $\dim(N_{123}) \geq 2$. We also know that $\dim(N) = 3$ and that $\dim(N_{14}) \geq 2$. Thus $\dim(N_{123} \cap N_{14}) \geq 1$, contradicting the assumption that $A_1, \ldots, A_4$ do not have a common non-zero null vector. Thus $x_{14} \neq 0$. It follows that $x_{23} = 0$, for otherwise the rank of A_3 would be four. We may rescale e_4 without affecting A_1 and A_2 so that $x_{14} = 1$. In this way we obtain $A_3 = B_3$.

It remains to analyze the shape of A_4. We may add multiples of A_1, A_2 and A_3 to it in order to assume that

$$A_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & y_{15} \\ 0 & 0 & y_{23} & y_{24} & y_{25} \\ 0 & -y_{23} & 0 & y_{34} & y_{35} \\ 0 & -y_{24} & -y_{34} & 0 & y_{45} \\ -y_{15} & -y_{25} & -y_{35} & -y_{45} & 0 \end{pmatrix}.$$

The fact that A_1, A_2 and A_4 must have a common non-zero null vector implies that some non-zero combination of e_4 and e_5 is a null vector for A_4 and hence that $y_{45} = 0$. Similarly, the fact that A_1, A_3 and A_4 have a common non-zero null vector implies that $y_{35} = 0$ and the fact that A_2, A_3 and A_4 have a common non-zero null vector implies that $y_{25} = 0$. Since e_5 must not be a null vector of A_4, we conclude that $y_{15} \neq 0$. We may rescale e_5 without affecting A_1, A_2 and A_3 to assume that $y_{15} = 1$. With all of these assumptions, the requirement that $A_1 + A_2 + A_4$ have rank at most two implies that $y_{23} = y_{24} = y_{34} = 0$ and so $A_4 = B_4$. □

LEMMA 15. *Let $(A_1, \ldots, A_4) \in \mathcal{A}(5)_K^4$ and suppose that, for any vectors $(a_1, \ldots, a_4)$ and $(b_1, \ldots, b_4)$ in K^4, the matrices $a_1A_1 + \cdots + a_4A_4$ and $b_1A_1 + \cdots + b_4A_4$ have a common non-zero null vector. Then either $A_1, \ldots, A_4$ have a common non-zero null vector or $(A_1, \ldots, A_4)$ is equivalent under the action of H_K to a quadruple such that all the non-zero entries of each matrix lie in the first row or column.*

Proof. For $s, t \in K^\times$, let

$$\nu(t, s) = \big(\operatorname{diag}(t, 1, 1, 1), \operatorname{diag}(s, 1, 1, 1, 1)\big).$$

If $A_1, \dots, A_4$ do not have a common non-zero null vector then we may find $g \in G_K$ such that $g(A_1, \dots, A_4) = (B_1, \dots, B_4)$ as in Lemma 14. We may choose s and t such that $\nu(t,s)g \in H_K$ and clearly $\nu(t,s)(B_1, \dots, B_4)$ has the required form. □

Let R be a quintic ring over Z. We may choose a restricted basis $1, v_1, \dots, v_4$ of $R[5]$ such that each v_i has trace zero. With respect to such a restricted basis, the first restricted structure tensor of $R[5]$ has certain components C_{ij}^k. These components may be regarded as a function $(i,j,k) \mapsto C_{ij}^k$ from $\{1,2,3,4\}^3$ to Z. Let $\mathcal{S}_Z[5]$ be the set of all such functions arising in this way from all quintic rings over Z. The following result collects some elementary properties of $\mathcal{S}_Z[5]$ for later reference.

