ESSENTIAL DIMENSIONS OF ALGEBRAIC GROUPS AND A RESOLUTION THEOREM FOR G-VARIETIES

ZINOVY REICHSTEIN AND BORIS YOUSSIN,
(WITH AN APPENDIX BY JÁNOS KOLLÁR AND ENDRE SZABÓ)

Abstract. Let G be an algebraic group and let X be a generically free G-variety. We show that X can be transformed, by a sequence of blowups with smooth G-equivariant centers, into a G-variety X' with the following property: the stabilizer of every point of X' is isomorphic to a semidirect product $U \rtimes A$ of a unipotent group U and a diagonalizable group A.

As an application of this result, we prove new lower bounds on essential dimensions of some algebraic groups. We also show that certain polynomials in one variable cannot be simplified by a Tschirnhaus transformation.

Contents

1991 *Mathematics Subject Classification.* 14L30, 14E15, 14E05, 12E05, 20G10.
Z. Reichstein was partially supported by NSF grant DMS-9801675.

1. Introduction

Let k be an algebraically closed base field of characteristic zero, let G be an algebraic group and let X be a G-variety, both defined over k. Assume X is generically free, i.e., the G-action is free on a dense open subset of X. Recall that by a theorem of Rosenlicht [Ro_1], [Ro_2] the rational quotient map $X \dashrightarrow B$ separates orbits of X in general position; in other words, we can think of X as a G-torsor over B.

We shall say that X is defined in dimension d if there exists a dominant rational map $X \dashrightarrow X_1$ of generically free G-varieties

$$\begin{array}{ccc} X & \dashrightarrow & X_1 \\ \pi \downarrow & & \downarrow \pi_1 \\ B & \dashrightarrow & B_1 \end{array} \tag{1.1}$$

with $\dim(B_1) \leq d$. (Here the vertical arrows represent rational quotient maps for the G-action.) The smallest integer d such that X is defined in dimension d will be called the *essential dimension* of X and denoted by $\mathrm{ed}(X)$; cf. Definition 6.1. In the sequel we shall refer to the rational map (1.1) as a *compression* (or a *G-compression*) of X; see §2.5.

We will say that the essential dimension $\mathrm{ed}(G)$ of the group G is equal to d if every generically free G-variety is defined in dimension d, and d is the smallest integer with this property. The essential dimension is a numerical invariant of the group; it can often be characterized as the minimal number of independent parameters required to describe all algebraic objects of a certain type. These objects are field extensions if $G = \mathrm{S}_n$, division algebras if $G = \mathrm{PGL}_n$, quadratic forms if $G = O_n$, Cayley algebras if $G = G_2$, Albert algebras if $G = F_4$, etc. Groups of essential dimension 0 are precisely the *special groups* introduced by Serre [Se_1] and classified by Grothendieck [Gro] in the 1950s. For details we refer the reader to [Re$_2$]; for results on essential dimensions of finite groups see also [BR$_1$] and [BR$_2$].

The lower bounds on $\mathrm{ed}(G)$ in [Re$_2$] are proved in one of two ways. One approach, due to J.-P. Serre, uses cohomological invariants (see Lemma 6.9 and [Re$_2$, Section 12]); the second method, due to the first author, relies on applying the Tsen—Lang theorem to appropriately defined anisotropic forms.

In this paper we develop an alternative approach, based on the following resolution procedure.

Theorem 1.1. *(Corollary 3.6 and Theorem 4.1) Let X be a generically free G-variety. Then there exists a sequence*

$$X_n \xrightarrow{\pi_n} X_{n-1} \cdots \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0 = X$$

of blowups with smooth G-invariant centers such that X_n is smooth and for every $x \in X_n$ the stabilizer $\mathrm{Stab}(x)$ is isomorphic to a semidirect product $U \rtimes A$, where U is unipotent and A is diagonalizable. □

In fact, we show that a sequence of equivariant blowups can be chosen so that X_n is in "standard form"; see Definition 3.1 and Corollary 3.6. The proof of this result depends on canonical resolution of singularities; see Section 3.

In Sections 5–7 we use the above resolution procedure to prove the following lower bound on $\mathrm{ed}(X)$ and $\mathrm{ed}(G)$, and the related numerical invariants $\mathrm{ed}(X;p)$ and $\mathrm{ed}(G;p)$; see Definition 6.3. Recall that the rank of a finite abelian group H is the minimal number of generators of H or, equivalently, the minimal dimension of a faithful k-representation of H. We shall denote this number by $\mathrm{rank}(H)$.

Theorem 1.2. *Let G be a semisimple group and let H be an abelian subgroup of G, whose centralizer is finite.*

(a) (Theorem 7.7) Suppose X is a generically free G-variety, x is a smooth point of X, and $\mathrm{Stab}(x)$ contains H. Then $\mathrm{ed}(X) \geq \mathrm{rank}(H)$. If H is a p-group then $\mathrm{ed}(X;p) \geq \mathrm{rank}(H)$.

(b) (Theorem 7.8) $\mathrm{ed}(G) \geq \mathrm{rank}(H)$. If H is a p-group then $\mathrm{ed}(G;p) \geq \mathrm{rank}(H)$.

Informally speaking, under the assumptions of the theorem, x is an obstruction to compressing X (as in (1.1)). Note that while the essential dimension is a property of X at the generic point, this obstruction depends on the presence of special geometric points (namely smooth fixed points of H). This explains our use of biregular methods, such as resolution of singularities, in what is a priori a birational setting.

In Section 8 we apply Theorem 1.2 to a number of specific groups G. The new bounds we obtain are summarized in the following theorem. Note that $\mathrm{ed}(G) \geq \mathrm{ed}(G;p)$ for any prime p; see Definition 6.3.

Theorem 1.3. 1. *(Theorem 8.1) $\mathrm{ed}(PO_n;2) \geq n-1$,*

2. *(Theorem 8.16) If* $n \equiv 0$ *or* $\pm 1 \pmod 8$ *then* $\mathrm{ed}(\mathrm{Spin}_n; 2) \geq [\frac{n}{2}] + 1$.
3. *(Theorem 8.19(5–6))* $\mathrm{ed}(2E_7; 2) \geq 7$, $\mathrm{ed}(E_7; 2) \geq 8$. *Here* $2E_7$ *and* E_7 *denote, respectively, the simply connected and the adjoint groups of type* E_7.
4. *(Theorem 8.19(7–8))* $\mathrm{ed}(E_8; 2) \geq 9$, $\mathrm{ed}(E_8; 3) \geq 5$.

We remark that the bound of part (2) is known to be sharp for $n = 7$, 8 and 9 (see [Rost$_2$] and Remark 8.18) and that $\mathrm{ed}(2E_7; 2) \leq \mathrm{ed}(2E_7) \leq 9$ (see [Ko] and Remark 8.20). Further results on essential dimensions of specific groups can be found in Section 8.

Most previously known lower bounds on $\mathrm{ed}(G)$ can be derived from the existence of cohomological invariants; see Lemma 6.9 and [Re$_2$, Section 12]. The bounds of Theorem 1.3 cannot be proved in this way at the moment, since the necessary cohomological invariants are not known to exist. However, one can view these bounds (as well as the bound of Theorem 8.6) as an indication of what cohomological invariants may exist; see Remark 8.21.

In the last section we give an application of Theorem 1.2(a) to the problem of simplifying polynomials by Tschirnhaus transformations. Let F be a field and let

$$\alpha(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$

be an irreducible polynomial over F. Recall that a Tschirnhaus transformation (without auxiliary radicals) is an isomorphism of fields $F[x]/(\alpha(x)) \simeq F[t]/(\beta(t))$, where $\beta(t) \in F[t]$ is another irreducible monic polynomial of degree n. We shall say that $\beta(t)$ is obtained from $\alpha(x)$ via this Tschirnhaus transformation. In other words, $\beta(t)$ can be obtained from $\alpha(x)$ in this way if $\beta(t)$ is the minimal polynomial of a generator of the field extension $F \subset F[x]/(\alpha(x))$. (Note that all fields in this paper are assumed to contain a copy of the base field k and all field extensions and isomorphisms are defined over k; see §2.1.)

It is shown in [BR$_1$] that if $a_1, \ldots, a_n$ are algebraically independent over k, i.e., $\alpha(x)$ is the general polynomial of degree n, then at least $[n/2]$ coefficients of $\beta(t)$ are again algebraically independent over k. Our main result here is as follows.

Theorem 1.4. *(see Theorem 9.1) Suppose* $\frac{n}{2} \leq m \leq n-1$, *where* m *and* n *are positive integers. Let* $a_m, \ldots, a_n$ *be algebraically independent variables over* k, $F = k(a_m, \ldots, a_n)$ *and* $E = F[x]/(f(x))$, *where*

$$f(x) = x^n + a_m x^{n-m} + \cdots + a_{n-1}x + a_n \; .$$

Then any polynomial obtained from $f(x)$ *by a Tschirnhaus transformation has at least* $n - m$ *algebraically independent (over* k*) coefficients.*

Note that $f(x)$ has $n - m + 1$ algebraically independent coefficients. However, the form with $n - m$ independent coefficients is easily attained by the substitution $x = \dfrac{a_n}{a_{n-1}} y$; see the proof of Theorem 9.1. Thus the lower bound of the theorem is, indeed, the best possible.

Throughout this paper we shall work over a base field k of characteristic zero. This assumption will be needed when we appeal to equivariant resolution of singularities, the Levi decomposition of an algebraic group, and the Luna slice theorem. We do not know whether or not the results of this paper remain valid in prime characteristic.

Theorem 1.1 can be used in various other settings, not directly related to compressions or essential dimensions. In [RY_1] we apply it, along with the the results of Section 5 and the Appendix, to the study of splitting fields and splitting groups of G-varieties, including a new construction of noncrossed product division algebras. In [RY_2] we apply Theorem 1.1 to give a new algebro-geometric proof of the "Key Lemma" of Parusiński [P]. (The latter result was used in Parusiński's proof of the existence of Lipschitz stratifications of semianalytic sets.)

We remark that our resolution theorems in Section 3 are stated in greater generality than we need for the applications given in this paper. In particular, for the sake of these applications, it would have sufficed to assume that k is an algebraically closed field throughout. (Note, however, that this would not have changed the proofs.) The more general statements will be needed for further applications; see [RY_2].

Acknowledgements

We would like to thank J.-P. Serre for his help and encouragement. His suggestion to investigate the relationship between the essential dimension and the non-toral abelian subgroups of a given algebraic group G, was the starting point for the results of Sections 7 and 8. Serre also contributed Definition 6.3, Lemma 6.9, Remark 7.9, the statement of Proposition 5.6 and, most importantly, both the statement and the proof of Lemma 7.6. The last result greatly simplified our Theorem 7.8 and subsequent applications.

We are grateful to P. D. Milman for many helpful discussions of resolution of singularities, M. Rost for sharing with us his insights into cohomological invariants, spin groups and quadratic forms of low degree, and G. Seitz for answering our questions about elementary abelian subgroups of exceptional algebraic groups.

We also thank E. Bierstone, P. D. Milman, M. Rost, and J.-P. Serre for their comments on earlier versions of this paper.

2. Notation and terminology

The following notational conventions will be used throughout the paper.

k	a base field of characteristic 0
$\overline{k}$	the algebraic closure of k
G	an algebraic group defined over k; see §2.4
$C(H) = C_G(H)$	the centralizer of H in G
$\mathbb{A}^n = \mathbb{A}^n_k$	the affine space of dimension n over k
$\mathbb{G}_{\mathrm{m}} = \mathrm{GL}_1(k)$	the multiplicative group $\mathbb{A}^1 - \{0\}$ over k
X	an algebraic variety over k, often a G-variety
$\mathrm{Stab}(x)$	the stabilizer of x
ed	essential dimension; see Definitions 6.1 and 6.3

2.1. **The base field.** All algebraic objects in this paper, such as rings, fields, algebraic groups, algebraic varieties, group actions, etc. and all maps between them will be defined over a fixed base field k of characteristic 0. In Sections 4–8 we will generally assume that k is algebraically closed; we shall indicate which of the results are true without this assumption. In Sections 3 and 9 we will not assume that k is algebraically closed.

2.2. **Algebraic varieties.** Algebraic varieties in this paper are allowed to be reducible; in other words, an algebraic variety is a reduced separated scheme of finite type over k. (Note that here our terminology is different from that of Hartshorne [Ha], who defines abstract algebraic varieties to be irreducible.)

Given an algebraic variety X, we will denote its ring of rational functions by $k(X)$, where a rational function on a reducible variety is a collection of rational functions on its irreducible components; cf. §2.3 below. Note that $k(X)$ is a field if X is irreducible. In general, if X has irreducible components X_i then $k(X)$ is a direct sum of their function fields $k(X_i)$.

Unless otherwise specified, by a point of X we shall always mean a closed point.

