From Hilbert's 13th problem to essential dimension and back

Zinovy Reichstein

1 Introduction

The problem of solving polynomial equations in one variable, i.e., equations of the form

$$f(x) = 0, \quad \text{where} \quad f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \qquad (1)$$

goes back to ancient times. Here by "solving" I mean finding a procedure or a formula which produces a solution x for a given set of coefficients $a_1, \ldots, a_n$. The terms "procedure" and "formula" are ambiguous; to get a well-posed problem, we need to specify what kinds of operations we are allowed to perform to obtain x from $a_1, \ldots, a_n$. In the simplest setting, we are only allowed to perform the four arithmetic operations: addition, subtraction, multiplication and division. In other words, we are asking if the polynomial (1) has a root x which is expressible as a rational function of $a_1, \ldots, a_n$. For a general polynomial of degree $n \geqslant 2$, the answer is clearly "no"; this was already known to the ancient Greeks. The focus then shifted to the problem of "solving polynomials in radicals", where one is allowed to use the four arithmetic operations and radicals of any degree. Here the mth radical (or root) of t is a solution to

$$x^m - t = 0. \qquad (2)$$

Mathematicians attempted to solve polynomial equations this way for centuries, but only succeeded for $n = 1$, 2, 3 and 4. It was shown by Ruffini, Abel and Galois in the early 19th century that a general polynomial of degree $n \geqslant 5$ cannot be solved in radicals. This was a ground-breaking discovery. However, the story does not end there.

Suppose we allow one additional operation, namely solving

$$x^5 + tx + t = 0. \qquad (3)$$

That is, we start with $a_1, \ldots, a_n$, and at each step, we are allowed to enlarge this collection by adding one new number, which is the sum, difference, product or quotient of two numbers in our collection, or a solution to (2) or (3) for any t in our collection. In 1786, Bring [16] showed that every polynomial equation of degree 5 can be solved using these operations.

Note that the coefficients of (2) and (3) only depend on one parameter t. Thus roots of these equations can be thought of as "algebraic functions" of one variable. By contrast, the coefficients of the general polynomial equation (1) depend on n independent parameters $a_1, \ldots, a_n$. With this in mind, we define the resolvent degree $\mathrm{rd}(f)$ of a polynomial $f(x)$ in (1) as the smallest positive integer r such that every root of $f(x)$ can be obtained from $a_1, \ldots, a_n$ in a finite number of steps, assuming that at each step we are allowed to perform the four arithmetic operations and evaluate algebraic functions of r variables. Let us denote the largest possible value of $\mathrm{rd}(f)$ by $\mathrm{rd}(n)$, as $f(x)$ ranges over all polynomials of degree n. The algebraic form of Hilbert's 13th problem asks for the value of $\mathrm{rd}(n)$.

The actual wording of the 13th problem is a little different: Hilbert asked for the minimal integer r one needs to solve every polynomial equation of degree n, assuming that at each step one is allowed to perform the four arithmetic operations and apply any continuous (rather than algebraic) function in r variables. Let us denote the maximal possible resolvent degree in this setting by $\mathrm{crd}(n)$, where "c" stands for "continuous". Specifically, Hilbert asked whether or not $\mathrm{crd}(7) = 3$. In this form, Hilbert's 13th problem was solved by Kolmogorov [37] and Arnold [1] in 1957.[1] They showed that, contrary to Hilbert's expectation, $\mathrm{crd}(n) = 1$ for every n. In other words, continuous functions in 1 variable are enough to solve any polynomial equation of any degree. Moreover, any continuous function in n variables can be expressed as a composition of functions of one variable and addition.

In spite of this achievement, Wikipedia lists the 13th problem as "unresolved". While this designation is subjective, it reflects the view of many mathematicians that Hilbert's true intention was to ask about $\mathrm{rd}(n)$, not $\mathrm{crd}(n)$. They point to the body of work on $\mathrm{rd}(n)$ going back centuries before Hilbert (see, e.g., [21]) and to Hilbert's own 20th century writings, where only $\mathrm{rd}(n)$ was considered (see, e.g., [31]). Arnold himself was a strong proponent of this point of view [13, pp. 45–46], [2].

Progress on the algebraic form of Hilbert's 13th problem has been slow. From what I said above, $\mathrm{rd}(n) = 1$ when $n \leqslant 5$; this was

[1] Arnold was a 19 year old undergraduate student in 1957. He later said that all of his numerous subsequent contributions to mathematics were, in one way or another, motivated by Hilbert's 13th problem; see [2].

known before Hilbert and even before Galois. The value of $\mathrm{rd}(n)$ remains open for every $n \geqslant 6$, and the possibility that $\mathrm{rd}(n) = 1$ for every n has not been ruled out. The best known upper bounds on $\mathrm{rd}(n)$ are of the form $\mathrm{rd}(n) \leqslant n - \alpha(n)$, where $\alpha(n)$ is an unbounded but very slow growing function of n. The list of people who have proved inequalities of this form includes some of the leading mathematicians of the past two centuries: Hamilton, Sylvester, Klein, Hilbert, Chebotarev, Segre, Brauer. Recently, their methods have been refined and their bounds sharpened by Wolfson [63], Sutherland [60] and Heberle–Sutherland [30].

There is another reading of the 13th problem, to the effect that Hilbert meant to allow global multi-valued continuous functions; see [2, p. 613]. These behave in many ways like algebraic functions. If we denote the resolvent degree in this sense by $\mathrm{Crd}(n)$, where "C" stands for "global continuous", then

$$1 = \mathrm{crd}(n) \leqslant \mathrm{Crd}(n) \leqslant \mathrm{rd}(n) \leqslant n - \alpha(n).$$

As far as I am aware, nothing else is known about $\mathrm{Crd}(n)$ or $\mathrm{rd}(n)$ for $n \geqslant 6$.

On the other hand, in recent decades, considerable progress has been made in studying a related but different invariant, the essential dimension.[2] Joe Buhler and I [14] introduced this notion in the late 1990s. In special instances, it came up earlier, e.g., in the work of Kronecker [38], Klein [35], Chebotarev [15], Procesi [48][3] and Kawamata [34][4]. Our focus in [14] was on polynomials and field extensions. It later became clear that the notion of essential dimension is of interest in other contexts: quadratic forms, central simple algebras, torsors, moduli stacks, representations of groups and algebras, etc. In each case, it poses new questions about the underlying objects and occasionally leads to solutions of preexisting open problems.

This paper has two goals. The first is to survey some of the research on essential dimension in Sections 2–7. This survey is not comprehensive; it is only intended to convey the flavor of the subject and sample some of its highlights. My second goal for this paper is to define the notion of resolvent degree of an algebraic group in Section 8, building on the work of Farb and Wolfson [25] but focusing on connected, rather than finite groups. The quantity $\mathrm{rd}(n)$ defined above is recovered in this setting as $\mathrm{rd}(\mathrm{S}_n)$. For more comprehensive surveys of essential dimension and resolvent degree, see [41, 51] and [25], respectively.

2 Essential dimension of a polynomial

Let k be a base field, K be a field containing k and L be a finite-dimensional K-algebra (not necessarily commutative, associative or unital). We say that L descends to an intermediate field $k \subset K_0 \subset K$ if there exists a finite-dimensional K_0-algebra L_0 such that $L = L_0 \otimes_{K_0} K$. Equivalently, recall that, for any choice of an K-vector space basis $e_1, \dots, e_n$ of L, one can encode multiplication in L into the n^3 structure constants $c_{ij}^h \in K$ given by $e_i e_j = \sum_{h=1}^n c_{ij}^h e_h$. Then L descends to $K_0 \subset K$ if and only if there exists a basis $e_1, \dots, e_n$ such that all of the structure constants e_{ij}^h with respect to this basis lie in K_0. The essential dimension $\mathrm{ed}_k(L/K)$ is defined as the minimal value of the transcendence degree $\mathrm{trdeg}_k(K_0)$, where L descends to K_0. If the reference to the base field k is clear from the context, we will write ed in place of ed_k.

If $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ is a polynomial over K, for some $a_1, \dots, a_n$, as in (1), we define $\mathrm{ed}_k(f)$ as $\mathrm{ed}_k(L/K)$, where $L = K[x]/(f(x))$. Note that if $f(x)$ (or equivalently, L) is separable over K, then L descends to K_0 if and only if there exists an element $\bar{y} \in L$ which generates L as an K-algebra and such that the minimal polynomial $g(y) = y^n + b_1 y^{n-1} + \cdots + b_n$ of $\bar{y}$ lies in $K_0[y]$.

In classical language, the passage from $f(x)$ to $g(y)$ is called a Tschirnhaus transformation. Note that

$$\bar{y} = c_0 + c_1 \bar{x} + \cdots + c_{n-1} \bar{x}^{n-1} \tag{4}$$

for some $c_0, c_1, \dots, c_{n-1} \in K$. Here $\bar{x} \in L$ is x modulo $(f(x))$. Tschirnhaus' strategy for solving polynomial equations in radicals by induction on degree was to transform $f(x)$ to a simpler polynomial $g(y)$, find a root of $g(y)$ and then recover a root of $f(x)$ from (4) by solving a polynomial equation of degree $\leqslant n - 1$. In his 1683 paper [62], Tschirnhaus successfully implemented this strategy for $n = 3$ but made a mistake in implementing it for higher n. Tschirnhaus did not know that a general polynomial of degree $\geqslant 5$ cannot be solved in radicals or that his method for solving cubic polynomials had been discovered by Cardano a century earlier.

