COMPOSITIO MATHEMATICA

Galois theory for general systems of polynomial equations

A. Esterov

Compositio Math. **155** (2019), 229–245.

doi:10.1112/S0010437X18007868

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

Compositio Math. 155 (2019) 229–245
doi:10.1112/S0010437X18007868

Galois theory for general systems of polynomial equations

A. Esterov

To R. K. Gordin on the occasion of his 70th birthday

Abstract

We prove that the monodromy group of a reduced irreducible square system of general polynomial equations equals the symmetric group. This is a natural first step towards the Galois theory of general systems of polynomial equations, because arbitrary systems split into reduced irreducible ones upon monomial changes of variables. In particular, our result proves the multivariate version of the Abel–Ruffini theorem: the classification of general systems of equations solvable by radicals reduces to the classification of lattice polytopes of mixed volume 4 (which we prove to be finite in every dimension). We also notice that the monodromy of every general system of equations is either symmetric or imprimitive. The proof is based on a new result of independent importance regarding dual defectiveness of systems of equations: the discriminant of a reduced irreducible square system of general polynomial equations is a hypersurface unless the system is linear up to a monomial change of variables.

1. Introduction

Galois theory for lattice polytopes

A problem of enumerative geometry asks how many geometric objects satisfy a generic geometric constraint in a given space of constraints P. Galois theory for this enumerative problem studies how the solutions of this problem permute as the constraint runs along loops in P. In the last decade, particularly strong results were obtained in Galois theory of Schubert calculus; see [SW15] and references therein.

We develop Galois theory in the same vein for another well-known enumerative problem, the Kouchnirenko–Bernstein theorem, counting the solutions of a system of generic polynomial equations composed of a given finite collection of monomials. More accurately, let us identify points $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$ with monomials $x^a = x_1^{a_1} \dots x_n^{a_n}$; then every finite set of monomials $A \subset \mathbb{Z}^n$ gives rise to the space of Laurent polynomials $\mathbb{C}^A = \{\sum_{a\in A} c_a x^a,\ c_a \in \mathbb{C}\}$, *supported at* A. These polynomials are defined as functions on the complex torus $(\mathbb{C}\backslash 0)^n$.

Theorem 1.1 (Kouchnirenko–Bernstein [Ber75]). *For every collection of finite sets* $A = (A_1, \dots, A_n)$ *in* $\mathbb{Z}^n$, *there exists a proper exceptional algebraic set* $B_A \subset \mathbb{C}^A = \mathbb{C}^{A_1} \oplus \dots \oplus \mathbb{C}^{A_n}$, *such that the number of common roots* $x \in (\mathbb{C}\backslash 0)^n$ *of a system of polynomial equations* $f_1(x) = \dots = f_n(x) = 0$ *for every tuple of polynomials* $(f_1, \dots, f_n) \in \mathbb{C}^A$ *outside* B_A *equals the lattice mixed volume of (the convex hulls of)* $A_1, \dots, A_n$.

Received 17 April 2018, accepted in final form 14 September 2018, published online 7 January 2019.
2010 Mathematics Subject Classification 14H05, 14H30, 20B15, 52B20, 58K10.
Keywords: topological Galois theory, monodromy, discriminant, Newton polytope, dual defect, mixed volume.
Research supported by the Russian Science Foundation grant, project 16-11-10316.

In the setting of the Kouchnirenko–Bernstein theorem, denote the mixed volume by V. Then every loop in $\mathbb{C}^A\backslash B_A$, pointed at some tuple $f=(f_1,\dots,f_n)$, defines a permutation of the roots of $f=0$. For all loops in $\mathbb{C}^A\backslash B_A$, these permutations form a subgroup of the group S_V of all permutations of the V roots of $f=0$. This subgroup will be called *the monodromy group of the general system of polynomial equations supported at* A and denoted by G_A.

We shall be interested in the following two problems:

(I) Compute G_A.

(II) Classify *solvable tuples* A, for which the multivalued function $\mathbb{C}^A\backslash B_A\to(\mathbb{C}\backslash 0)^n$, assigning the roots of the system $f=0$ to an element $f\in\mathbb{C}^A\backslash B_A$, can be expressed by radicals.

The first problem helps to solve the second one, because a solvable tuple A has a solvable monodromy group G_A (see, for example, [Kho15]).

Example 1.2. For $n=1$ and $A=A_1=\{0,1,\dots,d\}$, the problems above ask (I) for the monodromy of the generic univariate polynomial $c_dx^d+c_{d-1}x^{d-1}+\dots+c_0$ and (II) for the expression of its roots by radicals in terms of the coefficients $c_0,c_1,\dots,c_d$. It is classically known that the monodromy G_A equals S_d, and thus the general equation of degree d is solvable for $d\leqslant 4$.

For arbitrary n, the second problem, though not the first one, can be reduced without loss of generality to *reduced irreducible* tuples $A=(A_1,\dots,A_n)$ in the sense of the following Definition 1.3. Thus, the subsequent Theorem 1.5 leads to a complete solution of problem (II), and seems to be a natural first step towards the solution of problem (I).

Definition 1.3. (1) A tuple of finite sets $A_1,\dots,A_k$ in $\mathbb{Z}^n$ is said to be reduced, if they cannot be shifted to the same proper sublattice of $\mathbb{Z}^n$.

(2) A tuple of finite sets $A_1,\dots,A_k$ in $\mathbb{Z}^n$ is said to be irreducible (respectively, linearly independent), if it is impossible to shift all but m (respectively, $m-1$) of them to the same sublattice of codimension m, for $m>0$.

Remark 1.4. (1) Mind the difference between reduced and reducible (i.e. non-irreducible).

(2) Similar conditions were introduced by various authors for particular values of $n-k$ (cf., for instance, essential tuples in [Stu94] for $k=n+1$). We prefer the terms 'linearly independent', 'reduced' and 'irreducible' (introduced in [Kho78] and [EG16] for $k=n$), because discriminants and other geometric objects, related to the system of equations $f=0$ for the general tuple $f\in\mathbb{C}^A$, tend to be reduced and irreducible in the sense of algebraic geometry if the tuple $A=(A_1,\dots,A_k)$ has the property of the same name. See Remark 3.17 and Theorem 3.21 for some instances of this correspondence.

Theorem 1.5. *If $A=(A_1,\dots,A_n)$ is a reduced irreducible tuple, then the monodromy group G_A equals the symmetric group S_V.*

The proof is given at the end of this section.

Systems of equations, solvable by radicals

Since S_V is not solvable for $V>4$, Theorem 1.5 implies the following corollary.

Corollary 1.6 [EG16, Conjecture 1]. *For a reduced irreducible tuple $(A_1,\dots,A_n)$, the general system of equations supported at $(A_1,\dots,A_n)$ is solvable by radicals if and only if it has at most four solutions, that is, the lattice mixed volume of $A_1,\dots,A_n$ does not exceed 4.*

This fact actually gives the inductive classification of all solvable tuples $A=(A_1,\dots,A_n)$.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Classification 1.7. (0) We can and will assume without loss of generality that every A_i contains 0. Indeed, otherwise shift A_i by a vector $-a_i$, $a_i \in A_i$, to a set $\widetilde{A}_i$ containing 0. Now, instead of polynomials $f_i \in \mathbb{C}^{A_i}$, we can study polynomials $f_i(x)/x^{a_i} \in \mathbb{C}^{\widetilde{A}_i}$, because they have the same roots as f_i.

