Math. Res. Lett.
Volume 30, Number 4, 1011–1044, 2023

Computing structure constants for rings of finite rank from minimal free resolutions

Tom Fisher and Lazar Radičević

We show how the minimal free resolution of a set of n points in general position in projective space of dimension $n-2$ explicitly determines structure constants for a ring of rank n. This generalises previously known constructions of Levi-Delone-Faddeev and Bhargava in the cases $n = 3, 4, 5$.

1. Introduction

A classical construction, known as the Levi-Delone-Faddeev correspondence [9, 15] (see also [13]), shows that a binary cubic form

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$$

naturally determines a ring of rank 3. Explicitly, if ξ is a symbol formally satisfying $f(\xi, 1) = 0$ then $\omega = a\xi$ and $\theta = -d\xi^{-1}$ satisfy the relations

$$\begin{aligned} \omega^2 &= -ac - b\omega + a\theta, \\ \omega\theta &= -ad, \\ \theta^2 &= -bd - d\omega + c\theta. \end{aligned} \tag{1}$$

These relations may be used to define a commutative and associative multiplication on the free module with basis $1, \omega, \theta$. The construction works over any base ring, and gives a discriminant preserving bijection between equivalence classes of binary cubic forms and isomorphism classes of rings of rank 3. This construction was extended to rings of rank 4 and 5 by Bhargava [1, 3], who considered pairs of quadratic forms in 3 variables, and 5×5 alternating matrices of linear forms in 4 variables.

We describe an extension to rings of rank n for any integer $n \geqslant 3$. Our main result (Theorem 2.8) shows how a set of n points $X \subset \mathbb{P}^{n-2}$ in general position determines, by means of an explicit construction involving the minimal free resolution of X, structure constants for an algebra A of rank n. In particular we show that this algebra A is isomorphic to the coordinate ring of X.

We should say straight away that we are not expecting to fully generalise Bhargava's work, and count number fields of degree $n > 5$. Instead our motivation comes from the study of genus one curves. If $C \subset \mathbb{P}^{n-1}$ is a genus one curve of degree n, embedded by a complete linear system, then a generic hyperplane section of C will be a set of n points in general position. The first author showed in [12] how to associate to such a curve C a matrix of quadratic forms Ω describing the invariant differential. One application of Theorem 2.8 is that the associative law then determines some of the equations defining the space of all such Ω's. Another application is given by the second author in his PhD thesis [16] where for $E/\mathbb{Q}$ an elliptic curve and $n \geqslant 2$ an integer, he gives a simple bound on the least discriminant of a degree n number field over which each element of order n in the Tate Shafarevich group of E capitulates.

Having mentioned these applications to the study of curves, in the rest of this article we only consider finite sets of points in projective space.

For the statement of Theorem 2.8 we work over a field K of characteristic 0. However, examination of the proofs shows that all we need is that the characteristic does not divide $2n$. In Section 3 (with the main proof postponed to Section 10) we describe a slightly more complicated variant of our construction that works in all characteristics. It is this construction that reduces (in the cases $n = 3, 4, 5$) to the earlier work of Levi-Delone-Faddeev and Bhargava. It also gives better bounds in [16, Theorem 1.0.1].

In Section 4 we review the connection between non-degenerate algebras of dimension n and sets of n points in $\mathbb{P}^{n-2}$ in general position. Then, as explained in Section 5, the proof of Theorem 2.8 comes down to (i) checking our construction of the structure constants behaves well under all changes of co-ordinates, and (ii) checking that the theorem holds for the standard set of n points:

$$(1:0:\ldots:0),\ (0:1:0:\ldots:0),\ \ldots\ ,(0:\ldots:0:1),\ (1:1:\ldots:1).$$

We give the proof of (i) in Sections 6 and 7. We may check (ii) for any given n by computer algebra. We give a proof that works for all n in Sections 8 and 9, using an explicit description of the minimal free resolution due to Wilson [17].

2. Statement of the main theorem

We recall a few basic notions from commutative algebra that will be needed to state our main theorem. Throughout, we work over a field K with algebraic closure $\bar{K}$. Let $R = K[x_1, \ldots, x_m]$ be the polynomial ring with its usual grading. For $M = \oplus_d M_d$ a graded R-module, we write $M(c) = \oplus_d M_{c+d}$ for the graded R-module with grading shifted by c. A direct sum of modules of the form $R(c)$ is a called a *graded free R-module.*

Definition 2.1. A *graded free resolution* of a graded R-module M is a chain complex $F_\bullet$ of graded free R-modules

$$F_r \xrightarrow{\phi_r} F_{r-1} \xrightarrow{\phi_{r-1}} \ldots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0,$$

that is exact in degree > 0, and has $H_0(F_\bullet) = F_0/\phi_1(F_1) \cong M$. Let $\mathfrak{m} = (x_1, \ldots, x_m)$ be the maximal homogeneous ideal of R. We say a resolution $F_\bullet$ is *minimal* if we have $\phi_k(F_k) \subset \mathfrak{m}F_{k-1}$ for every $k \geqslant 1$.

Our interest is in the case $M \cong R/I$, where I is a homogeneous ideal in R.

Remark 2.2. The minimal free resolution of a module is unique up to an isomorphism of chain complexes. Any such isomorphism consists of changes of bases for the free R-modules F_k in the resolution, see [11, Theorem 20.2].

We require that the maps ϕ_k respect the grading of the modules. For example, a homomorphism of modules $R(-m) \to R$ is defined by multiplication by an element $f \in R$, and this is a graded homomorphism if and only if f is homogeneous of degree m (or zero). By choosing bases for each module F_k in the resolution, we may represent the maps ϕ_k as matrices of homogeneous polynomials. By abuse of notation we also write ϕ_k for these matrices.

Remark 2.3. The condition that the resolution is minimal means that every non-zero entry of every matrix has positive degree. By Nakayama's lemma, this is equivalent to requiring that ϕ_k takes the basis of F_k to a minimal set of generators for the kernel of ϕ_{k-1}, see [10, Corollary 1.5]. This characterisation makes it clear that every finitely generated graded module admits a minimal free resolution.

A minimal free resolution of an ideal contains the data of a set of generators for the ideal, the data of all relations (syzygies) that these generators satisfy, the data of relations that these relations satisfy, and so on iteratively. We illustrate this in the following example.

Example 2.4. Let X be the set of four points $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:1)$ in $\mathbb{P}^2$. The homogeneous ideal I of X in $R = K[x_1, x_2, x_3]$ is generated by the quadratic forms $A = x_1(x_2 - x_3)$ and $B = x_2(x_1 - x_3)$. For the first step of the resolution, we can take $F_0 = R$, $F_1 = R(-2)^2$, and let $\phi_1 : R(-2)^2 \to R$ be the map represented by the row matrix (A, B), so that $\operatorname{coker}(\phi_1) \cong R/I$. To compute the second step, we observe that A and B satisfy the relation $B \cdot A + (-A) \cdot B = 0$. Furthermore, any equation $f \cdot A + g \cdot B = 0$ is obtained by multiplying this relation by some $r \in R$, i.e., we have $f = r \cdot B$ and $g = -r \cdot A$. We now take $F_2 = R(-4)$, and let $\phi_2 : R(-4) \to R(-2)^2$ be the map represented by the column matrix $(B, -A)^T$. Since this map is injective, this is where the resolution stops. We obtain the chain complex

$$0 \longrightarrow R(-4) \xrightarrow{(B,-A)^T} R(-2)^2 \xrightarrow{(A,B)} R \longrightarrow 0 \tag{2}$$

which is exact at the middle term and on the left, and is hence the minimal free resolution of R/I.

More generally we consider sets of points of the following form.

Definition 2.5. A zero dimensional variety $X \subset \mathbb{P}^{n-2}$ defined over K is a *set of n points in general position*, if X has degree n and the set of geometric points $X(\bar{K})$ consists of n points in general position, meaning that no subset of $X(\bar{K})$ of size $n-1$ is contained in a hyperplane.

Theorem 2.6. *Let $n \geqslant 4$, and let $R = K[x_1, \ldots, x_{n-1}]$ be the coordinate ring of $\mathbb{P}^{n-2}$. Let $X \subset \mathbb{P}^{n-2}$ be a set of n points in general position. Let $I \subset R$ be the homogeneous ideal of X. Then I is (arithmetically) Gorenstein, and the minimal free resolution $F_\bullet$ of R/I takes the form*

$$0 \longrightarrow R(-n) \xrightarrow{\phi_{n-2}} R(-n+2)^{b_{n-3}} \xrightarrow{\phi_{n-3}} R(-n+3)^{b_{n-4}} \xrightarrow{\phi_{n-4}} \ldots$$
$$\ldots \xrightarrow{\phi_3} R(-3)^{b_2} \xrightarrow{\phi_2} R(-2)^{b_1} \xrightarrow{\phi_1} R \longrightarrow 0,$$

where the Betti numbers are given by $b_i = n\binom{n-2}{i} - \binom{n}{i+1}$.

Proof. The minimal free resolution is as described in [17, Theorem 138], and the references cited there. For the statement that I is Gorenstein see [17, Corollary 140]. $\square$

We note that ϕ_1 and ϕ_{n-2} are represented by matrices of quadratic forms, while the maps ϕ_i, for $1 < i < n-2$, are represented by matrices of linear forms. In Section 9 we make use of an explicit description of these maps (for a specific choice of X) due to Wilson [17, Chapter 5].

Definition 2.7. The resolution $F_\bullet$ determines the following quadratic forms in the variables $x_1, \ldots, x_{n-1}$.

i) For $1 \leqslant a_1, a_2, \ldots, a_{n-2} \leqslant n-1$ we define

$$[a_1, a_2, \ldots, a_{n-2}]_{F_\bullet} = \frac{\partial \phi_1}{\partial x_{a_1}} \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \frac{\partial \phi_{n-2}}{\partial x_{a_{n-2}}},$$

where the partial derivative of a matrix is the matrix of partial derivatives of its entries, and the product is matrix multiplication. We note that the first and last terms in the product are linear in $x_1, \ldots, x_{n-1}$, whereas all the others are constants. Overall this gives a quadratic form.

ii) Let σ be the $(n-2)$-cycle $(12\ldots n-2)$ in the symmetric group S_{n-2}. We define

$$[[a_1, a_2, \ldots, a_{n-2}]]_{F_\bullet} = \sum_{k=1}^{n-2} [a_{\sigma^{2k}(1)}, a_{\sigma^{2k}(2)}, \ldots, a_{\sigma^{2k}(n-2)}]_{F_\bullet}.$$

iii) For $1 \leqslant j \leqslant n-1$ we define $\Omega_j = (-1)^j [[1, 2, \ldots, \widehat{j}, \ldots, n-1]]_{F_\bullet}$.

The choice of resolution will usually be fixed, and we therefore drop the subscripts $F_\bullet$.

For our main result we work over a field K of characteristic 0.