LEMMA 16. *With the above described notation, the following hold.*

(1) *The set $\mathcal{S}_Z[5]$ is closed under scalar multiplication by elements of Z.*

(2) *If $C \in \mathcal{S}_Z[5]$ then C satisfies the congruences listed in Proposition* 1 *with $n = 5$.*

(3) *If $C \in \mathcal{S}_Z[5]$ then $\sum C_{ij}^j = 0$ for all i.*

(4) *Let $\widetilde{R}$ be a quintic ring and $\widetilde{C} \in \mathcal{S}_Z[5]$ be any of the associated first restricted structure tensors. Then $\widetilde{R} \cong R[N]$ for some $N \in Z$ and some quintic ring R if and only if $\widetilde{C} = NC$ for some $C \in \mathcal{S}_Z[5]$.*

Proof. For brevity, we shall refer to a restricted basis $1, v_1, \dots, v_4$ such that $\mathrm{tr}(v_i) = 0$ for all i as a *traceless* restricted basis. Take $C \in \mathcal{S}_Z[5]$ and let R be a quintic ring and $1, v_1, \dots, v_4$ be a traceless restricted basis of $R[5]$ such that C is the first restricted structure tensor of $R[5]$ with respect to $1, v_1, \dots, v_4$. If $N \in Z$ then $1, Nv_1, \dots, Nv_4$ is a traceless restricted basis of $R[5N] = R[N][5]$ and the first restricted structure tensor of $R[N][5]$ with respect to this basis is NC. This proves (1). There is a restricted basis $1, v_1^*, \dots, v_4^*$ for R such that $v_i = a_i \cdot 1 + 5v_i^*$ for some $a_i \in Z$ and all i. A routine calculation now verifies (2). The evaluation in (3) follows at once from the fact that $\mathrm{tr}(v_i) = \sum C_{ij}^j$ for all i.

Let $\widetilde{R}$ be a quintic ring, $1, \tilde{v}_1, \dots, \tilde{v}_4$ be a traceless restricted basis for $\widetilde{R}[5]$ and $\widetilde{C} \in \mathcal{S}_Z[5]$ be the associated first restricted structure tensor. Suppose that $\widetilde{R} \cong R[N]$ for some quintic ring R and some $N \in Z$. It is harmless to replace the isomorphism by literal equality and we do so. There are $a_i \in Z$ and $v_i' \in R[5]$ such that $\tilde{v}_i = a_i \cdot 1 + Nv_i'$. By taking the trace on both sides, we obtain $5a_i = -N\,\mathrm{tr}(v_i')$. Since $v_i' \in R[5]$, $\mathrm{tr}(v_i')$ is divisible by 5; thus we may set $\mathrm{tr}(v_i') = 5t_i$. It follows that $a_i = -Nt_i$ and $\tilde{v}_i = N(-t_i \cdot 1 + v_i')$. Let $v_i = -t_i \cdot 1 + v_i'$. Then $1, v_1, \ldots, v_4$ is a traceless restricted basis for $R[5]$ and $\tilde{v}_i = Nv_i$. If $C \in \mathcal{S}_Z[5]$ is the first restricted structure tensor of $R[5]$ with respect to $1, v_1, \ldots, v_4$ then $\widetilde{C} = NC$. This proves one implication in (4).

Suppose, on the other hand, that there is some $C \in \mathcal{S}_Z[5]$ such that $\widetilde{C} = NC$. Let R be a quintic ring such that C is the first restricted structure tensor of $R[5]$ with respect to some traceless basis. Then, as in (1), $\widetilde{C} = NC$ is the first restricted structure tensor of $R[5N]$ with respect to some traceless basis and, by the remark after Lemma 2, it follows that $\widetilde{R}[5] \cong R[5N] \cong R[N][5]$. By Lemma 4, we conclude that $\widetilde{R} \cong R[N]$. This establishes the other implication in (4). □

We will say that a quintic ring R over Z is *indivisible* if the points in $\mathcal{S}_Z[5]$ associated to R are not divisible in $\mathcal{S}_Z[5]$ by any non-unit $N \in Z$. Part (4) of Lemma 16 implies that if R is an integrally closed quintic ring over Z then R is indivisible. Note, however, that the converse is not generally true.