Let us denote the maximal value of $\mathrm{ed}(f)$ taken over all field extensions K/k and all separable polynomials $f(x) \in K[x]$ of degree n by $\mathrm{ed}_k(n)$. Kronecker [38] and Klein [35] showed that

$$\mathrm{ed}_{\mathbb{C}}(5) = 2. \tag{5}$$

This classical result is strengthened in [14] as follows.

Theorem 1. *Assume* $\mathrm{char}(k) \neq 2$. *Then* $\mathrm{ed}_k(1) = 0$,

$$\mathrm{ed}_k(2) = \mathrm{ed}_k(3) = 1, \quad \mathrm{ed}_k(4) = \mathrm{ed}_k(5) = 2, \quad \mathrm{ed}_k(6) = 3$$

and $\mathrm{ed}_k(n+2) \geqslant \mathrm{ed}_k(n) + 1$ *for every* $n \geqslant 1$. *In particular,*

$$\left\lfloor \frac{n}{2} \right\rfloor \leqslant \mathrm{ed}_k(n) \leqslant n - 3 \tag{6}$$

for every $n \geqslant 5$.

[2] The term "essential dimension" was coined by Joe Buhler. The term "resolvent degree" was introduced by Richard Brauer in [8].

[3] Procesi asked about the minimal number of independent parameters required to define a generic division algebra of degree n. In modern terminology, this number is the essential dimension of the projective linear group PGL_n.

[4] Kawamata defined an invariant $\mathrm{Var}(f)$ of an algebraic fiber space $f\colon X \to S$, which he informally described as "the number of moduli of fibers of f in the sense of birational geometry". In modern terminology, $\mathrm{Var}(f)$ is the essential dimension of f.

I recently learned that a variant of the inequality $\mathrm{ed}_{\mathbb{C}}(n) \geqslant \lfloor \frac{n}{2} \rfloor$ was known to Chebotarev [15] as far back as 1943.

The problem of finding the exact value of $\mathrm{ed}(n)$ may be viewed as being analogous to Hilbert's 13th problem with $\mathrm{rd}(n)$, $\mathrm{crd}(n)$ or $\mathrm{Crd}(n)$ replaced by $\mathrm{ed}(n)$. Since Hilbert specifically asked about $\mathrm{rd}(7)$, the case where $n = 7$ is of particular interest.

Theorem 2 (Duncan [23]). *If* $\mathrm{char}(k) = 0$, *then* $\mathrm{ed}_k(7) = 4$.

The proof of Theorem 2 relies on the same general strategy as Klein's proof of (5); I will discuss it further it in Section 6. Combining Theorem 2 with the inequality $\mathrm{ed}_k(n+2) \geqslant \mathrm{ed}_k(n) + 1$ from Theorem 1, we can slightly strengthen (6) in characteristic 0 as follows:

$$\Big\lfloor \frac{n+1}{2} \Big\rfloor \leqslant \mathrm{ed}(n) \leqslant n-3 \quad \text{for every } n \geqslant 7. \tag{7}$$

Beyond (7), nothing is known about $\mathrm{ed}_{\mathbb{C}}(n)$ for any $n \geqslant 8$. I will explain where I think the difficulty lies in Section 5.

Analogous questions can be asked about polynomials that are not separable, assuming $\mathrm{char}(k) = p > 0$. In this setting, the role of the degree is played by the "generalized degree" $(n, \mathbf{e})$. Here $n = [S : K]$, where S is the separable closure of K in $L = K[x]/(f(x))$ and $\mathbf{e} = (e_1, \dots, e_r)$ is the so-called type of the purely inseparable algebra L/S defined as follows. Given $x \in L$, let us define the exponent $\exp(x, S)$ to be the smallest integer e such that $x^{p^e} \in S$. Then e_1 is the largest value of $\exp(x, S)$ as x ranges over L. Choose an $x_1 \in L$ of exponent e_1, and define e_2 as the largest value of $\exp(x, S[x_1])$. Now choose $x_2 \in L$ of exponent e_2, and define e_3 as the largest value of $\exp(x, S[x_1, x_2])$, etc. We stop when $S[x_1, \dots, x_r] = L$. By a theorem of Pickert, the resulting integer sequence $e_1, \dots, e_r$ satisfies $e_1 \geqslant \dots \geqslant e_r \geqslant 1$ and does not depend on the choice of the elements $x_1, \dots, x_r$. One can now define $\mathrm{ed}_k(n, \mathbf{e})$ by analogy with $\mathrm{ed}_k(n)$: $\mathrm{ed}_k(n, \mathbf{e})$ is the maximal value of $\mathrm{ed}_k(f)$, as K ranges over all field extension of k and $f(x) \in K[x]$ ranges over all polynomials of generalized degree $(n, \mathbf{e})$. Surprisingly, the case where $\mathbf{e} \neq \emptyset$ (i.e., the polynomials $f(x)$ in question are not separable) turns out to be easier. We refer the reader to [53], where an exact formula for $\mathrm{ed}(n, \mathbf{e})$ is obtained.

3 Essential dimension of a functor

Following Merkurjev [6], we will now define essential dimension for a broader class of objects, beyond polynomials or finite-dimensional algebras. Let k be a base field, which we assume to be fixed throughout, and $\mathcal{F}$ be a covariant functor from the category of field extensions K/k to the category of sets. Any object $\alpha \in \mathcal{F}(K)$ in the image of the natural ("base change") map $\mathcal{F}(K_0) \to \mathcal{F}(K)$ is said to *descend* to K_0. The essential dimension $\mathrm{ed}_k(\alpha)$ is defined as the minimal value of $\mathrm{trdeg}_k(K_0)$, where the minimum is taken over all intermediate fields $k \subset K_0 \subset K$ such that α descends to K_0.

For example, consider the functor Ass_n of n-dimensional associative algebras given by

$$\mathrm{Ass}_n(K) = \{n\text{-dimensional associative } K\text{-algebras, up to } K\text{-isomorphism}\}.$$

For $A \in \mathrm{Ass}_n(K)$, the new definition of $\mathrm{ed}_k(A)$ is the same as the definition in the previous section. Recall that, after choosing a K-basis for A, we can describe A completely in terms of the n^3 structure constants c_{ij}^h. In particular, A descends to the subfield $K_0 = k(c_{ij}^h)$ of K, and consequently, $\mathrm{ed}_k(A) \leqslant n^3$.

Another interesting example is the functor of non-degenerate n-dimensional quadratic forms,

$$\mathrm{Quad}_n(K) = \{\text{non-degenerate quadratic forms on } K^n, \text{ up to } K\text{-isomorphism}\}.$$

For simplicity, let us assume that the base field k is of characteristic different from 2. Under this assumption, a quadratic form q on K^n is the same thing as a symmetric bilinear form b. One passes back and forth between q and b using the formulas

$$q(v) = b(v, v) \quad \text{and} \quad b(v, w) = \frac{q(v+w) - q(v) - q(w)}{2}$$

for any $v, w \in K^n$. The form q (or equivalently, b) is called degenerate if the linear form $b(v, *)$ is identically zero for some $0 \neq v \in K^n$. A variant of the Gram–Schmidt process shows that there exists an orthogonal basis of K^n with respect to b. In other words, in some basis $e_1, \dots, e_n$ of K^n, q can be written as

$$q(x_1 e_1 + \dots + x_n e_n) = a_1 x_1^2 + \dots + a_n x_n^2$$

for some $a_1, \dots, a_n$ in K. In particular, we have that q descends to $K_0 = k(a_1, \dots, a_n)$, and thus $\mathrm{ed}_k(q) \leqslant n$. Note that q is non-degenerate if and only if $a_1, \dots, a_n \neq 0$.

Yet another interesting example is provided by the functor of elliptic curves,

$$\mathrm{Ell}(K) = \{\text{elliptic curves over } K, \text{ up to } K\text{-isomorphism}\}.$$

For simplicity, assume that $\mathrm{char}(k) \neq 2$ or 3. Then every elliptic curve X over K is isomorphic to the plane curve cut out by a Weierstrass equation $y^2 = x^3 + ax + b$ for some $a, b \in K$. Hence, X descends to $K_0 = k(a, b)$ and $\mathrm{ed}(X) \leqslant 2$.