Theorem 2.8. *Let $n \geqslant 3$ and let $X \subset \mathbb{P}^{n-2}$ be a set of n points in general position. Let $\Omega_1, \ldots, \Omega_{n-1}$ be the quadratic forms associated to a minimal free resolution of X. Then there exists a commutative and associative K-algebra A, of dimension n, and a K-basis $1 = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ for A, such that for each $1 \leqslant i, j \leqslant n-1$ we have*

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{n-1} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \alpha_k,$$

for some constant $c_{ij}^0 \in K$. Moreover A is isomorphic to the affine coordinate ring (i.e., ring of global functions) of X, and the α_i for $1 \leqslant i \leqslant n-1$ span the trace zero subspace.

We expect that the basis for the algebra in Theorem 2.8 is the same as the basis defined in Section 2.4 of the 2022 PhD thesis of Lee [14].

Remark 2.9. Following [3, page 68] we can use the associative law to solve for the c_{ij}^0. Explicitly, for any $1 \leqslant i, j, k \leqslant n-1$ with $i \neq k$, comparing coefficients of α_k in $\alpha_i(\alpha_j \alpha_k) = (\alpha_i \alpha_j)\alpha_k$ gives

$$c_{ij}^0 = \sum_{r=1}^{n-1} \left(\frac{\partial^2 \Omega_r}{\partial x_j \partial x_k} \frac{\partial^2 \Omega_k}{\partial x_r \partial x_i} - \frac{\partial^2 \Omega_r}{\partial x_i \partial x_j} \frac{\partial^2 \Omega_k}{\partial x_r \partial x_k} \right).$$

Remark 2.10. The construction of $[a_1, a_2, \ldots, a_{n-2}]$, and hence of $\Omega_1, \ldots, \Omega_{n-1}$, is independent of the choice of basis for the free R-modules in the resolution $F_\bullet$, except for the leftmost module $R(-n)$. The quadratic forms $\Omega_1, \ldots, \Omega_{n-1}$ are therefore uniquely determined up to multiplying through by an overall scalar. It is clear that this gives an isomorphic K-algebra.

3. Constructing orders in number fields

In this section we explain the connection between Theorem 2.8 and the previously known constructions due to Levi-Delone-Faddeev and Bhargava for $n = 3, 4, 5$. Whereas we work with algebras over a field of characteristic zero, the latter constructions work for rings of rank n, i.e., algebras over $\mathbb{Z}$. We discuss to what extent this earlier work generalises to larger n.

Let A be an n-dimensional commutative K-algebra with K-basis $1, \alpha_1, \ldots, \alpha_{n-1}$. The structure constants c_{ij}^k for $1 \leqslant i, j, k \leqslant n-1$ are determined by

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{n-1} c_{ij}^k \alpha_k.$$

As noted in Remark 2.9, the c_{ij}^0 may be recovered from the other structure constants using the associative law. We say that bases $1, \alpha_1, \ldots, \alpha_{n-1}$ and $1, \beta_1, \ldots, \beta_{n-1}$ differ by a *shear* if $\beta_i = \alpha_i + \lambda_i \cdot 1$ for some $\lambda_1, \ldots, \lambda_{n-1} \in K$.

When $n = 3$ the algebra constructed by Levi-Delone-Faddeev (as defined by (1) in the introduction) is uniquely determined, up to shear, by

$$c_{11}^2 = a, \qquad c_{11}^1 - 2c_{12}^2 = -b, \qquad c_{22}^2 - 2c_{12}^1 = c, \qquad c_{22}^1 = -d. \tag{3}$$

To see this we note that, for example, changing α_1 to $\alpha_1 + \lambda \cdot 1$ increases c_{11}^1 and c_{12}^2 by 2λ and λ respectively. To compare with the algebra in Theorem 2.8 we consider the minimal free resolution

$$0 \longrightarrow R(-3) \xrightarrow{f} R \longrightarrow 0$$

where $f(x_1, x_2) = ax_1^3 + bx_1^2 x_2 + cx_1 x_2^2 + dx_2^3$. Using Definition 2.7, we compute

$$\Omega_1 = -[[2]] = -[2] = -\frac{\partial f}{\partial x_2} = -bx_1^2 - 2cx_1x_2 - 3dx_2^2$$

and

$$\Omega_2 = [[1]] = [1] = \frac{\partial f}{\partial x_1} = 3ax_1^2 + 2bx_1x_2 + cx_2^2.$$

From this it is easy to check that

$$c_{ij}^k = \frac{1}{6}\frac{\partial^2 \Omega_k}{\partial x_i \partial x_j}$$

is a solution to (3).

When $n \geqslant 4$ a similar argument to that in the case $n = 3$ shows that the algebra is uniquely determined, up to shear, by the linear combinations of structure constants in the left hand column of Table 3.1, where i, j, k range over all triples of distinct integers with $1 \leqslant i, j, k \leqslant n-1$. These linear combinations appear, with what we believe is a type error, in [3, Equation (21)]. The remaining columns are explained below.

	$n=4$	$n=5$	$n \geqslant 4$
c_{ij}^k	$\pm\{jjii\}$	$\pm\{ii\ell jj\}$	$\pm\{i,i,1,2,\ldots\widehat{i},\ldots,\widehat{j},\ldots,\widehat{k},\ldots,n-1,j,j\}$
c_{ii}^j	$\pm\{iiik\}$	$\pm\{\ell iiik\}$	$\pm\{i,i,1,\ldots,\widehat{i},\ldots,\widehat{j},\ldots,n-1,i\}$
$c_{ij}^j - c_{ik}^k$	$\pm\{iijk\}$	$\pm\{jk\ell ii\}$	$\pm\{i,i,1,\ldots,\widehat{i},\ldots,\widehat{j},\ldots,\widehat{k},\ldots,n-1,j,k\}$
$c_{ii}^i - c_{ij}^j - c_{ik}^k$	$\pm\{ikij\}$	$\pm\{ij\ell ki\}$	$\pm\{i,j,1,\ldots,\widehat{i},\ldots,\widehat{j},\ldots,\widehat{k},\ldots,n-1,k,i\}$

Table 3.1: Structure constants for rings of rank n (up to shear)

Let $F_\bullet$ be a minimal free resolution of a set of n points in general position, with differentials $\phi_1, \ldots, \phi_{n-2}$ represented by matrices of linear and quadratic forms. We write

$$\phi_1 = \sum_{i \leqslant j} P(i,j) x_i x_j \quad \text{and} \quad \phi_{n-2} = \sum_{i \leqslant j} Q(i,j) x_i x_j,$$

where the $P(i,j)$ are row vectors, and the $Q(i,j)$ are column vectors. We put $P(i,j) = P(j,i)$ and $Q(i,j) = Q(j,i)$ for $i > j$. We then define

$$\{a_1 a_2 \ldots a_n\} := P(a_1, a_2)\frac{\partial \phi_2}{\partial x_{a_3}} \cdots \frac{\partial \phi_{n-3}}{\partial x_{a_{n-2}}} Q(a_{n-1}, a_n).$$

When $n = 4$ the minimal free resolution $F_\bullet$ takes the form (2) where A and B are ternary quadratic forms. The symbols $\{ijk\ell\}$ were denoted $\lambda_{k\ell}^{ij}$ in [1, Section 3.2]. The structure constants in *loc. cit.*, up to shear, are then as recorded in Table 3.1, where $\pm$ denotes the sign of the permutation taking $1, 2, 3$ to i, j, k.

When $n = 5$ the structure theorem of Buchsbaum and Eisenbud [6] for Gorenstein ideals of codimension 3 shows that the minimal free resolution takes the form

$$0 \longrightarrow R(-5) \xrightarrow{P^T} R(-3)^5 \xrightarrow{\Phi} R(-2)^5 \xrightarrow{P} R \longrightarrow 0,$$

where Φ is a 5×5 alternating matrix of linear forms, and P is the (signed) row vector of 4×4 Pfaffians of Φ. Our symbols $\{ijk\ell m\}$ differ only by some factors of 2 from those defined in [3, Section 4]. The structure constants in *loc. cit.*, up to shear, are again as recorded in Table 3.1, where $\pm$ denotes the sign of the permutation taking $1, 2, 3, 4$ to i, j, k, ℓ.

The expressions we give in the right hand column of Table 3.1 are new.

Theorem 3.1. *Let $n \geqslant 4$ be an integer. Then the structure constants*

$$c_{ij}^k = \frac{1}{2n} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j}$$

satisfy the system of equations in Table 3.1.

Proof. It is clear from the definition that the symbol $\{\cdots\}$ does not depend on the order of its first two arguments, or the order of its last two arguments.

If $n = 4$ then by (2) we have $[i, j] = -[j, i]$ and $\{ijk\ell\} = -\{k\ell ij\}$. Let i, j, k be an even permutation of $1, 2, 3$. By Definition 2.7 we have $\Omega_k = -2[i, j]$. Using the product rule we compute

$$\begin{aligned}
\frac{\partial^2 [j,i]}{\partial x_i \partial x_j} &= 4\{jjii\} + \{ijij\} = 4\{jjii\}, \\
\frac{\partial^2 [i,k]}{\partial x_i^2} &= 2\{iiik\} + 2\{iiik\} = 4\{iiik\}, \\
\frac{\partial^2 [i,k]}{\partial x_i \partial x_j} + \frac{\partial^2 [i,j]}{\partial x_i \partial x_k} &= 2\{iijk\} + \{ijik\} + 2\{iijk\} + \{ikij\} \\
&= 4\{iijk\}, \\
\frac{\partial^2 [k,j]}{\partial x_i^2} + \frac{\partial^2 [k,i]}{\partial x_i \partial x_j} + \frac{\partial^2 [i,j]}{\partial x_i \partial x_k} &= 2\{ikij\} + \{ikij\} + 2\{jkii\} + 2\{iijk\} + \{ikij\} \\
&= 4\{ikij\}.
\end{aligned}$$

This proves the theorem in the case $n = 4$. We give the proof for $n \geqslant 5$, and specify the correct choice of signs $\pm$, in Theorem 10.1. It may also be checked, using Lemma 10.2, that the expressions in Table 3.1 for $n \geqslant 4$ do indeed specialise to those in the previous two columns when $n = 4$ and $n = 5$. $\square$

We have now checked that Theorem 2.8 agrees, up to a shear, with the previously known constructions for $n = 3, 4, 5$. However the structure constants do not agree exactly, since in Theorem 2.8 the basis elements $\alpha_1, \ldots, \alpha_{n-1}$ are normalised (up to shear) so that they have trace zero, whereas the algebras in [1, 3, 9] are normalised so that

$$\begin{array}{ll} n = 3 & c_{12}^1 = c_{12}^2 = 0, \\ n = 4 & c_{12}^1 = c_{12}^2 = c_{13}^1 = 0, \\ n = 5 & c_{12}^1 = c_{12}^2 = c_{34}^3 = c_{34}^4 = 0. \end{array}$$

In general we could normalise our basis by choosing a convention such as

$$c_{12}^2 = c_{23}^3 = c_{34}^4 = \ldots = c_{n-2,n-1}^{n-1} = c_{n-1,1}^1 = 0, \tag{4}$$

or when n is odd

$$c_{12}^1 = c_{12}^2 = c_{34}^3 = c_{34}^4 = \ldots = c_{n-2,n-1}^{n-2} = c_{n-2,n-1}^{n-1} = 0. \tag{5}$$

With either convention, it is clear that there is a unique way to modify our basis by a shear so that it satisfies the convention.

