Proceedings of the International Congress of Mathematicians
Hyderabad, India, 2010

Essential dimension

Zinovy Reichstein *

Abstract. Informally speaking, the essential dimension of an algebraic object is the minimal number of independent parameters one needs to define it. This notion was initially introduced in the context where the objects in question are finite field extensions [BuR97]. Essential dimension has since been investigated in several broader contexts, by a range of techniques, and has been found to have interesting and surprising connections to many problems in algebra and algebraic geometry.

The goal of this paper is to survey some of this research. I have tried to explain the underlying ideas informally through motivational remarks, examples and proof outlines (often in special cases, where the argument is more transparent), referring an interested reader to the literature for a more detailed treatment. The sections are arranged in rough chronological order, from the definition of essential dimension to open problems.

Mathematics Subject Classification (2000). Primary 14L30, 20G10, 11E72.

Keywords. Essential dimension, linear algebraic group, Galois cohomology, cohomological invariant, quadratic form, central simple algebra, algebraic torus, canonical dimension

1. Definition of essential dimension

Informally speaking, the essential dimension of an algebraic object is the minimal number of parameters one needs to define it. To motivate this notion, let us consider an example, where the object in question is a quadratic form.

Let k be a base field, K/k be a field extension and q be an n-dimensional quadratic form over K. Assume that $\mathrm{char}(k) \neq 2$ and denote the symmetric bilinear form associated to q by b. We would now like to see if q can be defined over a smaller field $k \subset K_0 \subset K$. This means that there is a K-basis $e_1, \dots, e_n$ of K^n such that $b(e_i, e_j) \in K_0$ for every $i, j = 1, \dots, n$. If we can find such a basis, we will say that q *descends* to K_0 or that K_0 is a *field of definition* of q. It is natural to ask if there is a minimal field K_{min}/k (with respect to inclusion) to which q descends. The answer to this question is usually "no". For example, it is not difficult to see that the "generic" form $q(x_1, \dots, x_n) = a_1 x_1^2 + \dots + a_n x_n^2$ over the field $K = k(a_1, \dots, a_n)$, where $a_1, \dots, a_n$ are independent variables, has no minimal field of definition. We will thus modify our question: instead of asking

*The author is grateful to S. Cernele, A. Duncan, S. Garibaldi, R. Lötscher, M. Macdonald, A. Merkurjev and A. Meyer for helpful comments and to the National Science and Engineering Council of Canada for financial support through its Discovery and Accelerator Supplement grants

for a minimal field of definition K_0 for q, we will ask for the minimal value of the transcendence degree $\operatorname{tr}\deg_k(K_0)$. [1] This number is called the *essential dimension* of q and is denoted by $\operatorname{ed}(q)$.

Note that the above definition of $\operatorname{ed}(q)$ is in no way particular to quadratic forms. In a similar manner one can consider fields of definition of any polynomial in $K[x_1, \dots, x_n]$, any finite-dimensional K-algebra, any algebraic variety defined over K, etc. In each case the minimal transcendence degree of a field of definition is an interesting numerical invariant which gives us some insight into the "complexity" of the object in question.

We will now state these observations more formally. Let k be a base field, Fields_k be the category of field extensions K/k, Sets be the category of sets, and $\mathcal{F}\colon \operatorname{Fields}_k \to \operatorname{Sets}$ be a covariant functor. In the sequel the word "functor" will always refer to a functor of this type. If $\alpha \in \mathcal{F}(K)$ and L/K is a field extension, we will denote the image of α in $\mathcal{F}(L)$ by α_L.

For example, $\mathcal{F}(K)$ could be the set of K-isomorphism classes of quadratic forms on K^n, or of n-dimensional K-algebras, for a fixed integer n, or of elliptic curves defined over K. In general we think of $\mathcal{F}$ as specifying the type of algebraic object we want to work with, and elements of $\mathcal{F}(K)$ as the of algebraic objects of this type defined over K.

Given a field extension K/k, we will say that $a \in \mathcal{F}(K)$ *descends* to an intermediate field $k \subseteq K_0 \subseteq K$ if a is in the image of the induced map $\mathcal{F}(K_0) \to \mathcal{F}(K)$. The *essential dimension* $\operatorname{ed}(a)$ of $a \in \mathcal{F}(K)$ is the minimum of the transcendence degrees $\operatorname{tr}\deg_k(K_0)$ taken over all fields $k \subseteq K_0 \subseteq K$ such that a descends to K_0. The essential dimension $\operatorname{ed}(\mathcal{F})$ of the functor $\mathcal{F}$ is the supremum of $\operatorname{ed}(a)$ taken over all $a \in \mathcal{F}(K)$ with K in Fields_k.

These notions are relative to the base field k; we will sometimes write ed_k in place of ed to emphasize the dependence on k. If $\mathcal{F}\colon \operatorname{Fields}_k \to \operatorname{Sets}$ be a covariant functor and $k \subset k'$ is a field extension, we will write $\operatorname{ed}_{k'}(\mathcal{F})$ for $\operatorname{ed}(\mathcal{F}_{k'})$, where $\mathcal{F}_{k'}$ denotes the restriction of $\mathcal{F}$ to $\operatorname{Fields}_{k'}$. Is easy to see that in this situation

$$\operatorname{ed}_k(\mathcal{F}) \geq \operatorname{ed}_{k'}(\mathcal{F})\,; \tag{1.1}$$

cf. [BF03, Proposition 1.5]. In particular, taking k' to be an algebraic closure of k, we see that for the purpose of proving a lower bound of the form $\operatorname{ed}_k(\mathcal{F}) \geq d$, where d does not depend on k, we may assume that k is algebraically closed.

Let $\boldsymbol{\mu}_n$ denote the group of nth roots of unity, defined over k. Whenever we consider this group, we will assume that it is smooth, i.e., that $\operatorname{char}(k)$ does not divide n.

Example 1.1. Let $\mathcal{F}(K) := H^r(K, \boldsymbol{\mu}_n)$ be the Galois cohomology functor. Assume k is algebraically closed. If $\alpha \in H^r(K, \boldsymbol{\mu}_n)$ is non-trivial then by the Serre vanishing theorem (see, e.g., [Se02, II.4.2, Prop. 11, p. 83]) $\operatorname{ed}(\alpha) \geq r$.

Example 1.2. Once again, assume that k is algebraically closed. Let $\mathbf{Forms}_{n,d}(K)$ be the set of homogeneous polynomials of degree d in n variables. If $\alpha \in \mathbf{Forms}_{n,d}(K)$

[1] One may also ask which quadratic forms have a minimal field of definition. To the best of my knowledge, this is an open question; see Section 7.1.

is anisotropic over K then by the Tsen-Lang theorem (see, e.g., [Pf95]), $n \le d^{\mathrm{ed}(\alpha)}$ or equivalently, $\mathrm{ed}(\alpha) \ge \log_d(n)$.

Of particular interest to us will be the functors $\mathcal{F}_G$ given by $K \to H^1(K, G)$, where G is an algebraic group over k. Here, as usual, $H^1(K, G)$ denotes the set of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$. The essential dimension of this functor is a numerical invariant of G, which, roughly speaking, measures the complexity of G-torsors over fields. We write $\mathrm{ed}\, G$ for $\mathrm{ed}\, \mathcal{F}_G$. Essential dimension was originally introduced in this context (and only in characteristic 0); see [BuR97, Rei00, RY00]. The above definition of essential dimension for a general functor $\mathcal{F}$ is due to A. Merkurjev; see [BF03].

In special cases this notion was investigated much earlier. To the best of my knowledge, the first non-trivial result related to essential dimension is due to F. Klein [Kl1884]. In our terminology, Klein showed that the essential dimension of the symmetric group S_5 over $k = \mathbb{C}$, is 2. (Klein referred to this result as "Kroeneker's theorem", so it may in fact go back even further.) The essential dimension of the projective linear group $\mathbf{PGL}_n$ first came up in C. Procesi's pioneering work on universal division algebras in the 1960s; see [Pr67, Section 2]. The problems of computing the essential dimension of the symmetric group S_n and the projective linear group $\mathbf{PGL}_n$ remain largely open; see Section 7.

If k is an algebraically closed field then groups of essential dimension zero are precisely the *special groups*, introduced by J.-P. Serre [Se58]. Recall that an algebraic group G over k is called special if $H^1(K, G) = 0$ for every field extension K/k. Over an algebraically closed field of characteristic zero these groups were classified by A. Grothendieck [Gro58] in the 1950s. The problem of computing the essential dimension of an algebraic group may be viewed as a natural extension of the problem of classifying special groups.

2. First examples

Recall that an action of an algebraic group G on an algebraic k-variety X is called *generically free* if X has a dense G-invariant open subset U such that the stabilizer $\mathrm{Stab}_G(x) = \{1\}$ for every $x \in U(\overline{k})$ and *primitive* if G permutes the irreducible components of X. Here $\overline{k}$ denotes an algebraic closure of k. Equivalently, X is primitive if $k(X)^G$ is a field.

If K/k is a finitely generated field extension then elements of $H^1(K, G)$ can be interpreted as birational isomorphism classes of generically free primitive G-varieties (i.e., k-varieties with a generically free primitive G-action) equipped with a k-isomorphism of fields $k(X)^G \simeq K$; cf. [BF03, Section 4]. If X is a generically free primitive G-variety, and $[X]$ is its class in $H^1(K, G)$ then

$$\mathrm{ed}([X]) = \min \dim(Y) - \dim(G)\,, \tag{2.1}$$

where the minimum is taken over all dominant rational G-equivariant maps $X \dashrightarrow Y$ such that the G-action on Y is generically free.

An important feature of the functor $H^1(\ *\ , G)$ is the existence of so-called *versal objects*; see [GMS03, Section I.5]. If $\alpha \in H^1(K, G)$ is a versal torsor then it is easy to see that $\operatorname{ed}(\alpha) \geq \operatorname{ed}(\beta)$ for any field extension L/k and any $\beta \in H^1(L, G)$. In other words, $\operatorname{ed}(\alpha) = \operatorname{ed}(G)$. If $G \to \mathbf{GL}(V)$ is a generically free k-linear representation of G then the class $[V]$ of V in $H^1(k(V)^G, G)$ is versal. By (2.1), we see that

$$\operatorname{ed}(G) = \min \dim(Y) - \dim(G)\,, \tag{2.2}$$

where the minimum is taken over all dominant rational G-equivariant maps $V \dashrightarrow Y$, such that G-action on Y is generically free. In particular,

$$\operatorname{ed}(G) \leq \dim(V) - \dim(G)\,. \tag{2.3}$$

Moreover, unless k is a finite field and G is special, we only need to consider closed G-invariant subvarieties Y of V. That is,

$$\operatorname{ed}(G) = \min\{\dim \operatorname{Im}(f)\} - \dim(G)\,, \tag{2.4}$$

where the minimum is taken over all G-equivariant rational maps $f\colon V \dashrightarrow V$ such that the G-action on $\operatorname{Im}(f)$ is generically free; see [Me09, Theorem 4.5].