2.3. **Rational maps.** A rational map $f\colon X \dashrightarrow Y$ is an equivalence class of regular morphisms from dense open subsets of X to Y, as in [EGA I, Définition 7.1.2]. Equivalently, f is a collection of rational maps $f_i\colon X_i \dashrightarrow Y$, one for each irreducible component X_i of X. The largest open subset U of X where f is defined is called *the domain* of f; $f(U)$ is called *the range* of f. A rational map is said to be *dominant* if its range is dense in Y.

A dominant rational map $f\colon X \dashrightarrow Y$ is said to be $d:1$ if there exists a dense open subset Y_0 of its range such that f is defined on $f^{-1}(Y_0)$ and $|f^{-1}(y)(\overline{k})| = d$ for every $y \in Y_0(\overline{k})$.

A birational isomorphism between X and Y is a pair of rational maps $X \dashrightarrow Y$ and $Y \dashrightarrow X$ inverse to each other, or equivalently, a 1—1 correspondence between the irreducible components X_i of X and Y_i of Y and a birational isomorphism between X_i and Y_i for each i.

2.4. **Algebraic groups.** If G is an algebraic group (defined over k; see §2.1) *we shall always assume that $G(k)$ is Zariski dense in G.* Note that this is a rather mild assumption; in particular, it is obviously satisfied if k is algebraically closed or if G is a finite group all of whose points are defined over k (e.g., S_n, viewed as an algebraic group over k). It is also satisfied if G is connected (see [Hu, Theorem 34.4(d)]) and, more generally, if every irreducible component of G has a k-point.

Our results are, in fact, true, without the above assumption; however, leaving it out would complicate the proofs in Section 3 (see Remark 3.3). Since this assumption is satisfied in every setting we want to consider, we chose to impose it throughout this paper.

2.5. **G-varieties.** Let G be an algebraic group. We shall call an algebraic variety X a G-variety if X is equipped with a regular action of G, i.e., an action given by a regular morphism $G \times X \longrightarrow X$.

If X and Y are G-varieties then by a regular map $X \longrightarrow Y$ of G-varieties we mean a regular G-equivariant map. The same applies to rational maps of G-varieties, biregular and birational isomorphisms of G-varieties, etc.

A G-variety is X called *generically free* if G acts freely (i.e., with trivial stabilizers) on a dense open subset if X.

A *G-compression* $X \dashrightarrow Y$ is a dominant rational map of generically free G-varieties. We will also use the term *compression* if the reference to G is clear from the context.

2.6. **Rational quotients and primitive varieties.** Let X be a G-variety. A rational map $\pi \colon X \dashrightarrow Y$ is called *the rational quotient map* (and Y, *the rational quotient*) if $\pi^*(k(Y)) = k(X)^G$. The rational quotient exists for any G-variety; we will denote it by X/G.

We will say that X is a *primitive* G-variety if the rational quotient X/G is irreducible or, equivalently, if $k(X)^G$ is a field. It is easy to see that X is primitive if and only if G transitively permutes the irreducible components of X; see, e.g., [Re_2, Lemma 2.2].

By a theorem of Rosenlicht the rational quotient map separates the G-orbits in a dense Zariski open subset of X; see [Ro_1, Theorem 2], [PV, Theorem 2.3] and [Ro_2]. In particular, if X is primitive then each component of X has dimension $\dim(Y) + \dim(G)$.

3. Equivariant resolution of singularities

Much of this paper relies on the resolution of singularities theorem and especially on its canonical version which only recently became available; see the references below. In this section we derive several consequences of this result in the setting of G-varieties.

Definition 3.1. We shall say that a generically free G-variety X is *in standard form with respect to a divisor Y* if

(i) X is smooth and Y is a normal crossing divisor on X

(ii) the G-action on $X - Y$ is free, and

(iii) for every $g \in G$ and for every irreducible component Z of Y either $g(Z) = Z$ or $g(Z) \cap Z = \emptyset$.

We will say that X is *in standard form* if it is in standard form with respect to some divisor Y.

Our interest in G-varieties in standard form is explained by the fact that they have "small" stabilizers. This property will be explored in Section 4; see Theorem 4.1. We will now prove that every generically free G-variety can be brought into standard form by a sequence of blowups with smooth G-equivariant centers.

Theorem 3.2. *Let X be a smooth G-variety and $Y \subset X$ be a closed nowhere dense G-invariant subvariety such that the action of G on $X - Y$ is free. Then there is a sequence of blowups*

$$\pi\colon X_n \xrightarrow{\pi_n} X_{n-1} \cdots \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0 = X \tag{3.1}$$

with smooth G-invariant centers $C_i \subset X_i$ such that X_n is in standard form with respect to $D_n \cup \pi^{-1}(Y)$, where D_n is the exceptional divisor of π (and, in particular, $D_n \cup \pi^{-1}(Y)$ is a normal crossing divisor in X_n).

Remark 3.3. Recall that throughout this paper we assume $G(k)$ is Zariski dense in G; see §2.4. This assumption is used only in this section (in Theorem 3.2 and Corollary 3.6) and only for the purpose of lifting a G-action on an algebraic variety to its canonical resolution of singularities.

In fact, our results are true without this assumption because *an algebraic group action always lifts to the canonical resolution of singularities* of Bierstone—Milman [BM_2] (see also [BM_1]).

The last assertion follows from the fact that the canonical resolution commutes with base field extensions. This reduces the question of lifting a group action to the case where k is algebraically closed and thus $G(k)$ is Zariski dense in G. Commutativity with base extensions follows from [BM_2, Remark 3.8].

Alternatively, the above assertion about lifting the action of G can be derived (by an argument more natural than the one we give in the proof of Theorem 3.2 below) from the fact that the canonical resolution is functorial with respect to smooth morphisms. Functoriality with respect to smooth morphisms follows from [BM_2, Remark 1.5] and the constructive definition of the invariant in [BM_2, §§4, 6].

As we do not need the stronger statements of the results of this section (without the assumption that $G(k)$ is Zariski dense in G), we omit the details of these arguments.

Note also that it is quite possible that the canonical resolution of Villamayor [V_2] (see also [V_1]) has the same properties.

We begin with a preliminary lemma. Let

$$\pi\colon X_n \xrightarrow{\pi_n} X_{n-1} \cdots \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0 = X \tag{3.2}$$

be a sequence of blowups with smooth G-invariant centers. Recall that the exceptional divisor E of π is the union of the preimages in X_n of the centers of the blowups $\pi_1, \dots, \pi_n$; the composition π is an isomorphism in the complement of E.

Lemma 3.4. *Let X be a G-variety, let $\pi \colon X_n \longrightarrow X$ be as in (3.2), and let E_1 be an irreducible component of the exceptional divisor E of π. Then for any $g \in G$, either $g(E_1) = E_1$ or $g(E_1) \cap E_1 = \emptyset$.*

Proof. Each irreducible component of E is the preimage in X_n of an irreducible component, say, $C_{i,1}$, of the center C_i of one of the blowups $\pi_{i+1} \colon X_{i+1} \longrightarrow X_i$.

Since C_i is a smooth G-invariant subvariety in X_i, its irreducible components $C_{i,1}, \dots, C_{i,m}$ are disjoint.

We have $E_1 = (\pi_i \dots \pi_n)^{-1} C_{i,1}$; hence, for any $g \in G$,

$$g(E_1) = (\pi_i \dots \pi_n)^{-1} g(C_{i,1}) \ .$$

As C_i is G-invariant and $C_{i,1}$ is its connected component, $g(C_{i,1})$ is also a connected component of C_i, say, $g(C_{i,1}) = C_{i,j}$. Thus

$$g(E_1) = (\pi_i \dots \pi_n)^{-1} C_{i,j} \ .$$

If $j = 1$ then $g(E_1) = E_1$; if $j \neq 1$ then $g(E_1) \cap E_1 = \emptyset$, since $C_{i,1}$ and $C_{i,j}$ are disjoint. ☐

Proof of Theorem 3.2. Let D_i be the exceptional divisor of $\pi_1 \dots \pi_i \colon X_i \longrightarrow X$. Inductively, assume that D_i is a normal crossing divisor in X_i. We shall give a construction of each blowup center C_i so that C_i and D_i simultaneously have only normal crossings. It was observed by Hironaka [Hi] that this implies that D_{i+1} is a normal crossing divisor in X_{i+1}; this way all D_i are normal crossing divisors.

Denote by Y_i the union of D_i and the preimage of Y in X_i. Let

$$X_{n-1} \xrightarrow{\pi_{n-1}} \dots \xrightarrow{\pi_1} X_0 = X \tag{3.3}$$

be a canonical embedded resolution of singularities of $Y \subset X$, as in [BM$_2$, Theorem 1.6]; then D_{n-1} and the strict transform C_{n-1} of Y in X_{n-1} simultaneously have only normal crossings.

Let

$$X_n \xrightarrow{\pi_n} X_{n-1} \tag{3.4}$$

be the blowup centered at C_{n-1}; then Y_n is a normal crossing divisor in X_n.

The action of each element $g \in G(k)$ lifts to the entire resolution sequence (3.3); this follows from [BM$_2$, Theorem 13.2(2)(ii)]. This means, inductively, that each blowup center C_i, $i = 0, 1, \dots, n-2$, is invariant under this action of g. Since we are assuming that $G(k)$ is Zariski dense in G (see §2.4), each of these C_i is G-invariant; this implies that the action of G lifts to the entire resolution tower (3.3), C_{n-1} — which is defined as the strict transform of

Y — is G-invariant, the action of G lifts to the blowup (3.4), and each Y_i, $i \leq n$, is G-invariant.

In particular, X_n is smooth, Y_n is a G-invariant normal crossing divisor in X_n and the action of G on $X_n - Y_n$ is free, since Y_n contains the preimage of Y. This implies that conditions (i) and (ii) of Definition 3.1 are satisfied for X_n and the divisor $Y_n \subset X_n$.

We claim that X_n and Y_n also satisfy condition (iii) of Definition 3.1. Indeed, since C_{n-1} is defined as the strict transform of Y in X_{n-1}, $(\pi_1 \dots \pi_{n-1})^{-1}(Y)$ is contained in $D_{n-1} \cup C_{n-1}$, and hence,

$$(\pi_1 \dots \pi_n)^{-1}(Y) \subset \pi_n^{-1}(D_{n-1}) \cup \pi_n^{-1}(C_{n-1}) = D_n \, .$$

Consequently, $Y_n = (\pi_1 \dots \pi_n)^{-1}(Y) \cup D_n = D_n$ is the exceptional divisor for $\pi_1 \dots \pi_n \colon X_n \longrightarrow X$. Lemma 3.4 now says that condition (iii) of Definition 3.1 is satisfied for the pair (X_n, Y_n), as claimed. □

Remark 3.5. At the beginning of the proof of Theorem 3.2, we could have taken an alternative approach by considering the canonical resolution of *the sheaf of ideals* $\mathcal{I}_Y$ *of* Y in X, as in [BM$_2$, Theorem 1.10], instead of first considering the canonical embedded resolution of singularities of Y, as in [BM$_2$, Theorem 1.6], and then blowing up the strict transform C_{l-1} of Y. Note that the action of $g \in G$ lifts to the canonical resolution of $\mathcal{I}_Y$; this may be deduced from [BM$_2$, Remark 1.5].

Alternatively, we could have used the constructive resolution of the idealistic space determined by the couple $(\mathcal{I}_Y, 1)$, as in [V$_2$, Definition 2.4.1 and Theorem 7.3]. The action of $g \in G$ lifts to this resolution by an argument similar to that of [V$_2$, Corollary 7.6.3].

Corollary 3.6. *Let X be a G-variety and $Y \subset X$ a closed nowhere dense G-invariant subvariety such that the action of G on $X - Y$ is free. Then there is a sequence of blowups*

$$\pi \colon X_n \xrightarrow{\pi_n} X_{n-1} \cdots \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0 = X \tag{3.5}$$

where the centers $C_i \subset X_i$ are smooth and G-invariant, and X_n is in standard form with respect to a divisor $\widetilde{Y} \subset X_n$ which contains $\pi^{-1}(Y)$.

Proof. Note that since Y is nowhere dense in X, it is nowhere dense in each irreducible component of X.

Consider the canonical resolution of singularities of X,

$$X_l \xrightarrow{\pi_l} \dots \xrightarrow{\pi_1} X_0 = X \ , \tag{3.6}$$

as in [V$_2$, Theorem 7.6.1] or [BM$_2$, Theorem 13.2]. The variety X_l is smooth; similarly to the proof of Theorem 3.2, we find that the centers $C_i \subset X_i$ are smooth and G-invariant, and the action of G lifts to the entire resolution sequence (3.6).

Let Y_l be the preimage of Y in X_l. Then Y_l is nowhere dense in each of the irreducible components of X_l, since Y is nowhere dense in each irreducible component of X. Consequently, Y_l is nowhere dense in X_l. Now apply

Theorem 3.2 to X_l and Y_l to obtain a sequence $X_n \xrightarrow{\pi_n} \dots \xrightarrow{\pi_{l+1}} X_l$ with smooth G-invariant centers, such that X_n is in standard form with respect to a divisor $\widetilde{Y} \subset X_n$ which contains $\pi^{-1}(Y)$. $\square$

4. G-varieties in standard form

With the exception of Remark 4.5, we shall assume throughout this section that the base field k is algebraically closed.