(1) We can and will assume that A is reduced. Indeed, otherwise A_i is the image of B_i under a lattice embedding $j : \mathbb{Z}^n \to \mathbb{Z}^n$ for a reduced tuple $B = (B_1, \dots, B_n)$, and we have the following fact: *the solvability of B is equivalent to the solvability of A.*

Proof. Consider the surjection of complex tori $h : (\mathbb{C}\backslash 0)^n \to (\mathbb{C}\backslash 0)^n$, corresponding to the embedding j of their character lattices, so that $h(x)^b = x^{j(b)}$ for $x \in (\mathbb{C}\backslash 0)^n$ and $b \in \mathbb{Z}^n$. Then every tuple of polynomials $f \in \mathbb{C}^A$ has the form $f(x) = g(h(x))$, $g \in \mathbb{C}^B$. Since h is invertible by radicals, it follows that $f = 0$ and $g = 0$ are solvable by radicals simultaneously. □

(2) We can and will assume that A is irreducible. Otherwise, up to reordering, the sets $A_1, \dots, A_k$, $0 < k < n$, belong to the same k-dimensional plane $L \subset \mathbb{Z}^n$, and, denoting the tuple of the images of the other A_i under the projection $\mathbb{Z}^n \to \mathbb{Z}^n/L$ by A'', we have the following fact: *the solvability of A is equivalent to the solvability of the smaller-dimensional tuples $A' = (A_1, \dots, A_k)$ and A''.*

Proof. Note that upon an appropriate automorphism of $(\mathbb{C}\backslash 0)^n$, the polynomial $f_i \in \mathbb{C}^{A_i}$ depends only on the first k coordinates for $i \leqslant k$, so, substituting these coordinates with a solution of $f_1 = \dots = f_k = 0$ in the system of equations $f_{k+1} = \dots = f_n = 0$, we obtain a system of the form $g = 0$, $g \in \mathbb{C}^{A''}$. Thus solving a generic system $f = 0$ supported in A amounts to solving a generic system $f_1 = \dots = f_k = 0$ supported in A' and a system $g = 0$, which is also generic in $\mathbb{C}^{A''}$ in the sense that assigning g to f is a dominant map $\mathbb{C}^A \to \mathbb{C}^{A''}$. □

(3) Finally, a reduced and irreducible tuple A is solvable if and only if the lattice mixed volume of $A_1, \dots, A_n$ does not exceed 4 (by Corollary 1.6).

This algorithm reduces the classification of solvable systems of equations to the classification of irreducible mixed volume 4 tuples of lattice sets. The latter classification is given in [EG16] in dimension 2, and is, moreover, finite in every dimension; see Theorem 1.11 below for details.

Remark 1.8. In the same way, the classification of systems of equations solvable by k-radicals in the sense of [Kho15] (i.e. those that can be reduced to solving univariate polynomial equations of degree at most k) is reduced to the classification of tuples of lattice sets of mixed volume at most k.

Example 1.9. For $n = 2$, if a reduced consistent general system of equations is solvable by radicals, then its Newton polygons either have lattice mixed volume at most 4 (there are 14 such maximal pairs up to automorphisms of $\mathbb{Z}^2$; see [EG16]), or equal a segment I of lattice length at most 4 and an arbitrary polygon P, whose support lines parallel to I are at the lattice distance not exceeding 4 from each other.

Classification of small polytopes

Each of the infinitely many pairs (I, P) in the preceding example has mixed volume at most 16, due to the following fact. We denote the lattice mixed volume of the convex hulls of $A_1, \dots, A_n$ by $\mathrm{MV}(A_1, \dots, A_n)$.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Theorem 1.10. *Let $B_1, \dots, B_N$ be lattice sets in $\mathbb{Z}^N$ and $A_1, \dots, A_M$ in $\mathbb{Z}^N \oplus \mathbb{Z}^M$. Then* $\mathrm{MV}(A_1, \dots, A_M, B_1, \dots, B_N) = \mathrm{MV}(pA_1, \dots, pA_M)\,\mathrm{MV}(B_1, \dots, B_N)$, *where $p : \mathbb{Z}^N \oplus \mathbb{Z}^M \to \mathbb{Z}^M$ is the standard projection.*

This well-known fact admits an especially simple proof in the spirit of Classification 1.7(2) ([Est06]; see, for example, [ST10, Lemma 4] for a geometric proof).

An algebraic proof. For $f_i \in \mathbb{C}^{A_i}$ and $g_j \in \mathbb{C}^B_j$, every solution of the system $f = g = 0$ is of the form (x_0, y_0), where $x_0 \in (\mathbb{C}\backslash 0)^N$ is a solution of the system $g = 0$ and $y_0 \in (\mathbb{C}\backslash 0)^M$ is a solution of the system $f(x_0, y) = 0$. For generic f and g, the number of solutions of the three mentioned systems equals the three lattice mixed volumes in the statement by the Kouchnirenko–Bernstein theorem. □

This reduces the infinite classification of tuples with small mixed volume to the classification of irreducible tuples, which is already finite.

Theorem 1.11. *For every n and V, there are finitely many irreducible tuples $(A_1, \dots, A_n)$ in $\mathbb{Z}^n$ of mixed volume V, up to automorphisms of $\mathbb{Z}^n$ and shifts of the sets.*

The proof is given in § 2. Moreover, if we restrict our attention to the *unmixed* case, where $A_1 = \dots = A_n = A$, the classification becomes essentially finite across all dimensions: it was shown in [EG16] that every reduced $A \subset \mathbb{Z}^n$ of lattice volume 4 can be obtained from 34 'elementary' configurations of dimension at most 6 by affine automorphisms of $\mathbb{Z}^n$ and constructing cones over lattice sets in the following sense.

Definition 1.12. The cone over $B \subset \mathbb{Z}^m$ is the set $c(B) = \{0\} \cup (B \times \{k\}) \subset \mathbb{Z}^{m+1}$.

Remark 1.13. (1) The same is true for every value of the volume, as shown in [HKN18, Corollary 3.1] (although, starting from volume 5, the classification of non-cones seems to be incomprehensibly large).

(2) In the notation of the preceding definition, the solution by radicals of the system $f_0 = \dots = f_m = 0$ supported at the cone $c(B)$ can be reduced to the solution by radicals of the system $g_1 = \dots = g_m = 0$ supported at its base B, by setting $g_i(x) = f_i(x)/f_{i,0} - f_0(x)/f_{0,0}$, where $f_{i,0}$ is the constant term of f_i. Thus the solution by radicals of all solvable unmixed systems of arbitrarily many variables reduces to the 34 elementary ones listed in [EG16].

(3) The classification of the 34 non-cones of volume 4 in [EG16] includes only reduced ones (or spanning ones, in terms of [HKN18]), because this suits the needs of Corollary 1.6. The classification of all (possibly non-reduced) non-cones of volume 4 is also possible, but is more complicated and not finite due to empty simplices; see [HT17].

Monodromy of reducible systems of equations

In contrast to the problem of solvability, the computation of the monodromy of an arbitrary tuple cannot easily be reduced to the case of reduced irreducible tuples. We formulate a conjecture regarding non-reduced tuples and show by an example that the case of reducible tuples is yet more complicated (so that we do not even make any predictions).

Conjecture 1.14. In the setting of step (1) of Classification 1.7, if the tuple B is reduced and irreducible of mixed volume d, then the monodromy group G_A equals the wreath product of $\operatorname{coker} j$ and S_d acting on $\{1, \dots, d\}$.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

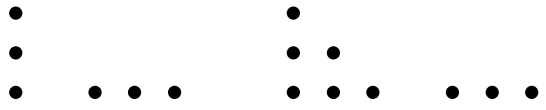

Figure 1. Two reducible tuples.

Remark 1.15. We now explain why G_A obviously embeds into this wreath product, so the problem is whether the embedding is actually an isomorphism. In the notation of part (1) of Classification 1.7, the roots of $f = 0$ split into the fibres of the surjection $h : \{f = 0\} \to \{g = 0\}$. All fibres are cosets of the subgroup $\operatorname{coker} j \subset (\mathbb{C}\backslash 0)^n$, and every monodromy permutation of the set $\{f = 0\}$ 'respects j', that is to say, it sends every fibre into a fibre, preserving its $(\operatorname{coker} j)$-torsor structure. In particular, the group G_A is contained in the group of all permutations respecting j, and the latter is exactly the wreath product sought.