Example 2.1. Let G be a connected adjoint semisimple group over k. Then $\operatorname{ed}(G) \leq \dim(G)$. To prove this inequality, apply (2.3) to the generically free representation $V = \mathcal{G} \times \mathcal{G}$, where $\mathcal{G}$ is the adjoint representation of G on its Lie algebra.

Note that the inequality $\operatorname{ed}(G) \leq \dim(G)$ can fail dramatically if G is not adjoint; see Corollary 4.3.

We now turn to lower bounds on $\operatorname{ed}(G)$ for various algebraic groups G and more generally, on $\operatorname{ed}(\mathcal{F})$ for various functors $\mathcal{F}\colon \operatorname{Fields}_k \to \operatorname{Sets}$. The simplest approach to such bounds is to relate the functor $H^1(\ *\ , G)$ (and more generally, $\mathcal{F}$) to the functors in Examples 1.1 or 1.2, using the following lemma, whose proof is immediate from the definition; cf. [BF03, Lemma 1.9].

Lemma 2.2. *Suppose a morphism of functors $\phi\colon \mathcal{F} \to \mathcal{F}'$ takes α to β. Then $\operatorname{ed}(\alpha) \geq \operatorname{ed}(\beta)$. In particular, if ϕ is surjective then $\operatorname{ed}(\mathcal{F}) \geq \operatorname{ed}(\mathcal{F}')$.*

A morphism of functors $\mathcal{F} \to H^d(\ *\ , \boldsymbol{\mu}_n)$ is called a *cohomological invariant* of degree d; it is said to be nontrivial if $\mathcal{F}(K)$ contains a non-zero element of $H^d(K, \boldsymbol{\mu}_n)$ for some K/k. Using Lemma 2.2 and Example 1.1 we recover the following observation, due to Serre.

Lemma 2.3. *Suppose k is algebraically closed. If there exists a non-trivial cohomological invariant $\mathcal{F} \to H^d(\ *\ , \boldsymbol{\mu}_n)$ then $\operatorname{ed}(\mathcal{F}) \geq d$.*

In the examples below I will, as usual, write $\langle a_1, \dots, a_n\rangle$ for the quadratic form $(x_1, \dots, x_n) \mapsto a_1x_1^2 + \dots + a_nx_n^2$ and $\ll a_1, \dots, a_r \gg$ for the r-fold Pfister form $\langle 1, -a_1\rangle \otimes_K \dots \otimes \langle 1, -a_r\rangle$.

Example 2.4. Suppose $\mathrm{char}(k) \neq 2$. Let Pf_r be the functor that assigns to a field K/k the set of K-isomorphism classes of r-fold Pfister forms, $q = \ll a_1, \dots, a_r \gg$. Then $\mathrm{ed}_k(\mathrm{Pf}_r) = r$.

Indeed, since q is defined over $k(a_1, \dots, a_r)$, we have $\mathrm{ed}_k(\mathrm{Pf}_r) \leq r$. To prove the opposite inequality, we may assume that k is algebraically closed. Let $a_1, \dots, a_r$ be independent variables and $K = k(a_1, \dots, a_r)$. Then the tautological map $\mathrm{Pf}_r(K) \to \mathbf{Forms}_{2^r,2}(K)$ takes $q = \ll a_1, \dots, a_r \gg$ to an anisotropic form in 2^r variables; see, e.g., [Pf95, p. 111]. Combining Lemma 2.2 and Example 1.2 we conclude that $\mathrm{ed}(\mathrm{Pf}_r) \geq r$, as desired.

Alternatively, the inequality $\mathrm{ed}(\mathrm{Pf}_r) \geq r$ also follows from Lemma 2.3, applied to the cohomological invariant $\mathrm{Pf}_r \to H^r(*, \boldsymbol{\mu}_2)$, which takes $\ll a_1, \dots, a_r \gg$ to the cup product $(a_1) \cup \dots \cup (a_r)$.

Since $H^1(*, \mathbf{G}_2)$ is naturally isomorphic to Pf_3, we conclude that $\mathrm{ed}(\mathbf{G}_2) = 3$. Here $\mathbf{G}_2$ stands for the split exceptional group of type $\mathbf{G}_2$ over k.

Example 2.5. If $\mathrm{char}(k) \neq 2$ then $\mathrm{ed}_k(\mathbf{O}_n) = n$.

Indeed, since every quadratic form over K/k can be diagonalized, we see that $\mathrm{ed}_k(\mathbf{O}_n) \leq n$. To prove the opposite inequality, we may assume that k is algebraically closed. Define the functor $\phi\colon H^1(*, \mathbf{O}_n) \to \mathrm{Pf}_n$ as follows. Let b be the bilinear form on $V = K^n$, associated to $q = \langle a_1, \dots, a_n \rangle \in H^1(K, \mathbf{O}_n)$. Then b naturally induces a non-degenerate bilinear form on the 2^n-dimensional K-vector space $\bigwedge(V)$. We now set $\phi(q)$ to be the 2^r-dimensional quadratic form associated to $\wedge(b)$. One easily checks that $\phi(q)$ is the n-fold Pfister form $\phi(q) = \ll a_1, \dots, a_n \gg$. Since ϕ is clearly surjective, Lemma 2.2 and Example 2.4 tell us that $\mathrm{ed}(\mathbf{O}_n) \geq \mathrm{ed}(\mathrm{Pf}_n) = n$.

We remark that $\phi(q)$ is closely related to the nth Stiefel-Whitney class $\mathrm{sw}_n(q)$ (see [GMS03, p. 41]), and the inequality $\mathrm{ed}(\mathbf{O}_n) \geq n$ can also be deduced by applying Lemma 2.3 to the cohomological invariant $\mathrm{sw}_n\colon H^1(K, \mathbf{O}_n) \to H^n(K, \boldsymbol{\mu}_2)$.

Example 2.6. If k contains a primitive nth root of unity then $\mathrm{ed}_k(\boldsymbol{\mu}_n^r) = r$.

Indeed, the upper bound, $\mathrm{ed}(\boldsymbol{\mu}_n^r) \leq r$, follows from (2.3). Alternatively, note that any $(\overline{a_1}, \dots, \overline{a_r}) \in H^1(K, \boldsymbol{\mu}_n^r)$ is defined over the subfield $k(a_1, \dots, a_r)$ of K, of transcendence degree $\leq r$.

To prove the opposite inequality we may assume that k is algebraically closed. Now apply Lemma 2.3 to the cohomological invariant

$$H^1(K, \boldsymbol{\mu}_n^r) = K^*/(K^*)^n \times \dots \times K^*/(K^*)^n \to H^r(K, \boldsymbol{\mu}_n)$$

given by $(\overline{a_1}, \dots, \overline{a_r}) \to (a_1) \cup \dots \cup (a_r)$. Here $\overline{a}$ denotes the class of $a \in K^*$ in $K^*/(K^*)^n$.

Remark 2.7. Suppose H is a closed subgroup of G and $G \to \mathbf{GL}(V)$ is a generically free linear representation. Since every rational G-equivariant map $V \dashrightarrow Y$ is also H-equivariant, (2.2) tells us that

$$\mathrm{ed}(G) \geq \mathrm{ed}(H) + \dim(H) - \dim(G)\,. \tag{2.5}$$

In particular, if a finite group G contains a subgroup $H \simeq (\mathbb{Z}/p\mathbb{Z})^r$ for some prime p and if $\mathrm{char}(k) \neq p$ (so that we can identify $(\mathbb{Z}/p\mathbb{Z})^r$ with $\boldsymbol{\mu}_p^r$ over $\overline{k}$) then

$$\mathrm{ed}_k(G) \geq \mathrm{ed}_{\overline{k}}(G) \geq \mathrm{ed}_{\overline{k}}(H) = r\,.$$

In the case where G is the symmetric group S_n and $H \simeq (\mathbb{Z}/2\mathbb{Z})^{[n/2]}$ is the subgroup generated by the commuting 2-cycles (12), (34), (56), etc., this yields $\mathrm{ed}(S_n) \geq [n/2]$; cf. [BuR97].

Example 2.8. Recall that elements of $H^1(K, \mathbf{PGL}_n)$ are in a natural bijective correspondence with isomorphism classes of central simple algebras of degree n over K. Suppose $n = p^s$ is a prime power, and k contains a primitive pth root of unity. Consider the morphism of functors $\phi\colon H^1(K, \mathbf{PGL}_n) \to \mathbf{Forms}_{n^2,p}$ given by sending a central simple K-algebra A to the degree p trace form $x \to \mathrm{Tr}_{A/K}(x^p)$.

If $a_1, \dots, a_{2s}$ are independent variables over k, $K = k(a_1, \dots, a_{2s})$, and

$$A = (a_1, a_2)_p \otimes_K \otimes \cdots \otimes (a_{2s-1}, a_{2s})_p$$

is a tensor product of s symbol algebras of degree p then one can write out $\phi(A)$ explicitly and show that it is anisotropic over K; see [Rei99]. Lemma 2.2 and Example 1.2 now tell us that $\mathrm{ed}_k(A) \geq \mathrm{ed}_{\overline{k}}(A) \geq 2s$. Since $\mathrm{tr\,deg}_k(K) = 2s$, we conclude that, in fact

$$\mathrm{ed}_k(A) = 2s \text{ and consequently, } \mathrm{ed}_k(\mathbf{PGL}_{p^s}) \geq 2s. \tag{2.6}$$

The following alternative approach to proving (2.6) was brought to my attention by P. Brosnan. Consider the cohomological invariant given by the composition of the natural map $H^1(K, \mathbf{PGL}_n) \to H^2(K, \boldsymbol{\mu}_n)$, which sends a central simple algebra to its Brauer class, and the divided power map $H^2(*, \boldsymbol{\mu}_n) \to H^{2s}(*, \boldsymbol{\mu}_n)$; see [Kahn00, Appendix]. The image of A under the resulting cohomological invariant

$$H^1(*, \mathbf{PGL}_n) \to H^{2s}(*, \boldsymbol{\mu}_n)$$

is $(a_1) \cup (a_2) \cup \cdots \cup (a_{2s}) \neq 0$ in $H^{2s}(K, \boldsymbol{\mu}_n)$. Lemma 2.3 now tells us that $\mathrm{ed}_k(A) \geq 2s$, and (2.6) follows. The advantage of this approach is that it shows that the essential dimension of the Brauer class of A is also $2s$.

3. The fixed point method

The following lower bound on $\mathrm{ed}(G)$ was conjectured by Serre and proved in [GR07]. Earlier versions of this theorem have appeared in [RY00] and [CS06].

Theorem 3.1. *If G is connected, A is a finite abelian subgroup of G and* $\mathrm{char}(k)$ *does not divide $|A|$, then* $\mathrm{ed}_k(G) \geq \mathrm{rank}(A) - \mathrm{rank}\ C_G^0(A)$.

Here $\mathrm{rank}(A)$ stands for the minimal number of generators of A and $\mathrm{rank}\ C_G^0(A)$ for the dimension of the maximal torus of the connected group $C_G^0(A)$. Note that

if A is contained in a torus $T \subset G$ then $\operatorname{rank}(C_G^0(A)) \geq \operatorname{rank}(T) \geq \operatorname{rank}(A)$, and the inequality of Theorem 3.1 becomes vacuous. Thus we are primarily interested in non-toral finite abelian subgroups A of G. These subgroups have come up in many different contexts, starting with the work of Borel in the 1950s. For details and further references, see [RY00].