Theorem 4.1. *Let X be a generically free G-variety in standard form, and let Y be as in Definition 3.1. Suppose $x \in X$ lies on exactly m irreducible components of Y. Then $\mathrm{Stab}(x)$ is isomorphic to a semidirect product $U \rtimes A$, where U is a unipotent group and A is a diagonalizable group of rank $\leq m$.*

Our proof of Theorem 4.1 relies on the following lemma.

Lemma 4.2. *Let H be a diagonalizable group, X an H-variety, and let X^H be the fixed point set of H in X. If X is smooth at a point x and $x \in X^H$ then X^H is also smooth at x; moreover, $T_x(X^H) = T_x(X)^H$.*

Proof. Note that if X is affine then the lemma is a consequence of the Luna Slice Theorem; see [PV, Corollary to Theorem 6.4]. Moreover, since every quasiaffine H-variety can be equivariantly embedded into an affine H-variety (see [PV, Theorem 1.6]), the lemma also holds if X is quasiaffine. Thus it is sufficient to show that x has an open quasiaffine H-invariant neighborhood $U \subset X$.

After replacing X by its smooth locus (which is open and H-invariant), we may assume X is smooth. Let H^0 be the identity component of H; since H is diagonalizable, H^0 is a torus (possibly $H^0 = \{1\}$). By a result of Sumihiro (see [Su, Corollary 2]) there exists an affine H^0-invariant neighborhood X_0 of x in X. We now define U as

$$U = \bigcap_{\overline{h} \in H/H^0} \overline{h}(X_0) \ .$$

Since H/H^0 is a finite group, U is an open H-invariant quasiaffine neighborhood of x, as claimed. $\square$

Proof of Theorem 4.1. Consider the Levi decomposition $\mathrm{Stab}(x) = U \rtimes A$, where A is reductive and U is unipotent; see, e.g., [OV, Section 6.4]. We want to show that A is, in fact, a diagonalizable group of rank $\leq m$.

Denote the irreducible components of Y passing through x by $Z_1, \dots, Z_m$. They intersect transversely at x; in particular, $W = Z_1 \cap \dots \cap Z_m$ is smooth at x. Recall that by our assumption each Z_i is $\mathrm{Stab}(x)$-invariant; hence, W is also $\mathrm{Stab}(x)$-invariant.

As A is reductive, there is an A-invariant subspace V in $T_x(X)$ complementary to $T_x(W)$. We have an A-invariant decomposition

$$V = V_1 \oplus V_2 \cdots \oplus V_m$$

where

$$V_i = V \cap T_x(Z_1) \cap \cdots \cap \widehat{T_x(Z_i)} \cap \cdots \cap T_x(Z_m) \; ; \tag{4.1}$$

each V_i is one-dimensional. The group A acts on each V_i by a character, say, $\chi_i \colon A \longrightarrow \mathbb{G}_{\mathrm{m}}$ (possibly trivial). We claim that the homomorphism

$$\chi = (\chi_1, \ldots, \chi_m) \colon A \longrightarrow (\mathbb{G}_{\mathrm{m}})^m$$

is injective. Note that the theorem is an immediate consequence of this claim.

To prove the claim, note that $\mathrm{Ker}(\chi)$ is a reductive subgroup of A. Thus in order to prove that $\mathrm{Ker}(\chi) = \{1\}$, it is sufficient to show that every diagonalizable subgroup of $\mathrm{Ker}(\chi)$ is trivial. (Indeed, this immediately implies that the identity component $\mathrm{Ker}(\chi)^0$ is unipotent and, hence, trivial; see [Hu, Exercise 1, p. 137]. Thus $\mathrm{Ker}(\chi)$ is finite and every abelian subgroup of $\mathrm{Ker}(\chi)$ is trivial; this is only possible if $\mathrm{Ker}(\chi) = \{1\}$.)

Let $H \subset \mathrm{Ker}(\chi)$ be a diagonalizable group; we want to show that $H = \{1\}$. Assume the contrary. Denote the fixed point set of H by X^H. Since the action of G on $X - Y$ is free, $X^H \subset Y$. By Lemma 4.2, X^H is smooth. Consequently, only one irreducible component of X^H passes through x; denote this component by X_0^H. Then X_0^H is contained in one of the components $Z_1, \ldots, Z_m$, say in Z_i, and by Lemma 4.2,

$$T_x(X)^H = T_x(X^H) = T_x(X_0^H) \subset T_x(Z_i) \; . \tag{4.2}$$

Now note that by our assumption, $\chi_i|_H$ is trivial and thus $V_i \subset T_x(X)^H$ but, on the other hand, by (4.1) $V_i \not\subset T_x(Z_i)$, contradicting (4.2). This completes the proof of the claim. □

Corollary 4.3. *Suppose X is a G-variety in standard form and x is a point of X.*

(a) If $\mathrm{Stab}(x)$ *is connected then it is solvable.*

(b) if $\mathrm{Stab}(x)$ *is reductive then it is diagonalizable.*

(c) if $\mathrm{Stab}(x)$ *is finite then it is commutative.*

Proof. Immediate from Theorem 4.1. □

Remark 4.4. Our proof shows that

$$T_x(X)/T_x(W) = \bigoplus_{i=1}^{m} \frac{T_x(Z_1) \cap \cdots \cap \widehat{T_x(Z_i)} \cap \cdots \cap T_x(Z_m)}{T_x(W)} \; . \tag{4.3}$$

is a direct sum decomposition of the normal space $T_x(X)/T_x(W) \cong V$ as a direct sum of 1-dimensional character spaces for the natural action of A. Moreover, the above (diagonal) representation of A on V is faithful.

Remark 4.5. Suppose the base field k is not necessarily algebraically closed (but is of characteristic 0), X is a generically free G-variety in standard form, and $x \in X$ has a finite stabilizer of exponent e. Then the residue field k' of x contains a primitive e-th root of unity. Indeed, $\mathrm{Stab}(x)$ has a faithful diagonal representation (4.3) defined over k'; this is only possible if k' contains a primitive e-th root of unity.

Corollary 4.6. *Let X be a generically free G-variety in standard form. Suppose that $H = \mathrm{Stab}(x)$ is a finite group. Then $\dim(X) \geq \dim(G) + \mathrm{rank}(H)$.*

Here $\mathrm{rank}(H)$ denotes the rank of the finite abelian group $H = \mathrm{Stab}(x)$; see Corollary 4.3(c).

Proof. Let Y be as in Definition 3.1. Suppose exactly m irreducible components $Z_1, \dots, Z_m$ meet at x; then by Theorem 4.1 we have $m \geq \mathrm{rank}(H)$. Since $Z_1, \dots, Z_m$ intersect transversely at x, their intersection $W = Z_1 \cap \dots \cap Z_m$ is smooth at x and

$$\dim(X) = \dim_x(W) + m = \dim(W_0) + m \ ,$$

where W_0 is the (unique) component of W passing through X.

Since $m \geq \mathrm{rank}(H)$, it only remains to show that $\dim(W_0) \geq \dim(G)$. Indeed, let

$$G' = \{g \in G \mid g(Z_i) = Z_i \ \forall i = 1, \dots, m\} \ .$$

Then $G'x \subset W_0$. Since G' is a subgroup of finite index in G and $\mathrm{Stab}(x)$ is assumed to be finite, we have $\dim(W_0) \geq \dim(G'x) = \dim(G') = \dim(G)$, as claimed. □

5. The behavior of fixed points under rational morphisms

Suppose H is an algebraic group and $f \colon X \dashrightarrow Y$ is a rational map of H-varieties. In this section we shall be interested in two types of results (under certain additional assumptions on H, X, Y and f): *"going down"* results, which assert that if H fixes a point of X then it fixes a point of Y and *"going up"* results which assert the converse.

Note that the "going down" assertion is always true if f is a regular map; indeed, if $x \in X$ is fixed by H then so is $f(x) \in Y$. The situation is somewhat more complicated for rational maps; in particular, we need to make a strong assumption on the group H; see Remark A.3.

Throughout this section we shall assume that the base field k is algebraically closed.

The proofs we originally had in this section relied on canonical resolution of singularities; cf. Remark 5.4. Kollár and Szabó recently found simple characteristic-free proofs of Propositions 5.3 and 5.6. These proofs are presented in the Appendix at the end of this paper; we shall therefore omit most of our original arguments. We also note that our earlier versions of Lemma 5.1 and Proposition 5.3 assumed that H is diagonalizable; our earlier version of Proposition 5.3 (respectively, Proposition 5.6) assumed that Y (respectively X) is projective, rather than complete. The current Propositions 5.3 and 5.6 are characteristic zero versions of, respectively, Propositions A.2 and A.4.

We begin with a simple lemma.

Lemma 5.1. *Let $H = U \rtimes A$, where U is unipotent and A is diagonalizable, X be an H-variety and $\pi\colon X_1 \longrightarrow X$ be a blowup with a smooth H-invariant center $C \subset X$. If x is a smooth point of X which is fixed by H then there exists an $x_1 \in X_1$ such that $\pi(x_1) = x$ and x_1 is fixed by H.*

Proof. Recall that π is an isomorphism over $X - C$; thus if $x \notin C$ then we can take $x_1 = \pi_1^{-1}(x)$. On the other hand, if $x \in C$ then $f^{-1}(x) \simeq \mathbb{P}(V)$ (as H-varieties), where $V = N_x(C) = T_x(X)/T_x(C)$. The action of H has an eigenvector in V (see Lemma A.1); thus H fixes some $x_1 \in \mathbb{P}(V) = f^{-1}(x)$, as claimed. □

Remark 5.2. Lemma 5.1 shows that Theorem 1.1 is sharp in the sense that the stabilizers of points of X_n cannot be further reduced by additional blowups with smooth equivariant centers.

Going down.

Proposition 5.3. *Let $H = U \rtimes A$, where U is unipotent and A is diagonalizable. Suppose $f\colon X \dashrightarrow Y$ is a dominant rational map of H-varieties, where Y is complete. If H fixes a smooth point x in X then H fixes a point $y \in Y$.*

Proof. See Proposition A.2. □

Remark 5.4. We will now briefly outline our original proof of Proposition 5.3. It is more complicated than the proof of Proposition A.2 and only works in characteristic zero; however, we feel this argument may be of independent interest.

First we showed that there exists a sequence of blowups

$$X_n \xrightarrow{\pi_n} \cdots \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0 = X$$

with smooth H-invariant centers such that f lifts to a regular map

$$f'\colon X_n \longrightarrow Y$$

of H-varieties. This is, in fact, true for any algebraic group H and any H-equivariant rational map $f\colon X \dashrightarrow Y$; the proof relies on canonical resolution of singularities (see [RY$_3$]).

Applying Lemma 5.1 inductively to the above tower of blowups, we see that for every $i = 0, 1, \ldots, n$ there exists a (necessarily smooth) H-fixed point $x_i \in X_i$ lying above $x = x_0$. Now $y = f'(x_n)$ is an H-fixed point of Y. □

Going up. Let H be a diagonalizable group, $f\colon X \dashrightarrow Y$ be a rational map of H-varieties. We now want to prove that if H fixes a smooth point $y \in Y$ then H fixes a point of X. We clearly need to assume that f is dominant and the fibers of f are complete; the following example shows that these assumptions are not sufficient, even if X is irreducible.

Example 5.5. Let $H = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ be a finite abelian group, Y be an H-variety, P be a projective H-variety where H acts freely (i.e., all stabilizers are trivial), and $X = Y \times P$. Then H acts freely on X, hence, the "going up" assertion will fail for the map $f \colon X \longrightarrow Y$, where $f =$ projection to the first component. (Note that the fibers of this map are projective, so lack of completeness is not the problem here.) To construct P, let E be an elliptic curve and let p_i be a point of order n_i on E. Now set $P = E^n$ and define the H-action on P by

$$(i_1, \dots, i_r) \cdot (x_1, \dots, x_n) = (x_1 + i_1 p_1, \dots, x_r + i_r p_r) \ ,$$

where $+$ refers to addition on E. $\square$

Nevertheless, it turns out that one can still prove a useful "going up" property.

Proposition 5.6. *Let H be an abelian p-group and $f \colon X \dashrightarrow Y$ be a dominant rational $d:1$-map of generically free H-varieties. Assume X is complete, d is prime to p and $y \in Y$ is a smooth point fixed by H. Then H fixes a point $x \in X$.*

Proof. Note that since y is a smooth point of Y fixed by H, the irreducible component Y_0 of Y containing y, is preserved by H. Replacing Y by Y_0 and X by the union of its irreducible components which are mapped dominantly onto Y_0, we may assume that Y is irreducible and each component X_i of X is mapped dominantly onto Y.