Informally, we think of $\mathcal{F}$ as specifying the type of algebraic object under consideration (e.g., algebras or quadratic forms or elliptic curves), $\mathcal{F}(K)$ as the set of objects of this type defined over K, and $\mathrm{ed}_k(\alpha)$ as the minimal number of parameters required to define α. In most cases, essential dimension varies from object to object, and it is natural to consider what happens under a "worst case scenario", i.e., how many parameters are needed to define the most general object of a given type. This number is called the essential dimension of the functor $\mathcal{F}$. That is,

$$\mathrm{ed}_k(\mathcal{F}) = \sup_{K, \alpha} \mathrm{ed}_k(\alpha),$$

as K varies over all fields containing k and a varies over $\mathcal{F}(K)$. Note that $\mathrm{ed}_k(\mathcal{F})$ can be either a non-negative integer or ∞. In particular, the arguments above yield

$$\mathrm{ed}(\mathrm{Ass}_n) \leqslant n^3, \quad \mathrm{ed}(\mathrm{Quad}_n) \leqslant n \quad \text{and} \quad \mathrm{ed}(\mathrm{Ell}) \leqslant 2.$$

One can show that the last two of these inequalities are, in fact, sharp. The exact value of $\mathrm{ed}(\mathrm{Ass}_n)$ is unknown for most n; however, for large n,

$$\mathrm{ed}(\mathrm{Ass}_n) = 4n^3/27 + O(n^{8/3}).$$

Similarly,

$$\mathrm{ed}(\mathrm{Lie}_n) = 2n^3/27 + O(n^{8/3}),$$
$$\mathrm{ed}(\mathrm{Comm}_n) = 2n^3/27 + O(n^{8/3}),$$

where Lie_n and Comm_n are the functors of n-dimensional Lie algebras and commutative algebras, respectively. These formulas are deduced from the formulas for the dimensions of the varieties of structure constants for n-dimensional associative, Lie and commutative algebras due to Neretin [44].[5]

This brings us to the functor $H^1(*, G)$, where G is an algebraic group defined over k. The essential dimension of this functor is a numerical invariant of G. This invariant has been extensively studied; it will be our main focus in the next section. The functor $H^1(*, G)$ associates to a field K/k, the set $H^1(K, G)$ of isomorphism classes of G-torsors T over K. Recall that a G-torsor over T over K is an algebraic variety with a G-action defined over K such that, over the algebraic closure $\overline{K}$, T becomes equivariantly isomorphic to G acting on itself by left translations. If T has a K-point x, then $G \to T$ taking g to $g \cdot x$ is, in fact, an isomorphism over K. In this case, the torsor T is called “trivial” or “split”. The interesting (non-trivial) torsors over K have no K-points. For example, if $G = C_2$ is a cyclic group of order 2 and $\mathrm{char}(k) \neq 2$, then every C_2-torsor is of the form T_a, where T_a is the subvariety of $\mathbb{A}^1$ cut out by the quadratic equation $x^2 - a = 0$ for some $a \in K$. Informally, T_a is a pair of points (roots of this equation) permuted by C_2; it is split if and only if these points are defined over K (i.e., a is a complete square in K). In fact, $H^1(K, C_2)$ is in bijective correspondence with $K^*/(K^*)^2$ given by $T_a \mapsto a \bmod (K^*)^2$, where K^* is the multiplicative group of K. Note that, in this example, $H^1(K, G)$ is, in fact, a group. This is the case whenever G is abelian. For a non-abelian algebraic group G, $H^1(K, G)$ carries no natural group structure; it is only a set with a marked element (the trivial torsor).

For many linear algebraic groups G, the functor $H^1(*, G)$ parametrizes interesting algebraic objects. For example, when G is the orthogonal group O_n, $H^1(*, \mathrm{O}_n)$ is the functor Quad_n we considered above. When G is the projective linear group PGL_n, $H^1(K, \mathrm{PGL}_n)$ is the set of isomorphism classes of central simple algebras of degree n over K. When G is the exceptional group of type G_2, $H^1(K, G_2)$ is the set of isomorphism classes of octonion algebras over K.

4 Essential dimension of an algebraic group

The essential dimension of the functor $H^1(*, G)$ is abbreviated as $\mathrm{ed}_k(G)$. Here G is an algebraic group defined over k. This number is always finite if G is linear but may be infinite if G is an abelian variety [12]. If G is the symmetric group S_n, then

$$\mathrm{ed}_k(\mathrm{S}_n) = \mathrm{ed}_k(n), \tag{8}$$

where $\mathrm{ed}_k(n)$ is the quantity we defined and studied in Section 2. Indeed, $H^1(K, \mathrm{S}_n)$ is the set of étale algebras L/K of degree n. Étale algebras of degree n are precisely the algebras of the form $K[x]/(f(x))$, where $f(x)$ is a separable (but not necessarily irreducible) polynomial of degree n over K. Thus (8) is just a restatement of the definition of $\mathrm{ed}_k(n)$.

Another interesting example is the general linear group $G = \mathrm{GL}_n$. Elements of $H^1(K, \mathrm{GL}_n)$ are the n-dimensional vector spaces over K. Since there is only one n-dimensional K-vector space up to K-isomorphism, we see that $H^1(K, \mathrm{GL}_n) = \{1\}$. In particular, every object of $H^1(K, \mathrm{GL}_n)$ descends to k, and we conclude that $\mathrm{ed}_k(\mathrm{GL}_n) = 0$. I will now give a brief summary of three methods for proving lower bounds on $\mathrm{ed}_k(G)$ for various linear algebraic groups G.

4.1 Cohomological invariants

Let $\mathcal{F}$ be a covariant functor from the category of field extensions K/k to the category of sets, as in the previous section. A cohomological invariant of degree d for $\mathcal{F}$ is a morphism of functors

$$\mathcal{F} \to H^d(*, M)$$

for some discrete $\mathrm{Gal}(k)$-module M. In many interesting examples, $M = \mu_m$ is the module of mth roots of unity with a natural $\mathrm{Gal}(k)$-action (trivial if k contains a primitive m-th root of unity). The following observation is due to J.-P. Serre.

Theorem 3. *Assume that the base field k is algebraically closed. If $\mathcal{F}$ has a non-trivial cohomological invariant $\mathcal{F} \to H^d(*, M)$, then $\mathrm{ed}_k(\mathcal{F}) \geqslant d$.*

The proof is an immediate consequence of the Serre vanishing theorem. Cohomological invariants of an algebraic group G (or equivalently, of the functor $H^1(*, G)$) were introduced by Serre and Rost in the early 1990s, and have been extensively studied since then; see [57]. These invariants give rise to a number of interesting

[5] Note the resemblance of these asymptotic formulas to the classical theorem of Higman and Sims, which assert that the number of finite p-groups of order p^n (up to isomorphism) is asymptotically $p^{2n^3/27+O(n^{8/3})}$. This is not an accident; see [45].

lower bounds on $\mathrm{ed}_k(G)$ for various groups G; in particular,

(i) $\mathrm{ed}(\mathrm{O}_n) \geqslant n$,
(ii) $\mathrm{ed}(\mathrm{SO}_n) \geqslant n-1$ for every $n \geqslant 3$,
(iii) $\mathrm{ed}(G_2) \geqslant 3$,
(iv) $\mathrm{ed}(F_4) \geqslant 5$,
(v) $\mathrm{ed}(\mathrm{S}_n) \geqslant \lfloor \frac{n}{2} \rfloor$.

Inequalities (i), (ii) and (iii) turn out to be exact; (iv) is best known, and (v) is best known for even n; see (7).

4.2 Finite abelian subgroups

Theorem 4. *Let G be a reductive group over k and A be a finite abelian subgroup of G of rank r.*

(a) [55] *Assume* $\mathrm{char}(k) = 0$*. If the centralizer $C_G(A)$ is finite, then* $\mathrm{ed}(G) \geqslant r$.
(b) [29] *Assume* $\mathrm{char}(k)$ *does not divide $|A|$. If G is connected and the dimension of the maximal torus of $C_G(A)$ is d, then* $\mathrm{ed}(G) \geqslant r-d$.

Note that both parts are vacuous if A lies in a maximal torus T of G. Indeed, in this case, the centralizer $C_G(A)$ contains T, so $d \geqslant r$. In other words, only non-toral finite abelian subgroups A of linear algebraic groups are of interest here. These have been much studied and catalogued, starting with the work of Borel in the 1950s. Theorem 4 yields the best known lower bound on $\mathrm{ed}(G)$ in many cases, such as $\mathrm{ed}(E_7) \geqslant 7$ and $\mathrm{ed}(E_8) \geqslant 9$, where E_7 denotes the split simply connected exceptional group of type E_7 and similarly for E_8.

4.3 The Brauer class bound

Consider a linear algebraic group G defined over our base field k. Suppose G fits into a central exact sequence of algebraic groups (again, defined over k)

$$1 \to D \to G \to \overline{G} \to 1,$$

where D is diagonalizable over k. For every field extension K/k, this sequence gives rise to the exact sequence of pointed sets

$$H^1(K,G) \to H^1(K,\overline{G}) \overset{\partial}{\to} H^2(K,D).$$

Every element $\alpha \in H^2(K,D)$ has an index, $\mathrm{ind}(\alpha)$, defined as follows. If $D \simeq \mathbb{G}_m$, then α is a Brauer class over K, and $\mathrm{ind}(\alpha)$ denotes the Schur index of α, as usual. In general, we consider the character group $X(D)$ whose elements are homomorphisms $x\colon D \to \mathbb{G}_m$. Note that $X(D)$ is a finitely generated abelian group and each character $x \in X(D)$ induces a homomorphism

$$x_*\colon H^2(K,D) \to H^2(K,\mathbb{G}_m).$$

The index of $\alpha \in H^2(K,D)$ is defined as the minimal value of

$$\mathrm{ind}(x_1)_*(\alpha) + \cdots + \mathrm{ind}(x_r)_*(\alpha)$$

as $\{x_1, \ldots, x_r\}$ ranges over generating sets of $X(D)$. Here each $(x_i)_*(\alpha)$ lies in $H^1(K,\mathbb{G}_m)$, and $\mathrm{ind}(x_i)_*(\alpha)$ denotes its Schur index, as above. We now define $\mathrm{ind}(G,D)$ as the maximal index of $\alpha \in \partial(H^1(K,\overline{G})) \subset H^2(K,D)$, where the maximum is taken over all field extensions K/k, as α ranges over the image $H^1(K,\overline{G})$ in $H^2(K,D)$.