The proof of Theorem 3.1 relies on the following two simple results.

Theorem 3.2 (Going Down Theorem). *Suppose k is an algebraically closed base field and A is an abelian group such that* $\operatorname{char}(k)$ *does not divide $|A|$. Suppose A acts on k-varieties X and Y and $f\colon X \dashrightarrow Y$ is an A-equivariant rational map. If X has a smooth A-fixed point and Y is complete then Y has an A-fixed point.*

A short proof of Theorem 3.2, due to J. Kollár and E. Szabó, can be found in [RY00, Appendix].

Lemma 3.3. *Let A be a finite abelian subgroup, acting faithfully on an irreducible k-variety X. Suppose* $\operatorname{char}(k)$ *does not divide $|A|$. If X has a smooth A-fixed point then* $\dim(X) \geq \operatorname{rank}(A)$.

The lemma follows from the fact that the A-action on the tangent space $T_x(X)$ at the fixed point x has to be faithful; see [GR07, Lemma 4.1].

For the purpose of proving Theorem 3.1 we may assume that k is algebraically closed. To convey the flavor of the proof I will make the following additional assumptions: (i) $C_G(A)$ is finite and (ii) $\operatorname{char}(k) = 0$. The conclusion then reduces to

$$\operatorname{ed}(G) \geq \operatorname{rank}(A)\,. \tag{3.1}$$

This special case of Theorem 3.1 is proved in [RY00] but I will give a much simplified argument here, based on [GR07, Section 4].

Let $G \to \mathbf{GL}(V)$ be a generically free representation. By (2.2) we need to show that if $V \dashrightarrow Y$ is a G-equivariant dominant rational map and the G-action on Y is generically free, then

$$\dim(Y) - \dim(G) \geq \operatorname{rank}(A)\,. \tag{3.2}$$

To see how to proceed, let us first consider the "toy" case, where G is finite. Here (3.1) follows from (2.5), but I will opt for a different argument below, with the view of using a variant of it in greater generality.

After birationally modifying Y, we may assume that it is smooth and projective. (Note that this step relies on G-equivariant resolution of singularities and thus uses the characteristic 0 assumption.) Since V has a smooth A-fixed point (namely, the origin), the Going Down Theorem 3.2 tells us that so does Y. By Lemma 3.3, $\dim(Y) \geq \operatorname{rank}(A)$, which proves (3.2) in the case where G is finite.

If G is infinite, we can no longer hope to prove (3.2) by applying Lemma 3.3 to the A-action on Y. Instead, we will apply Lemma 3.3 to a suitable A-invariant subvariety $Z \subset Y$. This subvariety Z will be a cross-section for the G-action on Y, in the sense that a G-orbit in general position will intersect Z in a finite number of points. Hence, $\dim(Z) = \dim(Y) - \dim(G)$, and (3.2) reduces to

$\dim(Z) \geq \operatorname{rank}(A)$. We will then proceed as in the previous paragraph: we will use Theorem 3.2 to find an A-fixed point on a smooth complete model of Z, then use Lemma 3.3 to show that $\dim(Z) \geq \operatorname{rank}(A)$.

Let me now fill in the details. By [CGR06] Y is birationally isomorphic to $G \times^S Z$, where S is a finite subgroup of G and Z is an algebraic variety equipped with a faithful S-action. (A priori Z does not carry an A-action; however, we will show below that some conjugate A' of A lies in S and consequently, acts on Z. We will then replace A by A' and argue as above.) We also note that we are free to replace Z by an (S-equivariantly) birationally isomorphic variety, so we may (and will) take it to be smooth and projective.

Here, as usual, if S acts on normal quasi-projective varieties X and Z then $X \times^S Z$ denotes the geometric quotient of $X \times Z$ by the natural (diagonal) action of S. Since S is finite, there is no difficulty in forming the quotient map $\pi\colon X \times Z \to X \times^S Z$; cf. [GR07, Lemma 3.1]. Moreover, if the S-action on X extends to a $G \times S$-action, then by the universal property of geometric quotients $X \times^S Z$ inherits a G-action from $X \times Z$, where G acts on the first factor. I will write $[x, z] \in X \times^S Z$ for the image of (x, z) under π.

We now compactify $Y = G \times^S Z$ by viewing it as a G-invariant open subset of the projective variety $\overline{Y} := \overline{G} \times^S Z$, where $\overline{G}$ is a so-called "wonderful" (or "regular") compactification of G. Recall that $G \times G$ acts on $\overline{G}$, extending the right and left multiplication action of G on itself, The complement $\overline{G} \smallsetminus G$ is a normal crossing divisor $D_1 \cup \cdots \cup D_r$, where each D_i is irreducible, and the intersection of any number of D_i is the closure of a single $G \times G$-orbit in $\overline{G}$. The compactification $\overline{G}$ has many wonderful properties; the only one we will need is Lemma 3.4 below. For a proof, see [Br98, Proposition A1].

Lemma 3.4. *For every $x \in \overline{G}$, $P = \operatorname{pr}_1(\operatorname{Stab}_{G\times G}(x))$ is a parabolic subgroup of G. Here pr_1 is projection to the first factor. Moreover, $P = G$ if and only if $x \in G$.*

We are now ready to complete the proof of the inequality (3.2) (and thus of (3.1)) by showing that S contains a conjugate A' of A, and A' has a fixed point in Z. In other words, our goal is to show that some conjugate A' of A lies in $\operatorname{Stab}_S(z)$.

By the Going Down Theorem 3.2, $\overline{Y}$ has an A-fixed point. Denote this point by $[x, z]$ for some $x \in \overline{G}$ and $z \in Z$. That is, for every $a \in A$, $[ax, z] = [x, z]$ in $\overline{Y}$. Equivalently,

$$\begin{cases} ax = xs^{-1} \\ sz = z \end{cases} \tag{3.3}$$

for some $s \in S$. In other words, for every $a \in A$, there exists an $s \in \operatorname{Stab}_S(z)$ such that $(a^{-1}, s) \in \operatorname{Stab}_{G\times G}(x)$. Equivalently, the image of the natural projection $\operatorname{pr}_1\colon \operatorname{Stab}_{G\times G}(x) \to G$ contains A. Since we are assuming that $C^0_G(A)$ is finite, A cannot be contained in any proper parabolic subgroup of G. Thus $x \in G$; see Lemma 3.4. Now the first equation in (3.3) tells us that $A' := x^{-1}Ax \subset \operatorname{Stab}_S(z)$, as desired. □

Remark 3.5. The above argument proves Theorem 3.1 under two simplifying assumptions: (i) $C_G(A)$ is finite and (ii) $\operatorname{char}(k) = 0$. If assumption (i) is removed,

a variant of the same argument can still be used to prove Theorem 3.1 in characteristic 0; see [GR07, Section 4]. Assumption (ii) is more serious, because our argument heavily relies on resolution of singularities. Consequently, the proof of Theorem 3.1 in prime characteristic is considerably more complicated; see [GR07].

Corollary 3.6. *(a)* $\operatorname{ed}(\mathbf{SO}_n) \geq n-1$ *for any* $n \geq 3$, *(b)* $\operatorname{ed}(\mathbf{PGL}_{p^s}) \geq 2s$,

(c) $\operatorname{ed}(\mathbf{Spin}_n) \geq \begin{cases} [n/2] \text{ for any } n \geq 11, \\ [n/2]+1 \text{ if } n \equiv -1,\ 0 \text{ or } 1 \text{ modulo } 8, \end{cases}$

(d) $\operatorname{ed}(\mathbf{G}_2) \geq 3$, *(e)* $\operatorname{ed}(\mathbf{F}_4) \geq 5$, *(f)* $\operatorname{ed}(\mathbf{E}_6^{sc}) \geq 4$.

(g) $\operatorname{ed}(\mathbf{E}_7^{sc}) \geq 7$, *(h)* $\operatorname{ed}(\mathbf{E}_7^{ad}) \geq 8$, *(i)* $\operatorname{ed}(\mathbf{E}_8) \geq 9$.

Here the superscript ^{sc} *stands for "simply connected" and* ^{ad} *for "adjoint".*

Each of these inequalities is proved by exhibiting a non-toral abelian subgroup $A \subset G$ whose centralizer is finite. For example, in part (a) we can take $A \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ to be the subgroup of diagonal matrices of the form

$$\operatorname{diag}(\epsilon_1, \dots, \epsilon_n), \text{ where each } \epsilon_i = \pm 1 \text{ and } \epsilon_1 \cdot \ldots \cdot \epsilon_n = 1. \tag{3.4}$$

The details are worked out in [RY00], with the exception of the first line in part (c), which was first proved by V. Chernousov and J.-P. Serre [CS06], by a different method. I later noticed that it can be deduced from Theorem 3.1 as well; the finite abelian subgroups one uses here can be found in [Woo89].

Remark 3.7. The inequalities in parts (a), (b), (d), (e) and (f) can be recovered by applying Lemma 2.3 to suitable cohomological invariants. For parts (b) and (d), this is done in Examples 2.8 and 2.4, respectively; for parts (a), (e) and (f), see [Rei00, Example 12.7], [Rei00, Example 12.10] and [Gar01, Remark 2.12].

It is not known whether or not parts (g), (h) and (i) can be proved in a similar manner, i.e., whether or not there exist cohomological invariants of E_7^{sc}, E_7^{ad} and E_8 of dimensions 7, 8, and 9, respectively.

4. Central extensions

In this section we will discuss another more recent method of proving lower bounds on $\operatorname{ed}(G)$. This method does not apply as broadly as those described in the previous two sections, but in some cases it leads to much stronger bounds. Let

$$1 \to C \to G \to \overline{G} \to 1 \tag{4.1}$$

be an exact sequence of algebraic groups over k such that C is central in G and isomorphic to $\boldsymbol{\mu}_p^r$ for some $r \geq 1$. Given a character $\chi\colon C \to \boldsymbol{\mu}_p$, we will, following [KM07], denote by $\operatorname{Rep}^{\chi}$ the set of irreducible representations $\phi\colon G \to \mathbf{GL}(V)$, defined over k, such that $\phi(c) = \chi(c)\operatorname{Id}_V$ for every $c \in C$.

Theorem 4.1. *Assume that k is a field of characteristic $\neq p$ containing a primitive pth root of unity. Then*

$$\operatorname{ed}_k(G) \geq \min_{\langle \chi_1, \dots, \chi_r \rangle = C^*} \Big(\sum_{i=1}^{r} \gcd_{\rho_i \in \operatorname{Rep}^{\chi_i}} \dim(\rho_i) \Big) - \dim G\,. \tag{4.2}$$

Here gcd *stands for the greatest common divisor and the minimum is taken over all minimal generating sets $\chi_1, \dots, \chi_r$ of $C^* \simeq (\mathbb{Z}/p\mathbb{Z})^r$.*

Theorem 4.1 has two remarkable corollaries.