Theorem 2. *Suppose that R is an indivisible quintic ring over Z and that, for some $N \in Z$, the order $R[N]$ lies in the image of the orbit-ring map from $G_Z \backslash V_Z$. Then R lies in the image of the orbit-ring map from $G_Z \backslash V_Z$.*

Proof. Suppose that N is not a unit and let p be a prime divisor of N. We shall show that either $R[N/p]$ lies in the image of the orbit-ring map or that $p^2 \mid N$ and $R[N/p^2]$ lies in the image of the orbit-ring map. Since N can only have a finite number of prime divisors, counted with multiplicity, this will be sufficient.

Let $v \in V_Z$ be a point such that $R_v \cong R[N]$. Identify v with a quadruple $(A_1, \ldots, A_4)$ of alternating matrices over Z. By reduction modulo p, we obtain a quadruple of alternating matrices over the field $F_p = Z/pZ$. We shall apply Lemmas 13 and 15 to this situation. Before we begin, we shall make a simple observation which underlies what we do below. Suppose that $v \in V_Z$ and denote by $\bar{v}$ the reduction of v modulo p. Suppose that $\bar{v}' \in V_{F_p}$ lies in the H_{F_p}-orbit of $\bar{v}$ and choose $\bar{h} \in H_{F_p}$ such that $\bar{h}\bar{v} = \bar{v}'$. We may find some $h \in H_Z$ whose reduction modulo p is $\bar{h}$ and hence there is a point $v' = hv$ in the H_Z-orbit of v such that v' reduces to $\bar{v}'$ modulo p.

Consider the orbit under H_{F_p} of the quadruple $(A_1, \ldots, A_4) \pmod p$. Either, for every quadruple $(A'_1, \ldots, A'_4)$ in the orbit, A'_1 and A'_2 have a common non-zero null vector or there is some quadruple $(A'_1, \ldots, A'_4)$ in the orbit such that A'_1 and A'_2 do not have a common non-zero null vector. We consider these possibilities separately, beginning with the former.

Suppose then that for every $(A'_1, \ldots, A'_4)$ in the orbit of $(A_1, \ldots, A_4)$ $\pmod p$, A'_1 and A'_2 have a common non-zero null vector. By Lemma 15, either $A_1, \ldots, A_4$ have a common non-zero null vector over F_p or we may choose a point $(B_1, \ldots, B_4)$ in the H_Z-orbit of v such that all the non-zero entries in $B_i \pmod p$ lie in the first row or column. In the former case, we may replace $v = (A_1, \ldots, A_4)$ by a point $v' = (A'_1, \ldots, A'_4)$ in the same H_Z-orbit such that

$$A'_i = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \pmod p,$$

for all i by transporting the common non-zero null vector to e_5 modulo p. Let

$$\tau_1 = \big(I_4, \mathrm{diag}(1, 1, 1, 1, p^{-1})\big) \in G_Q$$

and $v'' = \tau_1 v'$. Then $v'' \in V_Z$ and, by Lemma 6, we have $C^k_{ij}(v') = p^2 C^k_{ij}(v'')$. Thus $C(v')$, which is a point in $\mathcal{S}_Z[5]$ associated to $R[N]$, is divisible by p^2 in $\mathcal{S}_Z[5]$. Since R is indivisible, it follows that $p^2 \mid N$. The point $C(v'')$ in $\mathcal{S}_Z[5]$ is associated to the ring $R[N/p^2]$ and so $R[N/p^2]$ lies in the image of the orbit-ring map from V_Z/G_Z.

Next suppose that v is equivalent under H_Z to a point $v' = (B_1, \ldots, B_4)$ such that all the non-zero entries of $B_i \pmod p$ lie in the first row or column. Let

$$\tau_2 = \big(p^{-1} I_4, \mathrm{diag}(p, p, 1, 1, 1)\big) \in G_Q$$

and let $v'' = \tau_2 v'$. Then $v'' \in V_Z$ and, by Lemma 6, we have $C^k_{ij}(v') = pC^k_{ij}(v'')$. This shows that $R[N/p]$ lies in the image of the orbit-ring map from V_Z, as required.