Similarly to the argument of the proof of Proposition A.4, we note that H acts on the set $\{X_i\}$; let $\mathcal{X}_j$ be the H-orbits in this set. Pick an element X_j^* in $\mathcal{X}_j$; then

$$d = \deg(X/Y) = \sum_j |\mathcal{X}_j| \cdot \deg(X_j^*/Y) \ .$$

As d is not divisible by p, there is an orbit $\mathcal{X}_0$ consisting of a single element X_0^* such that $\deg(X_0^*)$ is not divisible by p. Replacing X by X_0^*, we may assume that X is irreducible; now apply Proposition A.4. $\square$

6. Essential dimensions and cohomological invariants

Essential dimension. We now recall the definition of essential dimension from [Re$_2$]; in the case of finite groups, see also [BR$_1$] and [BR$_2$].

Definition 6.1. (1) The essential dimension of a primitive generically free G-variety X is the minimal value of $\dim(Y/G) = \dim(Y) - \dim(G)$, where Y/G denotes the rational quotient of Y by G and the minimum is taken over all G-compressions $X \dashrightarrow Y$; see §2.5 and §2.6. We denote this number by $\mathrm{ed}(X)$.

(2) If V is a generically free irreducible linear representation of G, we refer to $\mathrm{ed}(V)$ as the essential dimension of G and denote it by $\mathrm{ed}(G)$. By [Re$_2$, Theorem 3.4] this number is independent of the choice of V. Equivalently, $\mathrm{ed}(G)$ can be defined as the maximal value of $\mathrm{ed}(X)$, as X ranges over all primitive generically free G-varieties; see [Re$_2$, Section 3.2].

Remark 6.2. The definition of essential dimension of an algebraic group in [Re_2] assumes that the base field k is algebraically closed and of characteristic 0; the definition of essential dimension of a finite group in [BR_1] and [BR_2] is valid over an arbitrary field of characteristic 0. In this paper we will be interested, almost exclusively, in proving lower bounds on essential dimensions of various groups and G-varieties. Since $\mathrm{ed}(X) \geq \mathrm{ed}(X \otimes_k \overline{k})$ for any G-variety X, with G finite, as well as for any imaginable notion of $\mathrm{ed}(X)$ with G infinite, a lower bound on $\mathrm{ed}(G)$ or $\mathrm{ed}(X)$ over $\overline{k}$ will automatically be valid over k. For this reason, all lower bounds we prove under the assumption that k is algebraically closed, also hold without this assumption.

Essential dimension at p. We will also study the following related numerical invariants which were brought to our attention by J.-P. Serre.

Definition 6.3. (1) Let p be a prime integer and let X be a primitive generically free G-variety. We define the *essential dimension of X at p* as the minimal value of $\mathrm{ed}(X')$, where the minimum is taken over all dominant rational $d : 1$ maps $X' \dashrightarrow X$ of primitive G-varieties (see §§2.3, 2.5 and 2.6), with d prime to p. We shall denote this number by $\mathrm{ed}(X; p)$.

(2) The *essential dimension of G at p* is defined as the maximal value of $\mathrm{ed}(X; p)$, as X ranges over all primitive generically free G-varieties. We shall denote this number by $\mathrm{ed}(G; p)$.

Remark 6.4. $\mathrm{ed}(X; p)$ is closely related to the "relative essential dimension" $\mathrm{ed}^{m,H}(X; p)$ defined (for finite groups only) in [BR_2, Section 5]. More precisely, $\mathrm{ed}(X; p)$ is the maximal value of $\mathrm{ed}^{m,H}(X; p)$, as H ranges over all finite groups and m ranges over all positive integers prime to p. We shall not work with $\mathrm{ed}^{H,m}(X)$ in this paper.

Remark 6.5. Clearly, $\mathrm{ed}(X) \geq \mathrm{ed}(X; p)$ for every primitive generically free G-variety X and every prime p. In particular, $\mathrm{ed}(G) \geq \mathrm{ed}(G; p)$. Note also that if G is a simple group then $\mathrm{ed}(X; p) = 0$ unless p is one of the so-called exceptional primes. For details, including a list of exceptional primes, see [Se_2, Section 2].

The following lemma will not be needed in the sequel; we include it here to illustrate the similarity between the definitions of $\mathrm{ed}(G)$ and $\mathrm{ed}(G; p)$.

Lemma 6.6. *Suppose G is an algebraic group and p is a prime integer.*

(a) Let X be a primitive generically free G-variety and $f: X \dashrightarrow Y$ be a G-compression. Then $\mathrm{ed}(X; p) \leq \mathrm{ed}(Y; p)$.

(b) Let V be a generically free linear representation of G. Then $\mathrm{ed}(V; p) = \mathrm{ed}(G; p)$. *In other words,* $\mathrm{ed}(V; p) \geq \mathrm{ed}(X; p)$ *for any primitive generically free G-variety X; in particular,* $\mathrm{ed}(V; p)$ *is independent of the choice of V.*

Proof. (a) Suppose $Y' \dashrightarrow Y$ is a $d : 1$ dominant rational map of primitive G-varieties, where d is not divisible by p. It is enough to show that there exists a commutative diagram of rational maps

$$\begin{tikzcd} X' \arrow[r, dashed, "f'"] \arrow[d, "e:1"'] & Y' \arrow[d, "d:1"] \\ X \arrow[r, dashed, "f"] & Y \end{tikzcd} \tag{6.1}$$

of primitive G-varieties, where $X' \dashrightarrow X$ is an $e:1$ dominant rational map of primitive G-varieties and e is not divisible by p. Indeed, the existence of f' immediately implies $\mathrm{ed}(X') \leq \mathrm{ed}(Y')$ (cf. [Re$_2$, Lemma 3.3(b)]); taking the minimum over all Y', we obtain the desired inequality.

To construct the diagram (6.1), note that since X, Y and Y' are primitive, $k(X)^G$, $k(Y)^G$ and $k(Y')^G$ are, by definition, fields; see §2.6. Moreover, $[k(Y')^G : k(Y)^G] = d$. We claim that there exists a diagram of field extensions

$$\begin{tikzcd} L \arrow[dd, dash, "e"'] \arrow[dr, dash] & \\ & k(Y')^G \arrow[dd, dash, "d"] \\ k(X)^G \arrow[dr, dash] & \\ & k(Y)^G \end{tikzcd}$$

where L contains both $k(X)^G$ and $k(Y')^G$ and $p \nmid e = [L : k(X)^G]$. Indeed, write

$$k(X)^G \otimes_{k(Y)^G} k(Y')^G = L_1 \oplus \cdots \oplus L_m \ ,$$

where each L_i is a field; see [J$_1$, Section 5.6]. Since

$$\sum_{i=1}^{m} [L_i : k(X)^G] = \dim_{k(X)^G} \left(k(X)^G \otimes_{k(Y)^G} k(Y')^G \right) = [k(Y')^G : k(Y)^G] = d$$

is not divisible by p, we conclude that $p \nmid [L_i : k(X)^G]$ for some i. Now set $L = L_i$ and $e = [L_i : k(X)^G]$.

The above diagram gives rise to the following diagram of rational maps:

$$\begin{tikzcd} X_0 \arrow[r, dashed, "\overline{f'}"] \arrow[d, "e:1"'] & Y'/G \arrow[d, "d:1"] \\ X/G \arrow[r, dashed, "\overline{f}"] & Y/G \end{tikzcd}$$

where X_0 is an irreducible algebraic variety whose function field in L. Taking the fiber product of this diagram with Y over Y/G, and remembering that

$Y/G \times_{Y/G} Y \simeq Y$, $Y'/G \times_{Y/G} Y \simeq Y'$, and $X/G \times_{Y/G} Y \simeq X$ as G-varieties (see [Re$_2$, Lemma 2.14]), we obtain the desired diagram (6.1) with $X' = X_0 \times_{Y/G} Y$. Note that $X'/G \simeq X_0$ and thus X' is a primitive G-variety; see [Re$_2$, Lemma 2.14].

(b) Recall that by [Re$_2$, Corollary 2.17], for every primitive generically free G-variety X, there exists a G-compression $X \times \mathbb{A}^d \dashrightarrow V$, where $d = \dim(V)$ and G acts trivially on $\mathbb{A}^d$. (This fact is a consequence of the "no-name lemma".) Thus by part (a)

$$\mathrm{ed}(X \times \mathbb{A}^d; p) \leq \mathrm{ed}(V; p) \ . \tag{6.2}$$

On the other hand, the argument of [BR$_2$, Lemma 5.3] shows that

$$\mathrm{ed}(X \times \mathbb{A}^1; p) = \mathrm{ed}(X; p)$$

for any primitive generically free G-variety X; see Remark 6.4. This, along with (6.2), proves part (b). $\square$

Cohomological invariants. A simple but important relationship between the essential dimension of an algebraic group G and its cohomological invariants was observed by J.-P. Serre (see Lemma 6.9 below). This observation makes it possible to deduce lower bounds on $\mathrm{ed}(G; p)$ from the existence of non-trivial cohomological invariants.

In the next section we will develop a method for proving lower bounds on $\mathrm{ed}(G; p)$, which does not presuppose the existence of a non-trivial cohomological invariant. However, for the purpose of motivating our results and placing them in the proper context, we briefly explain the relationship between cohomological invariants and essential dimension. We will follow up on this theme in Remark 8.21.

Suppose F is field, $\overline{F}$ is the algebraic closure of F, $\Gamma = \mathrm{Gal}(\overline{F}, F)$ and M is a torsion abelian group. In the sequel, we shall denote the Galois cohomology group $H^i(\Gamma, M)$ by $H^i(F, M)$ (see [Se$_3$]); here we view M as a Γ-module with trivial Γ-action. Note that $H^i(\,\cdot\,, M)$ is a functor from the category of fields to the category of groups. We shall also consider the functor $H^1(\,\cdot\,, G)$ from the category of finitely generated field extensions of k to the category of sets. Recall that elements of the non-abelian cohomology set $H^1(F, G)$ are in 1—1 correspondence with primitive generically free G-varieties X such that $k(X)^G = F$; see [Se$_3$, I.5.2], [Po, Theorem 1.3.3] or [Re$_2$, Lemma 12.3].

Definition 6.7. A cohomological invariant α of G-varieties is a morphism of functors $H^1(\,\cdot\,, G) \longrightarrow H^d(\,\cdot\,, M)$. In other words, α assigns a cohomology class $\alpha(X) \in H^d(k(X)^G, M)$ to every primitive generically free G-variety X, so that for every compression $X \dashrightarrow Y$, $\alpha(X)$ is the image of $\alpha(Y)$ under the natural restriction homomorphism $H^d(k(Y)^G, M) \longrightarrow H^d(k(X)^G, M)$.

Remark 6.8. The above notion of cohomological invariant (and the equivalent notion used in [Re$_2$, Section 12]) are somewhat more narrow than the usual definition (see [Se$_2$, 6.1] or [KMRT, 31B]), due to the fact that we work over an algebraically closed field k. This means that a cohomological invariant in the sense of [Se$_2$, Section 6.2] or [KMRT, Section 31B] is also a cohomological invariant in our sense but the converse may not be true.

The following observation, due to J.-P. Serre, relates the essential dimension G to cohomological invariants.

Lemma 6.9. *Let G be an algebraic group. Suppose there exists a non-trivial cohomological invariant $\alpha\colon H^1(\,\cdot\,,G) \longrightarrow H^i(\,\cdot\,,M)$, where M is a p-torsion module. Then* $\operatorname{ed}(G;p) \geq i$.

Proof. It is sufficient to show that if $\operatorname{ed}(G;p) < i$ then that $\alpha(X) = 0$ for every generically free primitive G-variety X.

Indeed, for every generically free primitive G-variety X there exists a $d:1$-cover $X' \dashrightarrow X$ of G-varieties and a G-compression $X' \longrightarrow Y$ such that $\operatorname{trdeg}_k k(Y)^G = \dim(Y/G) < i$. Thus $H^i(k(Y)^G, M) = (0)$ (see [Se$_3$, II.4.2]) and consequently $\alpha(Y) = 0$. Since $\alpha(X')$ is a homomorphic image of $\alpha(Y)$, we conclude $\alpha(X') = 0$. Finally, since $[k(X')^G : k(X)^G] = d$ is prime to p, the restriction map $H^i(k(X)^G, M) \longrightarrow H^i(k(X')^G, M)$ is injective; see [Se$_3$, I.2.4]. Thus $\alpha(X) = 0$, as claimed. $\square$

7. Stabilizers as obstructions to compressions

In this section we assume that k is algebraically closed; see Remark 6.2.

A lower bound. We begin by recalling the following result of Sumihiro.

Proposition 7.1. *Every G-variety is birationally isomorphic to a complete G-variety.*

Proof. Let X be a G-variety. After removing the singular locus from X, we may assume that X is smooth. Then X is a disjoint union of smooth irreducible varieties. The group G acts on the set of irreducible components of X; the orbits of this action give a decomposition of X as a disjoint union of primitive G-varieties; cf. [Re$_2$, Lemma 2.2(a)]. Thus we may assume X to be smooth and primitive.