Corollary 4.2. (N. Karpenko – A. Merkurjev [KM07]) *Let G be a finite p-group and k be a field containing a primitive pth root of unity. Then*

$$\operatorname{ed}_k(G) = \min \dim(\phi)\,, \tag{4.3}$$

where the minimum is taken over all faithful k-representations ϕ of G.

Proof. We apply Theorem 4.1 to the exact sequence $1 \to C \to G \to G/C \to 1$, where C be the socle of G, i.e., $C := \{g \in Z(G) \mid g^p = 1\}$. Since $\dim(\rho)$ is a power of p for every irreducible representation ρ of G, we may replace gcd by min in (4.2). Choosing a minimal set of generators $\chi_1, \dots, \chi_r$ of C^* so that the sum on the right hand side of (4.2) has minimal value, and $\rho_i \in \operatorname{Rep}^{\chi_i}$ of minimal dimension, we see that (4.2) reduces to $\operatorname{ed}_k(G) \geq \dim(\rho_1) + \dots + \dim(\rho_r)$. Equivalently, $\operatorname{ed}_k(G) \geq \dim(\rho)$, where $\rho := \rho_1 \oplus \dots \oplus \rho_r$ is faithful by elementary p-group theory. This shows that $\operatorname{ed}_k(G) \geq \min \dim(\phi)$ in (4.3). The opposite inequality follows from (2.3). □

Corollary 4.3. *Let $\mathbf{Spin}_n$ be the split spinor group over a a field k of characteristic 0. Assume $n \geq 15$. Then*

(a) $\operatorname{ed}(\mathbf{Spin}_n) = 2^{(n-1)/2} - \frac{n(n-1)}{2}$*, if n is odd,*

(b) $\operatorname{ed}(\mathbf{Spin}_n) = 2^{(n-2)/2} - \frac{n(n-1)}{2}$*, if $n \equiv 2 \pmod 4$, and*

(c) $2^{(n-2)/2} - \frac{n(n-1)}{2} + 2^m \leq \operatorname{ed}(\mathbf{Spin}_n) \leq 2^{(n-2)/2} - \frac{n(n-1)}{2} + n$*, if $n \equiv 0 \pmod 4$. Here 2^m is the largest power of 2 dividing n.*

We remark that M. Rost and S. Garibaldi have computed the essential dimension of $\mathbf{Spin}_n$ for every $n \leq 14$; see [Rost06] and [Gar09].

Proof outline. The lower bounds (e.g., $\operatorname{ed}(\mathbf{Spin}_n) \geq 2^{(n-1)/2} - \frac{n(n-1)}{2}$, in part (a)) are valid whenever $\operatorname{char}(k) \neq 2$; they can be deduced either directly from Theorem 4.1 or by applying the inequality (2.5) to the finite 2-subgroup H of $G = \mathbf{Spin}_n$, where H is the inverse image of the diagonal subgroup $\boldsymbol{\mu}_2^{n-1} \subset \mathbf{SO}_n$, as in (3.4), under the natural projection $\pi\colon \mathbf{Spin}_n \to \mathbf{SO}_n$. Here $\operatorname{ed}(H)$ is given by Corollary 4.2.

The upper bounds (e.g., $\operatorname{ed}(\mathbf{Spin}_n) \leq 2^{(n-1)/2} - \frac{n(n-1)}{2}$, in part (a)) follow from the inequality (2.3), where V is spin representation V_{spin} in part (a), the half-spin representation $V_{\text{half-spin}}$ in part (b), and to $V_{\text{half-spin}} \oplus V_{\text{natural}}$ in part

(c), where V_{natural} is the natural n-dimensional representation of $\mathbf{SO}_n$, viewed as a representation of $\mathbf{Spin}_n$ via π. The delicate point here is to check that these representations are generically free. In characteristic 0 this is due to E. Andreev and V. Popov [AP71] for $n \geq 29$ and to A. Popov [Po85] in the remaining cases.

For details, see [BRV10a] and (for the lower bound in part (c)) [Me09, Theorem 4.9]. □

To convey the flavor of the proof of Theorem 4.1, I will consider a special case, where G is finite and $r = 1$. That is, I will start with a sequence

$$1 \to \boldsymbol{\mu}_p \to G \to \overline{G} \to 1 \tag{4.4}$$

of finite groups and will aim to show that

$$\operatorname{ed}_k(G) \geq \gcd_{\rho \in \operatorname{Rep}'} \dim(\rho)\,, \tag{4.5}$$

where k contains a primitive pth root and Rep' denotes the set of irreducible representations of G whose restriction to $\boldsymbol{\mu}_p$ is non-trivial. The proof relies on the following two results, which are of independent interest.

Theorem 4.4. (Karpenko's Incompressibility Theorem; [Kar00, Theorem 2.1]) *Let X be a Brauer-Severi variety of prime power index p^m, over a field K and let $f\colon X \dashrightarrow X$ be a rational map defined over K. Then $\dim_K \operatorname{Im}(f) \geq p^m - 1$.*

Theorem 4.5. (Merkurjev's Index Theorem [KM07, Theorem 4.4]; cf. also [Me96]) *Let K/k be a field extension, and $\partial_K\colon H^1(K, \overline{G}) \to H^2(K, \boldsymbol{\mu}_p)$ be the connecting map induced by the short exact sequence* (4.4)*. Then the maximal value of the index of $\partial_K(a)$, as K ranges over all field extension of k and a ranges over $H^1(K, \overline{G})$, equals $\gcd_{\rho \in \operatorname{Rep}'} \dim(\rho)$.*

Recall that $H^2(K, \boldsymbol{\mu}_p)$ is naturally isomorphic to the p-torsion subgroup of the Brauer group $\operatorname{Br}(K)$, so that it makes sense to talk about the index.

I will now outline an argument, due to M. Florence [Fl07], which deduces the inequality (4.5) from these two theorems. To begin with, let us choose a faithful representation V of G, where C acts by scalar multiplication. In particular, we can induce V from a faithful 1-dimensional representation $\chi\colon C = \boldsymbol{\mu}_p \to k^*$. We remark that χ exists because we assume that k contains a primitive pth root of unity and that we do not require V to be irreducible.

By (2.4), there exists a non-zero G-equivariant rational map $f\colon V \dashrightarrow V$ defined over k (or a *rational covariant*, for short) whose image has dimension $\operatorname{ed}(G)$. We will now replace f by a non-zero *homogeneous* rational covariant $f_{\text{hom}}\colon V \dashrightarrow V$. Here "homogeneous" means that $f_{\text{hom}}(tv) = t^d f_{\text{hom}}(v)$ for some $d \geq 1$. Roughly speaking, f_{hom} is the "leading term" of f, relative to some basis of V, and it can be chosen so that

$$\dim \operatorname{Im}(f_{\text{hom}}) \leq \dim \operatorname{Im}(f) = \operatorname{ed}(G)\,;$$

see [KLS09, Lemma 2.1]. Since we no longer need the original covariant f, we will replace f by f_{hom} and thus assume that f is homogeneous. Note that G may

not act faithfully on the image of f but this will not matter to us in the sequel. Since f is homogeneous and non-zero, it descends to an $\overline{G}$-equivariant rational map $\overline{f}\colon \mathbb{P}(V) \dashrightarrow \mathbb{P}(V)$ defined over k, whose image has dimension $\leq \operatorname{ed}_k(G) - 1$.

Now, given a field extension K/k and a $\overline{G}$-torsor $T \to \operatorname{Spec}(K)$ in $H^1(K, \overline{G})$, we can twist $\mathbb{P}(V)$ by T. The resulting K-variety ${}^T\mathbb{P}(V)$ is defined as the quotient of $\mathbb{P}(V) \times_K T$ by the natural (diagonal) $\overline{G}$-action. One can show, using the theory of descent, that this action is in fact free, i.e., the natural projection map $\mathbb{P}(V) \times_K T \to^T \mathbb{P}(V)$ is a $\overline{G}$-torsor; see [Fl07, Proposition 2.12 and Remark 2.13]. Note that we have encountered a variant of this construction in the previous section, where we wrote $\mathbb{P}(V) \times^{\overline{G}} T$ in place of ${}^T\mathbb{P}(V)$.

We also remark that ${}^T\mathbb{P}(V)$ is a K-form of $\mathbb{P}(V)$, i.e., is a Brauer-Severi variety defined over K. Indeed, if a field extension L/K splits T then it is easy to see that ${}^T\mathbb{P}(V)$ is isomorphic to $\mathbb{P}(V)$ over L. One can now show that the index of this Brauer-Severi variety equals the index of $\partial_K(T) \in H^2(K, \boldsymbol{\mu}_p)$; in particular, it is a power of p. By Theorem 4.5 we can choose K and T so that

$$\operatorname{ind}({}^T\mathbb{P}(V)) = \gcd_{\rho \in \operatorname{Rep}'} \dim(\rho)\,.$$

The $\overline{G}$-equivariant rational map $\overline{f}\colon \mathbb{P}(V) \dashrightarrow \mathbb{P}(V)$ induces a $\overline{G}$-equivariant rational map $\overline{f} \times \operatorname{id}\colon \mathbb{P}(V) \times T \dashrightarrow \mathbb{P}(V) \times T$, which, in turn, descends to a K-rational map ${}^T\overline{f}\colon {}^T\mathbb{P}(V) \dashrightarrow^T \mathbb{P}(V)$. Since the dimension of the image of $\overline{f}$ is $\leq \operatorname{ed}_k(G) - 1$, the dimension of the image of $\overline{f} \times \operatorname{id}$ is $\leq \operatorname{ed}_k(G) - 1 + \dim(G)$, and thus the dimension of the image of ${}^T\overline{f}$ is $\leq \operatorname{ed}_k(G) - 1$. By Theorem 4.4,

$$\operatorname{ed}_k(G) - 1 \geq \dim_K(\operatorname{Im}({}^T\overline{f})) \geq \operatorname{ind}({}^T\mathbb{P}(V)) - 1 = \gcd_{\rho \in \operatorname{Rep}'} \dim(\rho) - 1\,,$$

and (4.5) follows. □

Remark 4.6. Now suppose G is finite but $r \geq 1$ is arbitrary. The above argument has been modified by R. Lötscher [Lö08] to prove Theorem 4.1 in this more general setting. The proof relies on Theorem 4.5 and a generalization of Theorem 4.4 to the case where X is the direct product of Brauer-Severi varieties $X_1 \times \cdots \times X_r$, such that $\operatorname{ind}(X_i)$ is a power of p for each i; see [KM07, Theorem 2.1].

Here we choose our faithful k-representation V so that $V = V_1 \times \cdots \times V_r$, where C acts on V_i by scalar multiplication via a multiplicative character $\chi_i \in C^*$, and $\chi_1, \dots, \chi_r$ generate C^*. Once again, there exists a G-equivariant rational map $f\colon V \dashrightarrow V$ whose image has dimension $\operatorname{ed}(G)$. To make the rest of the argument go through in this setting one needs to show that f can be chosen to be multi-homogeneous, so that it will descend to a $\overline{G}$-equivarint rational map

$$\overline{f}\colon \mathbb{P}(V_1) \times \dots \mathbb{P}(V_r) \dashrightarrow \colon \mathbb{P}(V_1) \times \dots \mathbb{P}(V_r)\,.$$

If G is finite, this is done in [Lö08]. The rest of the argument goes through unchanged.