Theorem 5.

(a) $\mathrm{ind}(G,D)$ *is the greatest common divisor of* $\dim(\rho)$*, where ρ ranges over the linear representations of G over k such that the restriction $\rho_{|D}$ is faithful.*
(b) *Let p be a prime different from* $\mathrm{char}(k)$*. Assume that the exponent of every element of $H^2(K,D)$ in the image of*

$$\partial\colon H^1(K,\overline{G}) \to H^2(K,D)$$

is a power of p for every field extension K/k. (This is automatic if D is a p-group.) Then $\mathrm{ed}_k(G) \geqslant \mathrm{ind}(G,D) - \dim(G)$.

Part (a) is known as Merkurjev's index formula. The inequality of part (b) is based on Karpenko's incompressibility theorem. Part (b) first appeared in [9] in the special case where $D = \mathbb{G}_m$ or μ_{p^r} and in [26] in an even more special case, where $D = \mu_p$. It was proved in full generality in [33].

Theorem 5 is responsible for some of the strongest results in this theory, including the exact formulas for the essential dimension of a finite p-group (Theorem 6 below), the essential p-dimension of an algebraic torus, and the essential dimension of spinor groups Spin_n. The latter turned out to increase exponentially in n:

$$\mathrm{ed}(\mathrm{Spin}_n) \geqslant 2^{\lfloor (n-1)/2 \rfloor} - \frac{n(n-1)}{2}. \tag{9}$$

This inequality was first proved in [9]. The exact value of $\mathrm{ed}(\mathrm{Spin}_n)$ subsequently got pinned down in [10, 18] in characteristic 0, [28] in characteristic $p \neq 2$ and [61] in characteristic 2. When $n \geqslant 15$, inequality (9) is sharp for $n \not\equiv 0$ modulo 4, and is off by $2^{v_2(n)}$ otherwise. Here $2^{v_2(n)}$ is the largest power of 2 dividing n.

The exponential growth of $\mathrm{ed}(\mathrm{Spin}_n)$ came as a surprise. Prior to [9], the best known lower bounds on $\mathrm{ed}(\mathrm{Spin}_n)$ were linear (see [19, Section 7]), on the order of $\frac{n}{2}$. Moreover, the exact values of $\mathrm{ed}(\mathrm{Spin}_n)$ for $n \leqslant 14$ obtained by Rost and Garibaldi [27] appeared to suggest that these linear bounds should be sharp. The fact that $\mathrm{ed}(\mathrm{Spin}_n)$ increases exponentially in n has found interesting applications in the theory of quadratic forms. For details, see [10, 18].

5 Essential dimension at p

Once again, fix a base field k, and let $\mathcal{F}$ be a covariant functor from the category of field extensions K/k to the category of sets. The essential dimension $\mathrm{ed}_k(\alpha; p)$ of an object $\alpha \in \mathcal{F}(K)$ at a prime p

is defined as the minimal value of $\mathrm{ed}_k(\alpha'; p)$, where the minimum ranges over all finite field extensions K'/K of degree prime to p and α' denotes the image of α under the natural map $\mathcal{F}(K) \to \mathcal{F}(K')$. Finally, the essential dimension $\mathrm{ed}_k(\mathcal{F}; p)$ of $\mathcal{F}$ at p is the maximal value of $\mathrm{ed}_k(\alpha)$, as K ranges over all fields containing k and α ranges over $\mathcal{F}(K)$. When $\mathcal{F} = H^1(*, G)$ for an algebraic group G, we write $\mathrm{ed}_k(G; p)$ in place of $\mathrm{ed}_k(\mathcal{F}; p)$. Once again, if the reference to the base field is clear from the context, we will abbreviate ed_k as ed. By definition, $\mathrm{ed}(\alpha; p) \leqslant \mathrm{ed}(\alpha)$ and $\mathrm{ed}(\mathcal{F}; p) \leqslant \mathrm{ed}(\mathcal{F})$.

The reason to consider $\mathrm{ed}(\mathcal{F}; p)$ in place of $\mathrm{ed}(\mathcal{F})$ is that the former is often more accessible. In fact, most of the methods we have for proving a lower bound on $\mathrm{ed}_k(\alpha)$ (respectively, $\mathrm{ed}_k(\mathcal{F})$) turn out to produce a lower bound on $\mathrm{ed}_k(\alpha; p)$ (respectively, $\mathrm{ed}_k(\mathcal{F}; p)$) for some prime p. For example, the lower bound in Theorem 5 (b) is really $\mathrm{ed}_k(G; p) \geqslant \mathrm{ind}(G, D) - \dim(G)$. In Theorem 4, one can usually choose A to be a p-group, in which case the conclusion can be strengthened to $\mathrm{ed}(G; p) \geqslant r$ in part (a) and $\mathrm{ed}(G; p) \geqslant r - d$ in part (b). In Theorem 3, if M is p-torsion (which can often be arranged), then $\mathrm{ed}(G; p) \geqslant d$.

This is a special case of a general meta-mathematical phenomenon: many problems concerning algebraic objects (such as finite-dimensional algebras or polynomials or algebraic varieties) over fields K can be subdivided into two types. In type 1 problems, we are allowed to pass from K to a finite extension K'/K of degree prime to p, for one prime p, whereas in type 2 problems this is not allowed. For example, given an algebraic variety X defined over K, deciding whether or not X has a 0-cycle of degree 1 is a type 1 problem (it is equivalent to showing that there is a 0-cycle of degree prime to p, for every prime p), whereas deciding whether or not X has a K-point is a type 2 problem. As I observed in [51, Section 5], most of the technical tools we have are tailor-made for type 1 problems, whereas many long-standing open questions across several areas of algebra and algebraic geometry are of type 2.

In the context of essential dimension, the problem of computing $\mathrm{ed}(G; p)$ for a given algebraic group G and a given prime p is of type 1, whereas the problem of computing $\mathrm{ed}(G)$ is of type 2. For simplicity, let us assume that G is a finite group. In this case, $\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G_p; p)$, where G_p is the Sylow p-subgroup of G. In other words, the problem of computing $\mathrm{ed}_k(G; p)$ reduces to the case where G is a p-group. In this case, we have the following remarkable theorem of Karpenko and Merkurjev [32].

Theorem 6. *Let p be a prime and k be a field containing a primitive pth root of unity. Then, for any finite p-group P,*

$$\mathrm{ed}_k(P) = \mathrm{ed}_k(P; p) = \mathrm{rdim}_k(P),$$

where $\mathrm{rdim}_k(P)$ *denotes the minimal dimension of a faithful representation of P defined over k.*

Theorem 6 reduces the computation of $\mathrm{ed}_k(G; p)$ to $\mathrm{rdim}_k(G_p)$. For a given finite p-group P, one can often (though not always) compute $\mathrm{rdim}_k(P)$ in closed form using the machinery of character theory; see, e.g., [3, 36, 42, 43].

The situation is quite different when computing $\mathrm{ed}_k(G)$ for an arbitrary finite group G. Clearly, $\mathrm{ed}_k(G) \geqslant \max_p \mathrm{ed}_k(G; p)$, where p ranges over the prime integers. In those cases, where $\mathrm{ed}_k(G)$ is strictly larger than $\max_p \mathrm{ed}_k(G; p)$, the exact value of $\mathrm{ed}_k(G)$ is usually difficult to establish. The only approach that has been successful to date relies on classification results in algebraic geometry, which are currently only available in low dimensions. I will return to this topic in the next section.

To illustrate the distinction between type 1 and type 2 problems, consider the symmetric group $G = \mathrm{S}_n$. For simplicity, assume that $k = \mathbb{C}$ is the field of complex numbers. Here the type 1 problem is solved completely: $\mathrm{ed}_{\mathbb{C}}(\mathrm{S}_n; p) = \lfloor \frac{n}{p} \rfloor$ for every prime p. Thus $\max_p \mathrm{ed}_{\mathbb{C}}(\mathrm{S}_n; p) = \lfloor \frac{n}{2} \rfloor$, and (7) tells us that

$$\mathrm{ed}_{\mathbb{C}}(\mathrm{S}_n) > \max_p \mathrm{ed}_{\mathbb{C}}(G; p) \quad \text{for every odd } n \geqslant 7.$$

The remaining type 2 problem is to bridge the gap between $\lfloor \frac{n}{2} \rfloor$ and the true value of $\mathrm{ed}_{\mathbb{C}}(\mathrm{S}_n)$. This problem has only been solved for $n \leqslant 7$; see Theorems 1, 2 and (8).

Note that the algebraic form of Hilbert's 13th problem is also of type 2 in the sense that

$$\mathrm{rd}(f; p) \leqslant 1 \tag{10}$$

for any prime p, every field K and every separable polynomial $f(x) \in K[x]$.[6] Indeed, denote the Galois group of $f(x)$ by G. Then, after passing from K to a finite extension K'/K whose degree $[K' : K] = [G : G_p]$ is prime to p, we may replace G by its p-Sylow subgroup G_p. Since every p-group is solvable, this means that $f(x)$ becomes solvable in radicals over K', and hence its resolvent degree becomes $\leqslant 1$, as desired.