Let X_0 be an irreducible component of X, let G_0 be the subgroup of G that preserves X_0, and let X_0' be Sumihiro's equivariant completion of X_0 as an irreducible G_0-variety; see [Su, Theorem 3]. Then $X' = X_0' \times_{G_0} G$ is a G-equivariant completion of X; it is a disjoint finite union of copies of X_0'. In particular, X' and X are birationally isomorphic as G-varieties. $\square$

We are now ready to prove our first lower bound on the essential dimension of a G-variety.

Theorem 7.2. *Let H be a finite abelian subgroup of G such that*

(a) *the centralizer of H is finite, and*
(b) *H does not normalize any non-trivial unipotent subgroup of G.*

Suppose X is a primitive generically free G-variety, x is a smooth point of X fixed by H, and $X \dashrightarrow Y$ is a G-compression. Then

1. $\dim(X) \geq \operatorname{rank}(H) + \dim(G)$.
2. *Moreover,* $\dim(Y) \geq \operatorname{rank}(H) + \dim(G)$. *In other words,* $\operatorname{ed}(X) \geq \operatorname{rank}(H)$.
3. *If H is a p-group then* $\operatorname{ed}(X;p) \geq \operatorname{rank}(H)$.

Note that since X is primitive, $\dim(X)$ is the dimension of every irreducible component of X. Moreover, since X is primitive, so is Y; hence, $\dim(Y)$ is the dimension of every irreducible component of Y.

Proof. (1) By Corollary 3.6 there exists a tower

$$\pi \colon X_n \xrightarrow{\pi_n} X_{n-1} \cdots \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0 = X$$

of blowups with smooth G-invariant centers such that X_n is in standard form. Thus, in view of Lemma 5.1, we may replace X by X_n, i.e., we may assume without loss of generality that X is in standard form.

By Theorem 4.1 $\operatorname{Stab}(x) = U \rtimes A$, where U is unipotent and A is diagonalizable. Recall that $H \subset \operatorname{Stab}(x)$. Since U is normal in $\operatorname{Stab}(x)$, it is normalized by H. Hence, in view of assumption (b), we conclude that $U = \{1\}$ and thus $\operatorname{Stab}(x) = A$. In particular, $A \subset C_G(H)$; thus A is finite. Now by Corollary 4.6

$$\dim(X) \geq \operatorname{rank}(A) + \dim(G) \geq \operatorname{rank}(H) + \dim(G) ,$$

as claimed.

(2) By Proposition 7.1 we may assume Y is complete. Moreover, in view of Corollary 3.6 we may also assume that Y is smooth. By Proposition 5.3, there exists a point $y \in Y$ such that $H \subset \operatorname{Stab}(y)$. Now apply part (1) to Y.

(3) Let $X' \dashrightarrow X$ be a G-equivariant $d:1$-cover of X. We want to show $\operatorname{ed}(X') \geq \operatorname{rank}(H)$. By Proposition 7.1 we may assume X' is complete; moreover, by Corollary 3.6 we may also assume X' is smooth. By Proposition 5.6 there exists a point $x' \in X'$ that is fixed by H. We now apply part (2) to X' to conclude that $\operatorname{ed}(X') \geq \operatorname{rank}(H)$. □

Corollary 7.3. *Let G be an algebraic group and H be an abelian subgroup of G such that (a) the centralizer of H is finite and (b) H does not normalize any non-trivial unipotent subgroup of G. Then* $\operatorname{ed}(G) \geq \operatorname{rank}(H)$. *Moreover, if H is a p-group then* $\operatorname{ed}(G,p) \geq \operatorname{rank}(H)$.

Proof. Apply Theorem 7.2(2) and (3) to $X = V =$ generically free linear representation of G and $x = 0 \in V$. □

Example 7.4. Let G be a finite group and $H \simeq (\mathbb{Z}/p\mathbb{Z})^m$ be a subgroup of G. Then $\operatorname{ed}(G;p) \geq m$. In particular, $\operatorname{ed}(\mathrm{S}_n;p) \geq [n/p]$; cf. [BR$_1$, Section 6.1] and [BR$_2$, Section 7].

A lemma of Serre. The difficulty in applying Theorem 7.2 and Corollary 7.3 is that condition (b) is often hard to verify. Fortunately, under rather general assumptions, there is an easy way around this problem.

Remark 7.5. Let G be an algebraic group. Assume there exists an abelian subgroup H of G satisfying conditions (a) and (b) of Theorem 7.2. Then the identity component of G is semisimple.

Proof. Assume G is not reductive. Then the unipotent radical $R_u(G)$ is a non-trivial normal unipotent subgroup of G, and thus condition (b) fails.

Now assume G is reductive. The radical $R(G)$ is the connected component of the center of G (see [Hu, 19.5]); hence, condition (a) fails unless $R(G)$ is trivial. This means that the identity component of G is semisimple, as claimed. $\square$

Thus if G is connected, we may assume without loss of generality that it is semisimple. The following lemma, communicated to us by J.-P. Serre, shows that in this case conditions (a) and (b) of Theorem 7.2 are equivalent.

Lemma 7.6. *Let G be a connected semisimple group and let H be a (not necessarily connected) reductive subgroup of G. Then the following conditions are equivalent.*

(a) The centralizer $C_G(H)$ of H in G is infinite.

(b) H normalizes a non-trivial unipotent subgroup of G.

(c) H is contained in a proper parabolic subgroup of G.

Proof. We will first show that (c) $\Longrightarrow$ (b), then use this implication to prove that (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (a).

(c) $\Longrightarrow$ (b): If H is contained in a proper parabolic subgroup P then H normalizes the unipotent radical $R_u(P) \neq \{1\}$.

(a) $\Longrightarrow$ (b): Assume $C_G(H)$ is infinite. If $C_G(H)$ contains a non-trivial unipotent element u then H centralizes (and, hence, normalizes) the unipotent subgroup $\overline{<u>} \neq \{1\}$ and thus (b) holds. If the centralizer $C_G(H)$ does not contain a non-trivial unipotent element, then the identity component of $C_G(H)$ is a non-trivial torus T. In this case $H \subset C_G(T)$, and $C_G(T)$ is a Levi subgroup of some non-trivial parabolic subgroup of G; see [Hu, 30.2]. Thus (c) holds, and, hence, so does (b).

(b) $\Longrightarrow$ (c): Suppose H normalizes a non-trivial unipotent subgroup U of G. Recall that the Borel—Tits construction associates, in a canonical way, a parabolic subgroup $P(U)$ to U so that U is contained in the unipotent radical of $P(U)$; see [Hu, 30.3]. In particular, $P(U)$ is proper. Moreover, by our assumption $H \subset N_G(U)$, where $N_G(U)$ denotes the normalizer of U in G. Since $N_G(U) \subset P(U)$ (see [Hu, Corollary 30.3A]), H is contained in the proper parabolic subgroup $P(U)$. This proves (c).

(c) $\Longrightarrow$ (a): If H is contained in a proper parabolic subgroup P of G then, by Levi's decomposition theorem, H is contained in some Levi subgroup L of

P; see [OV, Theorem 6.4.5]. Then $C_G(L) \subset C_G(H)$. Since the center $Z(L)$ contains a non-trivial torus (see [Hu, 30.2]), and $Z(L) \subset C_G(L) \subset C_G(H)$, we conclude that $C_G(H)$ is infinite. □

A better bound. We can now prove the main results of this section.

Theorem 7.7. *Let G be an algebraic group, H be an abelian subgroup of G, and X is a generically free G-variety. Suppose $H \subset \operatorname{Stab}(x)$ for a smooth point x of X.*

(1) Assume G is (connected and) semisimple and the centralizer $C_G(H)$ is finite. Then $\operatorname{ed}(X) \geq \operatorname{rank}(H)$. Moreover, if H is a p-group then $\operatorname{ed}(X;p) \geq \operatorname{rank}(H)$.

(2) More generally, if the identity component G^0 of G is semisimple and the centralizer $C_{G^0}(H \cap G^0)$ is finite then $\operatorname{ed}(X) \geq \operatorname{rank}(H)$. Moreover, if H is a p-group then $\operatorname{ed}(X;p) \geq \operatorname{rank}(H)$.

Proof. It is enough to verify that G and H satisfy conditions (a) and (b) of Theorem 7.2. In part (1) this follows immediately from Lemma 7.6.

(2) To check condition (a), note that $C_{G^0}(H \cap G^0)$ is of finite index in $C_G(H \cap G^0)$. This implies that $C_G(H \cap G^0)$ is finite and, hence, so is $C_G(H)$. To check condition (b), note that since we are working over a field of characteristic 0, unipotent subgroups of G are connected (see, e.g., [OV, 3.2.2, Corollary 2]) and, hence, contained in G^0. By Lemma 7.6, $H \cap G^0$ does not normalize any of them (except for $\{1\}$). Hence, neither does H. □

Theorem 7.8. *Let G be an algebraic group and H be an abelian subgroup of G.*

(1) Suppose G is (connected and) semisimple and the centralizer $C_G(H)$ is finite. Then $\operatorname{ed}(G) \geq \operatorname{rank}(H)$. Moreover, if H is a p-group then $\operatorname{ed}(G;p) \geq \operatorname{rank}(H)$.

(2) More generally, if the identity component G^0 of G is semisimple and the centralizer $C_{G^0}(H \cap G^0)$ is finite then $\operatorname{ed}(G) \geq \operatorname{rank}(H)$. Moreover, if H is a p-group then $\operatorname{ed}(G;p) \geq \operatorname{rank}(H)$.

Proof. Apply Theorem 7.7 with $X = V =$ generically free linear representation of G and $x = 0$. □

Remark 7.9. Let G be a semisimple algebraic group and $H = (\mathbb{Z}/p^{i_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{i_r}\mathbb{Z})$ be an abelian p-subgroup of G of rank r satisfying the assumptions of Theorem 7.8(1). Then $\operatorname{ed}(G;p) \geq r$ and, in particular, $\operatorname{ed}(V;p) \geq r$ for any generically free linear representation of G; cf. Lemma 6.6(b).

Moreover, there exists an irreducible G-variety X such that $\operatorname{ed}(X;p) = r$. Indeed, let $W = \mathbb{A}^r$ be a faithful representation of H, where the ith cyclic factor of H acts by a faithful character on the ith coordinate of $\mathbb{A}^r$, and trivially on all other coordinates. Let $X = G \times_H W$ be the induced G-variety. Since X is the quotient of the smooth variety $G \times W$ by the free H-action $h(g,w) = (gh^{-1}, hw)$, X is smooth and $\dim X = \dim G + r$. By our construction the point $x = (1_G, 0_W)$ is fixed by H. Theorem 7.7(1) shows that $\operatorname{ed}(X;p) \geq r$; on the other hand, $\dim X - \dim G = r$, and hence, $\operatorname{ed}(X;p) = r$.

The same construction goes through if G and H satisfy the assumptions of Theorem 7.8(2), except that in this case X will be primitive and not necessarily irreducible.

8. Applications

We now want to apply Theorem 7.8 to specific groups G. In most cases we will choose H to be an elementary abelian p-subgroup of G. Note that the theorem does not apply if H is contained in a subtorus T of G because in this case the centralizer of H contains T and, hence, is infinite. Thus we are interested in nontoral finite abelian subgroups of G. These subgroups have been extensively studied; see, e.g., [A], [Bo], [BS], [CS], [Gri], [Wo].

Before we proceed with the applications, we make two additional remarks. First of all, for the purpose of applying Theorem 7.8 we may restrict our attention to maximal finite abelian subgroups of G. Indeed, we lose nothing if we replace H by a larger (with respect to containment) finite abelian subgroup; this will only have the effect of making the centralizer smaller and improving the resulting bound on $\operatorname{ed}(G)$. Secondly, a nontoral finite abelian subgroup of G, even a maximal one, may have an infinite centralizer and, hence, not be suitable for our purposes. Thus our task is to find maximal finite abelian subgroups of G with finite centralizers.

We shall assume that k is an algebraically closed field throughout this section; cf. Remark 6.2.

Orthogonal groups.

Theorem 8.1. 1. *$\operatorname{ed}(O_n; 2) \geq n$ for every $n \geq 1$.*
2. *$\operatorname{ed}(SO_n; 2) \geq n - 1$ for every $n \geq 3$.*
3. *$\operatorname{ed}(PO_n; 2) \geq n - 1$ for every $n \geq 3$.*

Proof. Apply Theorem 7.8 with
(1) $H \simeq (\mathbb{Z}/2\mathbb{Z})^n$ = the diagonal subgroup of $G = O_n$.
(2) $H \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ = the diagonal subgroup of $G = SO_n$.
(3) $H \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ = the diagonal subgroup of $G = PO_n$. □

Remark 8.2. For alternative proofs of (1) see [Re_2, Theorem 10.3 and Example 12.6]. For alternative proofs of (2) see [Re_2, Theorem 10.4 and Example 12.7]. (Note that equality holds in both cases.) The inequality (3) is new to us.