This completes our consideration of the first of the two possibilities identified above. Now we consider the second. We may thus assume, possibly after replacing v by some other point in its H_Z-orbit, that A_1 and A_2 have no non-zero common null vector over F_p. Thus, after applying an element of H_Z, we may assume that $(A_1, A_2) \pmod p$ is in one of the first two canonical forms described in Lemma 13. Note that, for the reason explained immediately after the proof of the lemma, we do not have to consider the third canonical form from Lemma 13. Suppose first that $(A_1, A_2) \pmod p$

is equal to the pair (M_0, N_0) from Lemma 13. Suppose that we have

$$A_i = \begin{pmatrix} 0 & y_{i12} & y_{i13} & y_{i14} & y_{i15} \\ -y_{i12} & 0 & y_{i23} & y_{i24} & y_{i25} \\ -y_{i13} & -y_{i23} & 0 & y_{i34} & y_{i35} \\ -y_{i14} & -y_{i24} & -y_{i34} & 0 & y_{i45} \\ -y_{i15} & -y_{i25} & -y_{i35} & -y_{i45} & 0 \end{pmatrix}$$

for $i = 3, 4$. By Lemma 12, $\frac{1}{5}C^k_{ij}$ is a polynomial with integer coefficients in the coordinates on V_Z, provided that $k \notin \{i, j\}$. Thus if $v', v'' \in V_Z$ are congruent modulo p then $\frac{1}{5}C^k_{ij}(v') \equiv \frac{1}{5}C^k_{ij}(v'') \pmod{p}$, provided that $k \notin \{i, j\}$, *even when* $p \,|\, 5$. Thus, in order to evaluate $\frac{1}{5}C^k_{ij}(v) \pmod{p}$ when $k \notin \{i, j\}$, we may assume that $(A_1, A_2) = (M_0, N_0)$ and carry out a direct computation of $\frac{1}{5}C^k_{ij}$. Among the resulting values, we find

$$\begin{aligned} \frac{1}{5}C^3_{11}(v) &\equiv -y_{445} \pmod{p}, & \frac{1}{5}C^4_{11}(v) &\equiv y_{345} \pmod{p}, \\ \frac{1}{5}C^3_{12}(v) &\equiv -y_{435} \pmod{p}, & \frac{1}{5}C^4_{12}(v) &\equiv y_{335} \pmod{p}, \\ \frac{1}{5}C^3_{22}(v) &\equiv y_{434} \pmod{p}, & \frac{1}{5}C^4_{22}(v) &\equiv -y_{334} \pmod{p}. \end{aligned}$$

Since $R_v \cong R[N]$, $C^k_{ij}(v)$ is divisible by N, and hence by p, in $\mathcal{S}_Z[5]$, by part (4) of Lemma 16. From this and part (2) of Lemma 16, we see that $\frac{1}{5}C^k_{ij}(v)$ is divisible by p when $k \notin \{i, j\}$. We conclude from this that y_{i34}, y_{i35} and y_{i45} are all divisible by p for $i = 3, 4$. Thus the non-zero entries of $A_1, \ldots, A_4$ modulo p all occur in the first and second row or column of the matrices. It follows that $v' = \tau_2 v$ (with τ_2 as above) lies in V_Z. As before, $C^k_{ij}(v) = pC^k_{ij}(v')$ and so the image of v' under the orbit-ring map is $R[N/p]$.

In the last remaining case, we may assume that $(A_1, A_2) \pmod{p}$ is equal to the pair $(M_1(c), N_1(1))$ from Lemma 13 for some $c \in F_p$. We take A_3 and A_4 to have the form given in the display above. By adding a linear combination of A_1 and A_2 to A_3 and A_4, we may assume that y_{i12} and y_{i13} are divisible by p for $i = 3, 4$. A direct calculation shows that

$$\frac{1}{5}C^3_{22}(v) \equiv y_{423} \pmod{p}, \quad \frac{1}{5}C^4_{22}(v) \equiv -y_{323} \pmod{p},$$

and so y_{i23} is divisible by p for $i = 3, 4$.