Compared to normalising $\alpha_1, \ldots, \alpha_{n-1}$ to have trace zero, these conventions break symmetry, but have the advantage of working in all characteristics. They are also useful for constructing orders in number fields as we now explain.

We take $K = \mathbb{Q}$ and suppose that the minimal free resolution $F_\bullet$ has integer coefficients, i.e. the differentials ϕ_k in Theorem 2.6 are represented by matrices of polynomials in $\mathbb{Z}[x_1, \ldots, x_{n-1}]$. By Definition 2.7 the structure constants for the $\mathbb{Q}$-algebra A in Theorem 2.8 are integral, and so determine an order $B = \mathbb{Z} \oplus \mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_{n-1} \subset A$. This ring decomposes (as a $\mathbb{Z}$-module) as $B = \mathbb{Z} \oplus B_0$ where $B_0 = \mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_{n-1}$ is the subset of elements of trace zero. Therefore $\mathrm{Tr}_{A/\mathbb{Z}}(B) = n\mathbb{Z}$, and so any prime dividing n necessarily ramifies in B. More generally, this order can never be maximal at the primes dividing $2n$. Indeed, if we choose our structure constants using Table 3.1 and one of the normalisation conventions (4) or (5), then these define an order B' with $B \subset B' \subset A$. From the factor $2n$ in the statement of Theorem 3.1 we see that $B' = \mathbb{Z} \oplus \mathbb{Z}\alpha'_1 \oplus \ldots \oplus \mathbb{Z}\alpha'_{n-1}$, where $\frac{1}{2n}\alpha_1, \ldots, \frac{1}{2n}\alpha_{n-1}$ and $\alpha'_1, \ldots, \alpha'_{n-1}$ differ by a shear, and hence the index of B in B' is $(2n)^{n-1}$. For $n = 3, 4, 5$, the ring B' is the one constructed in [1, 3, 9]. For general n, working with B' rather than B gives a larger order with smaller discriminant, and hence a sharper bound in [16, Theorem 1.0.1].

Remark 3.2. We briefly mention three respects in which the theory for $n = 3, 4, 5$, as described in [1, 3, 13], is still more developed than that for general n.

i) We conjecture than any order in an étale $\mathbb{Q}$-algebra of rank n is necessarily of the form B' for some minimal free resolution $F_\bullet$ with integer coefficients. This is known for $n = 3, 4, 5$. It is also true for the ring $\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ by the calculations in Sections 8 and 9. We hope to investigate this conjecture further in future work.

ii) For $n = 3, 4, 5$ the binary cubics, pairs of ternary quadratics, and alternating matrices of linear forms, parameterise all rings of rank n, including degenerate rings such as $\mathbb{Z}[x]/(x^n)$. It would be interesting to determine if there is a suitable class of "degenerate" minimal free resolutions for $n > 5$ that correspond to these rings.

iii) The results for $n = 3, 4, 5$ have been used by Davenport and Heilbronn [8] and Bhargava [2, 4] to give an asymptotic count of number fields of degree n ordered by discriminant. Since we do not have a description of the space of minimal free resolutions that lends itself to the counting arguments used in the geometry of numbers, it remains a difficult problem to extend these results to $n > 5$.

4. Points in general position and étale algebras

In this section we give a slightly different perspective on the classical fact that there is an equivalence of categories between the category of finite sets of points with a continuous action of the absolute Galois group, and the category of finite-dimensional étale algebras. These ideas feature prominently in works of Bhargava, see especially the discussion in [3, page 59], as well as the work of his students Wood [18] and Wilson [17].

We fix an integer $n \geqslant 3$. Let

$$\mathcal{X} = \{X \subset \mathbb{P}^{n-2} : \ X \text{ is a set of } n \text{ points in general position}\}.$$

Note that $\mathcal{X}(K)$ consists of sets X which (viewed as zero-dimensional varieties) are defined over K but the individual (geometric) points of X need not be defined over K. The group $\mathrm{PGL}_{n-1}(K)$ acts on $\mathcal{X}(K)$ by changes of coordinates.

An n-dimensional commutative K-algebra A is *non-degenerate* if the trace form associated to A is non-degenerate. This is equivalent to requiring that A is étale over K, or that there exists an isomorphism $A \otimes_K \bar{K} \cong \bar{K}^n$.

For example, the ring $A = \Gamma(X, \mathcal{O}_X)$ of global functions on a set of n points $X \in \mathcal{X}(K)$ is a non-degenerate K-algebra of dimension n.

The following fact seems to be well-known: see for example [7, Corollary 2.3].

Proposition 4.1. *Let $\mathcal{A}$ be the set of isomorphism classes of non-degenerate n-dimensional K-algebras. Then the map $X \mapsto \Gamma(X, \mathcal{O}_X)$ induces a bijection between the set of $\mathrm{PGL}_{n-1}(K)$-orbits of $\mathcal{X}(K)$ and the set $\mathcal{A}$.*

Any two elements of $\mathcal{X}(K)$ that lie in the same $\mathrm{PGL}_{n-1}(K)$-orbit have isomorphic rings of global functions, and so map to the same element of $\mathcal{A}$. Therefore the map in Proposition 4.1 is well defined. We must show it is a bijection. First we need two lemmas.

Lemma 4.2.
i) *Let A be a non-degenerate n-dimensional K-algebra. Let M be a locally free A-module of rank 1. Then M is free, i.e., it is isomorphic to A as an A-module.*
ii) *Let $X \subset \mathbb{P}^{n-2}$ be a set of n distinct points, and let $A = \Gamma(X, \mathcal{O}_X)$. Then X is the image of a map $\operatorname{Spec} A \to \mathbb{P}^{n-2}$ given by $(\alpha_1 : \ldots : \alpha_{n-1})$ for some $\alpha_1, \ldots, \alpha_{n-1} \in A$.*

Proof. (i) Since A is non-degenerate it is isomorphic as an algebra to a direct product of fields, say, $A \cong A_1 \times \cdots \times A_k$. For each $1 \leqslant i \leqslant k$, let e_i be the idempotent corresponding to the factor A_i, so that $\sum_{i=1}^k e_i = 1$, $Ae_i \cong A_i$ as an A-module, $e_i^2 = e_i$ and $e_i e_j = 0$ for all $i \neq j$. Then we have the decomposition $M = e_1 M \oplus e_2 M \oplus \cdots \oplus e_k M$, where each module $e_i M$ is an A_i-vector space. Since M is locally free of rank 1, each $e_i M$ is 1-dimensional, and so we may choose a basis vector f_i. Then $M = Af \cong A$, where $f = \sum_{i=1}^k f_i$.
(ii) The embedding of $X = \operatorname{Spec} A$ in $\mathbb{P}^{n-2}$ is given by global sections $\ell_1, \ldots, \ell_{n-1}$ belonging to the A-module $M = \Gamma(X, \mathcal{O}_X(1))$. We see by (i) that M is a free A-module of rank 1, say generated by $m \in M$. We then write $\ell_i = \alpha_i m$ for some $\alpha_i \in A$. □

Lemma 4.3. *Let A be a non-degenerate n-dimensional K-algebra. Let X be the image of the map $\operatorname{Spec} A \to \mathbb{P}^{n-2}$ given by $(\alpha_1 : \ldots : \alpha_{n-1})$ for some $\alpha_1, \ldots, \alpha_{n-1} \in A$. Then X is a set of n points in general position if and only if there exists a unit $\lambda \in A^\times$ such that $\lambda\alpha_1, \ldots, \lambda\alpha_{n-1}$ is a K-basis for the trace zero subspace of A. Moreover, if such a λ exists then it is unique up to multiplication by an element of $K^\times$.*

Proof. We may assume that $\alpha_1, \ldots, \alpha_{n-1}$ are linearly independent over K, since otherwise it is clear that neither condition is satisfied.

The uniqueness follows from the non-degeneracy of the trace form. For existence, it is clear by linear algebra over K that there exists non-zero $\lambda \in A$ such that $\mathrm{Tr}_{A/K}(\lambda\alpha_j) = 0$ for all $1 \leqslant j \leqslant n-1$. It remains to show that λ is a unit.

Since A is isomorphic to a product of fields, we may write any element of A as a unit times an idempotent. It therefore suffices to consider λ an idempotent. Writing $\sigma_1, \ldots, \sigma_n$ for the distinct K-algebra homomorphisms $A \to \bar{K}$ we have

$$X(\bar{K}) = \{(\sigma_i(\alpha_1) : \ldots : \sigma_i(\alpha_{n-1})) : 1 \leqslant i \leqslant n\} \subset \mathbb{P}^{n-2}(\bar{K}).$$

Since λ is an idempotent we assume by reordering the σ_i that $(\sigma_1(\lambda), \ldots, \sigma_n(\lambda)) = (1, \ldots, 1, 0, \ldots 0)$ where there are (say) m ones and $n-m$ zeros. Then $\sum_{i=1}^{m} \sigma_i(\alpha_j) = \mathrm{Tr}_{A/K}(\lambda\alpha_j) = 0$ for all $1 \leqslant j \leqslant n-1$. Since X is in general position, this forces $m = n$, and so $\lambda = 1$ as required. $\square$

Proof of Proposition 4.1. First, to prove surjectivity, we suppose that A is a non-degenerate n-dimensional K-algebra. Then we pick $\alpha_1, \ldots, \alpha_{n-1}$ a K-basis for the trace zero subspace of A, and let X be the image of the map $\mathrm{Spec}\, A \to \mathbb{P}^{n-2}$ given by $(\alpha_1 : \ldots : \alpha_{n-1})$. Lemma 4.3 shows that X is in general position, and we then have $X \mapsto A$. Next, to prove injectivity, we suppose that X_1 and X_2 both map to A. By Lemmas 4.2 and 4.3 both X_1 and X_2 are embedded in $\mathbb{P}^{n-2}$ using (possibly) different choices of bases for the trace zero subspace of A. Hence there exists an element of $\mathrm{PGL}_{n-1}(K)$ taking X_1 to X_2. $\square$

5. Overview of the proof

Let $V = \langle x_1, \ldots, x_{n-1} \rangle$ be the space of linear forms on $\mathbb{P}^{n-2}$, and denote the dual basis of V^* by $x_1^*, \ldots, x_{n-1}^*$. The quadratic forms $\Omega_1, \ldots, \Omega_{n-1}$ determine an element Ω in $V^* \otimes S^2V$ via the formula

$$\Omega := \sum_{j=1}^{n-1} x_j^* \otimes \Omega_j. \tag{6}$$

The following proposition, which we prove in Section 7, shows that the construction of Ω from the minimal free resolution is invariant under change of basis of V.