Inequality (10) accounts, at least in part, for the difficulty of showing that $\mathrm{rd}(n) \geqslant 2$ for any n. The methods used to prove lower bounds on the essential dimension of algebraic groups in Section 4, and anything resembling these methods, cannot possibly work here; otherwise, we would also be able to prove that $\mathrm{rd}(f; p) \geqslant 2$ for some prime p, contradicting (10).

A similar situation arises in computing the essential dimension of a finite p-group G over a field k of characteristic p. Superficially this problem looks very different from Hilbert's 13th problem (where one usually works over $k = \mathbb{C}$); the common feature is that both are type 2 problems. Indeed, it is shown in [54] that $\mathrm{ed}_k(G; p) = 1$ for every non-trivial p-group G. Using the method described in the next section, one can often show that $\mathrm{ed}_k(G) \geqslant 2$, but we are not able to prove that $\mathrm{ed}_k(G) > 2$ for any p-group G and any field k of characteristic p. On the other hand, Ledet [39]

[6] For the precise definitions of $\mathrm{rd}(f)$ and $\mathrm{rd}(f; p)$, see Section 8.

conjectured that

$$\mathrm{ed}_k(C_{p^n}) = n \tag{11}$$

for any prime p and any infinite field k of characteristic p. Here C_{p^n} denotes the cyclic group of order p^n. Ledet showed that $\mathrm{ed}_k(C_{p^n}) \leqslant n$ for every $n \geqslant 1$ and that equality holds when $n \leqslant 2$.

My general feeling is that type 2 problems arising in different contexts are linked in some way, and that solving one of them (e.g., proving Ledet's conjecture) can shed light on the others (e.g., Hilbert's 13th problem). The only bit of evidence I have in this direction is the following theorem from [11] linking a priori unrelated type 2 problems in characteristic p and in characteristic 0.

Theorem 7. *Let p be a prime and G be a finite group satisfying the following conditions:*

(i) *G does not have a non-trivial normal p-subgroup, and*

(ii) *G has an element of order p^n.*

If Ledet's conjecture (11) *holds, then* $\mathrm{ed}_{\mathbb{C}}(G) \geqslant n$.

The following family of examples is particularly striking. Let p be a prime and n a positive integer. Choose a positive integer m such that $q = mp^n + 1$ is a prime. Note that, by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many such m. Let C_q be a cyclic group of order q. Then $\mathrm{Aut}(C_q)$ is cyclic of order mp^n; let $C_{p^n} \subseteq \mathrm{Aut}(C_q)$ denote the unique subgroup of order p^n. Applying Theorem 7 to $G = C_q \rtimes C_{p^n}$, we obtain the following.

Corollary 8. *If Ledet's conjecture* (11) *holds, then*

$$\mathrm{ed}_{\mathbb{C}}(C_q \rtimes C_{p^n}) \geqslant n.$$

Note that, since the Sylow subgroups of $C_q \rtimes C_{p^n}$ are all cyclic,

$$\mathrm{ed}_{\mathbb{C}}(C_q \rtimes C_{p^n}; l) \leqslant 1$$

for every prime l, so the inequality of Corollary 8 is a type 2 result. An unconditional proof of this inequality or even of the weaker inequality $\mathrm{ed}_{\mathbb{C}}(C_q \rtimes C_{p^n}) > 3$ is currently out of reach for any specific choice of q and p^n.

6 Essential dimension and the Jordan property

An alternative (equivalent) definition of essential dimension of a finite group G is as follows. An action of G on an algebraic variety X is said to be linearizable if there exists a G-equivariant dominant rational map $V \dashrightarrow X$ for some linear representation $G \to \mathrm{GL}(V)$. Then $\mathrm{ed}_k(G)$ is the minimal value of $\dim(X)$, as X ranges over all linearizable varieties with a faithful G-action defined over k. In particular, $\mathrm{ed}_k(G) \leqslant \mathrm{rdim}_k(G)$, where $\mathrm{rdim}_k(G)$ is the minimal dimension of a faithful linear representation of G over k, as in Theorem 6.

This geometric interpretation of $\mathrm{ed}_k(G)$ can sometimes be used to prove lower bounds on $\mathrm{ed}(G)$ by narrowing the possibilities for X and ruling them out one by one using Theorem 4 (a). For the remainder of this section, I will assume that G is a finite group and the base field k is the field of complex numbers and will write ed in place of $\mathrm{ed}_{\mathbb{C}}$.

Suppose $\mathrm{ed}(G) = 0$. Then X is a single point, and only the trivial group can act faithfully on a point. Thus $\mathrm{ed}(G) = 0$ if and only if G is the trivial group.

Now suppose $\mathrm{ed}(G) = 1$. Then X is a curve with a dominant map $V \dashrightarrow X$. By Lüroth's theorem, X is birationally isomorphic to $\mathbb{P}^1$ and thus G is a subgroup of PGL_2. Finite subgroups of PGL_2 were classified by Klein [35]. Here is a complete list: cyclic groups C_n and dihedral groups D_n for every n, A_4, S_4 and A_5. Theorem 4 (a) rules out the groups on this list which contain $A = C_2 \times C_2$. We thus obtain the following.

Theorem 9 ([14, Theorem 6.2])**.** *Let G be a finite group. Then* $\mathrm{ed}(G) = 1$ *if and only if G is either cyclic or odd dihedral.*

To classify groups of essential dimension d (or more realistically, show that $\mathrm{ed}(G) > d$ for a particular finite group G) in a similar manner, we need a classification of finite subgroups of $\mathrm{Bir}(X)$, extending Klein's classification of finite subgroups in $\mathrm{Bir}(\mathbb{P}^1)$. Here X ranges over the unirational complex varieties of dimension d, and $\mathrm{Bir}(X)$ denotes the groups of birational automorphisms of X. In dimension 2, every unirational variety is rational, so we are talking about classifying finite subgroups of the Cremona group $\mathrm{Bir}(\mathbb{P}^2)$. Such a classification exists, though it is rather complicated; see [22]. Serre used this approach to show that $\mathrm{ed}(\mathrm{A}_6) = 3$ (see [59, Theorem 3.6]). Again, this is a type 2 phenomenon since $\max_p \mathrm{ed}(\mathrm{A}_6; p) = 2$. Duncan [24] subsequently extended Serre's argument to a full classification of finite groups of essential dimension 2.

In dimension 3, there is the additional complication that unirational complex varieties do not need to be rational. Here only a partial analogue of Klein's classification exists, namely the classification of rationally connected 3-folds with the action of a finite simple group G, due to Prokhorov [49]. Duncan used this classification to prove Theorem 2. More specifically, he showed that $\mathrm{ed}(\mathrm{S}_7) = \mathrm{ed}(\mathrm{A}_7) = 4$; see (8). Subsequently, Beauville [4] showed that the only finite simple groups of essential dimension 3 are A_6 and possibly $\mathrm{PSL}_2(\mathbb{F}_{11})$.[7]

In dimension $d \geqslant 4$, even a partial analogue of Klein's classification of finite subgroups of $\mathrm{Bir}(\mathbb{P}^1)$ is out of reach. However, a recent break-through in Mori theory gives us a new insight into the asymptotic behavior of $\mathrm{ed}(G_n)$ for certain infinite sequences $G_1, G_2, \ldots$ of finite groups. Recall that an abstract group Γ is called *Jordan* if there exists an integer j (called a Jordan constant of Γ) such that every finite subgroup $G \subset \Gamma$ has a normal abelian sub-

[7] It is not known whether the essential dimension of $\mathrm{PSL}_2(\mathbb{F}_{11})$ is 3 or 4.

group A of index $[G : A] \leqslant j$. This definition, due to Popov [46], was motivated by the classical theorem of Camille Jordan which asserts that $\mathrm{GL}_n(\mathbb{C})$ is Jordan, and by a theorem of Serre [58] which asserts that the Cremona group $\mathrm{Bir}(\mathbb{P}^2)$ is also Jordan. The following result, due to Prokhorov, Shramov and Birkar[8], is a far-reaching generalization of Serre's theorem.

I will say that a collection of abstract groups is uniformly Jordan if they are all Jordan with the same constant.

Theorem 10. *Fix $d \geqslant 1$. Then the groups $\mathrm{Bir}(X)$ are uniformly Jordan, as X ranges over d-dimensional rationally connected complex varieties.*

Unirational varieties are rationally connected. The converse is not known, though it is generally believed to be false. Rationally connected varieties naturally arise in the context of Mori theory, and we are forced to consider them even if we are only really interested in unirational varieties. Note that Theorem 10 does not become any easier to prove if one requires X to be unirational. In fact, prior to Birkar [7] (respectively, prior to Prokhorov–Shramov [49]), it was an open question, due to Serre [58, Section 6], whether for each $d \geqslant 4$ (respectively, for $d = 3$) there exists even a single finite group which does not embed into $\mathrm{Bir}(\mathbb{P}^d)$.[9]

Now observe that, while every finite group is obviously Jordan, being uniformly Jordan is a strong condition on a sequence of finite groups

$$G_1, G_2, G_3, \dots. \tag{12}$$

Suppose sequence (12) is chosen so that no infinite subsequence is uniformly Jordan. Then we claim that

$$\lim_{n \to \infty} \mathrm{ed}(G_n) = \infty. \tag{13}$$

Indeed, if $\mathrm{ed}(G_n) = d$, then there exists a d-dimensional linearizable variety X with a faithful G_n-action. In particular, G_n is contained in $\mathrm{Bir}(X)$. Since X is linearizable, it is unirational and hence rationally connected. On the other hand, since no infinite subsequence of (12) is uniformly Jordan, Theorem 10 tells us that there are at most finitely many groups G_n with $\mathrm{ed}(G_n) = d$, and (13) follows. Here is an interesting family of examples.