If $y_{i24}, y_{i34} \equiv 0 \pmod{p}$ for $i = 3, 4$ then all non-zero entries of the matrices $A_1, \ldots, A_4$ modulo p are contained in the first and fifth row and column. Thus, if we set

$$\tau_3 = (p^{-1}I_4, \mathrm{diag}(p, 1, 1, 1, p)) \in G_Q,$$

then $v' = \tau_3 v$ lies in V_Z, $C^k_{ij}(v) = pC^k_{ij}(v')$ and $R[N/p]$ lies in the image of the orbit-ring map. Suppose instead that one of the entries y_{i24}, y_{i34} is not divisible by p. Next we argue that we may assume that y_{324} is not divisible by p. We require some further notation. For $1 \le \alpha, \beta \le 5$, let $E_{\alpha\beta}(r)$ be the 5-by-5 matrix with (α, β)-entry equal to r and all other entries equal to zero. For $1 \le i, j \le 4$, let $e_{ij}(r)$ be the 4-by-4 matrix with (i, j)-entry equal to r and all other entries equal to zero. If y_{324} is divisible by p, but y_{424} is not then we may interchange A_3 and A_4 and change the sign of A_3 to get what we want. Suppose then that y_{424} is also divisible by p. One of y_{334} and y_{434} is not divisible by p, and, interchanging A_3 and A_4 and changing the sign of A_3 if necessary, we may assume that y_{334} is not divisible by p. Let

$$\nu_1 = (I_4 + e_{12}(-1), I_5 + E_{23}(1)) \in H_Z$$

and act by ν_1 on v. Calculation shows that the result of applying ν_1 to v is the quadruple $(M_1(c-1), N_1(1), A_3', A_4')$, where the $(2, 4)$ entry in A_3' is congruent to y_{334} modulo p and hence is not divisible by p. This establishes the claim. We continue to denote the new point by v, its four entries by $A_1, \ldots, A_4$, and we write c instead of $c - 1$. By adding a multiple of A_3 to A_4, we may assume that y_{424} is divisible by p. The element

$$\nu_2 = (I_4, I_5 + E_{54}(r)) \in H_Z$$

adds r times y_{324} to y_{325} and leaves the first two matrices unchanged modulo p. Thus we may further assume that y_{325} is divisible by p.

We must now divide into cases according as c is or is not divisible by p. We first assume that c is not divisible by p. Calculation shows that

$$\frac{1}{5}C^2_{11}(v) \equiv c y_{425} y_{324} \pmod{p}$$

and so y_{425} is divisible by p. Then we find that

$$C^1_{11}(v) \equiv c y_{435} y_{324} \pmod{p}$$

and so y_{435} is divisible by p. Finally,

$$\frac{1}{5}C^4_{23}(v) \equiv y_{324} y_{335} \pmod{p}$$

and so y_{335} is divisible by p. We now know that y_{i25} and y_{i35} are divisible by p for $i = 3, 4$. Interchange the fourth and fifth row and fourth and fifth column in all four matrices and change the sign of the fourth rows and fifth columns (this is the action of an element of H_Z). The resulting matrices all have their non-zero entries modulo p concentrated in the first and fifth row and column. Thus we may apply τ_3 as above to obtain an integral point $v' \in V_Z$ that maps to the ring $R[N/p]$ under the orbit-ring map.