In his (still unpublished) Ph. D. thesis Lötscher has extended this proof of Theorem 4.1 to the case where G is no longer assumed to be finite. His only requirement

on G is that it should have a completely reducible faithful k-representation. The only known proof of Theorem 4.1 in full generality uses the notion of essential dimension for an algebraic stack, introduced in [BRV07]; cf. also [BRV10b]. For details, see [Me09, Theorem 4.8 and Example 3.7], in combination with [KM07, Theorem 4.4 and Remark 4.5].

5. Essential dimension at p and two types of problems

Let p be a prime integer. I will say that a field extension L/K is *prime-to-p* if $[L : K]$ is finite and not divisible by p.

This section is mostly "metamathematical"; the main point I would like to convey is that some problems in Galois cohomology and related areas are sensitive to prime-to-p extensions and some aren't. Loosely speaking, I will refer to such problems as being of "Type 2" and "Type 1", respectively.

More precisely, suppose we are given a functor $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}$ and we would like to show that some (or every) $\alpha \in \mathcal{F}(K)$ has a certain property. For example, this property may be that $\mathrm{ed}(\alpha) \leq d$ for a given d. If our functor is $\mathcal{F}(K) = H^1(K, \mathbf{O}_n)$, we may want to show that the quadratic form representing α is isotropic over K. If our functor is $\mathcal{F}(K) = H^1(K, \mathbf{PGL}_n)$, we may ask if the central simple algebra representing α is a crossed product. Note that in many interesting examples, including the three examples above, the property in question is functorial, i.e., if $\alpha \in \mathcal{F}(K)$ has it then so does α_L for every field extension L/K.

The problem of whether or not $\alpha \in \mathcal{F}(K)$ has a property we are interested in can be broken into two steps. For the first step we choose a prime p and ask whether or not α_L has the desired property for some prime-to-p extension L/K. This is what I call a *Type 1 problem*. If the answer is "no" for some p then we are done: we have solved the original problem in the negative. If the answer is "yes" for every prime p, then the remaining problem is to determine whether or not α itself has the desired property. I refer to problems of this type as *Type 2 problems*. Let me now explain what this means in the context of essential dimension.

Let $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a functor and $a \in \mathcal{F}(K)$ for some field K/k. The essential dimension $\mathrm{ed}(a; p)$ of a at a prime integer p is defined as the minimal value of $\mathrm{ed}(a_L)$, as L ranges over all finite field extensions L/K such that p does not divide the degree $[L : K]$. The essential dimension $\mathrm{ed}(\mathcal{F}; p)$ is then defined as the maximal value of $\mathrm{ed}(a; p)$, as K ranges over all field extensions of k and a ranges over $\mathcal{F}(K)$.

As usual, in the case where $\mathcal{F}(K) = H^1(K, G)$ for some algebraic group G defined over k, we will write $\mathrm{ed}(G; p)$ in place of $\mathrm{ed}(\mathcal{F}; p)$. Clearly, $\mathrm{ed}(a; p) \leq \mathrm{ed}(a)$, $\mathrm{ed}(\mathcal{F}; p) \leq \mathrm{ed}(\mathcal{F})$, and $\mathrm{ed}(G; p) \leq \mathrm{ed}(G)$ for every prime p.

In the previous three sections we proved a number of lower bounds of the form $\mathrm{ed}(G) \geq d$, where G is an algebraic group and d is a positive integer. A closer look reveals that in every single case the argument can be modified to show that $\mathrm{ed}(G; p) \geq d$, for a suitable prime p. (Usually p is a so-called "exceptional

prime" for G; see, e.g., [St75] or [Me09]. Sometimes there is more than one such prime.) In particular, the arguments we used in Examples 2.4, 2.5, 2.6 and 2.8 show that $\operatorname{ed}(\mathbf{G}_2; 2) = 3$, $\operatorname{ed}(\mathbf{O}_n; 2) = n$, $\operatorname{ed}(\boldsymbol{\mu}_p^r; p) = r$ and $\operatorname{ed}(\mathbf{PGL}_{p^s}; p) \geq 2s$, respectively. In Theorem 3.1 we may replace $\operatorname{ed}(G)$ by $\operatorname{ed}(G; p)$, as long as A is a p-group; see [GR07, Theorem 1.2(b)]. Consequently, in Corollary 3.6 $\operatorname{ed}(G)$ can be replaced by $\operatorname{ed}(G; p)$, where $p = 2$ in parts (a), (c), (d), (e), (g), (h), (i) and $p = 3$ in part (f). Theorem 4.1 remains valid with $\operatorname{ed}(G)$ replaced by $\operatorname{ed}(G; p)$.[2] Consequently, Corollary 4.2 remains valid if $\operatorname{ed}(G)$ is replaced by $\operatorname{ed}(G; p)$ (see [KM07]), and Corollary 4.3 remains valid if $\operatorname{ed}(\mathbf{Spin}_n)$ is replaced by $\operatorname{ed}(\mathbf{Spin}_n; 2)$ (see [BRV10a]).

The same is true of virtually all existing methods for proving lower bounds on $\operatorname{ed}(\mathcal{F})$ and, in particular, on $\operatorname{ed}(G)$: they are well suited to address Type 1 problems and poorly suited for Type 2 problems. In this context a Type 1 problem is the problem of computing $\operatorname{ed}(\mathcal{F}; p)$ for various primes p and a Type 2 problem is the problem of computing $\operatorname{ed}(\mathcal{F})$, assuming $\operatorname{ed}(\mathcal{F}; p)$ is known for all p.

I will now make an (admittedly vague) claim that this phenomenon can be observed in a broader context and illustrate it with three examples not directy related to essential dimension.

Observation 5.1. *Most existing methods in Galois cohomology and related areas apply to Type 1 problems only. On the other hand, many long-standing open problems are of Type 2.*

Example 5.2. The crossed product problem. Recall that a central simple algebra A/K of degree n is a crossed product if it contains a commutative Galois subalgebra L/K of degree n. We will restrict our attention to the case where $n = p^r$ is a prime power; the general case reduces to this one by the primary decomposition theorem. In 1972 Amitsur [Am72] showed that for $r \geq 3$ a generic division algebra $U(p^r)$ of degree p^r is not a crossed product, solving a long-standing open problem. L. H. Rowen and D. J. Saltman [RS92, Theorem 2.2] modified Amitsur's argument to show that, in fact, $UD(p^r)_L$ is a non-crossed product for any prime-to-p extension L of the center of $\mathrm{UD}(p^r)$.

For $r = 1, 2$ it is not known whether or not every central smple algebra A of degree p^r is a crossed product. It is, however, known that every such algebra becomes a crossed product after a prime-to-p extension of the center; see [RS92, Section 1]. In other words, the Type 1 part of the crossed product problem has been completely solved, and the remaining open questions, for algebras of degree p and p^2, are of Type 2.

Example 5.3. The torsion index. Let G be an algebraic group defined over k and K/k be a field extension. The torsion index n_α of $\alpha \in H^1(K, G)$ was defined by Grothendieck as the greatest common divisor of the degrees $[L : K]$, where L ranges over all finite splitting fields L/K. The torsion index n_G of $\mathcal{G}$ is then the least common multiple of n_α taken over all K/k and all $\alpha \in H^1(K, G)$. One can

[2] At the moment the only known proof of this relies on the stack-theoretic approach; see the references at the end of Remark 4.6. The more elementary "homogenization" argument I discussed in the previous section has not (yet?) yielded a lower bound on $\operatorname{ed}(G; p)$.

show that $n_G = n_{\alpha_{\rm ver}}$, where $\alpha_{\rm ver} \in H^1(K_{versal}, G)$ is a versal G-torsor. One can also show, using a theorem of J. Tits [Se95], that the prime divisors of n_G are precisely the exceptional primes of G.

The problem of computing n_G and more generally, of n_α for $\alpha \in H^1(K, G)$ can thus be rephrased as follows. Given an exceptional prime p for G, find the highest exponent d_p such that p^{d_p} divides $[L : K]$ for every splitting extension L/K. It is easy to see that this is a Type 1 problem; d does not change if we replace α by $\alpha_{K'}$, where K'/K is a prime-to-p extension. This torsion index n_G has been computed Tits and B. Totaro, for all simple groups G that are either simply connected or adjoint; for details and further references, see [Ti92, To05].

The remaining Type 2 problem consists of finding the possible values of $e_1, \dots, e_r$ such that $\alpha_{\rm ver}$ is split by a field extension L/K of degree $p_1^{e_1} \dots p_r^{e_r}$, where $p_1, \dots, p_r$ are the exceptional primes for G. This problem is open for many groups G. It is particularly natural for those G with only one exceptional prime, e.g., $G = \mathbf{Spin}_n$.

Example 5.4. Canonical dimension. Let G be a connected linear algebraic group defined over k, K/k be a field extension, and X be a G-torsor over K. Recall that the *canonical dimension* $\operatorname{cdim}(X)$ of X is the minimal value of $\dim_K(\operatorname{Im}(f))$, where the minimum is taken over all rational maps $f\colon X \dashrightarrow X$ defined over K. In particular, X is split if and only if $\operatorname{cdim}(X) = 0$. The maximal possible value of $\operatorname{cdim}(X)$, as X ranges over all G-torsors over K and K ranges over all field extensions of k, is called the canonical dimension of G and is denoted by $\operatorname{cdim}(G)$. Clearly $0 \le \operatorname{cdim}(G) \le \dim(G)$ and $\operatorname{cdim}(G) = 0$ if and only if G is special. For a detailed discussion of the notion of canonical dimension, we refer the reader to [BerR05], [KM06] and [Me09].

Computing the canonical dimension $\operatorname{cdim}(G)$ of an algebraic group G is a largely open Type 2 problem. The associated Type 1 problem of computing the canonical p-dimension $\operatorname{cdim}(G; p)$ has been solved by Karpenko-Merkurjev [KM06] and K. Zainoulline [Zai07].

6. Finite groups of low essential dimension

Suppose we would like to determine the essential dimension of a finite group G. To keep things simple, we will assume throughout this section that, unless otherwise specified, the base field k is algebraically closed and of characteristic 0. Let us break up the problem of computing $\operatorname{ed}(G)$ into a Type 1 part and a Type 2 part, as we did in the previous section.

The Type 1 problem is to determine $\operatorname{ed}(G; p)$ for a prime p. It is not difficult to show that $\operatorname{ed}(G; p) = \operatorname{ed}(G_p; p)$, where p is a prime and G_p is a p-Sylow subgroup of G; see [MR09a, Lemma 4.1] or [Me96, Proposition 5.1]. The value of $\operatorname{ed}(G_p; p)$ is given by Corollary 4.2. So, to the extent that we are able to compute the dimension of the smallest faithful representation of G_p, our Type 1 problem has been completely solved, i.e., we know $\operatorname{ed}(G; p)$ for every prime p.