Example 1.16. If the tuple A is as shown on the left in Figure 1, then G_A is obviously equal to $V_4 \subset S_4$, generated by (12)(34) and (13)(24). However, if the tuple A is as shown on the right, then its Cayley discriminant (Definition 3.12) has codimension 1, so a small loop around this discriminant corresponds to a transposition in G_A (see Remark 3.26), thus the group is strictly greater than V_4 (actually, it equals D_8). This is despite, in the notation of step (2) of Classification 1.7, the groups $G_{A'}$ and $G_{A''}$ are the same (equal to S_2) for both examples. Thus G_A is not defined solely by $G_{A'}$ and $G_{A''}$.

Nevertheless, we can confirm in our setting the 'symmetric or imprimitive' dichotomy, conjectured in [SW15] for Schubert enumerative problems, modulo one obvious exclusion.

Example 1.17. Let B and C be tuples of finite sets of lattice mixed volume 1 in $\mathbb{Z}^k$ and $\mathbb{Z}^m$ respectively, $k > 0$, $m \geqslant 0$ (see [EG15] or § 2 below for the classification of such tuples), and let $j : \mathbb{Z}^k \to \mathbb{Z}^k \oplus \mathbb{Z}^m$ send v to $(pv, 0)$ for some odd prime p. Let P' be the tuple $j(B)$ in $\mathbb{Z}^k \oplus \mathbb{Z}^m$, and let P'' be a tuple of m sets in $\mathbb{Z}^k \oplus \mathbb{Z}^m$ whose projections to $\mathbb{Z}^m$ form the tuple C. Then the mixed volume of a tuple $P = (P', P'')$ equals p, and, moreover, by Remark 1.15, the monodromy group G_P is a subgroup of $\mathbb{Z}/p\mathbb{Z}$, that is, equals $\mathbb{Z}/p\mathbb{Z}$ or the trivial group, of which the former is primitive and the latter is not. Actually one can check that G_P always equals $\mathbb{Z}/p\mathbb{Z}$ in accordance with Conjecture 1.14 (which is obvious in the one-dimensional case, that is, for the equation $c_p x^p + c_0 = 0$, corresponding to $P_1 = \{0, p\} \subset \mathbb{Z}^1$, and less obvious in general).

A tuple that can be identified with P by an isomorphism of lattices will be called a prime tuple.

Definition 1.18. A tuple of sets $A = (A_1, \dots, A_n)$ in $\mathbb{Z}^n$ is said to be numerically non-reduced, if there exist sets $B_1, \dots, B_k$ in $\mathbb{Z}^k$ and an embedding $j : \mathbb{Z}^k \to \mathbb{Z}^n$, such that the lattice mixed volume of $B_1, \dots, B_k$ is greater than 1, the embedding is not saturated (i.e. $\mathbb{Z}^n/j(\mathbb{Z}^k)$ is not free), and $j(B_1), \dots, j(B_k)$ coincide with k of the sets $A_1, \dots, A_n$ up to a shift.

The tuple A is said to be numerically reducible, if a quantity $k < n$ of A_i can be shifted to a k-dimensional sublattice L such that the lattice mixed volumes of both $A' =$ (the tuple of A_i shifted to L) and $A'' =$ (the tuple of the images of the rest of the A_i under the projection $\mathbb{Z}^n \to \mathbb{Z}^n/L$) are greater than 1.

The name is chosen because the mixed volume V of the tuple A equals the product of the mixed volumes of A' and A'' by Theorem 1.10.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Theorem 1.19. *For every non-prime tuple A (see Example 1.17), the monodromy group G_A is the symmetric group S_V if the tuple A is numerically reduced and irreducible, and is imprimitive otherwise.*

Proof. If the tuple A of subsets of $\mathbb{Z}^n$ is numerically non-reduced, then, in the notation of Definition 1.18, let $h : (\mathbb{C}\backslash 0)^n \to (\mathbb{C}\backslash 0)^k$ be the surjection of tori, corresponding to the embedding $j : \mathbb{Z}^k \to \mathbb{Z}^n$ of their character lattices so that $h(x)^b = x^{j(b)}$ for all $x \in (\mathbb{C}\backslash 0)^n$ and $b \in \mathbb{Z}^k$. Then every system of equations $f(x) = 0$, $f \in \mathbb{C}^A$ contains a subsystem of the form $g(h(x)) = 0$, $g \in \mathbb{C}^B$. By Remark 1.15, the fibres of the surjection $h : \{f = 0\} \to \{g = 0\}$ are blocks of the monodromy action of G_A. The number and size of the blocks are greater than 1, because the mixed volume of $B_1, \dots, B_k$ is greater than 1, and j is not saturated.

If A is numerically reducible, then, in the notation of Definition 1.18, upon an appropriate automorphism of $(\mathbb{C}\backslash 0)^n$ and reordering the tuple, we may assume that $A_1, \dots, A_k$ are contained in the first k-dimensional coordinate plane $L \subset \mathbb{Z}^n$, $0 < k < n$, and the mixed volumes V' and V'' of both $A' = (A_1, \dots, A_k)$ and $A'' =$ (the images of $A_{k+1}, \dots, A_n$ in $\mathbb{Z}^n/L$) are greater than 1. In this case, every common root of a generic tuple of polynomials $f = (f_1, \dots, f_n) \in \mathbb{C}^A$ is of the form (x', x''), where $x' \in (\mathbb{C}\backslash 0)^k$ is one of the V' roots of the system $f' = (f_1, \dots, f_k)$. In particular, the fibres of the projection $\{f = 0\} \to \{f' = 0\}$ are $V' > 1$ blocks of size $V'' > 1$ for the action of the monodromy group G_A, so this action is imprimitive.

If the tuple A is numerically reduced, numerically irreducible and not prime, then it is reduced. So, if A is irreducible in this case, then G_A is symmetric by Theorem 1.5.

Thus, it remains to consider reducible A that is numerically reduced, numerically irreducible and not prime. In this case, in the notation of part (2) of Classification 1.7, the tuples A' and A'' are also numerically reduced, numerically irreducible and not prime, and the mixed volume of one of them equals 1. Thus G_A equals the monodromy group of the other one, which is symmetric by induction on the dimension. □

Structure of the paper

In § 2 we prove and discuss Theorem 1.11. The rest of the paper is devoted to the proof of Theorem 1.5. In § 3 we reduce the assumption of irreducibility to a more general notion of dual effectiveness (antonym to dual defectiveness; see Definition 3.14 below).

Theorem 1.20. *A reduced irreducible tuple of n sets in $\mathbb{Z}^n$ is dual effective unless, upon an automorphism of the lattice, all of its sets can be shifted to the standard simplex (i.e. the system of equations is essentially linear).*

For the proof, see Corollary 3.23. Besides the relation to Galois theory, this result may be important as an illustration of a new approach to dual defectiveness in the toric setting, independent of the known ones [DiR06, DFS07, CC07, Est18, FI16, For17].

Remark 1.21. (1) In the case of full-dimensional tuples, Theorem 1.20 was deduced from [FI16] in [BN18], settling the conjecture from [CCDDS13]. Our proof is independent of [FI16], and it would be important to extend the technique of [BN18] from full-dimensional tuples to irreducible ones.

(2) It would be important to drop the irreducibility assumption and completely classify dual defective tuples in various senses (see Remark 3.16), as Example 1.16 suggests.

Theorem 1.22. *If A is a reduced dual effective tuple, then the monodromy G_A contains a transposition.*

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Roughly speaking, the transposition is produced by running a small loop around the discriminant; see Theorem 3.25 for the proof and Theorem 3.27 for a possible generalization to non-square systems of equations.

Theorem 1.23. *If A is a reduced irreducible tuple, then the monodromy G_A is doubly transitive.*

The proof is standard and is given in § 4.