Proposition 5.1. *Let $F_\bullet$ be a minimal free resolution for a set $X \subset \mathbb{P}^{n-2}$ of n points in general position. We write $x_1, \ldots, x_{n-1}$ for our coordinates on $\mathbb{P}^{n-2}$. Let $x'_j = \sum_{i=1}^{n-1} g_{ij} x_i$ for some $g = (g_{ij}) \in \mathrm{GL}_{n-1}$. Writing $\phi_1, \ldots, \phi_{n-2}$ for the matrices representing the maps in the resolution $F_\bullet$, let $F'_\bullet$ be the resolution whose maps are given by matrices $\phi'_1, \ldots, \phi'_{n-2}$ where*

$$\phi'_r(x_1, \ldots, x_{n-1}) = \phi_r(x'_1, \ldots, x'_{n-1}).$$

Let Ω and Ω' be the elements of $V^* \otimes S^2 V$ associated to the resolutions $F_\bullet$ and $F'_\bullet$ respectively. Then we have

$$\Omega' = (\det g)(g \cdot \Omega),$$

where the action of g on Ω is the standard action of GL_{n-1} on $V^* \otimes S^2 V$.

Our main theorem (Theorem 2.8) gives an expression for the structure constants of the algebra A in terms of the quadratic forms $\Omega_1, \ldots, \Omega_{n-1}$ determined by a minimal free resolution of X. In fact we prove the following strengthening of that theorem.

Theorem 5.2. *Let $n \geqslant 3$ and let $X \subset \mathbb{P}^{n-2}$ be a set of n points in general position. Let $A = \Gamma(X, \mathcal{O}_X)$ be the coordinate ring of X and let V be the trace zero subspace of A.*

i) *There is a K-basis $\alpha_1, \ldots, \alpha_{n-1}$ of V, unique up to multiplication by an overall scalar, such that the embedding of $X = \operatorname{Spec} A$ in $\mathbb{P}^{n-2}$ is given by $(\alpha_1 : \ldots : \alpha_{n-1})$.*

ii) *Let $\alpha_1, \ldots, \alpha_{n-1}$ be as in (i) and let $\alpha_0^*, \alpha_1^*, \ldots, \alpha_n^*$ be the basis for A that is dual to $1, \alpha_1, \ldots, \alpha_{n-1}$ with respect to the trace pairing $(x, y) \mapsto \mathrm{Tr}_{A/K}(xy)$. If $\Omega_1, \ldots, \Omega_{n-1}$ are the quadratic forms determined by a minimal free resolution of X then there exist constants $\lambda, c_{ij}^0 \in K$ such that*

$$\alpha_i^* \alpha_j^* = c_{ij}^0 + \lambda \sum_{k=1}^{n-1} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \alpha_k^*, \tag{7}$$

for all $1 \leqslant i, j \leqslant n-1$.

Proof. (i) This follows from Lemmas 4.2 and 4.3.
(ii) We claim we are free to make changes of coordinates on $\mathbb{P}^{n-2}$. This is proved by considering the effect of such a change of coordinates on each term

in (7). We may organise this calculation as follows. First we use the trace pairing to identify $A = (K \cdot 1) \oplus V^*$. Then multiplication in A determines a symmetric bilinear map $V^* \times V^* \to V^*$ and hence an element of $V^* \otimes S^2V$. Next we use part (i) of the theorem to identify V with the space of linear forms on $\mathbb{P}^{n-2}$. The quadratic forms $\Omega_1, \ldots, \Omega_{n-1}$ determine an element Ω in $V^* \otimes S^2V$ via (6). The theorem asserts that these two elements of $V^* \otimes S^2V$ are equal, up to multiplication by a scalar. To prove our claim it suffices to show that these two elements transform, under a change of coordinates, according to the natural action of $\mathrm{GL}(V)$ on $V^* \otimes S^2V$. In the first case this is clear from the construction, and in the second case we use Proposition 5.1.

We are also free to extend our base field K, and so may assume by a change of coordinates that X is the standard set of n points in general position given by $P_1 = (1 : 0 \ldots : 0), P_2 = (0 : 1 : 0 \ldots : 0), \ldots, P_{n-1} = (0 : \ldots : 0 : 1)$ and $P_n = (1 : 1 : \ldots : 1)$. Having reduced to this special case, we identify $A \cong K^n$ via $\alpha \mapsto (\alpha(P_1), \ldots, \alpha(P_n))$. Then the K-basis for the trace zero subspace as determined in part (i) of the theorem is

$$\begin{aligned} \alpha_1 &= \frac{1}{n}(1, 0, 0, \ldots, 0, -1), \\ \alpha_2 &= \frac{1}{n}(0, 1, 0, \ldots, 0, -1), \\ &\vdots \\ \alpha_{n-1} &= \frac{1}{n}(0, 0, 0, \ldots, 1, -1), \end{aligned}$$

where at this stage the overall scaling by a factor $1/n$ is arbitrary, but has been chosen to simplify the calculations below. The multiplication on K^n is given by multiplication in each component separately, and the trace pairing on K^n is given by the standard dot product. Following the statement of part (ii) of the theorem, we compute:

$$\begin{aligned} \alpha_1^* &= (n-1, -1, -1, \ldots, -1), \\ \alpha_2^* &= (-1, n-1, -1, \ldots, -1), \\ &\vdots \\ \alpha_{n-1}^* &= (-1, -1, \ldots, n-1, -1). \end{aligned}$$

Then for $1 \leqslant i, j \leqslant n-1$, the multiplication is given by

$$\alpha_i^* \alpha_j^* = \begin{cases} -1 - \alpha_i^* - \alpha_j^* & \text{if } i \neq j, \\ (n-1) + (n-2)\alpha_i^* & \text{if } i = j. \end{cases}$$

Equation (7) with $\lambda = 1/2$ then follows from the next lemma. □

Lemma 5.3. *Let $n \geqslant 3$ and let $X \subset \mathbb{P}^{n-2}$ be the standard set of n points in general position. Then the quadratic forms Ω_i in Definition 2.7 are given, up to an overall scalar, by $\Omega_i = nx_i^2 - 2x_i \sum_{j=1}^{n-1} x_j$ for all $1 \leqslant i \leqslant n-1$.*

The proof of Lemma 5.3 is given in Sections 8 and 9. However for specific small values of n (say $n \leqslant 10$) it is also possible to check the lemma directly by computer algebra.

6. Some symmetries

We prove some symmetries satisfied by the square bracket and double square bracket symbols (see Definition 2.7). For convenience in this section we put $m = n - 2$, since all our resolutions have length m.

Lemma 6.1. *If $2 \leqslant r \leqslant m-2$ then*

$$[a_1, \dots, a_r, a_{r+1}, \dots, a_m] = -[a_1, \dots, a_{r+1}, a_r, \dots, a_m].$$

Proof. For this range of r, both ϕ_r and ϕ_{r+1} are matrices of linear forms. We differentiate the relation $\phi_r \phi_{r+1} = 0$. By the Leibniz rule,

$$0 = \frac{\partial^2(\phi_r\phi_{r+1})}{\partial x_{a_r}\partial x_{a_{r+1}}} = \frac{\partial \phi_r}{\partial x_{a_r}}\frac{\partial \phi_{r+1}}{\partial x_{a_{r+1}}} + \frac{\partial \phi_r}{\partial x_{a_{r+1}}}\frac{\partial \phi_{r+1}}{\partial x_{a_r}},$$

hence the desired relation. □

Remark 6.2. The lemma holds only for $2 \leqslant r \leqslant m-2$. Indeed, swapping the first two a's or the last two a's need not simply result in a sign change. See Lemma 8.1 for an explicit example. We introduce the symbols $[[a_1, a_2, \dots, a_m]]$ to rectify this; see Lemma 6.5 below.

Lemma 6.3. *We have $[a_1, a_2, \dots, a_{m-1}, a_m] = \pm[a_m, a_{m-1}, \dots, a_2, a_1]$, where the sign is $+1$ if $m \equiv 0, 1 \pmod 4$ and -1 if $m \equiv 2, 3 \pmod 4$.*

Proof. The dual of an R-module M is $M^* = \mathrm{Hom}_R(M, R)$. If an R-module map $M \to N$ between free R-modules is represented by a matrix ϕ (with respect to some bases) then the dual map $N^* \to M^*$ is represented by the transpose matrix ϕ^T (with respect to the dual bases).

We saw in Theorem 2.6 that X is Gorenstein. This implies that its minimal free resolution $F_\bullet$ is self-dual. Explicitly, there is a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r, "\phi_m"] \arrow[d, "\pm 1"'] & F_{m-1} \arrow[r] \arrow[d] & \dots \arrow[r] & F_1 \arrow[r, "\phi_1"] \arrow[d] & R \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & R \arrow[r, "\phi_1^T"] & F_1^* \arrow[r] & \dots \arrow[r] & F_{m-1}^* \arrow[r, "\phi_m^T"] & R \arrow[r] & 0 \end{tikzcd}$$

where the vertical maps are isomorphisms, the right most one is the identity map, and the left most one is multiplication by ± 1. According to [5, page 123], the sign is $+$ if and only if $m \equiv 0, 1 \pmod 4$. The lemma now follows from the definition of the square brackets notation. $\square$

Lemma 6.4. *If the terms indicated by $\dots$ are the same in each case then*

i) $[a, \dots, b] + [b, \dots, a] = 0$, *and*

ii) $[a, b, \dots, c, d] + [b, a, \dots, c, d] + [a, b, \dots, d, c] + [b, a, \dots, d, c] = 0.$

Proof. Part (i) follows from Lemmas 6.1 and 6.3. For the second part, as $\phi_1 \phi_2 = 0$ and $\phi_{m-1}\phi_m = 0$, we have

$$0 = \frac{\partial^2(\phi_1\phi_2)}{\partial x_a \partial x_b} = \frac{\partial \phi_1}{\partial x_a}\frac{\partial \phi_2}{\partial x_b} + \frac{\partial \phi_1}{\partial x_b}\frac{\partial \phi_2}{\partial x_a} + \frac{\partial^2 \phi_1}{\partial x_a \partial x_b}\phi_2,$$

and similarly,

$$0 = \frac{\partial^2(\phi_{m-1}\phi_m)}{\partial x_c \partial x_d} = \frac{\partial \phi_{m-1}}{\partial x_c}\frac{\partial \phi_m}{\partial x_d} + \frac{\partial \phi_{m-1}}{\partial x_d}\frac{\partial \phi_m}{\partial x_c} + \phi_{m-1}\frac{\partial^2 \phi_m}{\partial x_c \partial x_d}.$$

Thus it suffices to show that

$$\frac{\partial^2 \phi_1}{\partial x_a \partial x_b}\phi_2 \frac{\partial \phi_3}{\partial x_{a_3}} \cdots \frac{\partial \phi_{m-2}}{\partial x_{a_{m-2}}}\phi_{m-1}\frac{\partial^2 \phi_m}{\partial x_c \partial x_d} = 0.$$

For $2 \leqslant r \leqslant m-3$ we have

$$\phi_r \frac{\partial \phi_{r+1}}{\partial x_p} = -\frac{\partial \phi_r}{\partial x_p}\phi_{r+1}.$$

We use this relation to move the undifferentiated term to the right until we get an expression involving $\phi_{m-2}\phi_{m-1}$, which vanishes. $\square$

As in Definition 2.7, we let $\sigma = (123\dots m) \in S_m$ and define

$$[[a_1, \dots, a_m]] = \sum_{r=0}^{m-1} [a_{\sigma^{2r}(1)}, \dots, a_{\sigma^{2r}(m)}].$$

Lemma 6.5. *For $\tau \in S_m$ we have*

$$[[a_{\tau(1)}, \dots, a_{\tau(m)}]] = \operatorname{sign}(\tau)[[a_1, \dots, a_m]].$$

Proof. For $m \leqslant 3$ the lemma follows easily from Lemma 6.4(i), so we may assume $m \geqslant 4$.