Projective linear groups. The essential dimension of PGL_n is closely related to the structure of central simple algebras of degree n; we begin by briefly recalling this connection.

We shall say that a field extension K/F is *prime-to-p* if it is a finite extension of degree prime to p.

Definition 8.3. (a) Let F be a field and let A be a finite-dimensional F-algebra. We will say that A is defined over F_0 if there exists an F_0-algebra A_0 such that $A \simeq A_0 \otimes_{F_0} F$ (as F-algebras). Equivalently, A is defined over F_0 if there exists an F-basis $e_1, \dots, e_d$ of A such that

$$e_i e_j = \sum_{h=1}^{d} c_{ij}^h e_h$$

and every structure constant c_{ij}^h is contained in F_0.

(b) $\tau(A)$ is defined as the minimal value of $\mathrm{trdeg}_k(F_0)$. Here the minimum is taken over all subfields F_0 of F such that $k \subset F_0$ and A is defined over F_0.

(c) Let p be a prime. Then $\tau(A;p)$ is defined as the minimal value of $\tau(A \otimes_F K)$, where K ranges over prime-to-p extensions of F.

Example 8.4. If $A = \mathrm{M}_n(F)$ then $\tau(A) = 0$, since $A = \mathrm{M}_n(k) \otimes_k F$.

Lemma 8.5.
1. $\mathrm{ed}(\mathrm{PGL}_n)$ *is the maximal value of* $\tau(A)$ *as* A *ranges over all central simple algebras of degree* n *containing* k *as a central subfield.*
2. $\mathrm{ed}(\mathrm{PGL}_n)$ *is the maximal value of* $\tau(D)$ *as* D *ranges over all division algebras of degree* n *containing* k *as a central subfield.*
3. $\mathrm{ed}(\mathrm{PGL}_n;p)$ *is the maximal value of* $\tau(A;p)$ *as* A *ranges over all central simple algebras of degree* n *containing* k *as a central subfield.*
4. $\mathrm{ed}(\mathrm{PGL}_n;p)$ *is the maximal value of* $\tau(D;p)$ *as* D *ranges over all division algebras of degree* n *containing* k *as a central subfield.*
5. $\mathrm{ed}(\mathrm{PGL}_n;p) = \mathrm{ed}(\mathrm{PGL}_{p^r};p)$, *where* p^r *is the highest power of* p *dividing* n.
6. $\mathrm{ed}(\mathrm{PGL}_n;p) = 0$ *if* n *is not divisible by* p.
7. $\mathrm{ed}(\mathrm{PGL}_p;p) = 2$.

Proof. (1) and (2) are proved in [Re$_2$, Lemma 9.2]. (3) and (4) follow from [Re$_2$, Lemma 9.1, Proposition 8.6 and Theorem 8.8(a)].

(5) Suppose $n = p^r m$, where m is not divisible by p. If D is a division algebra of degree p^r with center F and $A = \mathrm{M}_m(D)$ then $\tau(A) = \tau(D)$; see [Re$_2$, Lemma 9.7]. Thus for any prime-to-p extension K/F, we have $\tau(A \otimes_F K) = \tau(D \otimes_F K)$. By part (3) the maximal value of the left hand side (over all D and K) is $\leq \mathrm{ed}(\mathrm{PGL}_n;p)$. On the other hand, by part (4), the maximal value of the right hand side is $\mathrm{ed}(\mathrm{PGL}_{p^r};p)$. Thus $\mathrm{ed}(\mathrm{PGL}_{p^r};p) \leq \mathrm{ed}(\mathrm{PGL}_n;p)$.

Conversely, given any division algebra D of degree n with center F, there exists a prime-to-p extension K/F such that $D \otimes_F K = \mathrm{M}_m(D_0)$, where D_0 is a division algebra of degree p^r with center K; see [Row, Theorem 3.1.21]. Thus by part (4)

$$\tau(D;p) \leq \tau(D \otimes_F K;p) = \tau(D_0;p) \leq \mathrm{ed}(\mathrm{PGL}_{p^r};p) \ .$$

Taking the maximum over all D and using part (4) once again, we obtain $\mathrm{ed}(\mathrm{PGL}_n;p) \leq \mathrm{ed}(\mathrm{PGL}_{p^r};p)$, as desired.

(6) Follows from part (5) with $r = 0$.

(7) It is enough to show $\tau(D; p) = 2$ for every division algebra D of degree p. To show $\tau(D; p) \geq 2$, note that for any prime-to-p extension K/F, $D \otimes_F K$ is a division algebra; see [Row, Corollary 3.1.19]. By Tsen's theorem, $\tau(D \otimes_F K) \geq 2$; see [Re$_2$, Lemma 9.4(a)]. This proves $\tau(D; p) \geq 2$.

On the other hand, by a theorem of Albert, there exists a prime-to-p extension K/F such that $D' = D \otimes_F K$ is a cyclic division algebra. Then by [Re$_2$, Lemma 9.4(b)] $\tau(D') \leq 2$ and hence, $\tau(D; p) \leq 2$. □

The following inequality is a consequence of [Re$_1$, Theorem 16.1(b)] and Lemma 8.5(3) above.

Theorem 8.6. $\mathrm{ed}(\mathrm{PGL}_{p^r}; p) \geq 2r$.

We will now give an alternative proof based on Theorem 7.8. In fact, we will prove a slightly stronger result; see Theorem 8.13. We begin with the following elementary construction.

Definition 8.7. Let A is an abelian group of order n. and let $V = k[A]$ be the group algebra of A.

(a) The regular representation $P\colon A \longrightarrow \mathrm{GL}(V) = \mathrm{GL}_n$ is given by $a \mapsto P_a \in \mathrm{GL}(V) = \mathrm{GL}_n$, where

$$P_a\Big(\sum_{b \in A} c_b b\Big) = \sum_{b \in A} c_b ab$$

for any $a \in A$ and $c_b \in k$.

(b) The representation $D\colon A^* \longrightarrow \mathrm{GL}(V) = \mathrm{GL}_n$ is defined by $\chi \mapsto D_\chi \in \mathrm{GL}(V)$, where

$$D_\chi\Big(\sum_{a \in A} c_a a\Big) = \sum_{a \in A} c_a \chi(a) a$$

for any $\chi \in A^*$ and $c_a \in k$.

Note that in the basis $\{a \mid a \in A\}$ of V, each P_a is represented by a permutation matrix and each D_χ is represented by a diagonal matrix; this explains our choice of the letters P and D.

Lemma 8.8. *Let A be a finite abelian group, $a, b \in A$ and $\chi, \mu \in A^*$. Then*

(a) $D_\chi P_a = \chi(a) P_a D_\chi$.

(b) $(P_a D_\chi)(P_b D_\mu)(P_a D_\chi)^{-1} = \chi(b)\mu^{-1}(a)(P_b D_\mu)$

Proof. Part (a) can be verified directly from Definition 8.7. Part (b) is an immediate consequence of part (a). □

Lemma 8.9. *Suppose A is an abelian group of order n such that its 2-Sylow subgroup is either (i) non-cyclic or (ii) trivial (the latter occurs when n is odd). Then*

(a) $P_a \in \mathrm{SL}_n$ for every $a \in A$ and

(b) $D_\chi \in \mathrm{SL}_n$ for every $\chi \in A^*$.

Proof. (a) Recall that P_a is a permutation matrix representing the permutation $\sigma_a : A \longrightarrow A$ given by $b \longrightarrow ab$. Thus $\det(P_a) = (-1)^{\mathrm{sign}(\sigma_a)}$, and we only need to show σ_a is even.

Assume, to the contrary, that σ_a is odd. Let m be the order of a. Since σ_a is a product of $\frac{n}{m}$ disjoint m-cycles, both $\frac{n}{m}$ and $m-1$ are odd. In particular, m and, hence, n is even. Thus assumption (ii) fails. On the other hand, since $\frac{n}{m} = [A : <a>]$ is odd, the Sylow 2-subgroup of A is contained in $<a>$ and, thus assumption (i) fails. This contradiction proves that σ_a is an even permutation.

(b) Suppose χ is an element of A^* of order m and let ζ_m be a primitive m-th root of unity. The matrix D_χ is diagonal with entries $\chi(a)$, as a ranges over A; here $\chi(a)$ assumes the value $(\zeta_m)^i$ exactly $\frac{n}{m}$ times for each $i = 0, 1, \ldots, m-1$. Hence,

$$\det(D_\chi) = \Big(\prod_{i=0}^{m-1} (\zeta_m)^i\Big)^{\frac{n}{m}} = (\zeta_m)^{m \cdot \frac{m-1}{2} \cdot \frac{n}{m}} .$$

Assume, to the contrary that $\det(D_\chi) \neq 1$. Then both $\frac{n}{m}$ and $m-1$ are odd. Arguing as in part (a), we conclude that $n = |A^*|$ is even and the Sylow 2-subgroup of A^* is cyclic. Since A and A^* are isomorphic, this contradicts our assumption. Hence, $\det(D_\chi) = 1$, as claimed. $\square$

Definition 8.10. Assume A is an abelian group of order n, e is an integer dividing n and ζ_e is a primitive eth root of unity.

(i) Let $\phi_n : A \times A^* \longrightarrow \mathrm{PGL}_n$ be the map of sets given by $\phi_n(a, \chi) =$ image of $P_a D_\chi$ in PGL_n. We define H_n as the image of ϕ_n in PGL_n.

(ii) Suppose A satisfies the conditions of Lemma 8.9. Then we define $\phi_e : A \times A^* \longrightarrow \mathrm{SL}_n / <\zeta_e I_n>$ by the formula $\phi_e(a, \chi) = P_a D_\chi \pmod{<\zeta_e I_n>}$. We define H_e as the image of ϕ_e in $\mathrm{SL}_n / <\zeta_e I_n>$.

Note that $\mathrm{SL}_n / <\zeta_n I_n> = \mathrm{PGL}_n$. If A satisfies the conditions of Lemma 8.9 then the two definitions of ϕ_n (and thus H_n) coincide.

Lemma 8.11. *Under the assumptions of Definition 8.10,*

(i) H_n is a subgroup of PGL_n and ϕ_n is an isomorphism between $A \times A^*$ and H_n;

(ii) H_e is a subgroup of $\mathrm{SL}_n / <\zeta_e I_n>$ and ϕ_e is an isomorphism between $A \times A^*$ and H_e, provided that A satisfies the conditions of Lemma 8.9 and the exponent of A divides e.

The lemma says, in particular, that, if e is divisible by the exponent of A then H_e is a subgroup of $\mathrm{SL}_n / <\zeta_e I_n>$ whenever H_e is defined. (Note that in part (i), $e = n = |A|$ is necessarily divisible by the exponent of A.)

Proof. By Lemma 8.8(a), P_a and D_χ commute modulo $<\zeta_n I_n>$ in case (i) and modulo $<\zeta_e I_n>$ in case (ii). The lemma is an easy consequence of this fact. $\square$

In the sequel we shall assume that A is an abelian p-group of order p^r and $e = p^i$, where $1 \leq i \leq r$ is chosen so that e is divisible by the exponent of A. Note that under these assumptions H_e is always well-defined and is a subgroup of $SL_n/{<}\zeta_e I_n{>}$. (Indeed, if the conditions of Lemma 8.9 fail to be satisfied then $p = 2$, A is cyclic and hence, $e = n$, so that H_e is given by Definition 8.7(i).)

Lemma 8.12. *Suppose A is an abelian p-group of order $n = p^r$, and $e = p^i$ with $1 \leq i \leq r$. Assume the exponent of A divides e. Let $\pi \colon SL_n/{<}\zeta_e I_n{>} \longrightarrow \mathrm{PGL}_n$ be the natural projection, let $H = \pi^{-1}(H_n)$ and let $K = \mathrm{Ker}(\pi)$ be the center of $SL_n/{<}\zeta_e I_n{>}$. Then*

(a) $H = H_e \times K \simeq A \times A^* \times (\mathbb{Z}/p^{r-i}\mathbb{Z})$.

(b) H_n is self-centralizing in PGL_n,

(c) H is self-centralizing in $SL_n/{<}\zeta_e I_n{>}$.

Proof. (a) The surjective homomorphism $\pi|_H \colon H \longrightarrow H_n$ splits: the complement of K in H is H_e. Since K is central, part (a) follows.

(b) Denote the centralizer of H_n in PGL_n by $C(H_n)$. Lemma 8.8(b) shows that for every $b \in A$ and $\mu \in A^*$, the matrix $P_b D_\mu$ spans a one-dimensional representation space for the conjugation action of H_n on $\mathrm{M}_n(k)$; moreover, H_n acts on these $|H_n|$ spaces by distinct characters. Since there are $n^2 = p^{2r}$ of these spaces and $\dim(\mathrm{M}_n) = |H_n| = n^2$, we conclude that $\mathrm{M}_n(k)$ decomposes as a direct sum of these one-dimensional representations. Any $g \in C(H_n) \subset \mathrm{PGL}_n$ is represented by a non-zero matrix lying in one of them, i.e., by a non-zero constant multiple of $P_a D_\chi$ for some $a \in A$ and $\chi \in A^*$. This shows that $C(H_n) = H_n$ in PGL_n, as claimed.