Proof of Theorem 1.5. Unless the system of equations generically has one solution (satisfying $G_A = S_1$), Theorem 1.20 ensures that the tuple is dual effective, so the monodromy contains a transposition by Theorem 1.22. Since it is also doubly transitive by Theorem 1.23, it coincides with the symmetric group. □

2. Lattice polytopes of small mixed volume

Theorem 2.1 [LZ91]. *For any n, there are finitely many convex lattice polytopes of a given lattice volume in $\mathbb{Z}^n$ up to affine automorphisms of the lattice.*

Theorem 2.2 (Minkowski [Min11]). *A tuple is linearly dependent if and only if its mixed volume equals* 0.

Proof of Theorem 1.11. Tuples $(B_1, B_1, B_3, \dots, B_N)$ and $(B_2, B_2, B_3, \dots, B_N)$ are said to be AF-descendants of $(B_1, B_2, B_3, \dots, B_N)$, if both of them are linearly independent. If the tuple B' is the AF-descendant of B, then, by the Aleksandrov–Fenchel inequality and Theorem 2.2, we have

$$\operatorname{MV} B' \leqslant (\operatorname{MV} B)^2. \tag{$*$}$$

Every linearly independent tuple B that entirely consists of sets contained in the irreducible tuple A, can be obtained from A by taking a sequence of AF-descendants $A', A'', \dots, A^{(k)} = B$. Applying the inequality ($*$) to this sequence, we conclude that if all sets of the tuple B are contained in the irreducible tuple A, then

$$\operatorname{MV} B \leqslant (\operatorname{MV} A)^{2^N}. \tag{$**$}$$

Note that ($**$) trivially holds also for linearly dependent tuples B by Theorem 2.2.

We can now estimate the lattice volume of the Minkowski sum $A_1 + \dots + A_N$ as follows. Write it as $\operatorname{MV}(A_1 + \dots + A_N, \dots, A_1 + \dots + A_N)$, open the brackets and estimate every term by the inequality ($**$). As a result, for every irreducible tuple $(A_1, \dots, A_N)$ of mixed volume V, the volume of the Minkowski sum $A_1 + \dots + A_N$ is at most $N^N V^{2^N}$, so by Theorem 2.1 there are finitely many possibilities for $A_1 + \dots + A_N$ and hence for $(A_1, \dots, A_N)$. □

Remark 2.3. It would be interesting to obtain a sharper estimate on the volume of $A_1 + \dots + A_N$ in terms of the mixed volume of an irreducible tuple $(A_1, \dots, A_N)$.

The classification of irreducible tuples is known only up to mixed volume 4 in dimension 2 (see [EG16]), and up to mixed volume 1 in arbitrary dimension.

Corollary 2.4 (Minkowski). *The unique irreducible tuple of mixed volume* 0 *is a point in $\mathbb{Z}^1$.*

Theorem 2.5 [EG15]. *The unique (up to automorphisms of the lattice and shifts of polytopes) maximal (by inclusion) irreducible tuple of lattice polytopes of mixed volume* 1 *in $\mathbb{Z}^N$ is the tuple of N copies of the standard simplex.*

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

3. Discriminants and dual defectiveness

Mixed resultants

Let $A = (A_0, \dots, A_n)$ be a tuple of finite sets in $\mathbb{Z}^n$.

Definition 3.1. The A-resultant R_A is the closure of the set of all tuples of polynomials $f = (f_0, \dots, f_n) \in \mathbb{C}^A$ that have a common root $f_0(x) = \dots = f_n(x) = 0$, $x \in (\mathbb{C}\backslash 0)^n$.

Example 3.2. For $n = 1$, the set R_A is the zero locus of the classical Sylvester resultant.

Theorem 3.3 ([Est07, Theorem 2.26]; see also [Stu94] for the first part of the statement). *If A is irreducible, then the resultant R_A is a non-empty irreducible hypersurface, and a generic tuple $f \in R_A$ has a unique common root in $(\mathbb{C}\backslash 0)^n$.*

Gelfand–Kapranov–Zelevinsky discriminants

Let $A \subset \mathbb{Z}^n$ be a finite set.

Definition 3.4 [GKZ94]. The A-discriminant D_A is the closure of the set of all polynomials $f \in \mathbb{C}^A$ that have a singular root $f(x) = 0$, $df(x) = 0$, $x \in (\mathbb{C}\backslash 0)^n$.

Example 3.5. For $n = 1$, the set D_A is the zero locus of the classical discriminant.

Definition 3.6. The tuple A is said to be dual defective if D_A is not a hypersurface, and dual effective otherwise.

This is equivalent to the fact that the projectively dual variety to the toric variety X_A is not a hypersurface (hence the name). The study of dual defective projective varieties is a classical topic in algebraic geometry [Ein86]. In particular, there is an extensive literature on the classification of dual defective lattice sets; see [DiR06, Est18] and [FI16] for some of the most explicit answers (the first one is for the case of smooth toric varieties).

Example 3.7. The set $A = \{(00), (10), (20), (01)\} \subset \mathbb{Z}^2$ is defective.

Theorem 3.8 [GKZ94]. *If a dual effective A cannot be shifted to a proper sublattice of $\mathbb{Z}^n$, then a generic polynomial $f \in D_A$ has a unique singular root $x \in (\mathbb{C}\backslash 0)^n$, and the Hessian of f at this root is non-degenerate.*

If A is dual effective, then the set D_A is the zero locus of a unique irreducible integer polynomial on $\mathbb{C}^A$ (up to the choice of sign). This polynomial is also called the A-discriminant. The coefficients $c_a, a \in A$, of the general Laurent polynomial $\sum_{a\in A} c_a x^a$ in $\mathbb{C}^A$ form the natural system of coordinates in $\mathbb{C}^A$, and we shall consider the A-discriminant as a polynomial of c_a, $a \in A$.

Lemma 3.9 [Est10, Lemma 2.21]. *For every dual effective $A \subset \mathbb{Z}^n$ and every $a \in A$, the A-discriminant has positive degree in c_a.*

Remark 3.10. For every $B \subset A$, there is a natural forgetful projection $\mathbb{C}^A \to \mathbb{C}^B$, sending $\sum_{a\in A} c_a x^a$ to $\sum_{a\in B} c_a x^a$, and we shall denote the preimage of D_B under this map also by D_B.

Corollary 3.11. *If A is dual effective, then $D_A \neq D_B$ for every $B \subsetneq A$.*

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Discriminants of systems of equations

For a tuple $A = (A_1, \dots, A_k)$ of finite sets in $\mathbb{Z}^n$, $2 \leqslant k \leqslant n$, the concept of the discriminant of the system of equations supported at A is ambiguous. We introduce three different versions of this notion that appear in the literature, and it will be important for us that all of them coincide for irreducible tuples. Denote the standard basis in $\mathbb{Z}^k$ by $e_1, \dots, e_k$, and, for every $I \subset \{1, \dots, k\}$, let A_I be the *Cayley configuration* $\bigcup_{i \in I} \{e_i\} \times A_i \subset \mathbb{Z}^k \times \mathbb{Z}^n$. For every $f \in \mathbb{Z}^A$, let f_I be the polynomial $\sum_{i \in I} \lambda_i f_i(x) \in \mathbb{C}^{A_I}$ of variables $\lambda = (\lambda_1, \dots, \lambda_k) \in (\mathbb{C}\backslash 0)^k$ and $x \in (\mathbb{C}\backslash 0)^n$.

DEFINITION 3.12. (1) The *naive A-discriminant* [Est10] is the closure of the set of all tuples $f \in \mathbb{C}^A$ having a singular common root $x \in (\mathbb{C}\backslash 0)^n$ (so that $f_1(x) = \dots = f_k(x) = 0$ and $df_1(x), \dots, df_k(x)$ are linearly dependent).