We first prove the lemma in the case $\tau = (12)$. We have

$$[[a_1, a_2, a_3, \dots, a_m]] = [a_1, a_2, a_3, \dots, a_m] + [a_3, a_4, \dots, a_m, a_1, a_2] + \dots.$$

We consider the effect of switching a_1 and a_2 on each term on the right. For the terms we have not written out, the answer is that they change sign, and indeed this follows from Lemmas 6.1 and 6.4(i), the latter being used for the term $[a_2, a_3, \dots, a_m, a_1]$ which only occurs if n is odd. We are left with the two terms we did write out. We treat these together. By repeatedly using Lemma 6.1 to move a_3 to the right, we have

$$[a_2, a_1, a_3, \dots, a_m] = (-1)^m [a_2, a_1, a_4, \dots, a_{m-1}, a_3, a_m],$$

and similarly

$$\begin{aligned}[a_3, a_4, \dots, a_m, a_2, a_1] &= -[a_1, a_4, \dots, a_m, a_2, a_3] \\ &= (-1)^m [a_1, a_2, a_4, \dots, a_{m-1}, a_m, a_3],\end{aligned}$$

where the first equality is a consequence of Lemma 6.4(i) and the second is a repeated application of Lemma 6.1. By Lemma 6.4(ii) we have

$$\begin{aligned}&(-1)^m([a_2, a_1, a_4, \dots, a_{m-1}, a_3, a_m] + [a_1, a_2, a_4, \dots, a_{m-1}, a_m, a_3]) \\ &= (-1)^{m+1}([a_1, a_2, a_4, \dots, a_{m-1}, a_3, a_m] + [a_2, a_1, a_4, \dots, a_{m-1}, a_m, a_3]).\end{aligned}$$

This is equal, by Lemma 6.4(i) and repeated application of Lemma 6.1, to

$$-[a_1, a_2, a_3, \dots, a_m] - [a_3, a_4, \dots, a_m, a_1, a_2].$$

This completes the proof in the case $\tau = (12)$.

It is immediate from the definition of $[[\ldots]]$ that the lemma holds with $\tau = \sigma^2$. If n is odd then σ^2 and (12) generate S_m and we are done. If n is even then S_m is generated by σ^2, (12) and (23). So it suffices to prove the lemma for $\tau = (23)$. However the proof in this case goes through term by term using Lemmas 6.1 and 6.4(i). $\square$

Remark 6.6. If n is odd then using σ instead of σ^2 would make no difference in the definition of $[[\ldots]]$. However if n is even then this would give an expression that is identically zero, as may be seen from Lemma 6.5, noting that σ is an odd permutation.

7. Changes of coordinates

In this section we prove Proposition 5.1. Let $V = \langle x_1, \ldots, x_{n-1} \rangle$ be the space of linear forms on $\mathbb{P}^{n-2}$, and let $x_1^*, \ldots, x_{n-1}^*$ be the dual basis for V^*. We identify $S^d V$ with the space of degree d homogeneous polynomials F in $K[x_1, \ldots, x_{n-1}]$. The natural left actions of GL_{n-1} on $S^d V$ and on V^* are given by

$$(g \cdot F)(x_1, \ldots, x_{n-1}) = F(x_1', \ldots, x_{n-1}'), \tag{8}$$

where $x_j' = \sum_{i=1}^{n-1} g_{ij} x_i$, and

$$g \cdot x_j^* = \sum_{i=1}^{n-1} (g^{-T})_{ij} x_i^*. \tag{9}$$

In Section 2 we defined quadratic forms $[[\ldots]]$ and Ω_j associated to a minimal free resolution with differentials ϕ_r. Fix any $g \in \mathrm{GL}_{n-1}$. We now write $[[\ldots]]'$ and Ω_j' for the quadratic forms associated to the minimal free resolution with differentials $\phi_r'(x_1, \ldots, x_{n-1}) = \phi_r(x_1', \ldots, x_{n-1}')$, where $x_j' = \sum_{i=1}^{n-1} g_{ij} x_i$. We must prove that

$$\sum_{j=1}^{n-1} x_j^* \otimes \Omega_j' = (\det g) \sum_{j=1}^{n-1} \left(g \cdot x_j^*\right) \otimes (g \cdot \Omega_j). \tag{10}$$

It suffices to prove this claim for g running over a set of generators for the group GL_{n-1}, and accordingly we consider g a diagonal matrix, g a permutation matrix, and g a unipotent matrix.

First we suppose that g is diagonal, say with diagonal entries $\lambda_1, \dots, \lambda_{n-1}$. By the chain rule, we have

$$[[a_1, a_2, \dots, a_{n-2}]]'(x_1, \dots, x_{n-1}) \\ = \lambda_{a_1} \cdots \lambda_{a_{n-2}} [[a_1, a_2, \dots, a_{n-2}]](x'_1, \dots, x'_{n-1}).$$

Therefore

$$\Omega'_j(x_1, \dots, x_{n-1}) = (\det g)\lambda_j^{-1} \Omega_j(x'_1, \dots, x'_{n-1}),$$

and so (10) follows by (8) and (9).

We next suppose that g is the permutation matrix corresponding to the transposition $\tau = (ab)$ for some $1 \leqslant a < b \leqslant n-1$. If $j \notin \{a, b\}$ then by Lemma 6.5 we have

$$[[\tau(1), \tau(2), \dots, \widehat{\tau(j)}, \dots, \tau(n-1)]] = -[[1, 2, \dots, \widehat{j}, \dots, n-1]],$$

and

$$\begin{aligned} [[1, \dots, \widehat{a}, \dots, b-1, a, b+1, \dots, n-1]] &= (-1)^{b-a-1}[[1, \dots, \widehat{b}, \dots, n-1]], \\ [[1, \dots, a-1, b, a+1, \dots, \widehat{b}, \dots, n-1]] &= (-1)^{b-a-1}[[1, \dots, \widehat{a}, \dots, n-1]]. \end{aligned}$$

Therefore

$$\Omega'_j(x_1, \dots, x_{n-1}) = \begin{cases} -\Omega_j(x'_1, \dots, x'_{n-1}) & \text{if } j \notin \{a, b\}, \\ -\Omega_b(x'_1, \dots, x'_{n-1}) & \text{if } j = a, \\ -\Omega_a(x'_1, \dots, x'_{n-1}) & \text{if } j = b, \end{cases}$$

and so (10) follows by (8) and (9).

Finally, we consider the case $g = I + tE_{21}$, where E_{ij} is the $(n-1) \times (n-1)$ matrix with a 1 in the (i, j)-place, and all other entries 0. The matrices ϕ'_r are given by

$$\phi'_r(x_1, \dots, x_{n-1}) = \phi_r(x_1 + tx_2, x_2, \dots, x_{n-1}).$$

So by the chain rule

$$\frac{\partial \phi'_r}{\partial x_j}(x_1, \dots, x_{n-1}) = \left(\frac{\partial \phi_r}{\partial x_j} + \delta_{j2} t \frac{\partial \phi_r}{\partial x_1} \right) (x_1 + tx_2, x_2, \dots, x_{n-1}).$$

Therefore, if $2 \notin \{a_1, \dots, a_{n-2}\}$ then

$$[[a_1, \dots, a_{n-2}]]'(x_1, \dots, x_{n-1}) = [[a_1, \dots, a_{n-2}]](x'_1, \dots, x'_{n-1}),$$

whereas if $a_k = 2$ then

$$\begin{aligned}&[[a_1, \ldots, a_{n-2}]]'(x_1, \ldots, x_{n-1})\\&\quad = [[a_1, \ldots, a_{n-2}]](x'_1, \ldots, x'_{n-1})\\&\qquad + t[[a_1, \ldots, a_{k-1}, 1, a_{k+1}, \ldots, a_{n-2}]](x'_1, \ldots, x'_{n-1}).\end{aligned}$$

Note that if $1 \in \{a_1, \ldots, a_{n-2}\}$ then the final term $[[a_1, \ldots, a_{k-1}, 1, a_{k+1}, \ldots, a_{n-2}]]$ vanishes by Lemma 6.5, since 1 appears twice. Then by definition of the Ω_j we have

$$\Omega'_j(x_1, \ldots, x_{n-1}) = \Omega_j(x'_1, \ldots, x'_{n-1}) - \delta_{j1} t \Omega_2(x'_1, \ldots, x'_{n-1}),$$

and hence

$$\sum_{j=1}^{n-1} x_j^* \otimes \Omega'_j(x_1, \ldots, x_{n-1}) = \sum_{j=1}^{n-1} \left(x_j^* - \delta_{j2} t x_1^*\right) \otimes \Omega_j(x'_1, \ldots, x'_{n-1}).$$

Now (10) follows by (8) and (9). This completes the proof of Proposition 5.1.

8. Reduction to the key lemma

In Section 5 we reduced the proof of Theorem 2.8 to a verification in the case of the standard set of n points: $P_1 = (1 : 0 \ldots : 0), P_2 = (0 : 1 : 0 \ldots : 0), \ldots, P_{n-1} = (0 : \ldots : 0 : 1)$ and $P_n = (1 : 1 : \ldots : 1)$. This verification depends on the following “key lemma”, the proof of which we postpone to the next section.

Lemma 8.1. *Let $n \geqslant 3$ and let $X \subset \mathbb{P}^{n-2}$ be the standard set of n points in general position. Fix a choice of minimal free resolution for X. Then there exists a scalar $\lambda \in K$ such that whenever $a_1, \ldots, a_{n-2}, b$ is a permutation of $1, 2, \ldots, n-1$ we have*

$$[a_1, \ldots, a_{n-2}] = \pm\lambda(x_b - x_{a_1} - x_{a_{n-2}})x_b,$$

where $\pm$ is the sign of the permutation, and the symbol $[\cdots]$ was defined in Section 2.

We use this lemma to compute the quadratic forms $\Omega_1, \ldots, \Omega_{n-1}$ associated to X.