Now our best hope of computing $\operatorname{ed}(G)$ is to obtain a strong upper bound $\operatorname{ed}(G) \le n$, e.g., by constructing an explicit G-equivariant dominant rational map

$V \dashrightarrow Y$, as in (2.2), with $\dim(Y) = n$. If $n = \mathrm{ed}(G; p)$ then we conclude that $\mathrm{ed}(G) = \mathrm{ed}(G; p)$, i.e., the remaining Type 2 problem is trivial, and we are done. In particular, this is what happens if G is a p-group.

If the best upper bound we can prove is $\mathrm{ed}(G) \leq n$, where n is strictly greater than $\mathrm{ed}(G; p)$ for every p then we are entering rather murky waters. Example 6.2 below shows that it is indeed possible for $\mathrm{ed}(G)$ to be strictly greater than $\mathrm{ed}(G; p)$ for every prime p. On the other hand, there is no general method for computing $\mathrm{ed}(G)$ in such cases. The only ray of light in this situation is that it may be possible to prove a lower bound of the form $\mathrm{ed}(G) > d$, where $d = 1$ or (with more effort) 2 and sometimes even 3.

Let us start with the simplest case where $d = 1$.

Lemma 6.1. (cf. [BuR97, Theorem 6.2]) Let G be a finite group. Then

(a) $\mathrm{ed}(G) = 0$ if and only if $G = \{1\}$,

(b) $\mathrm{ed}(G) = 1$ if and only if $G \neq \{1\}$ is either cyclic or odd dihedral.

Proof. Let V be a faithful linear representation of G. By (2.4) there exists a dominant G-equivariant rational map $V \dashrightarrow X$, where G acts faithfully on X and $\dim(X) = \mathrm{ed}(G)$.

(a) If $\mathrm{ed}(G) = 0$ then X is a point. This forces G to be trivial.

(b) If $\mathrm{ed}(G) = 1$ then X is a rational curve, by a theorem of Lüroth. We may assume that X is smooth and complete, i.e., we may assume that $X = \mathbb{P}^1$. Consequently, G is isomorphic to a subgroup of $\mathbf{PGL}_2$. By a theorem of Klein [Kl1884], G is cyclic, dihedral or is isomorphic to S_4, A_4 or S_5. If G is an even dihedral group, S_4, A_4 or S_5 then G contains a copy of $\mathbb{Z}/2 \times \mathbb{Z}/2\mathbb{Z} \simeq \boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2$. Hence,

$$\mathrm{ed}(G) \geq \mathrm{ed}(\boldsymbol{\mu}_2^2) = 2\,;$$

see Example 2.6. This means that if $\mathrm{ed}(G) = 1$ then G is cyclic or odd dihedral.

Conversely, if G is cyclic or odd dihedral then one can easily check that, under our assumption on k, $\mathrm{ed}_k(G) = 1$. □

Example 6.2. Suppose q and r are odd primes and q divides $r - 1$. Let $G = \mathbb{Z}/r\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ be a non-abelian group of order rq. Clearly all Sylow subgroups of G are cyclic; hence, $\mathrm{ed}(G; p) \leq 1$ for every prime p. On the other hand, since G is neither cyclic nor odd dihedral, Lemma 6.1 tells us that $\mathrm{ed}(G) \geq 2$. □

Similar reasoning can sometimes be used to show that $\mathrm{ed}(G) > 2$. Indeed, assume that $\mathrm{ed}(G) = 2$. Then there is a faithful representation V of G and a dominant rational G-equivariant map

$$V \dashrightarrow X\,, \tag{6.1}$$

where G acts faithfully on X and $\dim(X) = 2$. By a theorem of G. Castelnuovo, X is a rational surface. Furthermore, we may assume that X is smooth, complete, and is minimal with these properties (i.e., does not allow any G-equivariant blow-downs $X \to X_0$, with X_0 smooth). Such surfaces (called minimal rational G-surfaces)

have been classified by Yu. Manin and V. Iskovskikh, following up on classical work of F. Enriques; for details and further references, see [Du09a]. This classification is significantly more complicated than Klein's classification of rational curves but one can use it to determine, at least in principle, which finite groups G can act on a rational surface and describe all such actions; cf. [DI06]. Once all minimal rational G-surfaces X are accounted for, one then needs to decide, for each X, whether or not the G-action is versal, i.e., whether or not a dominant rational G-equivariant map (6.1) can exist for some faithful linear representation $G \to \mathbf{GL}(V)$. Note that by the Going Down Theorem 3.2 if some abelian subgroup A of G acts on X without fixed points then the G-action on X cannot be versal. If every minimal rational G-surface X can be ruled out this way (i.e., is shown to be non-versal) then one can conclude that $\mathrm{ed}(G) > 2$.

This approach was used by Serre to show that $\mathrm{ed}(\mathrm{A}_6) > 2$; see [Se08, Proposition 3.6]. Since the upper bound $\mathrm{ed}(\mathrm{A}_6) \le \mathrm{ed}(\mathrm{S}_6) \le 3$ was previously known (cf. (7.2) and the references there) this implies $\mathrm{ed}(\mathrm{A}_6) = 3$. Note that

$$\mathrm{ed}(\mathrm{A}_6; p) = \begin{cases} 2, \text{ if } p = 2 \text{ or } 3, \\ 1, \text{ if } p = 5, \text{ and} \\ 0, \text{ otherwise;} \end{cases}$$

see (7.1). A. Duncan [Du09a] has recently refined this approach to give the following complete classification of groups of essential dimension ≤ 2.

Theorem 6.3. *Let k be an algebraically closed field of characteristic 0 and $T = \mathbb{G}_m^2$ be the 2-dimensional torus over k. A finite group G has essential dimension ≤ 2 if and only if it is isomorphic to a subgroup of one of the following groups:*

(1) The general linear group $\mathbf{GL}_2(k)$,

(2) $\mathrm{PSL}_2(\mathbb{F}_7)$, the simple group of order 168,

(3) S_5, the symmetric group on 5 letters,

(4) $T \rtimes G_1$, where $|G \cap T|$ is coprime to 2 and 3 and

$$G_1 = \left\langle \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq D_{12},$$

(5) $T \rtimes G_2$, where $|G \cap T|$ is coprime to 2 and

$$G_2 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq D_8,$$

(6) $T \rtimes G_3$, where $|G \cap T|$ is coprime to 3 and

$$G_3 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\rangle \simeq \mathrm{S}_3,$$

(7) $T \rtimes G_4$, where $|G \cap T|$ is coprime to 3 and

$$G_4 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq \mathrm{S}_3\,.$$

If one would like to go one step further and show that $\mathrm{ed}(G) > 3$ by this method, for a particular finite group G, the analysis becomes considerably more complicated. First of all, while X in (6.1) is still unirational, if $\dim(X) \geq 3$, we can no longer conclude that it is rational. Secondly, there is no analogue of the Enriques-Manin-Iskovskikh classification of rational surfaces in higher dimensions. Nevertheless, in dimension 3 one can sometimes use Mori theory to get a handle on X. In particular, Yu. Prokhorov [Pr09] recently classified the finite simple groups with faithful actions on rationally connected threefolds. This classification was used by Duncan [Du09b] to prove the following theorem, which is out of the reach of all previously existing methods.

Theorem 6.4. *Let k be a field of characteristic 0. Then $\mathrm{ed}_k(A_7) = \mathrm{ed}_k(S_7) = 4$.*

Note that $\mathrm{ed}(\mathrm{A}_7; p) \leq \mathrm{ed}(\mathrm{S}_7; p) \leq 3$ for every prime p; cf. [MR09a, Corollary 4.2].

7. Open problems

7.1. Strongly incompressible elements. Let $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor. We say that an object $\alpha \in \mathcal{F}(K)$ is *strongly incompressible* if α does not descend to any proper subfield of K.

Examples of strongly incompressible elements in the case where G is a finite group, K is the function field of an algebraic curve Y over k, and $\mathcal{F} = H^1(*, G)$, are given in [Rei04]. In these examples α is represented by a (possibly ramified) G-Galois cover $X \to Y$. I do not know any such examples in higher dimensions.

Problem. *Does there exist a finitely generated field extension K/k of transcendence degree ≥ 2 and a finite group G (or an algebraic group G defined over k) such that $H^1(K, G)$ has a strongly incompressible element?*

For $G = \mathrm{O}_n$ Problem 7.1 is closely related to the questions of existence of a minimal field of definition of a quadratic form posed at the beginning of Section 1.

It is easy to see that if an element of $H^1(K, \mathbf{PGL}_n)$ represented by a non-split central simple algebra A is strongly incompressible and $\mathrm{tr\,deg}_k(K) \geq 2$ then A cannot be cyclic. In particular, if $n = p$ is a prime then the existence of a strongly incompressible element in $H^1(K, \mathbf{PGL}_n)$ would imply the existence of a non-cyclic algebra of degree p over K, thus solving (in the negative) the long-standing cyclicity conjecture of Albert.

7.2. Symmetric groups.

Problem. *What is the essential dimension of the symmetric group S_n? of the alternating group A_n?*

Let us assume that $\mathrm{char}(k)$ does not divide $n!$. Then in the language of Section 5, the above problem is of Type 2. The associated Type 1 problem has been

solved: $\mathrm{ed}(\mathrm{S}_n; p) = [n/p]$ (see [MR09a, Corollary 4.2]) and similarly

$$\mathrm{ed}(\mathrm{A}_n; p) = \begin{cases} 2[\frac{n}{4}], \text{ if } p = 2, \text{ and} \\ [\frac{n}{p}], \text{ otherwise.} \end{cases} \tag{7.1}$$

It is shown in [BuR97] that $\mathrm{ed}(\mathrm{S}_{n+2}) \geq \mathrm{ed}(\mathrm{S}_n) + 1$, $\mathrm{ed}(\mathrm{A}_{n+4}) \geq \mathrm{ed}(\mathrm{A}_n) + 2$, and

$$\mathrm{ed}(\mathrm{A}_n) \leq \mathrm{ed}(\mathrm{S}_n) \leq n - 3\,. \tag{7.2}$$

I believe the true value of $\mathrm{ed}(\mathrm{S}_n)$ is closer to $n-3$ than to $[n/2]$; the only piece of evidence for this is Theorem 6.4.

7.3. Cyclic groups.

Problem. *What is the essential dimension* $\mathrm{ed}_k(\mathbb{Z}/n\mathbb{Z})$*?*

Let us first consider the case where $\mathrm{char}(k)$ is prime to n. Under further assumptions that $n = p^r$ is a prime power and k contains a primitive pth root of unity ζ_p, Problem 7.3 has been solved by Florence [Fl07]. It is now a special case of Corollary 4.2:

$$\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z}) = \mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z}; p) = [k(\zeta_{p^r}) : k]\,; \tag{7.3}$$

see [KM07, Corollary 5.2]. This also settles the (Type 1) problem of computing $\mathrm{ed}_k(\mathbb{Z}/n\mathbb{Z}; p)$ for every integer $n \geq 1$ and every prime p. Indeed,

$$\mathrm{ed}_k(\mathbb{Z}/n\mathbb{Z}; p) = \mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z}; p)\,,$$

where p^r is the largest power of p dividing n. Also, since $[k(\zeta_p) : k]$ is prime to p, for the purpose of computing $\mathrm{ed}_k(\mathbb{Z}/n\mathbb{Z}; p)$ we are allowed to replace k by $k(\zeta_p)$; then formula (7.3) applies.