(2) The *mixed A-discriminant* ([CCDDS13] for $k = n$) is the closure of the set of all tuples $f \in \mathbb{C}^A$ having a *non-degenerate singular common root* $x \in (\mathbb{C}\backslash 0)^n$ (i.e. a singular common root such that no proper subtuple of $df_1(x), \dots, df_k(x)$ is linearly dependent).

(3) The *Cayley A-discriminant* [Est10] is the image of the discriminant $D_{A_{\{1,\dots,k\}}} \subset \mathbb{C}^{A_{\{1,\dots,k\}}}$ under the natural isomorphism $\mathbb{C}^{A_{\{1,\dots,k\}}} \to \mathbb{C}^A$ inverse to sending every f to $f_{\{1,\dots,k\}}$.

All of these sets obviously coincide for the Gelfand–Kapranov–Zelevinsky case $k = 1$. However, for $k > 1$ (including $k = n$), they may be pairwise different [CCDDS13, Example 1.2] and have irreducible components of different dimensions [Est10, Example 2.25]. Nevertheless, this difference disappears for irreducible tuples.

THEOREM 3.13. *If A is irreducible, the three discriminant sets of Definition 3.12 coincide up to irreducible components of codimension greater than* 1.

Proof. If the Cayley discriminant has codimension greater than 1, then so do the naive discriminant by [Est10, Theorem 2.31] and the mixed discriminant (as its subset).

To study the opposite case, define $\Sigma_{\{j_1,\dots,j_q\}}$ as the set of all tuples $f = (f_1, \dots, f_k) \in \mathbb{C}^A$ such that $f(x) = 0$ for some $x \in (\mathbb{C}\backslash 0)^n$ and $\sum_i \lambda_i df_{q_i}(x) = 0$ for some $(\lambda_1, \dots, \lambda_q) \in (\mathbb{C}\backslash 0)^q$ [Est10, Definition 2.33].

If the Cayley discriminant has codimension 1, then this hypersurface H is the only codimension 1 component of the naive discriminant by [Est10, Theorem 2.31] and the only codimension 1 set of the form Σ_J (namely, the one corresponding to $J = \{1, \dots, k\}$) by [Est10, Lemma 2.34]. The latter fact implies that a singular common root of a generic tuple $f \in H$ is non-degenerate (because the linear dependence of its differentials df_j for $j \in J' \neq \{1, \dots, k\}$ would imply that $\Sigma_{J'} = \Sigma_J$ also has codimension 1). Thus H is also a codimension 1 component of the mixed discriminant, and the latter has no other codimension 1 components, because it is contained in the naive discriminant. □

Dual defectiveness of systems of equations

DEFINITION 3.14. By Theorem 3.13, for an irreducible tuple A, we can denote the common hypersurface components of the three discriminant sets of Definition 3.12 by D_A, and call this hypersurface the A-discriminant. The irreducible tuple A is said to be dual defective if D_A is empty, and dual effective otherwise.

If the tuple A consists of one set $A_1 \subset \mathbb{Z}^n$, then it is irreducible, and its dual defectiveness is the same property as in Definition 3.6.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Conjecture 3.15. For irreducible tuples, the three discriminant sets of Definition 3.12 coincide completely, that is, they are the same irreducible set.

Remark 3.16. The interrelation between the three notions of the discriminant in Definition 3.12 is not yet completely understood for reducible tuples, particularly concerning the higher-codimension components. As a consequence, the notion of dual defectiveness for reducible tuples splits into several non-equivalent versions, looking for the non-existence of codimension 1 components and/or existence of higher-codimension components in any of the three notions of the discriminant. It would be important to understand how these numerous versions are related.

Remark 3.17. As we have observed, the irreducibility of the tuple A implies the irreducibility of the codimension 1 part of the naive A-discriminant. On the other hand, the codimension 1 part of the naive A-discriminant tends to be reducible if A is reducible; see [Est10, Lemma 2.34]. The situation with reduced tuples is similar: the codimension 1 components D_i of the naive A-discriminant come with natural multiplicities equal to the number of singular roots of the system $f = 0$ for a generic tuple $f \in D_i$. By Theorem 3.8, an irreducible tuple A is reduced if and only if D_A is reduced in the sense of the aforementioned multiplicity (see [Est13] for the computation of the multiplicities for non-reduced and reducible tuples).

Lemma 3.18. *An irreducible tuple A is dual effective if and only if some $f \in \mathbb{C}^A$ has an isolated singular root.*

Proof. If the tuple $f = (f_1, \dots, f_k)$ has an isolated singular root x, then the set of tuples in $\mathbb{C}^A$ that have a singular root contains a hypersurface in a small neighbourhood of f. Indeed, the projection π of the incidence set $\{(\tilde{x}, \tilde{f}) \mid \tilde{f}(\tilde{x}) = 0\} \subset (\mathbb{C}\backslash 0)^n \times \mathbb{C}^A$ to $\mathbb{C}^A$ has the critical set C of dimension one less than $\mathbb{C}^A$. Since x is an isolated singular root of f, the fibres of the projection $\pi : C \to \mathbb{C}^A$ near (x, f) are finite, thus the image of C contains a hypersurface passing through f. Thus, according to the naive version of the definition of the discriminant (see Definition 3.12), D_A contains a non-empty hypersurface.

To prove the statement in the other direction, recall that $f_{\{1,\dots,k\}}$ is a homogeneous polynomial in the variables $\lambda_1, \dots, \lambda_k$, so the equation $f_{\{1,\dots,k\}} = 0$ defines a subset in $\mathbb{CP}^{k-1} \times (\mathbb{C}\backslash 0)^n$. Denote the image of the torus $(\mathbb{C}\backslash 0)^k$ under the projection $\mathbb{C}^k \to \mathbb{CP}^{k-1}$ by T.

In this notation, if the tuple A is dual effective, then so is $A_{\{1,\dots,k\}}$, then, by Theorem 3.8, a generic polynomial $f_{\{1,\dots,k\}}$ in it has a unique (and thus isolated) singular root in $T \times (\mathbb{C}\backslash 0)^n$, then so does the tuple $f \in \mathbb{C}^A$. □

Proof of Theorem 1.20

For a finite set $A \subset \mathbb{Z}^n$, let $\mathbb{CP}^A$ be the projective space with the homogeneous coordinates z_a, $a \in A$, and let $m = m_A : (\mathbb{C}\backslash 0)^n \to \mathbb{CP}^A$ be the monomial map such that $m_A(x)$ has coordinates $z_a = x^a$.

Definition 3.19. The A-image of an algebraic set $V \subset (\mathbb{C}\backslash 0)^n$ is the image of $m_A(V)$ in $\mathbb{CP}^A$.

Remark 3.20. The A-image is usually not closed. In what follows, whenever we discuss its degree and irreducibility, we refer to the corresponding properties of its closure. On the other hand, its projectively dual set is defined as the set of all tangent hyperplanes to its smooth points, and is usually also not closed.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

THEOREM 3.21. *Let $A = (A_1, \dots, A_k)$ and $A' = (A_2, \dots, A_k)$ be tuples of finite sets in $\mathbb{Z}^n$, $n \geqslant k$, and let M be the A_1-image of the complete intersection $f = 0$ for a generic tuple of polynomials $f = (f_2, \dots, f_k) \in \mathbb{C}^{A'}$.*

(1) *If A is irreducible, then $f = 0$ and M are irreducible.*
(2) *If, besides being irreducible, A is reduced, then M is also reduced (in the sense that the map $m = m_{A_1} : \{f = 0\} \to M$ has degree 1).*
(3) *Assume that A is reduced and irreducible. Then the degree of M is greater than 1 unless the sets $A_1, \dots, A_k$ can be shifted to the same lattice simplex of lattice volume 1.*
(4) *Assume that A is reduced and irreducible. Then A is dual defective if and only if M is dual defective (i.e. its projectively dual set has codimension greater than 1). Moreover, if A and M are dual effective, then a generic tuple of polynomials in the discriminant D_A has a unique singular root, and this root is non-degenerate.*

Remark 3.22. (1) We shall apply this lemma for $k = n$, in which case by the non-degenerate singular root we mean just the root of multiplicity 2. However, part (4) makes sense for arbitrary $k \leqslant n$. In this case a root x of a system of equations $g = 0$ is said to be singular non-degenerate, if $g = 0$ defines an isolated singularity of a complete intersection in a neighbourhood of x, and its Milnor number equals 1 (see [Loo84]).