Proof of Lemma 5.3. Recall that we wrote σ for the $(n-2)$-cycle in S_{n-2} with $\sigma(1) = 2, \sigma(2) = 3, \ldots, \sigma(n-2) = 1$. Let $a_1, \ldots, a_{n-2}, b$ be as in the statement of Lemma 8.1. By the definition of $[[\cdots]]$, and the fact σ^2 is an even permutation, we compute

$$\begin{aligned}
[[a_1, a_2, \ldots, a_{n-2}]] &= \sum_{k=1}^{n-2} [a_{\sigma^{2k}(1)}, a_{\sigma^{2k}(2)}, \ldots, a_{\sigma^{2k}(n-2)}] \\
&= \lambda \sum_{k=1}^{n-2} (x_b - x_{a_{\sigma^{2k}(1)}} - x_{a_{\sigma^{2k}(n-2)}}) x_b \\
&= \lambda \left((n-2)x_b^2 - 2x_b \sum_{j \neq b} x_j \right) \\
&= \lambda \left(n x_b^2 - 2x_b \sum_{j=1}^{n-1} x_j \right).
\end{aligned}$$

It follows by the definition of the Ω_i and Lemma 6.5 that

$$\Omega_i = (-1)^i [[1, \ldots, \widehat{i}, \ldots, n-1]] = (-1)^{n-1} \lambda \left(n x_i^2 - 2x_i \sum_{j=1}^{n-1} x_j \right).$$

Since we are only computing the Ω_i up to an overall scalar, the factor $(-1)^{n-1}\lambda$ may be ignored. This completes the proof of Lemma 5.3. $\square$

9. Proof of the key lemma (=Lemma 8.1)

As before, let $X \subset \mathbb{P}^{n-2}$ be the standard set of n points in general position. In this section we prove Lemma 8.1. Our approach is inspired by an explicit description of the minimal free resolution of the set X, due to Wilson [17, Chapter 5]. In [16, Section 4.5] we gave a different proof of Lemma 8.1, based on the method of unprojection.

Lemma 9.1. *If $n \geqslant 4$ then the ideal $I := I(X) \subset K[x_1, \ldots, x_{n-1}] = R$ is generated by the quadratic forms $x_i(x_j - x_k)$ for $i, j, k \in \{1, 2, \ldots, n-1\}$ distinct. If $n = 3$ then I is generated by $x_1 x_2 (x_1 - x_2)$.*

Proof. The case $n = 3$ is obvious. The case $n \geqslant 4$ is [17, Lemma 146]. The proof is a simple computation, since by Theorem 2.6 we already know that I is generated by quadratic forms. $\square$

For the rest of this section we assume that $n \geqslant 5$, since the somewhat degenerate cases $n = 3, 4$ are easy to handle by a direct computation.

We fix a minimal graded free resolution $(F_\bullet, \phi)$ of I. The idea is to describe $F_\bullet$ by splicing together Koszul complexes. For each pair $J = (j,k)$, with $j,k \in \{1,2,\dots,n-1\}$ distinct, consider the ideal $I^J \subset I$ generated by the set of quadratic forms

$$\{x_i(x_j - x_k) : i = 1,2,\dots,\widehat{j},\dots,\widehat{k},\dots,n-1\}.$$

As a graded $K[x_1,\dots,x_{n-1}]$-module, I^J is isomorphic to the ideal generated by the linear forms $x_1,\dots,\widehat{x}_j,\dots,\widehat{x}_k,\dots,x_{n-1}$, and so is resolved by a Koszul complex. We write this complex as

$$K_\bullet^J: \quad 0 \longrightarrow \wedge^{n-3}E^J \xrightarrow{d_{n-3}} \wedge^{n-4}E^J \longrightarrow \dots \longrightarrow \wedge^2 E^J \xrightarrow{d_2} E^J \xrightarrow{d_1} R.$$

where E^J is a free R-module of rank $n-3$ with basis $e_1,\dots,\widehat{e}_j,\dots,\widehat{e}_k,\dots,e_{n-1}$, and the differentials d_m are given for $m > 1$ by

$$d_m(e_{i_1} \wedge \dots \wedge e_{i_m}) = \sum_{\ell=1}^{m} (-1)^\ell x_{i_\ell} \cdot (e_{i_1} \wedge \dots \wedge \widehat{e}_{i_\ell} \wedge \dots \wedge e_{i_m}) \tag{11}$$

and for $m = 1$ by $d_1(e_i) = x_i(x_j - x_k)$.

The inclusion $I^J \subset I$ induces a map of chain complexes $K_\bullet^J \to F_\bullet$, i.e. a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[r] & \wedge^{n-3}E^J \arrow[r] \arrow[d] & \dots \arrow[r] & \wedge^2 E_J \arrow[r, "d_2"] \arrow[d] & E^J \arrow[r, "d_1"] \arrow[d] & R \arrow[d, equal] \\
0 \arrow[r] & F_{n-2} \arrow[r, "\phi_{n-2}"] & F_{n-3} \arrow[r] & \dots \arrow[r] & F_2 \arrow[r, "\phi_2"] & F_1 \arrow[r, "\phi_1"] & R
\end{tikzcd}$$

With notation as in Section 2, we may equally write this as

$$\begin{tikzcd}
 & 0 \arrow[r] & R(-n+2) \arrow[r] \arrow[d] & \dots \arrow[r] & R(-3)^{a_2} \arrow[r, "d_2"] \arrow[d] & R(-2)^{a_1} \arrow[r, "d_1"] \arrow[d] & R \arrow[d, equal] \\
0 \arrow[r] & R(-n) \arrow[r, "\phi_{n-2}"] & R(-n+2)^{b_{n-3}} \arrow[r] & \dots \arrow[r] & R(-3)^{b_2} \arrow[r, "\phi_2"] & R(-2)^{b_1} \arrow[r, "\phi_1"] & R
\end{tikzcd}$$

where $a_i = \binom{n-3}{i}$ and the b_i are specified in Theorem 2.6. In particular, all the differentials d_i and ϕ_i are represented by matrices of linear forms, except for d_1, ϕ_1 and ϕ_{n-2} which are represented by matrices of quadratic forms. The map of chain complexes $K_\bullet^J \to F_\bullet$, which by construction is unique up to chain homotopy, is actually uniquely determined. This is because any such chain homotopy respects the grading of the modules in the resolutions, and hence must be zero.

We denote the image of $e_{i_1} \wedge \ldots \wedge e_{i_m}$ in F_m by the symbol $(i_1 \wedge \ldots \wedge i_m) \otimes (j,k)$. It follows from equation (11) that for $2 \leqslant m \leqslant n-3$ we have

$$\begin{aligned} &\phi_m((i_1 \wedge \ldots \wedge i_m) \otimes (j,k)) \\ &\qquad = \sum_{\ell=1}^{m} (-1)^\ell x_{i_\ell} \cdot (i_1 \wedge \ldots \wedge \widehat{i_\ell} \wedge \ldots \wedge i_m) \otimes (j,k). \end{aligned} \tag{12}$$

Lemma 9.2. i) *For any $i_1, \ldots, i_m, j, k \in \{1, 2, \ldots, n-1\}$ distinct we have*

$$(i_1 \wedge \cdots \wedge i_m) \otimes (j,k) + (i_1 \wedge \cdots \wedge i_m) \otimes (k,j) = 0.$$

ii) *For any $i_1, \ldots, i_m, j, k, \ell \in \{1, 2, \ldots, n-1\}$ distinct we have*

$$(i_1 \wedge \cdots \wedge i_m) \otimes (j,k) + (i_1 \wedge \cdots \wedge i_m) \otimes (k,\ell) + (i_1 \wedge \cdots \wedge i_m) \otimes (\ell,j) = 0.$$

iii) *The individual expressions $(i_1 \wedge \cdots \wedge i_m) \otimes (j,k)$ are non-zero.*

Proof. (i) and (ii). The left hand side of each equation has degree $m+1$ in $F_m \cong R(-m-1)^{b_m}$. Since ϕ_m in injective in this degree, it suffices to check the image under ϕ_m is zero. The proof is now by induction on m. If $m = 1$ then

$$\begin{aligned} &\phi_1(i \otimes (j,k) + i \otimes (k,j)) = x_i(x_j - x_k) + x_i(x_k - x_j) = 0, \\ &\phi_1(i \otimes (j,k) + i \otimes (k,\ell) + i \otimes (\ell,j)) \\ &\qquad = x_i(x_j - x_k) + x_i(x_k - x_\ell) + x_i(x_\ell - x_j) = 0. \end{aligned}$$

If $m > 1$ then we instead use (12) to give a linear combination of $x_1, \ldots, x_{n-1}$ where each coefficient vanishes by the induction hypothesis.
(iii) This is proved by a similar, but easier, induction. $\square$

We now give a formula for the differential $\phi_{n-2} : F_{n-2} \to F_{n-3}$.

Lemma 9.3. *The image of ϕ_{n-2} is generated as an R-module by*

$$t := \sum_{j<k} x_j x_k \cdot (i_1 \wedge \ldots \wedge i_{n-3}) \otimes (j,k), \tag{13}$$

where for each $j < k$ we pick $i_1, \ldots, i_{n-3}, j, k$ an even permutation of $1, 2, \ldots, n-1$.

Proof. We first note that t has degree n in $F_{n-3} \cong R(-n+2)^{b_{n-3}}$ and is non-zero by Lemma 9.2(iii). Since $F_{n-2} \cong R(-n)$ and $F_\bullet$ is exact, it suffices to show that t belongs to the kernel of ϕ_{n-3}. We find using (12) that the coefficient of $x_1x_2x_3$ in $\phi_{n-3}(t)$ is

$$\begin{aligned} &-(4\wedge\ldots\wedge(n-1))\otimes(1,2)\\ &\qquad -(4\wedge\ldots\wedge(n-1))\otimes(2,3)-(4\wedge\ldots\wedge(n-1))\otimes(3,1), \end{aligned}$$

which vanishes by Lemma 9.2(ii). The same argument applies to the other coefficients. $\square$

We now prove Lemma 8.1. The symbol $[\ldots]$ was defined in terms of the partial derivatives of $\phi_1, \ldots, \phi_{n-2}$, so we start by computing these. As $\phi_1(i \otimes (j,k)) = x_i(x_j - x_k)$, we see that

$$\begin{aligned} \frac{\partial \phi_1}{\partial x_i}(i\otimes(j,k)) &= x_j - x_k,\\ \frac{\partial \phi_1}{\partial x_j}(i\otimes(j,k)) &= x_i,\\ \frac{\partial \phi_1}{\partial x_k}(i\otimes(j,k)) &= -x_i. \end{aligned} \tag{14}$$

It is immediate from (12) that for $2 \leqslant m \leqslant n-3$ we have

$$\begin{aligned} &\frac{\partial \phi_m}{\partial x_i}((i_1\wedge\ldots\wedge i_m)\otimes(j,k))\\ &\quad = \begin{cases} (-1)^\ell (i_1\wedge\ldots\wedge\widehat{i_\ell}\wedge\ldots\wedge i_m)\otimes(j,k) & \text{if } i = i_\ell,\\ 0 & \text{if } i \notin \{i_1,\ldots,i_m\}. \end{cases} \end{aligned} \tag{15}$$

Since the statement of Lemma 8.1 allows for an overall scalar $\lambda \in K$, we may re-scale ϕ_{n-2} so that $\phi_{n-2}(1) = t$ where t is given by (13). Then by Lemma 9.2(i) we have

$$\frac{\partial \phi_{n-2}}{\partial x_k}(1) = \sum_{\substack{j=1\\ j\neq k}}^{n-1} x_j \cdot (i_1\wedge\ldots\wedge i_{n-3})\otimes(j,k) \tag{16}$$

where for each j we pick $i_1, \ldots, i_{n-3}, j, k$ an even permutation of $1, 2, \ldots, n-1$.