Theorem 11. *For each positive integer n, let C_n be a cyclic group of order n and H_n be a subgroup of $\mathrm{Aut}(C_n)$. If $\lim_{n \to \infty} |H_n| = \infty$, then $\lim_{n \to \infty} \mathrm{ed}(C_n \rtimes H_n) = \infty$.*

Note that this method does not give us any information about $\mathrm{ed}(C_n \rtimes H_n)$ for any particular choice of n and of $H_n \subset \mathrm{Aut}(C_n)$. For example, while Theorem 11 tells us that

$$\mathrm{ed}_{\mathbb{C}}(C_p \rtimes \mathrm{Aut}(C_p)) > 10$$

for all but finitely many primes p, it does not allow us to exhibit a specific prime for which this inequality holds. The reason is that, when $d > 3$, a specific Jordan constant for the family of groups $\mathrm{Bir}(X)$ in Theorem 10 is out of reach. In particular, an unconditional proof of Corollary 8 along these lines does not appear feasible. Nevertheless, Theorem 11 represents a big step forward: previously, it was not even known that $\mathrm{ed}_{\mathbb{C}}((C_p) \rtimes \mathrm{Aut}(C_p)) > 3$ for any prime p.

A classification of the subgroups of $\mathrm{Bir}(X)$, as X ranges over the unirational varieties of dimension d is a rather blunt instrument. It would be preferable to find some topological or algebro-geometric obstruction to the existence of a linearization map $V \dashrightarrow X$, which can be read off from the G-variety X without enumerating all the possibilities for X. Unfortunately, all known obstructions of this sort are of type 1: they do not distinguish between dominant rational maps $V \dashrightarrow X$ and correspondences $V \rightsquigarrow X$ of degree prime to p, for a suitable prime p and thus cannot help us if $\mathrm{ed}(G) > \max_p \mathrm{ed}(G; p)$.

Another draw-back of this method is that, as we mentioned in the previous section, beyond dimension 1,[10] none of the classification theorems we need are available in prime characteristic.

7 Essential dimension of a representation

7.1 *Representations of finite groups in characteristic* 0

Let G be a finite group of exponent e, k be a field of characteristic 0, K/k be a field extension, $\rho : G \to \mathrm{GL}_n(K)$ be a representation of G, and $\chi : G \to K$ be the character of ρ. Can we realize ρ over k? In other words, is there a representation $\rho' : G \to \mathrm{GL}(k)$ such that ρ and ρ' are equivalent over K? A celebrated theorem of Richard Brauer asserts that the answer is "yes" as long as k contains a primitive root of unity of degree e. If it does not, there is a classical way to quantify how far ρ is from being definable over k via the Schur index, at least in the case where ρ is absolutely irreducible and the character value $\chi(g)$ lies in k for every $g \in G$. The Schur index of ρ is defined as the index of the envelope

$$\mathrm{Env}_k(\rho) := \mathrm{Span}_k\{\rho(g) \mid g \in G\} \subset \mathrm{Mat}_n(K)$$

which, under our assumptions on ρ, is a central simple algebra of degree n over k. The Schur index of ρ is equal to the minimal degree $[l : k]$ of a field extension l/k such that ρ can be realized over l.

[8] Prokhorov and Shramov [50] proved this theorem assuming the Borisov–Alexeev–Borisov (BAB) conjecture. The BAB conjecture was subsequently proved by Birkar [7].

[9] For the current status of Serre's questions from [58, Section 6], see [47, Section 3].

[10] Groups of essential dimension 1 have been classified over an arbitrary field k; see [20, 40]. Recall that Theorem 9 assumes that $k = \mathbb{C}$.

The essential dimension $\mathrm{ed}_k(\rho)$ gives us a different way to quantify how far ρ is from being definable over k. Here we do not need to assume that ρ is irreducible or that its character values lie in k. We simply think of ρ as an object of the functor

$$\mathrm{Rep}_G\colon K \mapsto \{K\text{-representations of } G, \text{ up to } K\text{-isomorphism}\}.$$

The naive upper bound on $\mathrm{ed}(\rho)$ is rn^2, where n is the dimension of ρ and r is the minimal number of generators of G. Indeed, if G is generated by r elements $g_1, \dots, g_r$ and $\rho(g_h)$ is the $n \times n$ matrix (a_{ij}^h), then ρ descends to the field

$$K_0 = k(a_{ij}^h \mid i, j = 1, \dots, n;\ h = 1, \dots, r)$$

of transcendence degree at most rn^2 over k. It is shown in [32] that, in fact, $\mathrm{ed}(\rho) \leqslant n^2/4$ and, moreover, $\mathrm{ed}(\mathrm{Rep}_G) \leqslant |G|/4$. We have also proved lower bounds on $\mathrm{ed}_k(\rho)$ in many cases (for details, see [32]). Note that these are quite delicate: by Brauer's theorem, $\mathrm{ed}_k(G) = 0$ as long as k contains suitable roots of unity.

7.2 Representations of finite groups in positive characteristic

Here the situation is entirely different.

Theorem 12 ([5, 32]). *Let G be a finite group, k be a field of characteristic $p > 0$ and G_p be the Sylow p-subgroup of G. Then*

$$\mathrm{ed}_k(\mathrm{Rep}_G) = \begin{cases} 0 & \text{if } G_p \text{ is cyclic,} \\ \infty & \text{otherwise.} \end{cases}$$

Note that, by a theorem of Higman, in characteristic p, G_p is cyclic if and only if the group algebra kG is of finite representation type, i.e., if and only if kG (or equivalently, G) has only finitely many indecomposable representations. Since kG is always of finite representation type in characteristic 0, we obtain the following.

Corollary 13. *Let G be a finite group and k be a field of arbitrary characteristic. Then*

- $\mathrm{ed}_k(\mathrm{Rep}_G) < \infty$ *if kG is of finite representation type, and*
- $\mathrm{ed}_k(\mathrm{Rep}_G) = \infty$ *otherwise.*

7.3 Representations of algebras

For simplicity, let us assume that the base field k is algebraically closed. A celebrated theorem of Drozd asserts that every finite-dimensional k-algebra A falls into one of three categories: (a) finite representation type, (b) tame and (c) wild.

Informally speaking, A is of tame representation type if, for every positive integer n, the n-dimensional indecomposable A-modules occur in (at most) a finite number of one-parameter families. On the other hand, A is of wild representation type if the representation theory of A contains that of the free k-algebra on two generators.

We can define the functor of representations Rep_A in the same way as before: to a field K/k, it associates isomorphism classes of finite-dimensional $A \otimes_k K$-modules. Corollary 13 tells us that, when $A = kG$ is a group ring, the essential dimension of the functor Rep_A distinguishes between algebras A of finite representation type and algebras of the other two types. It does not distinguish between tame and wild representations types since $\mathrm{ed}(\mathrm{Rep}_A) = \infty$ in both cases. Benson suggested that it may be possible to distinguish between these two types of algebras by considering the rate of growth of $r_A(n) = \mathrm{ed}(\mathrm{Rep}_A[n])$, where $\mathrm{Rep}_A[n](K)$ is the set of isomorphism classes of K-representations of A of dimension $\leqslant n$. This is confirmed by the following theorem of Scavia [56].

Theorem 14.

(a) *If A is of finite representation type, then $r_A(n)$ is bounded from above as $n \to \infty$.*

(b) *If A is tame, then there exists a constant $c > 0$ such that $cn - 1 \leqslant r_A(n) \leqslant 2n - 1$ for every $n \geqslant 1$.*

(c) *If A is wild, then there exist constants $0 < c_1 < c_2$ such that $c_1 n^2 - 1 \leqslant r_A(n) \leqslant c_2 n^2$ for every $n \geqslant 1$.*

This gives us three new invariants of finite-dimensional algebras, $a_i(A) = \limsup_{n\to\infty} r_A(n)/n^i$ for $i = 0, 1, 2$. Informally, $a_2(A)$ (respectively, $a_1(A)$) quantifies "how wild" (respectively, "how tame") A is. Scavia [56] computed $a_1(A)$ and $a_2(A)$ explicitly in combinatorial terms in the case, where A is a quiver algebra.

8 Back to resolvent degree

8.1 The level of a field extension

Let k be a base field, K be a field containing k, and L/K be a field extension of finite degree. I will say that L/K is of level $\leqslant d$ if there exists a finite tower of subfields

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \tag{14}$$

such that $L \subset K_n$ and $\mathrm{ed}_k(K_{i+1}/K_i) \leqslant d$ for every i. The level of L/K is the smallest such d; I will denote it by $\mathrm{lev}_k(L/K)$. Clearly,

$$\mathrm{lev}_k(L/K) \leqslant \mathrm{ed}_k(L/K).$$

If K is a field of rational functions on some algebraic variety X defined over k, then it is natural to think of elements of K_1 as algebraic (multi-valued) functions on X in at most $\mathrm{ed}_k(K_1/K)$ variables, and elements of L as compositions of algebraic functions in at most $\mathrm{lev}_k(L/K)$ variables.