(c) Denote the centralizer of H in $SL_n/{<}\zeta_e I_n{>}$ by $C(H)$. Since H is abelian, $H \subset C(H)$. On the other hand, in view of part (b), $C(H) \subset \pi^{-1}(C(H_n)) = \pi^{-1}(H_n) = H$. $\square$

Theorem 8.13.

$$\mathrm{ed}(\mathrm{SL}_{p^r}/{<}\zeta_{p^i} I_{p^r}{>}; p) \geq \begin{cases} 2r+1 & \text{if } i = 1, \ldots, r-1 \ , \\ 2r & \text{if } i = r \ . \end{cases}$$

Note that if $i = r$ then $\mathrm{SL}_{p^r}/{<}\zeta_{p^i} I_{p^r}{>} = \mathrm{PGL}_{p^r}$, and we obtain the bound of Theorem 8.6.

Proof. Applying Lemma 8.12 to $A = (\mathbb{Z}/p\mathbb{Z})^r$; we obtain a finite abelian self-centralizing p-subgroup $H \subset \mathrm{SL}_{p^r}/{<}\zeta_{p^i} I_{p^r}{>}$. By part (a) $\mathrm{rank}(H) = 2r+1$ if $1 \leq i < r$ and $2r$ if $i = r$. The desired inequalities now follow from Theorem 7.8. $\square$

Remark 8.14. One can show that any abelian p-subgroup of PGL_{p^r} with a finite centralizer has rank $\leq 2r$. Thus the lower bounds of Theorem 8.13 cannot be improved by this method.

Spin groups. We will now apply Theorem 7.8 to obtain lower bounds on the essential dimension of some spin groups. Elementary abelian subgroups of Spin_n are described in some detail in [Wo]. In particular, if p is an odd prime then every elementary abelian p-group is toral (see [Se_2, Section 2.2], [Wo, Theorem 5.6], or [Gri, (2.22)]) and thus is not suitable for our purposes. We shall therefore concentrate on elementary abelian 2-subgroups.

Recall that Spin_n fits into an exact sequence

$$\{1\} \longrightarrow \{-1,1\} \longrightarrow \mathrm{Spin}_n \xrightarrow{f} SO_n \longrightarrow \{1\}\ ,$$

where $\{-1,1\}$ is the central subgroup of Spin_n. Let $D \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$ be the diagonal subgroup of SO_n and let $D' = f^{-1}(D) \subset \mathrm{Spin}_n$. We want to construct elementary abelian 2-subgroups of D'. (Note that every elementary abelian 2-subgroups of Spin_n is conjugate to a subgroup of D'; see [Wo, Theorem 5.6].)

Recall that a doubly even code L of length n is a vector subspace of $(\mathbb{Z}/2\mathbb{Z})^n$ with the property that the weight of every element of L is divisible by 4. (Here the weight of an element of $(\mathbb{Z}/2\mathbb{Z})^n$ is defined as the number of 1s among its coordinates.) We shall say that an $m \times n$-matrix over $\mathbb{Z}/2\mathbb{Z}$ is a generator matrix for L if its rows span L as a $\mathbb{Z}/2\mathbb{Z}$-vector space.

Doubly even codes of length n are in 1—1 correspondence with elementary abelian 2-subgroups of D' containing -1; this is explained in [Wo, Sections 1 and 2]; see also [St, Section 7]. Explicitly, let E_n be the (index 2) subgroup of $(\mathbb{Z}/2\mathbb{Z})^n$) consisting of all codewords of even weight. Consider the group isomorphism $\phi\colon (E_n,+) \longrightarrow (D,\cdot)$ given by

$$\phi(i_1,\dots,i_n) = \begin{pmatrix} (-1)^{i_1} & 0 & \dots & 0 \\ 0 & (-1)^{i_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & (-1)^{i_n} \end{pmatrix}. \tag{8.1}$$

If $L \in E_n$ is a doubly even code of dimension d then $\phi(L)$ is an elementary abelian 2-subgroup of SO_n of rank d. The preimage $H = f^{-1}(\phi(L))$ of this subgroup in Spin_n is thus an elementary abelian 2-subgroup of rank $d+1$. Note that by [Wo, Theorem 2.1], every elementary abelian subgroup of D' containing -1 is obtained in this way.

Recall that not every elementary abelian 2-subgroup is good for our purposes; in order to apply Theorem 7.8, we need to construct one whose centralizer is finite. Clearly the group $H = f^{-1}(\phi(L))$ has a finite centralizer in Spin_n if and only if its image $f(H) = \phi(D)$ has a finite centralizer in SO_n.

Lemma 8.15. *Let L be a doubly even code of length n and let*

$$\phi\colon E_n \longrightarrow SO_n$$

be as in (8.1). *Then $\phi(L)$ has a finite centralizer in SO_n if and only if a generator matrix of L has distinct columns.*

Proof. The map $\phi|_L$ may be viewed as an orthogonal representation of $L \simeq (\mathbb{Z}/2\mathbb{Z})^d$. This representation is given to us as a direct sum of characters

$\chi_1, \ldots, \chi_n : L \longrightarrow \mathbb{G}_m$, where $\chi_j(i_1, \ldots, i_n) = (-1)^{i_j}$. Note that a generator matrix of L has distinct columns if and only if these characters are distinct. If the characters are distinct then by Schur's Lemma the centralizer of $\phi(L)$ in SO_n consists of diagonal matrices and, hence, is finite. On the other hand, if two of these characters are equal then the centralizer of $\phi(L)$ contains a copy of SO_2 and, hence, is infinite. □

We are now ready to state our main result on spin groups.

Theorem 8.16. $\mathrm{ed}(\mathrm{Spin}_n; 2) \geq [\frac{n}{2}] + 1$ *for every* $n \equiv 0$, 1 *or* $-1 \pmod 8$.

Proof. The above discussion shows that it is sufficient to construct a doubly even code L of length n and dimension $[n/2]$ all of whose columns are distinct.

We now exhibit such codes in the three cases covered by the theorem. Let 0_i (respectively, J_i) denote, the i-tuple of zeros (respectively, the i-tuple of ones) in $(\mathbb{Z}/2\mathbb{Z})^i$. One can now check directly that each of the following codes is doubly even of dimension $[\frac{n}{2}]$; moreover, in each case the generator matrix (for the generating set given below) has distinct columns.

$n = 8m$. $L = <(a, a), (0_{4m}, J_{4m})>$, where a ranges over all elements of $(\mathbb{Z}/2\mathbb{Z})^{4m}$ of even weight.

$n = 8m + 1$. $L = <(0_1, a, a), (0_{4m+1}, J_{4m})>$, where a ranges over all elements of $(\mathbb{Z}/2\mathbb{Z})^{4m}$ of even weight.

$n = 8m - 1$. $L = <(a, a, 0_1), (0_{4m-1}, J_{4m})>$, where a ranges over all elements of $(\mathbb{Z}/2\mathbb{Z})^{4m-1}$ of even weight.

This completes the proof of the theorem. □

Remark 8.17. Recall the following exceptional isomorphisms of classical algebraic groups:

$$\begin{aligned} &\mathrm{Spin}_2 \simeq (\mathbb{G}_m)^2\,, \\ &\mathrm{Spin}_3 \simeq \mathrm{SL}_2\,, \\ &\mathrm{Spin}_4 \simeq \mathrm{SL}_2 \times \mathrm{SL}_2\,, \\ &\mathrm{Spin}_5 \simeq \mathrm{Sp}_4\,, \text{ and} \\ &\mathrm{Spin}_6 \simeq \mathrm{SL}_4\,. \end{aligned}$$

(This phenomenon is caused by the fact that while the Dynkin diagrams of types A_n, B_n, C_n, and D_n are distinct for large n, for small n there are some overlaps.) We conclude that all of these groups are special (see [Gro, Section 5], [PV, Section 2.6]) and thus

$$\mathrm{ed}(\mathrm{Spin}_n) = 0 \text{ for every } 2 \leq n \leq 6\,;$$

(see [Re$_2$, Section 5.2]). This shows that the condition $n \equiv 0$, 1 or -1 (mod 8) is not as arbitrary as it may seem at first glance.

Remark 8.18. The following results are due to M. Rost [Rost$_2$]:

$$\begin{aligned}
\mathrm{ed}(\mathrm{Spin}_7) &= 4\\
\mathrm{ed}(\mathrm{Spin}_8) &= 5\\
\mathrm{ed}(\mathrm{Spin}_9) &= 5\\
\mathrm{ed}(\mathrm{Spin}_{10}) &= 4\\
\mathrm{ed}(\mathrm{Spin}_{11}) &= 5\\
\mathrm{ed}(\mathrm{Spin}_{12}) &= 6\\
\mathrm{ed}(\mathrm{Spin}_{13}) &= 6\\
\mathrm{ed}(\mathrm{Spin}_{14}) &= 7\ .
\end{aligned}$$

The proofs rely on the properties of quadratic forms of dimension ≤ 14. In particular, our bound is sharp for $n = 7$, 8 and 9. On a lighter note, our bound is also sharp for $n = 1$, since $\mathrm{Spin}_1 = \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{ed}(\mathbb{Z}/2\mathbb{Z}) = 1$.

Exceptional groups.

Theorem 8.19. 1. $\mathrm{ed}(G_2; 2) \geq 3$.
2. $\mathrm{ed}(F_4; 2) \geq 5$.
3. $\mathrm{ed}(F_4; 3) \geq 3$.
4. $\mathrm{ed}(3E_6; 3) \geq 4$. *Here $3E_6$ denotes the simply connected group of type E_6 over k.*
5. $\mathrm{ed}(2E_7; 2) \geq 7$. *Here $2E_7$ denotes the simply connected group of type E_7 over k.*
6. $\mathrm{ed}(E_7; 2) \geq 8$. *Here E_7 denotes the adjoint E_7.*
7. $\mathrm{ed}(E_8; 2) \geq 9$.
8. $\mathrm{ed}(E_8; 3) \geq 5$.
9. $\mathrm{ed}(E_8; 5) \geq 3$.

Proof. In each case we exhibit an abelian subgroup H with a finite centralizer, then appeal to Theorem 7.8.

(1) Let O be the split octonion algebra generated by i, j, and l, as in [J$_2$, pp. 16–17]. We can identify $G_2 \subset \mathrm{GL}_8$ with the automorphism group of O. Now let $H = <\alpha, \beta, \gamma> \simeq (\mathbb{Z}/2\mathbb{Z})^3$, where

$$\begin{array}{lll}
\alpha(i) = -i & \alpha(j) = j & \alpha(l) = l\\
\beta(i) = i & \beta(j) = -j & \beta(l) = l\\
\gamma(i) = i & \gamma(j) = j & \gamma(l) = -l\ .
\end{array}$$

To prove that H is self-centralizing, note that the representation of H on O (viewed as an 8-dimensional vector space) is a direct sum of 8 distinct characters; cf. [Gri, Table I, p. 257] or [CS, p. 252].

(2) A self-centralizing $H = (\mathbb{Z}/2\mathbb{Z})^5 \subset F_4$ is described in [Gri, (7.3)].

(3) A self-centralizing $H = (\mathbb{Z}/3\mathbb{Z})^3 \subset F_4$ is described in [Gri, (7.4)].

(4) Use the maximal $H = (\mathbb{Z}/3\mathbb{Z})^4$ of $3E_6$ described in [Gri, (11.13)(i)]; see also [CS]. Note that by [Gri, (11.13)(i)] H has a finite normalizer in $3E_6$; hence, its centralizer is finite as well.

(5) Let u be an element of order 4 in $2E_7$ whose centralizer $C(u)$ is isomorphic to $\mathrm{SL}_8/(\pm I_8)$; see [Gri, bottom of p. 283]. (According to the

notational conventions of [Gri, (2.14)], u is an element of type **4A**.) Note that under the identification $C(u) \cong \mathrm{SL}_8/(\pm I_8)$, the element u corresponds to the central element of order 4 in $\mathrm{SL}_8/(\pm I_8)$ which is represented by the scalar matrix ζI_8, where ζ is a primitive 8th root of unity.

By Lemma 8.12(a), with $p = 2$, $r = 3$, $e = 2$ and $A = (\mathbb{Z}/2\mathbb{Z})^3$, the group $C(u) = \mathrm{SL}_8/(\pm I_8)$ contains a self-centralizing finite abelian subgroup $H \simeq (\mathbb{Z}/2\mathbb{Z})^6 \times (\mathbb{Z}/4\mathbb{Z})$, where the $\mathbb{Z}/4\mathbb{Z}$-factor is the center of $C(u)$, i.e., is equal to $<u>$. Moreover, H is self-centralizing in $C(u)$. Since $u \in H$, we conclude that H is self-centralizing in $2E_7$. Applying Theorem 7.8 to H, we obtain the desired inequality $\mathrm{ed}(2E_7) \geq \mathrm{rank}(H) = 7$.