Now let $a_1, \ldots, a_{n-2}, b$ be a permutation of $1, 2, \ldots, n-1$. We seek to compute

$$[a_1, a_2, \ldots, a_{n-2}] = \left(\frac{\partial \phi_1}{\partial x_{a_1}} \circ \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \circ \frac{\partial \phi_{n-2}}{\partial x_{a_{n-2}}} \right)(1).$$

By (16) this equals

$$\left(\frac{\partial \phi_1}{\partial x_{a_1}} \circ \frac{\partial \phi_2}{\partial x_{a_2}} \circ \cdots \circ \frac{\partial \phi_{n-3}}{\partial x_{a_{n-3}}} \right) \left(\sum_{\substack{j=1 \\ j \neq a_{n-2}}}^{n-1} x_j \cdot (i_1 \wedge \ldots \wedge i_{n-3}) \otimes (j, a_{n-2}) \right).$$

where for each j we pick $i_1, \ldots, i_{n-3}, j, a_{n-2}$ an even permutation of $1, 2, \ldots, n-1$. It is clear by (15) that for a non-zero contribution we need $\{a_2, \ldots, a_{n-3}\} \subset \{i_1, \ldots, i_{n-3}\}$, equivalently $\{a_1, a_{n-2}, b\} \supset \{j, a_{n-2}\}$. So the only terms to contribute to the sum are those with $j = a_1$ and $j = b$. Using (14) and (15) we compute

$$\begin{aligned} [a_1, a_2, \ldots, a_{n-2}] &= \pm \frac{\partial \phi_1}{\partial x_{a_1}} \Big(x_b \cdot a_1 \otimes (b, a_{n-2}) - x_{a_1} \cdot b \otimes (a_1, a_{n-2}) \Big) \\ &= \pm x_b (x_b - x_{a_1} - x_{a_{n-2}}). \end{aligned}$$

Finally, it may be checked that the sign $\pm$ only depends on n and the sign of the permutation sending $1, 2, \ldots, n-1$ to $a_1, a_2, \ldots, a_{n-2}, b$.

This completes the proof of Lemma 8.1, and hence of Theorem 2.8.

10. Proof of Theorem 3.1

In this section we prove Theorem 3.1 for general $n \geqslant 4$. This extends the proof for $n = 4$ in Section 3, and is based on the proof for n odd in [16, Section 3.8].

We write $1, \ldots, \widehat{ijk}, \ldots, n-1$ for the sequence of integers $1, 2, \ldots, n-1$, with i, j, k deleted (in whatever order they occur). Let ε_{ij} and ε_{ijk} be the signs of the permutations taking $1, 2, \ldots, n-1$ to $i, j, 1, \ldots, \widehat{ij}, \ldots, n-1$ and $i, j, k, 1, \ldots, \widehat{ijk}, \ldots n-1$, respectively.

With notation as in Sections 2 and 3, we prove the following theorem. It is a refinement of Theorem 3.1, in that we now specify the signs.

Theorem 10.1. *Let $1 \leqslant i, j, k \leqslant n-1$ distinct. Then*

$$\frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} = (-1)^{n+1} \varepsilon_{ijk} (2n)\{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, j\}, \tag{17}$$

$$\frac{\partial^2 \Omega_j}{\partial x_i^2} = \varepsilon_{ij} (2n)\{i, i, 1, \ldots, \widehat{ij}, \ldots, n-1, i\}, \tag{18}$$

$$\frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_k}{\partial x_i \partial x_k} = (-1)^n \varepsilon_{ijk} (2n)\{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, k\}, \tag{19}$$

$$\begin{aligned} &\frac{\partial^2 \Omega_i}{\partial x_i^2} - \frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_k}{\partial x_i \partial x_k} \\ &\qquad = (-1)^{n+1} \varepsilon_{ijk} (2n)\{i, j, 1, \ldots, \widehat{ijk}, \ldots, n-1, k, i\}. \end{aligned} \tag{20}$$

For the proof we need some properties of the symbols $\{\cdots\}$. First, it is immediate from the definition that the symbol does not depend on the order of the first two terms, or on the order of the last two terms. We have the following additional symmetry properties.

Lemma 10.2. i) *For any $\tau \in S_{n-4}$ we have*

$$\{i, j, a_{\tau(1)}, \ldots, a_{\tau(n-4)}, k, \ell\} = \operatorname{sign}(\tau)\{i, j, a_1, \ldots, a_{n-4}, k, \ell\}.$$

ii) *If $i \in \{a_1, \ldots, a_{n-3}\}$ then for any $\tau \in S_{n-3}$ we have*

$$\{i, a_{\tau(1)}, \ldots, a_{\tau(n-3)}, k, \ell\} = \operatorname{sign}(\tau)\{i, a_1, \ldots, a_{n-3}, k, \ell\}.$$

iii) *We have $\{i, j, a_1, \ldots, a_{n-4}, k, \ell\} = -\{k, \ell, a_1, \ldots, a_{n-4}, i, j\}$.*

Proof. (i) In the case where τ is a transposition of consecutive elements this is proved exactly as in Lemma 6.1. The general case follows.
(ii) Differentiating $\phi_1 \phi_2 = 0$ gives $\{i, i, j, \ldots\} + \{i, j, i, \ldots\} = 0$. We are done by (i).
(iii) Exactly as in Lemma 6.3, we have

$$\{i, j, a_1, \ldots, a_{n-4}, k, \ell\} = \pm\{k, \ell, a_{n-4}, \ldots, a_1, i, j\}$$

where the sign is + if and only if $n \equiv 2, 3 \pmod 4$. We are done by (i). $\square$

Lemma 10.3. *If $1 \leqslant i, j, k \leqslant n-1$ distinct then*

$$\{i, j, k, a_1, \ldots, a_{n-3}\} + \{j, k, i, a_1, \ldots, a_{n-3}\} + \{k, i, j, a_1, \ldots, a_{n-3}\} = 0.$$

Proof. This is proved by differentiating $\phi_1\phi_2 = 0$. □

We also have the analogues of Lemmas 10.2(ii) and 10.3 where each symbol is reversed. We write 1_A for the indicator function of the event A.

We prove (17) by taking $a_1, \ldots, a_{n-2} = 1, \ldots, \widehat{k}, \ldots, n-1$ in the following lemma.

Lemma 10.4. *Let $1 \leqslant i, j, k \leqslant n-1$ distinct. Let $a_1, \ldots, a_{n-2}, k$ be a permutation of $1, 2, \ldots, n-1$. Then*

$$\begin{aligned} \frac{\partial^2 [a_1, \ldots, a_{n-2}]}{\partial x_i \partial x_j} \\ = \pm \left(2 + 1_{i \in \{a_1, a_{n-2}\}} + 1_{j \in \{a_1, a_{n-2}\}}\right) \{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, j\} \end{aligned} \tag{21}$$

and

$$\frac{\partial^2 [[a_1, \ldots, a_{n-2}]]}{\partial x_i \partial x_j} = \pm 2n \{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, j\}, \tag{22}$$

where $\pm$ is the sign of the permutation taking $a_1, \ldots, a_{n-2}$ to $i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j$.

Proof. We first prove (21) when $\{a_1, a_{n-2}\} \cap \{i, j\} = \emptyset$. Using Lemma 10.2 we compute

$$\begin{aligned} \frac{\partial^2 [a_1, \ldots, a_{n-2}]}{\partial x_i \partial x_j} &= \{i, a_1, \ldots, a_{n-2}, j\} + \{j, a_1, \ldots, a_{n-2}, i\} \\ &= \pm \Big(\{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, j\} - \{j, j, 1, \ldots, \widehat{ijk}, \ldots, n-1, i, i\} \Big) \\ &= \pm 2 \{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, j\}. \end{aligned}$$

If $a_1 = i$ and $a_{n-2} \neq j$ then the first term picks up a factor of 2, and the second term is unchanged. If $a_1 = i$ and $a_{n-2} = j$ then the first term picks up a factor of 4 and the second term vanishes by Lemma 10.2(iii). The other cases are similar.

We deduce (22) from (21) by summing over the $n-2$ terms in Definition 2.7(ii). Since σ^2 is an even permutation, all the terms have the same sign. There are two terms starting or ending in i, and two terms starting or ending in j. This gives an overall numerical factor of $2(n-2) + 2 + 2 = 2n$. □

We prove (18) by taking $a_1, \ldots, a_{n-2} = 1, \ldots, \widehat{j}, \ldots, n-1$ in the following lemma.

Lemma 10.5. *Let $1 \leqslant i, j \leqslant n-1$ distinct. Let $a_1, \ldots, a_{n-2}, j$ be a permutation of $1, 2, \ldots, n-1$. Then*

$$\frac{\partial^2 [a_1, \ldots, a_{n-2}]}{\partial x_i^2} = \pm 2 \left(1 + 1_{i \in \{a_1, a_{n-2}\}}\right) \{i, i, 1, \ldots, \widehat{ij}, \ldots, n-1, i\}$$

and

$$\frac{\partial^2 [[a_1, \ldots, a_{n-2}]]}{\partial x_i^2} = \pm 2n \{i, i, 1, \ldots, \widehat{ij}, \ldots, n-1, i\},$$

where $\pm$ is the sign of the permutation taking $a_1, \ldots, a_{n-2}$ to $i, 1, \ldots, \widehat{ij}, \ldots, n-1$.

Proof. If $i \notin \{a_1, a_{n-2}\}$ then

$$\frac{\partial^2 [a_1, \ldots, a_{n-2}]}{\partial x_i^2} = 2\{i, a_1, \ldots, a_{n-2}, i\} = \pm \{i, i, 1, \ldots, \widehat{ij}, \ldots, n-1, i\}.$$

If $i \in \{a_1, a_{n-2}\}$ then we pick up an extra factor of 2. This proves the result for $[\cdots]$. We deduce the result for $[[\cdots]]$ exactly as before. $\square$

We prove (19) by taking $r = 0$ and $b_1, \ldots, b_s = 1, \ldots, \widehat{jk}, \ldots, n-1$ in the following lemma, and also using Lemma 6.5.