Example 15. If the field extension L/K is solvable, then we claim that $\mathrm{lev}_k(L/K) \leqslant 1$. Indeed, here we can choose the tower (14) so that each K_{i+1} is obtained from K_i by adjoining a single radical. Then $\mathrm{ed}_k(K_{i+1}/K_i) \leqslant 1$ for each i, and hence, $\mathrm{lev}_k(L/K) \leqslant 1$, as claimed.

8.2 The resolvent degree of a functor

Let $\mathcal{F}$ be a functor from the category of field extensions K/k to the category of sets with a marked element. We will denote the marked element in $\mathcal{F}(K)$ by 1 and will refer to it as being "split". We will say that a field extension L/K splits an object $\alpha \in \mathcal{F}(K)$ if $\alpha_L = 1$. Here, as usual, α_L denotes the image of α under the natural map $\mathcal{F}(K) \to \mathcal{F}(L)$. Let us assume that

$$\text{for every field } K/k \text{ and every } \alpha \in \mathcal{F}(K),\\ \alpha \text{ can be split by a field extension } L/K \text{ of finite degree.} \tag{15}$$

This is a strong condition of $\mathcal{F}$; in particular, it implies that $\mathcal{F}(K) = \{1\}$ whenever K is algebraically closed.

I will now define the resolvent degrees $\mathrm{rd}_k(\alpha)$ of $\alpha \in \mathcal{F}(K)$ and $\mathrm{rd}_k(\mathcal{F})$ of the functor $\mathcal{F}$ satisfying condition (15) by analogy with the definitions of $\mathrm{ed}_k(\alpha)$ and $\mathrm{ed}_k(\mathcal{F})$ in Section 3. The resolvent degree $\mathrm{rd}_k(\alpha)$ is the minimal integer $d \geqslant 0$ such that α is split by a field extension L/K of level d (or equivalently, of level $\leqslant d$). The resolvent degree $\mathrm{rd}_k(\mathcal{F})$ is the maximal value of $\mathrm{rd}_k(\alpha)$, as K ranges over all fields containing k and α ranges over $\mathcal{F}(K)$.

Example 16. Let $n \geqslant 2$ be an integer not divisible by $\mathrm{char}(k)$. Then the functor $H^2(*, \mu_n)$ satisfies condition (15). I claim that this functor has resolvent degree 1. Indeed, let $\alpha \in H^2(K, \mu_n)$, and let ζ be a primitive nth root of unity in $\bar{k}$. By the Merkurjev–Suslin theorem, over $K(\zeta)$, we can write

$$\alpha = (a_1) \cup (b_1) + (a_2) \cup (b_2) + \cdots + (a_r) \cup (b_r)$$

for some $0 \neq a_i, b_i \in K(\zeta)$. Now $L = K(\zeta, a_1^{1/n}, \ldots, a_r^{1/n})$ splits α. By our construction, L is solvable over K. Thus, as we saw in Example 15, $\mathrm{lev}_k(L/K) \leqslant 1$. This shows that $\mathrm{rd}_k(\alpha) \leqslant 1$, as claimed. Using the norm residue isomorphism theorem (formerly known as the Bloch–Kato conjecture) in place of Merkurjev–Suslin, one shows in the same manner that $H^d(*, \mu_n)$ has resolvent degree 1 for every $d \geqslant 1$.

The resolvent degrees $\mathrm{rd}_k(\alpha; p)$ and $\mathrm{rd}_k(\mathcal{F}; p)$ at a prime p are defined in the same way as $\mathrm{ed}_k(\alpha; p)$ and $\mathrm{ed}_k(\mathcal{F}; p)$. Here $\mathcal{F}$ is a functor satisfying (15), $\alpha \in \mathcal{F}(K)$ is an object of $\mathcal{F}$. That is, $\mathrm{rd}_k(\alpha; p)$ is the minimal value of $\mathrm{rd}_k(\alpha_{K'})$, as K' ranges over all field extension of K such that $[K' : K]$ is finite and prime to p, and $\mathrm{rd}_k(\mathcal{F}; p)$ is the maximal value of $\mathrm{rd}_k(\alpha; p)$, where K ranges over all field containing k, and α ranges over $\mathcal{F}(K)$. A variant of the argument we used to prove (10) shows that $\mathrm{rd}_k(\mathcal{F}; p) \leqslant 1$ for every base field k, every functor $\mathcal{F}$ satisfying (15) and every prime p.

8.3 The resolvent degree of an algebraic group

The functor $\mathcal{F} = H^1(*, G)$ whose objects over K are G-torsors over $\mathrm{Spec}(K)$ satisfies condition (15) for every algebraic group G defined over k. I will write $\mathrm{rd}_k(G)$ for the resolvent degree of this functor. For simplicity, let us assume that $k = \mathbb{C}$ for the remainder of this section. I will write rd in place of $\mathrm{rd}_{\mathbb{C}}$.

Note that the quantity $\mathrm{rd}(n)$ we defined in the introduction can be recovered in this setting as $\mathrm{rd}(\mathrm{S}_n)$; cf. (8). Moreover, for a finite group G, our definition of $\mathrm{rd}(G)$ coincides with the definition given by Farb and Wolfson in [25].

Recall that, for a polynomial $f(x) \in K[x]$, our definition of $\mathrm{rd}(f)$ was motivated by wanting to express a root of $f(x)$ as a composition of algebraic functions in $\leqslant d$ variables applied to the coefficients. Equivalently, we wanted to find the smallest d such that the 0-cycle in $\mathbb{A}^1_K$ given by $f(x) = 0$ has an L-point for some field extension L/K of level $\leqslant d$. If G is a linear algebraic group and $T \to \mathrm{Spec}(K)$ is a G-torsor, then our more general definition of $\mathrm{rd}(T)$ retains this flavor. Indeed, T is an affine variety defined over K, and saying that T is split by L is the same as saying that T has an L-point.

While little is known about $\mathrm{rd}(n) = \mathrm{rd}(\mathrm{S}_n)$, it is natural to ask what $\mathrm{rd}(G)$ is for other algebraic groups G. Such questions can be thought of as variants of Hilbert's 13th problem. Let us now take a closer look at the case where G is linear and connected. The following folklore conjecture is implicit in the work of Tits.

Conjecture 17. *Let G be a connected complex linear algebraic group and K be a field containing $\mathbb{C}$. Then every $\alpha \in H^1(K, G)$ is split by some solvable field extension L/K.*

Since solvable extensions are of level $\leqslant 1$, this conjecture implies that $\mathrm{rd}(G) \leqslant 1$ for every connected linear algebraic group G.[11] I can prove the following weaker inequality unconditionally [52].

Theorem 18. *Let G be a connected complex linear algebraic group. Then* $\mathrm{rd}(G) \leqslant 7$*.*

Note that if we knew that $\mathrm{rd}(\mathrm{S}_n) \leqslant d$ for every n, we would be able to conclude that $\mathrm{lev}(L/K) \leqslant d$ for every field extension L/K of finite degree. This would, in turn, imply that $\mathrm{rd}(\mathcal{F}) \leqslant d$ for every functor $\mathcal{F}$ satisfying (15). Setting $\mathcal{F} = H^1(*, G)$, we obtain $\mathrm{rd}(G) \leqslant d$ for every algebraic group G. In particular, if we were able to show that $\mathrm{rd}(\mathcal{F}) > 1$ for some functor $\mathcal{F}$ satisfying (15), we would be able to conclude that $\mathrm{rd}(\mathrm{S}_n) > 1$ for some n. This would constitute major progress on Hilbert's 13th problem. I do not see how to reverse this implication though: an upper bound on $\mathrm{rd}(G)$ for every connected group G (such as the inequality $\mathrm{rd}(G) \leqslant 7$ of Theorem 18) does not appear to tell us anything about $\mathrm{rd}(\mathrm{S}_n)$. However, Conjecture 17 and Theorem 18 make me take more seriously the possibility that $\mathrm{rd}(\mathrm{S}_n)$ may be identically 1 or at least bounded as $n \to \infty$.

[11] Other interesting consequences of Conjecture 17 are discussed in [17].

Acknowledgements. I am grateful to EMS Magazine's editor Vladimir L. Popov for asking me to write a survey on essential dimension and resolvent degree, and for his help with the exposition. I would also like to thank Mikhail Borovoi for stimulating discussions concerning Conjecture 17, and to Patrick Brosnan, Danny Ofek, Federico Scavia and Jesse Wolfson for constructive comments.