(2) Part (1) for $k < n$ actually occurs and will be proved under a strictly weaker assumption that we call coirreducibility (cf. Definition 1.3): no m sets of the tuple A' can be shifted to the same m-dimensional sublattice.

Proof. If A is irreducible and $k \leqslant n$, then the tuple A' is coirreducible (in the sense of Remark 3.22(2)), so part (1) follows from [Kho16] for $f = 0$ and thus also for M.

We shall now assume without loss of generality that $0 \in A_1$, because all properties of A mentioned in the statement are invariant under parallel translations. For every linear form l on $\mathbb{CP}^{A_1}$, denote the rational function l/z_0 by $\tilde{l}$. In this notation, assigning the function $f_1(x) = \tilde{l}(m(x))$ to a form l (or, in coordinates, assigning the polynomial $f_1(x) = \sum_{a \in A_1} c_a x^a$ to the form $l(z) = \sum_{a \in A_1} c_a z_a$), we establish an isomorphism between $\mathbb{C}^{A_1}$ and the space of linear forms on $\mathbb{CP}^{A_1}$.

Assume towards a contradiction that part (2) does not hold. Then, for generic linear forms $l_1, \dots, l_{n-k+2}$ such that the plane $l_\bullet = 0$ intersects M, an intersection point would have more than one preimage in $f = 0$, that is, a generic tuple of polynomials

$$(\tilde{l}_1(m(\cdot)), \dots, \tilde{l}_{n-k+2}(m(\cdot)), f_2, \dots, f_k) \in R_B$$

supported at the tuple

$$B = (\underbrace{A_1, \dots, A_1}_{n-k+2}, A_2, A_3, \dots, A_k)$$

would have more than one common root. This would contradict Theorem 3.3, because irreducibility of A implies irreducibility of B.

In the setting of part (3), we may assume without loss of generality by Theorem 2.5 that the tuple

$$B' = (\underbrace{A_1, \dots, A_1}_{n-k+1}, A_2, A_3, \dots, A_k)$$

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

has mixed volume greater than 1, because it is reduced and irreducible. Then the degree of M is greater than 1, because it equals the number of intersections of V with a generic plane $l_1 = \cdots = l_{n-k+1} = 0$, that is, the number of common roots of a generic tuple of polynomials $(\tilde{l}_1(m(\cdot)), \ldots, \tilde{l}_{n-k+1}(m(\cdot)), f_2, \ldots, f_k) \in \mathbb{C}^{B'}$, which equals the mixed volume of B' by the Kouchnirenko–Bernstein theorem.

It remains to prove part (4). If M is dual effective, then the hyperplane $l = 0$, corresponding to a smooth point of the projectively dual variety, is tangent to M at a unique point z, and the tangency is non-degenerate (in the sense that the restriction of $\tilde{l}$ to M has the non-degenerate Hessian at z). Then the restriction of the polynomial $f_1(x) = \tilde{l}(m(x))$ to the complete intersection $f = (f_2, \ldots, f_k) = 0$ has a unique and non-degenerate singular root, then the resulting tuple $(f_1, f_2, \ldots, f_k)$ has a unique and non-degenerate singular root. By Lemma 3.18, this implies that A is dual effective. The other direction is proved in the same way. □

Corollary 3.23 (Theorem 1.20 refined). *A reduced irreducible tuple of sets $A = (A_1, \ldots, A_n)$ in $\mathbb{Z}^n$ is dual effective unless, upon an automorphism of the lattice, all of its sets can be shifted to the standard simplex. Moreover, in this case a generic tuple $f \in D_A$ has a unique multiple root, and this root has multiplicity 2.*

Proof. By Theorem 3.21(1)–(3), the closure of M is a reduced irreducible curve of degree greater than 1. Since every such curve is dual effective, the sought statement follows from Theorem 3.21(4). □

Remark 3.24. Excluding the notion of the projectively dual variety from this reasoning, we can describe more explicitly the picture in $\mathbb{CP}^{A_1}$ corresponding to a minimally degenerate system of equations as follows. Taking a generic tuple $(f_2, \ldots, f_n) \in \mathbb{C}^{A'}$, the curve

$$M = m_{A_1}\{f_2 = \cdots = f_n = 0\}$$

is reduced, irreducible and not a line. Thus, a generic tangent hyperplane $\sum_{a \in A_1} c_a z_a = 0$ to M has a simple tangency and is transversal to M at the other intersection points. Then the system of equations $\sum_{a \in A_1} c_a x^a = f_2(x) = \cdots = f_n(x) = 0$ has one root of multiplicity 2, and the other roots are of multiplicity 1.

Proof of Theorem 1.22

We first need an explicit construction of the exceptional set B_A in the Kouchnirenko–Bernstein Theorem 1.1.

The restriction of a linear function $v : \mathbb{R}^n \to \mathbb{R}$ to a finite set $A \subset \mathbb{Z}^n$ takes its maximal value at certain points of A. The set of all such points will be denoted by A^v. For a tuple $A = (A_1, \ldots, A_k)$, denote the tuple $(A_1^v, \ldots, A_k^v)$ by A^v, and the naive discriminant of A^v (see Definition 3.12) by D_v. We shall consider D_v as a subset of $\mathbb{C}^A$ in the sense of Remark 3.10. The set

$$B = \bigcup_{v \in \mathbb{R}^n} D_v \subset \mathbb{C}^A$$

is algebraic, because there are only finitely many distinct algebraic sets among D_v, $v \in \mathbb{Z}^n$. More specifically, write $u \sim v$ if $A^u = A^v$; then this equivalence relation splits $\mathbb{R}^n$ into finitely many relatively open polyhedral cones. These cones form a fan Σ (see, for example, [Ful93]), and A^v and D_v depend only on the cone $C \in \Sigma$ containing v. So we shall also denote A^v and D_v by A^C and D_C, respectively.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

We claim that the set B can be taken as the exceptional set B_A in Theorem 1.1 in the following strong sense. Denote the incidence set

$$\{(x, f) \mid f(x) = 0\} \subset (\mathbb{C}\backslash 0)^n \times \mathbb{C}^A$$

by E and its projection to $\mathbb{C}^A$ by π.

THEOREM 3.25 (Theorem 1.22 refined). *Let the tuple $A = (A_1, \dots, A_n)$, the set B and the projection π be as above with $k = n$.*

(1) *The projection π is a covering outside the set B. In particular, every $f \in \mathbb{C}^A\backslash B$ has exactly $\mathrm{MV}(A)$ roots, and the group G_A is the monodromy group of this covering.*

(2) *If A is reduced and dual effective, then, for a generic $f \in D_A$:*

- *the system $f = 0$ has a unique singular root $x \in (\mathbb{C}\backslash 0)^n$, and its multiplicity is 2;*
- *we have $f \notin D_v$ for every non-zero $v : \mathbb{R}^n \to \mathbb{R}$.*

(3) *For such f, let $F : (\mathbb{C}, 0) \to (\mathbb{C}^A, f)$ be a germ of a smooth curve transversal to D_A. Then the monodromy of the covering from part (1) along the loop $F(\varepsilon \exp(2\pi i t))$ for small $\varepsilon > 0$ is a transposition.*

Remark 3.26. Instead of assuming dual effectiveness in part (2), it is enough to assume that the Cayley configuration $A_{\{1,\dots,n\}}$ is dual effective, and then a small loop around the Cayley discriminant $D_{A_{\{1,\dots,n\}}}$ still gives a transposition; see Theorem 3.27 below for this and some other generalizations.