All that remains is to deal with the case in which c is divisible by p. In this case, let

$$\nu_3 = (I_4 + e_{21}(-r), I_5 + E_{32}(r)) \in H_Z.$$

Since c is divisible by p, when the element ν_3 is applied to v, the matrices A_1 and A_2 are left unchanged modulo p. In the third matrix, the $(3, 4)$ entry is replaced modulo p by $y_{334} + ry_{324}$. Hence, by choosing r appropriately, we may assume that y_{334} is divisible by p. This done, we find that

$$\begin{aligned} C^2_{12}(v) &\equiv \quad y_{425}y_{324} \pmod p, \\ C^2_{22}(v) &\equiv -y_{435}y_{324} \pmod p, \\ \frac{1}{5}C^4_{23}(v) &\equiv \quad y_{335}y_{324} \pmod p \end{aligned}$$

and hence y_{335}, y_{425} and y_{435} are all divisible by p. We already know that y_{325} is divisible by p. Hence by interchanging the fourth and fifth row and fourth and fifth column in all four matrices and changing the sign of the fourth rows and fifth columns, we arrive at a quadruple such that all non-zero entries in all four matrices are concentrated in the first and fifth row and column. We may again apply the element τ_3, as above, to complete the proof. □

§7. The image of the orbit-ring map

The purpose of this section is to show that many quintic rings lie in the image of the orbit-ring map. For this we require the compatibility of the map constructed here with the map constructed in [32] when both are defined. We shall first formulate this compatibility precisely.

Suppose that Z is a PID of characteristic zero. Then we have constructed a orbit-ring map from $G_Z \backslash V_Z$ to the set of isomorphism classes of quintic rings over Z. We shall denote this map by OR_5. For the reader's convenience, we briefly recall the construction of the map. From $v \in V_Z$, representing a given orbit, we first obtain $C^k_{ij}(v) \in Z$ and $D_{ij}(v) \in Z$ for

$1 \leq i, j, k \leq 4$. These quantities are both polynomials in v, given explicitly in (29) and (31). From $C_{ij}^k(v)$ and $D_{ij}(v)$, we then construct a quintic ring $\widetilde{R}_v$ over Z by using C and D as structure constants for the ring. The procedure is made explicit in the paragraph surrounding (8). It then emerges that $\widetilde{R}_v$ is a subring of a slightly larger ring R_v. More precisely, we have $\widetilde{R}_v = Z \cdot 1 + 5R_v$, where 1 denotes the identity in R_v. Finally, we set $\mathrm{OR}_5(v) = R_v$.

If Z is, in fact, a field of characteristic zero then, in Section 2 of [32], a second map from $G_Z \backslash V_Z^{\mathrm{ss}}$ to the set of isomorphism classes of separable quintic Z-algebras was constructed. We shall denote this map by OR_5'. The construction of OR_5' was done via geometry and Galois cohomology, whereas OR_5 was constructed via invariant theory, and it is not immediately clear that the two constructions yield the same result. However, in Section 2 of [18], we proved that they do. The proof is self-contained and so we introduce no circularity by making use of it here.

THEOREM 3. *Let Q be a field of characteristic zero and $x \in V_Q^{\mathrm{ss}}$. Then $\mathrm{OR}_5(x) = \mathrm{OR}_5'(x)$.*

THEOREM 4. *Let Z be a PID of characteristic zero and R an indivisible quintic ring over Z. Let Q be the field of fractions of Z and suppose that $A = Q \otimes_Z R$ is a separable Q-algebra. Then R lies in the image of the orbit-ring map from $G_Z \backslash V_Z^{\mathrm{ss}}$. In particular, if F is a quintic number field and $\mathcal{O}_F$ is its ring of integers then $\mathcal{O}_F$ lies in the image of the orbit-ring map from $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}^{\mathrm{ss}}$.*