References

[1] V. I. Arnol'd, On functions of three variables. *Dokl. Akad. Nauk SSSR* **114**, 679–681 (1957)

[2] V. I. Arnol'd, From Hilbert's superposition problem to dynamical systems. *Amer. Math. Monthly* **111**, 608–624 (2004)

[3] M. Bardestani, K. Mallahi-Karai and H. Salmasian, Kirillov's orbit method and polynomiality of the faithful dimension of p-groups. *Compos. Math.* **155**, 1618–1654 (2019)

[4] A. Beauville, Finite simple groups of small essential dimension. In *Trends in contemporary mathematics*, Springer INdAM Ser. 8, Springer, Cham, 221–228 (2014)

[5] D. Benson and Z. Reichstein, Fields of definition for representations of associative algebras. *Proc. Edinb. Math. Soc. (2)* **62**, 291–304 (2019)

[6] G. Berhuy and G. Favi, Essential dimension: a functorial point of view (after A. Merkurjev). *Doc. Math.* **8**, 279–330 (2003)

[7] C. Birkar, Singularities of linear systems and boundedness of Fano varieties. *Ann. of Math. (2)* **193**, 347–405 (2021)

[8] R. Brauer, On the resolvent problem. *Ann. Mat. Pura Appl. (4)* **102**, 45–55 (1975)

[9] P. Brosnan, Z. Reichstein and A. Vistoli, Essential dimension and algebraic stacks. arXiv:math/0701903 (2007)

[10] P. Brosnan, Z. Reichstein and A. Vistoli, Essential dimension, spinor groups, and quadratic forms. *Ann. of Math. (2)* **171**, 533–544 (2010)

[11] P. Brosnan, Z. Reichstein and A. Vistoli, Essential dimension in mixed characteristic. *Doc. Math.* **23**, 1587–1600 (2018)

[12] P. Brosnan and R. Sreekantan, Essential dimension of abelian varieties over number fields. *C. R. Math. Acad. Sci. Paris* **346**, 417–420 (2008)

[13] F. E. Browder (ed.), *Mathematical developments arising from Hilbert problems*, Proceedings of Symposia in Pure Mathematics, Vol. XXVIII, American Mathematical Society, Providence (1976)

[14] J. Buhler and Z. Reichstein, On the essential dimension of a finite group. *Compositio Math.* **106**, 159–179 (1997)

[15] N. G. Chebotarev, The problem of resolvents and critical manifolds. *Bull. Acad. Sci. URSS. Sér. Math. [Izvestia Akad. Nauk SSSR]* **7**, 123–146 (1943)

[16] A. Chen, Y.-H. He and J. McKay, Erland Samuel Bring's "Transformation of Algebraic Equations", arXiv:1711.09253 (2017)

[17] V. Chernousov, P. Gille and Z. Reichstein, Resolving G-torsors by abelian base extensions. *J. Algebra* **296**, 561–581 (2006)

[18] V. Chernousov and A. Merkurjev, Essential dimension of spinor and Clifford groups. *Algebra Number Theory* **8**, 457–472 (2014)

[19] V. Chernousov and J.-P. Serre, Lower bounds for essential dimensions via orthogonal representations. *J. Algebra* **305**, 1055–1070 (2006)

[20] H. Chu, S.-J. Hu, M.-C. Kang and J. Zhang, Groups with essential dimension one. *Asian J. Math.* **12**, 177–191 (2008)

[21] J. Dixmier, Histoire du 13e problème de Hilbert. In *Analyse diophantienne et géométrie algébrique*, Cahiers Sém. Hist. Math. Sér. 2, Univ. Paris VI, Paris, 85–94 (1993)

[22] I. V. Dolgachev and V. A. Iskovskikh, Finite subgroups of the plane Cremona group. In *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I*, Progr. Math. 269, Birkhäuser, Boston, 443–548 (2009)

[23] A. Duncan, Essential dimensions of A_7 and S_7. *Math. Res. Lett.* **17**, 263–266 (2010)

[24] A. Duncan, Finite groups of essential dimension 2. *Comment. Math. Helv.* **88**, 555–585 (2013)

[25] B. Farb and J. Wolfson, Resolvent degree, Hilbert's 13th problem and geometry. *Enseign. Math.* **65**, 303–376 (2019)

[26] M. Florence, On the essential dimension of cyclic p-groups. *Invent. Math.* **171**, 175–189 (2008)

[27] S. Garibaldi, Cohomological invariants: exceptional groups and spin groups. *Mem. Amer. Math. Soc.* **200**, xii+81 (2009)

[28] S. Garibaldi and R. M. Guralnick, Spinors and essential dimension. *Compos. Math.* **153**, 535–556 (2017)

[29] P. Gille and Z. Reichstein, A lower bound on the essential dimension of a connected linear group. *Comment. Math. Helv.* **84**, 189–212 (2009)

[30] C. Heberle and A. J. Sutherland, Upper bounds on resolvent degree via sylvester's obliteration algorithm. arXiv:2110.08670 (2021)

[31] D. Hilbert, Über die Gleichung neunten Grades. *Math. Ann.* **97**, 243–250 (1927)

[32] N. Karpenko and Z. Reichstein, A numerical invariant for linear representations of finite groups. *Comment. Math. Helv.* **90**, 667–701 (2015)

[33] N. A. Karpenko and A. S. Merkurjev, Essential dimension of finite p-groups. *Invent. Math.* **172**, 491–508 (2008)

[34] Y. Kawamata, Minimal models and the Kodaira dimension of algebraic fiber spaces. *J. Reine Angew. Math.* **363**, 1–46 (1985)

[35] F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*. Revised ed., Dover Publications, New York (1956)

[36] H. Knight, The essential p-dimension of finite simple groups of Lie type. arXiv:2109.02698 (2021)

[37] A. N. Kolmogorov, On the representation of continuous functions of several variables by superpositions of continuous functions of a smaller number of variables. *Dokl. Akad. Nauk SSSR (N.S.)* **108**, 179–182 (1956)

[38] L. Kronecker, Ueber die Gleichungen fünften Grades. *J. Reine Angew. Math.* **59**, 306–310 (1861)

[39] A. Ledet, On the essential dimension of p-groups. In *Galois theory and modular forms*, Dev. Math. 11, Kluwer Acad. Publ., Boston, MA, 159–172 (2004)

[40] A. Ledet, Finite groups of essential dimension one. *J. Algebra* **311**, 31–37 (2007)

[41] A. S. Merkurjev, Essential dimension: a survey. *Transform. Groups* **18**, 415–481 (2013)

[42] A. Meyer and Z. Reichstein, Some consequences of the Karpenko–Merkurjev theorem. *Doc. Math.* 445–457 (2010)

[43] A. Moreto, On the minimal dimension of a faithful linear representation of a finite group. arXiv:2102.01463 (2021)

[44] Y. A. Neretin, An estimate for the number of parameters defining an *n*-dimensional algebra. *Izv. Akad. Nauk SSSR Ser. Mat.* **51**, 306–318, 447 (1987)

[45] B. Poonen, The moduli space of commutative algebras of finite rank. *J. Eur. Math. Soc. (JEMS)* **10**, 817–836 (2008)

[46] V. L. Popov, On the Makar-Limanov, Derksen invariants, and finite automorphism groups of algebraic varieties. In *Affine algebraic geometry*, CRM Proc. Lecture Notes 54, American Mathematical Society, Providence, 289–311 (2011)

[47] V. L. Popov, Three plots about Cremona groups. *Izv. Ross. Akad. Nauk Ser. Mat.* **83**, 194–225 (2019)

[48] C. Procesi, Non-commutative affine rings. *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. Ia (8)* **8**, 237–255 (1967)

[49] Y. Prokhorov, Simple finite subgroups of the Cremona group of rank 3. *J. Algebraic Geom.* **21**, 563–600 (2012)

[50] Y. Prokhorov and C. Shramov, Jordan property for Cremona groups. *Amer. J. Math.* **138**, 403–418 (2016)

[51] Z. Reichstein, Essential dimension. In *Proceedings of the International Congress of Mathematicians, Vol. II (Hyderabad, India, 2010)*, Hindustan Book Agency, New Delhi, 162–188 (2011)

[52] Z. Reichstein, Hilbert's 13th problem for connected groups. In preparation

[53] Z. Reichstein and A. K. Shukla, Essential dimension of inseparable field extensions. *Algebra Number Theory* **13**, 513–530 (2019)

[54] Z. Reichstein and A. Vistoli, Essential dimension of finite groups in prime characteristic. *C. R. Math. Acad. Sci. Paris* **356**, 463–467 (2018)

[55] Z. Reichstein and B. Youssin, Essential dimensions of algebraic groups and a resolution theorem for *G*-varieties. *Canad. J. Math.* **52**, 1018–1056 (2000)

[56] F. Scavia, Essential dimension of representations of algebras. *Comment. Math. Helv.* **95**, 661–702 (2020)

[57] J.-P. Serre, Cohomological invariants, Witt invariants, and trace forms. In *Cohomological invariants in Galois cohomology*, Univ. Lecture Ser. 28, American Mathematical Society, Providence, 1–100 (2003)

[58] J.-P. Serre, A Minkowski-style bound for the orders of the finite subgroups of the Cremona group of rank 2 over an arbitrary field. *Mosc. Math. J.* **9**, 193–208, back matter (2009)

[59] J.-P. Serre, Le groupe de Cremona et ses sous-groupes finis. *Astérisque*, Exp. No. 1000, vii, 75–100 (2010)

[60] A. J. Sutherland, Upper bounds on resolvent degree and its growth rate. arXiv:2107.08139 (2021)

[61] B. Totaro, Essential dimension of the spin groups in characteristic 2. *Comment. Math. Helv.* **94**, 1–20 (2019)

[62] E. W. Tschirnhaus, A method for removing all intermediate terms from a given equation. *ACM SIGSAM Bulletin*, **37**, 1–3 (2003)

[63] J. Wolfson, Tschirnhaus transformations after Hilbert. *Enseign. Math.* **66**, 489–540 (2020)

Zinovy Reichstein is a mathematician at the University of British Columbia in Vancouver, Canada. He was an invited ICM speaker in 2010 and was awarded the Jeffery-Williams Prize by the Canadian Mathematical Society in 2013.

reichst@math.ubc.ca