Proof of part (2). The first statement follows from Corollary 3.23, the second one from Corollary 3.11 applied to the Cayley discriminant $D_{A_{\{1,\dots,n\}}}$. □

Proof of parts (1) and (3). Choose a unimodular simplicial fan Σ', subdividing Σ (see [KKMS73] for its existence), and consider the corresponding smooth toric variety $X \supset (\mathbb{C}\backslash 0)^n$. Every cone $C \in \Sigma'$ corresponds to an orbit $O_C \subset X$, and, for $C \neq \{0\}$, the closure of the incidence set E in $X \times C^A$ contains a point of the form $(x, f) \in O_C \times \mathbb{C}^A$ only if $f \in D_C$. In particular, if $f \notin D_v$ for every non-zero $v : \mathbb{R}^n \to \mathbb{R}$, then, for a small neighbourhood $U \ni f$, its preimage $V = \pi^{-1}(U)$ is disjoint from the orbits O_C, $C \neq \{0\}$, that is, the restriction $\pi : V \to U$ is proper. Now consider two cases, corresponding to the setting of part (1) and part (3), respectively: $f \notin D_A$ and $f \in D_A$.

If $f \notin D_A$, then the restriction $\pi : V \to U$ also has no critical points (this claim makes sense, because E is smooth), so it is a trivial covering, and part (1) is proved.

If $f \in D_A$ has a unique multiple root x, and this root has multiplicity 2, then the local degrees of π at the point (x, f) and at the other points of the fibre $\pi^{-1}(f)$ equal 2 and 1, respectively. Thus π has an $\mathcal{A}_1$ singularity at (x, f) and no singularities at other points of the fibre $\pi^{-1}(f)$, that is, $\pi(z_1, z_2, \dots, z_N) = (z_1^2, z_2, \dots, z_N)$ in suitable local coordinates $(z_1, \dots, z_N)$ on T near (x, f). In particular, the monodromy along a small loop around the origin in the complex line $z_2 = \dots = z_N = 0$ is a transposition. □

Monodromy of non-square systems of equations

We outline a generalization of Theorem 3.25 to some reducible tuples A and to the case $k < n$ in order to clarify what happens in examples similar to Example 1.16 and what could be a natural counterpart of the topic of this paper for non-square systems of equations.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Theorem 3.27. *Let $A = (A_1, \dots, A_k)$, B and π be as above with arbitrary $k \leqslant n$.*

(1) *The projection π in a locally trivial fibration outside the set B. Moreover, B is the minimal closed set with this property. In particular, every loop in the complement to B gives rise to the monodromy automorphism in the cohomology H of the fibre of this fibration.*

(2) *The set B is a hypersurface unless $m+2$ of the sets in the tuple A can be shifted to the same m-dimensional plane (in which case the aforementioned fibration is empty).*

(3) *For a reduced tuple A, whose Cayley discriminant (Definition 3.12) is a hypersurface, and for a generic f in the Cayley discriminant:*

- *the system $f = 0$ has a unique singular root $x \in (\mathbb{C}\backslash 0)^n$, and this singular root is non-degenerate;*
- *we have $f \notin D_v$ for every non-zero $v : \mathbb{R}^n \to \mathbb{R}$.*

(4) *For such f, let $F : (\mathbb{C}, 0) \to (\mathbb{C}^A, f)$ be a germ of a smooth curve transversal to D_A. Then the ζ-function of the monodromy transformation from part (1), corresponding to the loop $F(\varepsilon \exp(2\pi i t))$ for small $\varepsilon > 0$, has the form $t^2 - 1$.*

Parts (1) and (2) follow from [Est13, Theorems 1.1 and 1.4]. The first statement of part (3) follows from the fact that the Cayley discriminant is a component of multiplicity 1 in the Euler discriminant E_A; see [Est13, Proposition 1.11]. (This works in particular for $k = n$, but we preferred to give a more straightforward proof of Theorem 3.25 in that case.) The rest is proved in the same way as for $k = n$ in Lemma 3.25.

Remark 3.28. In particular, the correspondence from Theorem 3.27(1) maps the fundamental group of the complement of B to the group $\mathrm{GL}(H)$. The image G_A is the monodromy group of the (non-square) system of equations supported at the tuple A. The results of the present paper give some hope that G_A can be quite explicitly described in terms of A at least for reduced irreducible A. This important study has been recently initiated in the simplest non-square case, $(k, n) = (1, 2)$; see [CL18, CL17, Sal17].

4. Double transitivity of monodromy

Consider a morphism π of an algebraic set E to an irreducible algebraic set C as an *abstract enumerative problem*: regard a point $z \in C$ as an incidence condition, and the points of its fibre $\pi^{-1}(z)$ as the solutions of the enumerative problem with a given incidence condition. The enumerative problem is said to be *well posed* if its generic fibre is finite. In this case, there exists a Zariski open set $U \subset C$ such that π is a covering over U. The monodromy group of this covering does not depend on the choice of U and is called the monodromy group of the enumerative problem.

Example 4.1. The enumerative problem of the present paper falls into this scheme, if we define

$$E = \{(x, f) \mid f(x) = 0\} \subset (\mathbb{C}\backslash 0)^n \times \mathbb{C}^A$$

and denote the projection of E to $C = \mathbb{C}^A$ by π. For every tuple $A = (A_1, \dots, A_n)$, it is well posed by Theorem 3.25(1).

Let us recall a classically known geometric criterion for the double transitivity of the monodromy of the abstract enumerative problem $\pi : E \to C$. Although its versions can be found

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

in [SW15] and other relevant works, we shall recall the proof to keep the story self-contained. Consider the fibre square

$$E_2 = \{(x, y) \mid \pi(x) = \pi(y)\} \subset E^2$$

and its projection $\pi_2 : E_2 \to C$, sending (x, y) to $\pi(x) = \pi(y) \in C$. If the enumerative problem is well posed, that is, for a certain Zariski open $U \subset C$, its preimage $V = \pi^{-1}(U)$ defines a covering $\pi : V \to U$, then the fibre square $V_2 = \pi_2^{-1}(U)$ also defines a covering $\pi_2 : V_2 \to U$. Note that the diagonal $D = \{(x, x) \mid x \in U\} \subset V_2$ is an irreducible component of V_2.

Theorem 4.2. *The monodromy of the well-posed enumerative problem $\pi : E \to C$ is doubly transitive if and only if V_2 has at most one irreducible component different from D.*

Proof. If $D = V_2$, then the monodromy is trivial. Otherwise, let F be the second component of V_2. In order to prove the double transitivity, we should take two pairs of distinct points (x, y) and (x', y') in the fibre $\pi^{-1}(z)$ of a point $z \in U$ and construct a loop in U such that the monodromy along this loop sends x to x' and y to y'. Since neither (x, y) nor (x', y') is contained in D, both of them are contained in F. Since F is irreducible, these two points can be connected with a path γ. Then $\pi_2(\gamma)$ is the loop sought. □

Corollary 4.3. *Let $\pi : E \to C$ be a well-posed enumerative problem. If at most one irreducible component of E_2 besides the diagonal D has the same dimension as D, then the monodromy is doubly transitive.*

Proof of Theorem 1.23. The idea is to apply Corollary 4.3 to the setting of Example 4.1. In this case we have

$$S = (\mathbb{C}\backslash 0)^n \times (\mathbb{C}\backslash 0)^n,$$
$$E_2 = \{(x, y, f) \mid f(x) = f(y) = 0\} \subset S \times \mathbb{C}^A.$$

In order to prove that G_A is doubly transitive, it is enough to prove that E_2 has at most one more irreducible component F of dimension $N = \dim \mathbb{C}^A$. We shall prove it by counting the dimension of fibres of the projection $p : E_2 \to S$. Every such fibre is a vector subspace of $\mathbb{C}^A$, but different fibres may have different dimension. Namely, assuming for convenience without loss of generality that every A_i contains 0, the fibre $p^{-1}(x, y)$ is given in $\mathbb{C}^A$ by

$$2n - d_{x,y} \tag{$*$}$$

independent linear equations, where $d_{x,y}$ is the number of A_i such that $x^a = y^a$ for all $a \in A_i$. Indeed, since $0 \in A_i$, the linear equations $f_i(x) = f_i(y) = 0$ on the element $f = (f_1, \dots, f_i, \dots, f_n) \in \mathbb{C}^A$ are dependent if and only if they coincide and if and only if $x^a = y^a$ for all $a \in A_i$, so ($*$) follows.