If we do not assume that $\zeta_p \in k$ then the best currently known upper bound on $\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z})$, due to A. Ledet [Led02], is $\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z}) \leq \varphi(d)p^e$. Here $[k(\zeta_{p^r}) : k] = dp^e$, where d divides $p-1$, and φ is the Euler φ-function.

Now let us suppose $\mathrm{char}(k) = p > 0$. Here it is easy to see that $\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z}) \leq r$; Ledet [Led04] conjectured that equality holds. This seems to be out of reach at the moment, at least for $r \geq 5$. More generally, essential dimension of finite (but not necessarily smooth) group schemes over a field k of prime characteristic is poorly understood; some interesting results in this direction can be found in [TV10].

7.4. Quadratic forms. Let us assume that $\mathrm{char}(k) \neq 2$. The following question is due to J.-P. Serre (private communication, April 2003).

Problem. *If q is a quadratic form over K/k, is it true that* $\mathrm{ed}(q; 2) = ed(q)$*?*

A similar question for central simple algebras A of prime power degree p^r is also open: is it true that $\mathrm{ed}(A; p) = \mathrm{ed}(A)$?

Here is another natural essential dimension question in the context of quadratic form theory.

Problem. *Assume* $\mathrm{char}(k) \neq 2$. *If* q *and* q' *are Witt equivalent quadratic forms over a field* K/k, *is it true that* $\mathrm{ed}_k(q) = \mathrm{ed}_k(q')$*?*

The analogous question for central simple algebras, with Witt equivalence replaced by Brauer equivalence, has a negative answer. Indeed, assume k contains a primitive 4th root of unity and $D = UD_k(4)$ is a universal division algebra of degree 4. Then $\mathrm{ed}(D) = 5$ (see [Me10a, Corollary 1.2], cf. also [Rost00]) while $\mathrm{ed}\, \mathrm{M}_2(D) = 4$ (see [LRRS03, Corollary 1.4]).

7.5. Canonical dimension of Brauer-Severi varieties. Let X be a smooth complete variety defined over a field K/k. The canonical dimension $\mathrm{cdim}(X)$ is the minimal dimension of the image of a K-rational map $X \dashrightarrow X$. For a detailed discussion of this notion, see [KM06] and [Me09].

Conjecture. (Colliot-Thélène, Karpenko, Merkurjev [CKM08]) *Suppose* X *is a Brauer-Severi variety of index* n. *If* $n = p_1^{e_1} \dots p_r^{e_r}$ *is the prime decomposition of* n *then* $\mathrm{cdim}(X) = p_1^{e_1} + \dots + p_r^{e_r} - r$.

This is a Type 2 problem. The associated Type 1 question is completely answered by Theorem 4.4: $\mathrm{cdim}(X; p_i) = p_i^{e_1} - 1$. Also, by Theorem 4.4 the conjecture is true if $r = 1$. The only other case where this conjecture has been proved is $n = 6$; see [CKM08]. The proof is similar in spirit to the results of Section 6; it relies on the classification of rational surfaces over a non-algebraically closed field. For other values of n the conjecture has not even been checked for one particular X.

Note that the maximal value of $\mathrm{cdim}(X)$, as X ranges over the Brauer-Severi varieties of index n, equals $\mathrm{cdim}(\mathbf{PGL}_n)$. As I mentioned in Example 5.4, computing the canonical dimension $\mathrm{cdim}(G)$ of a linear algebraic (and in particular, simple) group G is a largely open Type 2 problem. In particular, the exact value of $\mathrm{cdim}(\mathbf{PGL}_n)$ is only known if $n = 6$ or a prime power.

7.6. Essential dimension of $\mathbf{PGL}_n$.

Problem. *What is* $\mathrm{ed}(\mathbf{PGL}_n; p)$*?* $\mathrm{ed}(\mathbf{PGL}_n)$*?*

As I mentioned in Section 1, this problem originated in the work of Procesi [Pr67]; for a more detailed history, see [MR09a, MR09b]. The second question appears to be out of reach at the moment, except for a few small values of n. However, there has been a great deal of progress on the first (Type 1) question in the past year. By primary decomposition $\mathrm{ed}(\mathbf{PGL}_n; p) = \mathrm{ed}(\mathbf{PGL}_{p^r}; p)$, where p^r is the highest power of p dividing n. Thus we may assume that $n = p^r$. As I mentioned in Example 5.2, every central simple algebra A of degree p becomes cyclic after a prime-to-p extension. Hence, $\mathrm{ed}(\mathbf{PGL}_p; p) = 2$; cf. [RY00, Lemma 8.5.7]. For $r \geq 2$ we have

$$(r-1)p^r + 1 \leq \mathrm{ed}(\mathbf{PGL}_{p^r}; p) \leq p^{2r-2} + 1\,.$$

The lower bound is due to Merkurjev [Me10b]; the upper bound is proved in a recent preprint of A. Ruozzi [Ru10]. (A weaker upper bound, $\mathrm{ed}(\mathbf{PGL}_n; p) \leq$

$2p^{2r-2} - p^r + 1$, is proved in [MR09b].) In particular, $\mathrm{ed}(\mathbf{PGL}_{p^2}; p) = p^2 + 1$; see [Me10a].

Note that the argument in [Me10b] shows that if A is a generic $(\mathbb{Z}/p\mathbb{Z})^r$-crossed product then $\mathrm{ed}(A; p) = (r-1)p^r + 1$. As mentioned in Example 5.2, for $r \geq 3$ a general division algebra A/K of degree p^r is not a crossed product and neither is $A_L = A \otimes_K L$ for any prime-to-p extension L/K. Thus for $r \geq 3$ it is reasonable to expect the true value of $\mathrm{ed}(\mathbf{PGL}_{p^r}; p)$ to be strictly greater than $(r-1)p^r + 1$.

7.7. Spinor groups.

Problem. *Does Corollary 4.3 remain valid over an algebraically closed field of characteristic $p > 2$?*

As I mentioned at the beginning of the proof of Corollary 4.3, the lower bound in each part remains valid over any field of characteristic > 2. Consequently, Problem 7.7 concerns only the upper bounds. It would, in fact, suffice to show that the spin representation V_{spin} and the half-spin representation $V_{\mathrm{half-spin}}$ of $\mathbf{Spin}_n$ are generically free, if n is odd or $n \equiv 2 \pmod 4$, respectively; see [BRV10a, Lemma 3-7 and Remark 3-8].

Problem. *What is* $\mathrm{ed}_k(\mathbf{Spin}_{4m}; 2)$*?* $\mathrm{ed}_k(\mathbf{Spin}_{4m})$*? Here $m \geq 5$ is an integer.*

Corollary 4.3 answers this question in the case where m is a power of 2. In the other cases there is a gap between the upper and the lower bound in that corollary, even for $k = \mathbb{C}$.

7.8. Exceptional groups.

Problem. *Let G be an exceptional simple group and p be an exceptional prime for G. What is* $\mathrm{ed}_k(G; p)$*?* $\mathrm{ed}_k(G)$*? Here we assume that k is an algebraically closed field of characteristic* 0 *(or at least,* $\mathrm{char}(k)$ *is not an exceptional prime for G).*

For the exceptional group $G = \mathbf{G}_2$ we know that $\mathrm{ed}(\mathbf{G}_2) = \mathrm{ed}(\mathbf{G}_2; 2) = 3$; see Example 2.4.

For $G = \mathbf{F}_4$, the Type 1 problem has been completely solved: $\mathrm{ed}(\mathbf{F}_4; 2) = 5$ (see [MacD08, Section 5]), $\mathrm{ed}(\mathbf{F}_4; 3) = 3$ (see [GR07, Example 9.3]), and $\mathrm{ed}(\mathbf{F}_4; p) = 0$ for all other primes. It is claimed in [Ko00] that $\mathrm{ed}(\mathbf{F}_4) = 5$. However, the argument there appears to be incomplete, so the (Type 2) problem of computing $\mathrm{ed}(\mathbf{F}_4)$ remains open.

The situation is similar for the simply connected group $\mathbf{E}_6^{sc}$. The Type 1 problem has been solved,

$$\mathrm{ed}(\mathbf{E}_6^{sc}; p) = \begin{cases} 3, \text{ if } p = 2 \text{ (see [GR07, Example 9.4])}, \\ 4, \text{ if } p = 3 \text{ (see [RY00, Theorem 8.19.4 and Remark 8.20])}, \\ 0, \text{ if } p \geq 5. \end{cases}$$

(For the upper bound on the second line, cf. also [Gar09, 11.1].) The Type 2 problem of computing $\mathrm{ed}(\mathbf{E}_6^{sc})$ remains open.

For the other exceptional groups, $\mathbf{E}_6^{ad}$, $\mathbf{E}_7^{ad}$ $\mathbf{E}_7^{sc}$ and $\mathbf{E}_8$, even the Type 1 problem of computing $\operatorname{ed}(G;p)$ is only partially solved. It is known that $\operatorname{ed}(\mathbf{E}_6^{ad};2)=3$ (see [GR07, Remark 9.7]), $\operatorname{ed}(\mathbf{E}_7^{ad};3)=\operatorname{ed}(\mathbf{E}_7^{sc};3)=3$ (see [GR07, Example 9.6 and Remark 9.7]; cf. also [Gar09, Lemma 13.1]) and $\operatorname{ed}(\mathbf{E}_8;5)=3$ (see [RY00, Theorem 18.19.9] and [Gar09, Proposition 14.7]). On the other hand, the values of $\operatorname{ed}(\mathbf{E}_6^{ad};3)$, $\operatorname{ed}(\mathbf{E}_7^{ad};2)$, $\operatorname{ed}(\mathbf{E}_7^{sc};2)$, $\operatorname{ed}(\mathbf{E}_8;3)$ and $\operatorname{ed}(\mathbf{E}_8;2)$ are wide open, even for $k=\mathbb{C}$. For example, the best known lower bound on $\operatorname{ed}_{\mathbb{C}}(\mathbf{E}_8;2)$ is 9 (see Corollary 3.6(i)) but the best upper bound I know is $\operatorname{ed}_{\mathbb{C}}(\mathbf{E}_8;2)\le 120$. The essential dimension $\operatorname{ed}(G)$ for these groups is largely uncharted territory, beyond the upper bounds in [Lem04].

7.9. Groups whose connected component is a torus. Let G be an algebraic group over k and p be a prime. We say that a linear representation $\phi\colon G\to \mathbf{GL}(V)$ is *p-faithful* (respectively, *p-generically free*) if $\operatorname{Ker}(\phi)$ is a finite group of order prime to p and ϕ descends to a faithful (respectively, generically free) representation of $G/\operatorname{Ker}(\phi)$.

Suppose the connected component G^0 of G is a k-torus. One reason such groups are of interest is that the normalizer G of a maximal torus in a reductive k-group Γ is of this form and $\operatorname{ed}(G)$ (respectively $\operatorname{ed}(G;p)$) is an upper bound on $\operatorname{ed}(\Gamma)$ (respectively, $\operatorname{ed}(\Gamma;p)$). The last assertion follows from [Se02, III.4.3, Lemma 6], in combination with Lemma 2.2.