Proof. Let $R[5]^0 \subset R[5]$ be the submodule consisting of elements of trace zero, so that $R[5] = Z \oplus R[5]^0$. Let v_1, v_2, v_3, v_4 be an ordered Z-basis for $R[5]^0$ and $\widehat{C}_{ij}^k$ be the first restricted structure tensor of $R[5]$ with respect to the restricted basis $1, v_1, \ldots, v_4$. Since $A = Q \otimes_Z R$ is a separable Q-algebra, it follows from Proposition 2.15 of [32] that A lies in the image of OR_5'. Hence, by Theorem 3, A lies in the image of OR_5 over Q. Let $y \in V_Q^{\mathrm{ss}}$ be such that $\mathrm{OR}_5(y) = A$. Note that $A^0 = Q \otimes_Z R[5]^0$ is the subspace of A consisting of elements of trace zero. By construction, $C_{ij}^k(y)$ is the first restricted structure tensor of A with respect to some restricted basis $1, a_1, \ldots, a_4$ with $a_j \in A^0$. Now $v_1, \ldots, v_4$ is also a Q-basis for A^0; let $h \in \mathrm{GL}(4)_Q$ be the change-of-basis matrix from the a-basis to the v-basis and put $x = (h, I_5)y \in V_Q^{\mathrm{ss}}$. It follows from Lemma 6 that there is some $\lambda \in Q^\times$ such that $C_{ij}^k(x) = \lambda \widehat{C}_{ij}^k$ for all $1 \leq i, j, k \leq 4$. For any

$M \in Z$, we have $C_{ij}^k(Mx) = \lambda M^5 \widehat{C}_{ij}^k$. Let us choose $M \in Z$ in such a way that $Mx \in V_Z^{\mathrm{ss}}$ and $N = \lambda M^5 \in Z$. Then $C_{ij}^k(Mx) = N\widehat{C}_{ij}^k$ is the first restricted structure tensor of the order $R[5N]$ with respect to the restricted basis $1, Nv_1, \ldots, Nv_4$ and so $\mathrm{OR}_5(Mx) = R[N]$. This shows that $R[N]$ lies in the image of OR_5 from $G_Z \backslash V_Z^{\mathrm{ss}}$ and so, according to Theorem 2, R lies in the image of OR_5 from $G_Z \backslash V_Z^{\mathrm{ss}}$. The last statement is an immediate consequence of this. □

§8. Acknowledgements

The authors would like to thank M. Bhargava for making [2] available to them prior to its publication and the referee for his or her careful reading of the manuscript, which saved us from numerous slips and infelicities, and for pointing out the references mentioned in Section 4. The first author also benefitted from several seminar presentations on Bhargava's work given by D. Wright during the Fall semester of 2001.

References

[1] K. Amano, M. Fujigami and T. Kogiso, *Construction of Irreducible Relative Invariant of the Prehomogeneous Vector Space* $(SL_5 \times GL_4, \Lambda^2(\mathbb{C}^5) \otimes \mathbb{C}^4)$, Linear Algebra Appl., **355** (2002), 215–222.

[2] M. Bhargava, Higher Composition Laws, Ph.D. Thesis, Princeton University, 2001.

[3] M. Bhargava, *Gauss Composition and Generalizations*, Algorithmic Number Theory: 5th International Symposium (C. Fieker and D. R. Kohel, eds.), Springer Lecture Notes in Computer Science, vol. 2369, Springer, New York (2002), pp. 1–8.

[4] A. Cayley, *On the theory of linear transformations*, The Collected Mathematical Papers of Arthur Cayley, vol. 1, Cambridge University Press, Cambridge (1889), pp. 80–94.

[5] H. Cohen, F. Diaz y Diaz and M. Olivier, *Counting discriminants of number fields of degree up to four*, Algorithmic Number Theory (Leiden 2000), Lecture Notes in Computer Science, vol. 1838, Springer, Berlin (2000), pp. 269–283.

[6] C. W. Curtis and I. Reiner, Methods of Representation Theory with Applications to Finite Groups and Integral Orders, Vol. 1, Wiley Classics Library, John Wiley & Sons, New York, 1990.

[7] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, Bull. Lond. Math. Soc., **1** (1969), 345–348.

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

[9] B. N. Delone and D. K. Fadeev, Theory of Irrationalities of the Third Degree, Translations of Mathematical Monographs, Vol. 10, American Mathematical Society, Providence, 1964.

[10] J. Dieudonné, *Sur la reduction canonique des couples de matrices*, Bull. Soc. math. France, **74** (1946), 130–146.