This implies that $\dim p^{-1}(x, y)$ is the same for all (x, y) in the set U_L, defined as follows:

$$V_L = \{(x, y) \mid x^a = y^a \text{ for all } a \in L\} \subset S \text{ for a sublattice } L \subset \mathbb{Z}^n,$$
$$L_I \subset \mathbb{Z}^n \text{ is the sublattice generated by } A_i,\ i \in I,$$
$$U_L = V_L \Big\backslash \bigcup_{L_I \supsetneq L} V_{L_I}.$$

Namely, if $(x, y) \in U_L$, then, by ($*$), the fibre $p^{-1}(x, y)$ is given in $\mathbb{C}^A$ by

$$2n - d_L \tag{$**$}$$

independent linear equations, where d_L is the number of A_i contained in L.

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press

Therefore, denoting the preimage of U_L in E_2 by E_L, we conclude by (**) that $p : E_L \to U_L$ is a vector bundle of rank $N - 2n + d_L$, $N = \dim \mathbb{C}^A$. Moreover, since $\dim U_L = 2n - \dim L$, we conclude that $\dim E_L = N + d_L - \dim L$.

Since the tuple A is reduced and irreducible, we have

$$\dim E_L = N + d_L - \dim L < N$$

unless $L = \mathbb{Z}^n$, or L contains no A_i at all. In the latter cases, E_L equals the diagonal $D \subset E_2$ or one more N-dimensional subset $F \subset E_2$ (independent of L), respectively. Since E_2 is covered by E_L as L runs over all sublattices, we have proved that it has two N-dimensional components, so that Corollary 4.3 applies. □

Acknowledgements

I am grateful to Christopher Borger and Benjamin Nill, whose proof [BN18] of a conjecture from [CCDDS13] contributed to working out the present approach to the conjecture from [EG16], and to Yuri Burman and the referee for valuable remarks.

References

Ber75 D. N. Bernstein, *The number of roots of a system of equations*, Funct. Anal. Appl. **9** (1975), 183–185.

BN18 C. Borger and B. Nill, *On defectivity of families of full-dimensional point configurations*, Preprint (2018), arXiv:1801.07467.

CC07 E. Cattani and R. Curran, *Restriction of A-discriminants and dual defect toric varieties*, J. Symbolic Comput. **42** (2007), 115–135.

CCDDS13 E. Cattani, M. A. Cueto, A. Dickenstein, S. Di Rocco and B. Sturmfels, *Mixed discriminants*, Math. Z. **274** (2013), 761–778.

CL17 R. Cretois and L. Lang, *The vanishing cycles of curves in toric surfaces II*. J. Topol. Anal., to appear. Preprint (2017), arXiv:1706.07252.

CL18 R. Cretois and L. Lang, *The vanishing cycles of curves in toric surfaces I*, Compos. Math. **154** (2018), 1659–1697.

DFS07 A. Dickenstein, E. M. Feichtner and B. Sturmfels, *Tropical discriminants*, J. Amer. Math. Soc. **20** (2007), 1111–1133.

DiR06 S. Di Rocco, *Projective duality of toric manifolds and defect polytopes*, Proc. Lond. Math. Soc. (3) **93** (2006), 85–104.

Ein86 L. Ein, *Varieties with small dual varieties I and II*, Invent. Math. **86** (1986), 63–74; Duke Math. J. **52** (1985) 895–907.

Est06 A. Esterov, *Indices of 1-forms, intersection indices, and Newton polyhedra*, Sb. Math. **197** (2006), 1085–1108.

Est07 A. Esterov, *Determinantal singularities and newton polyhedra*, Proc. Steklov Inst. Math. **259** (2007), 20–38.

Est10 A. Esterov, *Newton polyhedra of discriminants of projections*, Discrete Comput. Geom. **44** (2010), 96–148.

Est13 A. Esterov, *The discriminant of a system of equations*, Adv. Math. **245** (2013), 534–572.

Est18 A. Esterov, *Characteristic classes of affine varieties and Plücker formulas for affine morphisms*, J. Eur. Math. Soc. (JEMS) **20** (2018), 15–59.

EG15 A. Esterov and G. Gusev, *Systems of equations with a single solution*, J. Symbolic Comput. **68** (2015), 116–130.

EG16 A. Esterov and G. Gusev, *Multivariate Abel–Ruffini*, Math. Ann. **365** (2016), 1091–1110.

For17 J. Forsgård, *Defective dual varieties for real spectra*. J. Algebraic Combin., to appear. Preprint (2017), arXiv:1710.02434.

Ful93 W. Fulton, *Introduction to toric varieties* (Princeton University Press, Princeton, NJ, 1993).

FI16 K. Furukawa and A. Ito, *A combinatorial description of dual defects of toric varieties*, Preprint (2016), arXiv:1605.05801.

GKZ94 I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky, *Discriminants, resultants and multidimensional determinants* (Birkhäuser, Boston, 1994).

HKN18 J. Hofscheier, L. Katthän and B. Nill, *Ehrhart theory of spanning lattice polytopes*, Int. Math. Res. Not. IMRN **2018** (2018), 5947–5973.

HT17 T. Hibi and A. Tsuchiya, *Classification of lattice polytopes with small volumes*, Preprint (2017), arXiv:1708.00413.

Kho78 A. G. Khovanskii, *Newton polyhedra and the genus of complete intersections*, Funct. Anal. Appl. **12** (1978), 38–46.

Kho15 A. G. Khovanskii, *Topological Galois theory*, Springer Monographs in Mathematics (Springer, Heidelberg, 2015).

Kho16 A. G. Khovanskii, *Newton polytopes and irreducible components of complete intersections*, Izv. Math. **80** (2016), 263–284.

KKMS73 G. Kempf, F. Knudsen, D. Mumford and B. Saint-Donat, *Toroidal embeddings 1*, Lecture Notes in Mathematics (Springer, Berlin, 1973).

Loo84 E. J. N. Looijenga, *Isolated singular points on complete intersections*, LMS Lecture Note Series, vol. 77 (Cambridge University Press, Cambridge, 1984).

LZ91 J. Lagarias and G. Ziegler, *Bounds for lattice polytopes containing a fixed number of interior points in a sublattice*, Canad. J. Math. **43** (1991), 1022–1035.

Min11 H. Minkowski, *Theorie der konvexen Körper, insbesonder der Begründung ihres Oberflächenbegriffs*, Gesammelte Abhandlungen, vol. 2 (Teubner, Leipzig, Berlin, 1911), 131–229.

Sal17 N. Salter, Monodromy and vanishing cycles in toric surfaces, Preprint (2017), arXiv:1710.08042.

ST10 R. Steffens and T. Theobald, *Mixed volume techniques for embeddings of Laman graphs*, Comput. Geom. **43** (2010), 84–93.

Stu94 B. Sturmfels, *On the Newton polytope of the resultant*, J. Algebraic Combin. **3** (1994), 207–236.

SW15 F. Sottile and J. White, *Double transitivity of Galois groups in Schubert calculus of Grassmannians*, Algebr. Geom. **2** (2015), 422–445.

A. Esterov aesterov@hse.ru
National Research University Higher School of Economics
Faculty of Mathematics NRU HSE, Usacheva str., 6, Moscow, 119048, Russia

https://doi.org/10.1112/S0010437X18007868 Published online by Cambridge University Press