For the sake of computing $\operatorname{ed}(G;p)$ we may assume that G/G^0 is a p-group and k is p-closed, i.e., the degree of every finite field extension k'/k is a power of p; see [LMMR09, Lemma 3.3]. It is shown in [LMMR09] that

$$\min\dim\nu-\dim(G)\le\operatorname{ed}(G;p)\le\min\dim\rho-\dim G\,, \tag{7.4}$$

where the two minima are taken over all p-faithful representations ν, and p-generically free representations ρ, respectively. In the case where $G=T$ is a torus or $G=F$ is a finite p-group or, more generally, G is a direct product $T\times F$, a faithful representation is automatically generically free. Thus in these cases the lower and upper bounds of (7.4) coincide, yielding the exact value of $\operatorname{ed}_k(G;p)$. If we only assume that G^0 is a torus, I do not know how to close the gap between the lower and the upper bound in (7.4). However, in every example I have been able to work out the upper bound in (7.4) is, in fact, sharp.

Conjecture. ([LMMR09]) *Let G be an extension of a p-group by a torus, defined over a p-closed field k of characteristic $\ne p$. Then* $\operatorname{ed}(G;p)=\min\dim\rho-\dim G$, *where the minimum is taken over all p-generically free k-representations ρ of G.*

References

[Am72] S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–420.

[AP71] E. M. Andreev, V. L. Popov, *The stationary subgroups of points in general position in a representation space of a semisimple Lie group* (in Russian), Funkcional.

Anal. i Priložen. **5** (1971), no. 4, 1–8. English Translation in Functional Anal. Appl. **5** (1971), 265–271.

[BF03] G. Berhuy and G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330.

[BerR05] G. Berhuy, Z. Reichstein, *On the notion of canonical dimension for algebraic groups*, Adv. Math. **198** (2005), no. 1, 128–171.

[Br98] M. Brion, *The behaviour at infinity of the Bruhat decomposition*, Comment. Math. Helv. **73** (1998), no. 1, 137–174.

[BRV07] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension and algebraic stacks*, 2007, arXiv:math/0701903.

[BRV10a] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension, spinor groups and quadratic forms*, Annals of Math., **171**, no. 1 (2010), 533–544.

[BRV10b] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension of moduli of curves and other algebraic stacks*, with an appendix by N. Fakhruddin, J. European Math. Soc., to appear.

[BuR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179.

[CGR06] V. Chernousov, Ph. Gille, Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), 561–581.

[CS06] V. Chernousov and J.-P. Serre, *Lower bounds for essential dimensions via orthogonal representations*, J. Algebra **305** (2006), no. 2, 1055–1070.

[CKM08] J.-L. Colliot-Thélène, N. A. Karpenko, A. S. Merkurjev, *Rational surfaces and the canonical dimension of the group* $\mathbf{PGL}_6$ (in Russian), Algebra i Analiz **19** (2007), no. 5, 159–178. English translation in St. Petersburg Math. J. **19** (2008), no. 5, 793–804.

[DI06] I. V. Dolgachev, V. A. Iskovskikh, *Finite subgroups of the plane Cremona group*, In Algebra, Arithmetic and Geometry: In honor of Yu. I. Manin, 443–549, vol. 1, Progress in Math. **269**, Springer-Verlag, 2009.

[Du09a] A. Duncan, *Finite Groups of Essential Dimension 2*, arXiv:0912.1644.

[Du09b] A. Duncan, *Essential Dimensions of* A_7 *and* S_7, Math. Res. Lett. **17** (2010), no. 2, 265–268.

[Fl07] M. Florence, *On the essential dimension of cyclic p-groups*, Inventiones Math., **171** (2007), 175–189.

[Gar01] S. Garibaldi, *Structurable Algebras and Groups of Type* E_6 *and* E_7, J. Algebra, **236** (2001), no. 2, 651–691.

[Gar09] S. Garibaldi, *Cohomological invariants: exceptional groups and spin groups*, with an appendix by D. W. Hoffmann, Memoirs of the American Mathematical Society **200** (2009), no. 937.

[GMS03] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003.

[GR07] Ph. Gille, Z. Reichstein, *A lower bound on the essential dimension of a connected linear group*, Comment. Math. Helv. **84** (2009), no. 1, 189-212.

[Gro58] A. Grothendieck, *Torsion homologique et sections rationnelles*, in: *Anneaux de Chow et Applications*, Séminaire C. Chevalley, 1958, exposé 5.

[Kahn00] B. Kahn, *Comparison of some field invariants*, J. Algebra, **232** (2000), no. 2, 485–492.

[Kar00] N. A. Karpenko, *On anisotropy of orthogonal involutions*, J. Ramanujan Math. Soc. **15** (2000), no. 1, 1–22.

[KM06] N. A. Karpenko, and A. S. Merkurjev, *Canonical p-dimension of algebraic groups*, Adv. Math. **205** (2006), no. 2, 410–433.

[KM07] N. Karpenko, A. Merkurjev, *Essential dimension of finite p-groups*, Inventiones Math., **172**, (2008), no. 3, 491–508.

[Kl1884] F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom 5ten Grade*, 1884.

[Ko00] V. E. Kordonskiĭ, *On the essential dimension and Serre's conjecture II for exceptional groups*, Mat. Zametki, **68**, (2000), no. 4, 539–547.

[KLS09] H. Kraft, R. Lötscher, G. M. Schwarz, *Compression of finite group actions and covariant dimension. II*, J. Algebra **322** (2009), no. 1, 94–107.

[Led02] A. Ledet, *On the essential dimension of some semi-direct products*, Canad. Math. Bull. **45** (2002), no. 3, 422–427.

[Led04] A. Ledet, *On the essential dimension of p-groups*, Galois theory and modular forms, 159–172, Dev. Math., 11, Kluwer Acad. Publ., Boston, MA, 2004.

[Lem04] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transform. Groups **9** (2004), no. 4, 337–379.

[LRRS03] M. Lorenz, Z. Reichstein, L. H. Rowen, D. J. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670.

[Lö08] R. Lötscher, *Application of multihomogeneous covariants to the essential dimension of finite groups*, arXiv:0811.3852.

[LMMR09] R. Lötscher, M. MacDonald, A. Meyer, Z. Reichstein, *Essential p-dimension of algebraic tori*, arXiv:0910.5574.

[MacD08] M. MacDonald, *Cohomological invariants of odd degree Jordan algebras*, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 2, 295–303.

[Me96] A. S. Merkurjev, *Maximal indexes of Tits algebras*, Doc. Math. **1** (1996), no. 12, 229–243

[Me09] A. S Merkurjev, *Essential dimension*, in Quadratic forms – algebra, arithmetic, and geometry (R. Baeza, W.K. Chan, D.W. Hoffmann, and R. Schulze-Pillot, eds.), Contemporary Mathematics **493** (2009), 299–326.

[Me10a] A. S. Merkurjev, *Essential p-dimension of* $\mathbf{PGL}(p^2)$, *J. Amer. Math. Soc.* **23** (2010), 693-712.

[Me10b] A. Merkurjev *A lower bound on the essential dimension of simple algebras*, `http://www.math.ucla.edu/~merkurev/publicat.htm`.

[MR09a] A. Meyer, Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra Number Theory, **3**, no. 4 (2009), 467–487.

[MR09b] A. Meyer, Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, to appear in Journal of Algebra, arXiv:0907.4496

[Pf95] A. Pfister, *Quadratic forms with applications to geometry and topology*, Cambridge University Press, 1995.

[Po85] A. M. Popov, *Finite stationary subgroups in general position of simple linear Lie groups* (Russian), Trudy Moskov. Mat. Obshch. **48** (1985), 7–59.

English translation in *Transactions of the Moscow Mathematical Society*, A translation of Trudy Moskov. Mat. Obshch. 48 (1985). Trans. Moscow Math. Soc. 1986. American Mathematical Society, Providence, RI, 1986, 3–63.

[Pr67] C. Procesi, *Non-commutative affine rings*, Atti Acc. Naz. Lincei, S. VIII, v. VIII, fo. 6 (1967), 239–255.

[Pr09] Yu. Prokhorov, *Simple finite subgroups of the Cremona group of rank* 3, arXiv:0908.0678

[Rei99] Z. Reichstein, *On a theorem of Hermite and Joubert*, Can. J. Math. **51**, No.1, 69-95 (1999).

[Rei00] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.

[Rei04] Z. Reichstein, *Compressions of group actions*, Invariant theory in all characteristics, 199–202, CRM Proc. Lecture Notes, 35, Amer. Math. Soc., Providence, RI, 2004.

[RY00] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, With an appendix by János Kollár and Endre Szabó.

[Rost00] M. Rost, *Computation of some essential dimensions*, 2000, `http://www.math.uni-bielefeld.de/~rost/ed.html`

[Rost06] M. Rost, *On the Galois cohomology of* **Spin**(14), `http://www.mathematik.uni-bielefeld.de/~rost/spin-14.html#ed`

[RS92] L. H. Rowen, D. J. Saltman, *Prime-to-p extensions of division algebras*, Israel J. Math. **78** (1992), no. 2-3, 197–207.

[Ru10] A. Ruozzi, *Essential p-dimension of* **PGL**, `http://www.mathematik.uni-bielefeld.de/lag/man/385.html`

[Se58] J.-P. Serre, *Espaces fibrés algébriques*, in: *Anneaux de Chow et Applications*, Séminaire C. Chevalley, 1958, exposé 1. Reprinted in J.-P. Serre, *Exposés de séminaires* 1950–1999, deuxième édition, augmentée, Documents mathématiques **1**, Société mathématique de France 2008, 107–140.

[Se95] J.-P. Serre, *Cohomologie galoisienne: progrès et problèmes*, Séminaire Bourbaki, Vol. 1993/94. Astérisque **227** (1995), Exp. No. 783, 4, 229–257.

[Se02] J.-P. Serre, *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.

[Se08] J.-P. Serre, *Le group de cremona et ses sous-groupes finis*, Séminaire Bourbaki, 2008/2009, Exp. No. 1000.

[St75] R. Steinberg, *Torsion in reductive groups*, Advances in Math. **15** (1975), 63–92.

[Ti92] J. Tits, *Sur les degrés des extensions de corps déployant les groupes algébriques simples*, C. R. Acad. Sci. Paris, t. 315, Série I (1992), 1131–1138.

[TV10] D. Tossici, A. Vistoli, *On the essential dimension of infinitesimal group schemes*, arXiv:1001.3988.

[To05] B. Totaro, *The torsion index of E_8 and other groups*, Duke Math. J. **129** (2005), no. 2, 219–248.

[Woo89] J. A. Wood, *Spinor groups and algebraic coding theory*, J. Combin. Theory Ser. A **51** (1989), no. 2, 277–313.

[Zai07] K. Zainoulline, *Canonical p-dimensions of algebraic groups and degrees of basic polynomial invariants*, Bull. Lond. Math. Soc. **39** (2007), no. 2, 301–304.

Department of Mathematics, University of British Columbia, Vancouver, BC, Canada
E-mail: reichst@math.ubc.ca