[11] I. M. Gel'fand, M. M. Kapranov and A. V. Zelevinsky, Discriminants, Resultants and Multidimensional Determinants, Mathematics: Theory and Applications, Birkhäuser, Boston, 1994.

[12] W. T. Gan, B. Gross and G. Savin, *Fourier Coefficients of Modular Forms on* G_2, preprint (2001).

[13] G. B. Gurevich, Foundations of the Theory of Algebraic Invariants, translated by J. R. M. Radok and A. J. M. Spencer, P. Noordhoff, Groningen, 1964.

[14] A. Gyoja and Y. Omoda, *Characteristic cycles of certain character sheaves*, Indag. Math. (N.S.), **12** (2001), 329–335.

[15] A. C. Kable, *Classes of integral* 3*-tensors on* 2*-space*, Mathematika, **47** (2000), 205–217.

[16] A. C. Kable, *The concomitants of a prehomogeneous vector space*, to appear in J. Algebra.

[17] A. C. Kable and A. Yukie, *Prehomogeneous vector spaces and field extensions II*, Invent. Math., **130** (1997), 315–344.

[18] A. C. Kable and A. Yukie, *On the Number of Quintic Fields*, preprint (2002).

[19] N. Kawanaka, *Generalized Gel'fand-Graev representations of exceptional simple algebraic groups over a finite field I*, Invent. math., **84** (1986), 575–616.

[20] T. Kimura, F. Sato and X.-W. Zhu, *On the poles of p-adic complex powers and the b-functions of prehomogeneous vector spaces*, Amer. J. Math., **112** (1990), 423–437.

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

[22] F. Knop and G. Menzel, *Duale Varietäten von Fahnenvarietäten*, Comment. Math. Helv., **62** (1987), 38–61.

[23] G. Lusztig, *Introduction to character sheaves*, The Arcata Conference on Representations of Finite Groups, Proc. Sympos. Pure Math., vol. 47, part 1, Amer. Math. Soc., Providence (1987), pp. 165–179.

[24] M. Muro, M. Sato and T. Shintani, *Theory of prehomogeneous vector spaces* (*algebraic part*) *– the English translation of Sato's lecture from Shintani's note*, Nagoya Math. J., **120** (1990), 1–34.

[25] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, PWN, Warsaw, 1974.

[26] I. Ozeki, *On the microlocal structure of the regular prehomogeneous vector space associated with* SL(5) × GL(4) *I*, Proc. Japan Acad. **55**, Ser. A (1979), 37–40.

[27] I. Ozeki, *On the microlocal structure of the regular prehomogeneous vector space associated with* SL(5) × GL(4) *I*, Publ. Res. Inst. Math. Sci., **26** (1990), no. 3, 539–584.

[28] R. Scharlau, *Paare alternierender Formen*, Math. Z., **147** (1976), 13–19.

[29] W. Schmidt, *Number fields of given degree and bounded discriminant*, Columbia University Number Theory Seminar (New York 1992), Astérisque, **228** (1995), 189–195.

[30] Waterloo Maple Inc., "Maple 7", copyright 2001.

[31] D. Witte, A. Yukie and R. Zierau, *Prehomogeneous vector spaces and ergodic theory II*, Trans. Amer. Math. Soc., **352** (2000), 1687–1708.

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

[33] A. Yukie, *Density theorems related to prehomogeneous vector spaces*, Automorphic forms, automorphic representations and automorphic L-functions over algebraic groups, Sūrikaisekikenkyūsho Kōkyūroku, **1173** (2000), 171–183.

[34] A. Yukie, Shintani Zeta Functions, Lond. Math. Soc. Lecture Notes, Vol. 183, Cambridge UP, Cambridge, 1993.

Anthony C. Kable
Department of Mathematics
Oklahoma State University
Stillwater, OK 74078
USA
akable@math.okstate.edu

Akihiko Yukie
Mathematical Institute
Tôhoku University
Sendai, 980-8578
Japan
yukie@math.tohoku.ac.jp