Lemma 10.6. *Let $1 \leqslant i, j, k \leqslant n-1$ distinct. Let $a_1, \ldots, a_r, b_1, \ldots, b_s, j, k$ be a permutation of $1, 2, \ldots, n-1$. Then*

$$\begin{aligned} &\frac{\partial^2 [a_1, \ldots, a_r, k, b_1, \ldots, b_s]}{\partial x_i \partial x_j} + \frac{\partial^2 [a_1, \ldots, a_r, j, b_1, \ldots, b_s]}{\partial x_i \partial x_k} \\ &\qquad = \pm (-1)^s \left(2 + 1_{i \in \{a_1, b_s\}} + 1_{rs=0}\right) \{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, k\}, \end{aligned}$$

and

$$\begin{aligned} &\frac{\partial^2 [[a_1, \ldots, a_r, k, b_1, \ldots, b_s]]}{\partial x_i \partial x_j} + \frac{\partial^2 [[a_1, \ldots, a_r, j, b_1, \ldots, b_s]]}{\partial x_i \partial x_k} \\ &\qquad = \pm (-1)^s (2n) \{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, k\}, \end{aligned}$$

where $\pm$ is the sign of the permutation taking $a_1, \ldots, a_r, b_1, \ldots, b_s$ to $i, 1, \ldots, \widehat{ijk}, \ldots, n-1$.

Proof. We first suppose that $r, s \geqslant 1$. Using Lemmas 10.2 and 10.3, we compute

$$\begin{aligned}
&\{i, a_1, \ldots, a_r, k, b_1, \ldots, b_s, j\} + \{i, a_1, \ldots, a_r, j, b_1, \ldots, b_s, k\} \\
&\quad = (-1)^{s-1}\big(\{i, a_1, \ldots, a_r, b_1, \ldots, b_{s-1}, k, b_s, j\} \\
&\qquad + \{i, a_1, \ldots, a_r, b_1, \ldots, b_{s-1}, j, b_s, k\}\big) \\
&\quad = (-1)^s\{i, a_1, \ldots, a_r, b_1, \ldots, b_s, j, k\} \\
&\quad = \pm(-1)^s\{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, k\},
\end{aligned}$$

and

$$\begin{aligned}
&\{j, a_1, \ldots, a_r, k, b_1, \ldots, b_s, i\} + \{k, a_1, \ldots, a_r, j, b_1, \ldots, b_s, i\} \\
&\quad = (-1)^{r-1}\big(\{j, a_1, k, a_2, \ldots, a_r, b_1, \ldots, b_s, i\} \\
&\qquad + \{k, a_1, j, a_2, \ldots, a_r, b_1, \ldots, b_s, i\}\big) \\
&\quad = (-1)^r\{j, k, a_1, \ldots, a_r, b_1, \ldots, b_s, i\} \\
&\quad = \pm(-1)^{s-1}\{j, k, 1, \ldots, \widehat{ijk}, \ldots, n-1, i, i\} \\
&\quad = \pm(-1)^s\{i, i, 1, \ldots, \widehat{ijk}, \ldots, n-1, j, k\}.
\end{aligned}$$

If $i \notin \{a_1, b_s\}$ then we simply add these two expressions, giving a factor of 2. If $i \in \{a_1, b_s\}$ then we take twice one expression plus the other, giving a factor of 3.

We next suppose that $s = 0$. The first calculation in the last paragraph is modified by deleting the second line, and introducing a factor of 2 thereafter. If $a_1 \neq i$ then this gives an overall factor of 3. If $a_1 = i$ then we must take twice the first expression, but the second expression vanishes by Lemma 10.2(iii). This gives an overall factor of 4. The case $r = 0$ is similar.

We deduce the result for $[[\cdots]]$ from that for $[\cdots]$ as before. $\square$

The following lemma prepares for the proof of (20).

Lemma 10.7. *Let $1 \leqslant i, j \leqslant n-1$ distinct. Let $a_1, \ldots, a_{n-3}$ be a permutation of $1, 2, \ldots, \widehat{ij}, \ldots, n-1$ with sign ν. Then*

$$A(i,j) := \nu\left(\{i, j, a_1, \ldots, a_{n-3}, i\} + \{i, i, a_1, \ldots, a_{n-3}, j\}\right) \tag{23}$$

does not depend on the choice of $a_1, \ldots, a_{n-3}$.

Proof. If $\cdots$ denotes the same in each case, then by Lemma 10.3 we have

$$\{ij\cdots rsi\} + \{ij\cdots sri\} + \{ij\cdots irs\} = 0,$$
$$\{ii\cdots rsj\} + \{ii\cdots srj\} + \{ii\cdots jrs\} = 0.$$

Lemma 10.2(ii) shows that the final terms in these two sums differ by a sign. The right hand side of (23) is therefore invariant under switching the last two a's. The lemma now follows by Lemma 10.2(i). $\square$

Lemma 10.8. *Let* $1 \leqslant i, j \leqslant n-1$ *distinct. Let* $a_1, \ldots, a_r, b_1, \ldots, b_s, i, j$ *be a permutation of* $1, 2, \ldots, n-1$*. Then*

$$\frac{\partial^2[a_1, \ldots, a_r, j, b_1, \ldots, b_s]}{\partial x_i^2} + 2\frac{\partial^2[a_1, \ldots, a_r, i, b_1, \ldots, b_s]}{\partial x_i \partial x_j} = \pm(-1)^r 2\left(1 + 1_{rs=0}\right) A(i,j)$$

and

$$\frac{\partial^2[[a_1, \ldots, a_r, j, b_1, \ldots, b_s]]}{\partial x_i^2} + 2\frac{\partial^2[[a_1, \ldots, a_r, i, b_1, \ldots, b_s]]}{\partial x_i \partial x_j} = \pm(-1)^r (2n) A(i,j),$$

where $\pm$ *is the sign of the permutation taking* $a_1, \ldots, a_r, b_1, \ldots, b_s$ *to* $1, \ldots, \widehat{ij}, \ldots, n-1$.

Proof. If $r = 0$ then the left hand side equals

$$\begin{aligned} 2\{i, j, b_1, \ldots, b_s, i\} + 4\{i, i, b_1, \ldots, b_s, j\} + 2\{j, i, b_1, \ldots, b_s, i\} \\ = \pm 4A(i,j). \end{aligned} \tag{24}$$

If $r, s \geqslant 1$ then we instead obtain

$$2\{i, a_1, \ldots, a_r, j, b_1, \ldots, b_s, i\} + 2\{i, a_1, \ldots, a_r, i, b_1, \ldots, b_s, j\} + 2\{j, a_1, \ldots, a_r, i, b_1, \ldots, b_s, i\}.$$

Cancelling a factor $(-1)^r 2$ and applying Lemma 10.2 term by term gives

$$-\{i, a_1, j, \ldots, a_r, b_1, \ldots, b_s, i\} + \{i, i, a_1, \ldots, a_r, b_1, \ldots, b_s, j\} - \{j, a_1, i, \ldots, a_r, b_1, \ldots, b_s, i\}.$$

Applying Lemma 10.3 to the first and third terms shows that this equals $\pm A(i,j)$.

Finally, when $s = 0$ the left hand side is

$$2\{i, a_1, \dots, a_r, j, i\} + 2\{i, a_1, \dots, a_r, i, j\} + 4\{j, a_1, \dots, a_r, i, i\}.$$

By Lemma 10.2(iii) this is minus the expression we get by replacing $b_1, \dots, b_s$ by $a_2, \dots, a_r, a_1$ in (24). This gives the factor $(-1)^r$.

We deduce the result for $[[\cdots]]$ from that for $[\cdots]$ as before. $\square$

Taking $r = 0$ and $b_1, \dots, b_s = 1, \dots, \widehat{ij}, \dots, n-1$ in Lemma 10.8, and appealing to Lemma 6.5, gives

$$\frac{\partial^2 \Omega_i}{\partial x_i^2} - 2\frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} = -\varepsilon_{ij}(2n)A(i,j).$$

Taking $a_1, \dots, a_{n-3} = 1, \dots, \widehat{ijk}, \dots, n-1, k$ in Lemma 10.7 shows that this equals

$$(-1)^{n+1}\varepsilon_{ijk}(2n)\Big(\{i, j, 1, \dots, \widehat{ijk}, \dots, n-1, k, i\} \\ + \{i, i, 1, \dots, \widehat{ijk}, \dots, n-1, j, k\}\Big).$$

Adding (19) gives (20). This completes the proof of Theorem 10.1, and hence of Theorem 3.1.

Acknowledgements

This article is based on part of the second author's PhD thesis. We thank Manjul Bhargava and Melanie Wood for useful conversations, and Jack Thorne for alerting us to an oversight in an earlier version of Section 4.

References

[1] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Annals of Mathematics **159** (2004) 1329–1360.

[2] ———, *The density of discriminants of quartic rings and fields*, Annals of Mathematics **162** (2005) 1031–1063.

[3] ———, *Higher composition laws IV: The parametrization of quintic rings*, Annals of Mathematics **167** (2008) 53–94.

[4] ———, *The density of discriminants of quintic rings and fields*, Annals of Mathematics **172** (2010) 1559–1591.

[5] W. Bruns and H. J. Herzog, Cohen-Macaulay rings, Cambridge University Press (1998).

[6] D. A. Buchsbaum and D. Eisenbud, *Gorenstein ideals of height 3*, in Seminar D. Eisenbud/B. Singh/W. Vogel, Vol. 2, 30–48 (1982).

[7] G. Casnati and R. Notari, *On some Gorenstein loci in* $Hilb_6(P_k^4)$, J. Algebra **308** (2007), no. 2, 493–523.

[8] H. Davenport and H. A. Heilbronn, *On the density of discriminants of cubic fields. II*, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences **322** (1971), no. 1551, 405–420.

[9] B. N. Delone and D. K. Faddeev, The theory of irrationalities of the third degree, Vol. 10, American Mathematical Society (1964).

[10] D. Eisenbud, The geometry of syzygies: a second course in algebraic geometry and commutative algebra, Vol. 229, Springer (2005).

[11] ———, Commutative Algebra: with a view toward algebraic geometry, Vol. 150, Springer (2013).

[12] T. Fisher, *A formula for the Jacobian of a genus one curve of arbitrary degree*, Algebra & Number Theory **12** (2018) 2123–2150.

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

[14] S. H. Lee, Parametrizing rings of rank 6, Ph.D. thesis, Princeton University (2022).

[15] F. Levi, *Kubische Zahlkörper und binäre kubische Formenklassen*, Ber. Sächs. Akad. Wiss. Leipzig, Math.-Naturwiss **66** (1914) 26–37.

[16] L. Radicevic, Capitulation discriminants of genus one curves, Ph.D. thesis, University of Cambridge (2021).

[17] K. H. Wilson, Three perspectives on n points in $\mathbb{P}^{n-2}$, Ph.D. thesis, Princeton University (2013).

[18] M. M. Wood, Moduli spaces for rings and ideals, Ph.D. thesis, Princeton University (2009).

DPMMS, University of Cambridge
Centre for Mathematical Sciences
Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: T.A.Fisher@dpmms.cam.ac.uk
E-mail address: lazaradicevic@gmail.com

Received October 1, 2021
Accepted December 17, 2022