(6) A self-centralizing subgroup $H = (\mathbb{Z}/2\mathbb{Z})^8$ of E_7 is described in [Gri, Theorem 9.8(ii)]; see also [CS].

(7) E_8 has a maximal elementary abelian subgroup $H \simeq (\mathbb{Z}/2\mathbb{Z})^9$ called a "type 1 subgroup"; see [A], [Gri, (2.17)] and [CS]. By [Gri, (2.17)] this subgroup has a finite normalizer. Hence, its centralizer is finite as well. (In fact, one can show that H is self-centralizing; see [Gri, p. 258]).

(8)–(9) E_8 contains self-centralizing subgroups $H_1 \simeq (\mathbb{Z}/3\mathbb{Z})^5$; and $H_2 = (\mathbb{Z}/5\mathbb{Z})^3$; see [Gri, (11.5) and (10.3)] □

Remark 8.20. Alternative proofs of inequalities (1), (2) and (3) can be found in [Re$_2$, 12.14 and 12.15]. In fact, equality holds in all three cases: in the case of (1) this is proved in [Re$_2$], for (2) and (3) this was observed by J.-P. Serre [Se$_4$]. Moreover, V. E. Kordonsky [Ko] has shown that $\mathrm{ed}(F_4) \leq 5$ (and thus $\mathrm{ed}(F_4) = 5$).

One can show, by modifying the proof of [Re$_2$, Proposition 11.7] (or, alternatively, of [Ko, Theorem 9]) that $\mathrm{ed}(3E_6; 3) \leq \mathrm{ed}(F_4; 3) + 1 = 4$, so that inequality (4) is sharp as well. We do not know the exact value of $\mathrm{ed}(3E_6)$; however, Kordonsky has shown that $\mathrm{ed}(3E_6) \leq 6$; see [Ko, Section 4.2]. Thus $\mathrm{ed}(3E_6) = 4$, 5 or 6. We remark that alternative proofs of (4) were recently shown to us by M. Rost and by R. S. Garibaldi [Ga].

An alternative proof of part (9) is based on Lemma 6.9 and the existence of a nontrivial Rost invariant $H^1(\,\cdot\,, E_8) \longrightarrow H^5(\,\cdot\,, \mathbb{Z}/5\mathbb{Z})$; see [Se$_2$, 7.3] or [KMRT, (31.40) and (31.47)]. M. Rost has informed us that he can prove $\mathrm{ed}(E_8; 5) = 3$.

We do not know whether or not inequalities (5)–(8) are sharp. Regarding (5), we remark that by a theorem of Kordonsky $\mathrm{ed}(2E_7) \leq 9$ (see [Ko, Theorem 10]); thus $\mathrm{ed}(2E_7)$ and $\mathrm{ed}(2E_7; 2)$ are equal to 7, 8 or 9.

To the best of our knowledge, inequalities (5)–(8) are new.

A wish list for cohomological invariants.

Remark 8.21. Some of the lower bounds of this section allow alternative proofs based on the existence of certain cohomological invariants; see Lemma 6.9. For example, Theorem 8.1(1) follows from the existence of a non-trivial cohomological invariant $H^1(\,\cdot\,, O_n) \longrightarrow H^n(\,\cdot\,, \mathbb{Z}/2\mathbb{Z})$

(namely, the nth Stiefel—Whitney class, see [Se$_2$, Section 6.3]), Theorem 8.19(2) follows from the existence of the cohomological invariant of $H^1(\,\cdot\,, F_4) \longrightarrow H^5(\,\cdot\,, \mathbb{Z}/2\mathbb{Z})$ (see [Se$_2$, Section 9.2]), Theorem 8.19(3) follows from the existence of the Serre—Rost invariant $H^1(\,\cdot\,, F_4) \longrightarrow H^5(\,\cdot\,, \mathbb{Z}/3\mathbb{Z})$ (see [Se$_2$, Section 9.3]), etc.

Other inequalities cannot be proved in this way because the needed cohomological invariants are not known to exist. On the other hand, these bounds suggest that there may exist cohomological invariants of the types listed below. (Here by a mod p invariant of G-varieties in H^d we shall mean a cohomological invariant $H^1(\,\cdot\,, G) \longrightarrow H^d(\,\cdot\,, M)$ in the sense of Definition 6.7, with M p-torsion.)

1. (cf. Theorem 8.6) A mod p invariant of PGL_{p^r}-varieties in H^{2r}.
   In the case $p = r = 2$ an invariant of this type was recently constructed by J.-P. Serre [Se$_5$] (see also [Rost$_1$] and [RST]).
2. (cf. Theorem 8.16) A mod 2 invariant of Spin_n-varieties in $H^{[n/2]+1}$ for $n \equiv 0, \pm 1 \pmod 8$.
   For $n = 7$, 8 and 9 such invariants were recently constructed by M. Rost [Rost$_2$].
3. (cf. Theorem 8.19(6)) A mod 2 invariant of E_7-varieties in H^8.
4. (cf. Theorem 8.19(7)) A mod 2 invariant of E_8-varieties in H^9.
5. (cf. Theorem 8.19(8)) A mod 3 invariant of E_8-varieties in H^5.

The above-mentioned constructions of Serre and Rost represent the only currently known invariants of types 1–5.

9. Simplifying polynomials by Tschirnhaus transformations

Let E/F be a field extension of degree n such that $k \subset F$. Suppose $E = F(z)$ and

$$f_z(t) = t^n + \alpha_1(z)t^{n-1} + \ldots + \alpha_n(z)$$

is the minimal polynomial of z over F. We are interested in choosing the generator z whose minimal polynomial has the simplest possible form. More precisely, we want $\mathrm{trdeg}_k\, k(\alpha_1(z), \dots, \alpha_n(z))$ to be as small as possible. We shall denote the minimal value of $\mathrm{trdeg}_k\, k(\alpha_1(z), \dots, \alpha_n(z))$ by $\tau(E/F)$. Note that $\tau(E/F)$ is the same as $\tau(E)$ given by Definition 8.3, where E is viewed as an n-dimensional F-algebra. (We remark that $\tau(E/F)$ was denoted by $\mathrm{ed}(E/F)$ in [BR$_1$] and [BR$_2$].)

As we explained in the Introduction, a choice of a generator z (or, equivalently, an isomorphism of fields $E \simeq F[t]/(f_z))$ is called a Tschirnhaus transformation without auxiliary radicals. If E/F is given as the root field of a polynomial $f(x) \in F[x]$, i.e., $E = F[x]/(f(x))$, then the polynomial $f_z(t)$ is said to be obtained from $f(t)$ via the Tschirnhaus substitution $x \longmapsto z$. In this setting we are interested in simplifying the given polynomial $f(t) = f_x(t)$ by a Tschirnhaus substitution, where the "complexity" of a polynomial is measured by the number of algebraically independent coefficients (over k). The number $\tau(E/F)$ tells us to what extent $f(x)$ can be simplified.

A case of special interest is the generic field extension L/K of degree n. More precisely, $K = k(a_1, \dots, a_n)$, $L = K[x]/(g(x))$, and

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n ,$$

where $a_1, \dots, a_n$ are algebraically independent variables over k. The following results are proved in [BR$_1$] (see also [BR$_2$]): $\tau(L/K) = \mathrm{ed}(\mathrm{S}_n) \geq [n/2]$ and $\tau(L/K) \geq \tau(E/F)$, where E/F is any field extension of degree n.

The object of this section is to prove Theorem 1.4 stated in the Introduction. Using the terminology we introduced above, Theorem 1.4 can be rephrased as follows.

Theorem 9.1. *Suppose $\frac{n}{2} \leq m \leq n-1$, where m and n are positive integers. Let $a_m, \dots, a_n$ be algebraically independent variables over k, $F = k(a_m, \dots, a_n)$ and $E = F[x]/(f(x))$, where*

$$f(x) = x^n + a_m x^{n-m} + \dots + a_{n-1} x + a_n .$$

Then $\tau(E/F) = n - m$.

Note that $f(x)$ is an irreducible polynomial over F so that E is, in fact, a field. Indeed, by Gauss' Lemma (see [L, V.6]) it is enough to check irreducibility over the ring $k[a_m, \dots, a_n]$; now we can set $a_m = \dots = a_{n-1} = 0$ and apply the Eisenstein criterion (see [L, V.7]). Alternatively, the irreducibility of $f(x)$ follows from Lemma 9.4 below.

The variety $X_{m,n}$. Before we can proceed with the proof of Theorem 9.1, we need to establish several elementary properties of the variety $X_{m,n} \subset \mathbb{A}^n$ given by

$$X_{m,n} = \{x = (x_1, \dots, x_n) \mid s_1(x) = s_2(x) = \dots = s_{m-1}(x) = 0\} , \tag{9.1}$$

where $s_i(x)$ is the ith elementary symmetric polynomial in $x_1, \dots, x_n$. Note that $X_{m,n}$ can also be described as

$$X_{m,n} = \{x = (x_1, \dots, x_n) \mid p_1(x) = p_2(x) = \dots = p_{m-1}(x) = 0\} , \tag{9.2}$$

where $p_i(x) = x_1^i + \dots + x_n^i = 0$; the equivalence of the two definitions follows from Newton's formulas. (Recall that $\mathrm{char}(k) = 0$ throughout this paper.) Note that (9.2) defines $X_{m,n}$ for every positive integer m (of course, $X_{m,n} = \{0\}$ if $m > n$) and that the symmetric group S_n acts on $X_{m,n}$ by permuting the coordinates $x_1, \dots, x_n$.

To simplify the exposition, we shall assume that the base field k over which $X_{m,n}$ is defined, is algebraically closed; we note that Lemmas 9.3 and 9.4 are true without this assumption.

Lemma 9.2. *Suppose $x = (x_1, \dots, x_n) \in X_{m,n}$. Then either $x = 0$ or at least m of its coordinates $x_1, \dots, x_n$ are distinct.*

Proof. It is enough to prove the lemma under the assumption that $x_i \neq 0$ for every $i = 1, \dots, n$. Indeed if, say, $x_1 = \dots = x_r = 0$ and $x_{r+1}, \dots, x_n \neq 0$ then we can replace n by $n-r$ and x by $y = (x_{r+1}, \dots, x_n) \in X_{i,n-r}$.

After permuting the coordinates of x, we may assume $x_1, \dots, x_r$ are distinct and $x_1, \dots, x_n \in \{x_1, \dots, x_r\}$. Suppose n_1 of the coordinates $x_1, \dots, x_n$ are equal to x_1, n_2 of them are equal to x_2, ..., and n_r of them are equal to x_r. By definition of $X_{m,n}$ we have $p_1(x) = \dots = p_{m-1}(x) = 0$ or, equivalently,

$$\sum_{i=1}^{r} n_i x_i^j = 0 \quad \text{for every} \quad j = 1, ..., m-1 .$$

This means that the columns of the Vandermonde matrix

$$\begin{pmatrix} x_1 & x_2 & \dots & x_r \\ x_1^2 & x_2^2 & \dots & x_r^2 \\ \dots & \dots & \dots & \dots \\ x_1^{m-1} & x_2^{m-1} & \dots & x_r^{m-1} \end{pmatrix}$$

are linearly dependent. Since we are assuming $x_1, \dots, x_r$ are distinct non-zero elements of k, this is only possible if $r \geq m$, as claimed. $\square$

Lemma 9.3. *Every non-zero point of $X_{m,n}$ is smooth.*

Proof. We apply the Jacobian criterion to the system of polynomial equations $p_1(x) = \cdots = p_{m-1}(x) = 0$ defining $X_{m,n}$. The Jacobian matrix of this system is given by

$$J(x_1, \dots, x_n) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 2x_1 & 2x_2 & \dots & 2x_n \\ 3x_1^2 & 3x_2^2 & \dots & 3x_n^2 \\ \dots & \dots & \dots & \dots \\ (m-1)x_1^{m-2} & (m-1)x_2^{m-2} & \dots & (m-1)x_n^{m-2} \end{pmatrix} .$$

It is easy to see that this $(m-1) \times n$-matrix has rank $m-1$ whenever $m-1$ or more of the coordinates $x_1, \dots, x_n$ are distinct. By Lemma 9.2 this means that $J(x)$ has rank $m-1$ for every $0 \neq x \in X_{m,n}$. Thus every $0 \neq x \in X_{m,n}$ is smooth. $\square$

Lemma 9.4. *If $1 \leq m \leq n-1$ then $X_{m,n}$ is an irreducible variety of dimension $n-m+1$.*

Proof. Consider the morphism $\pi\colon X_{m,n} \longrightarrow \mathbb{A}^{n-m+1}$ given by

$$\pi(x) = (s_m(x), \dots, s_n(x)) \tag{9.3}$$

where s_j is the jth elementary symmetric polynomial, as before. Then π is surjective, and the fibers of π are precisely the S_n-orbits in $X_{m,n}$. This shows that $\dim(X_{m,n}) = n-m+1$. On the other hand, since $X_{m,n}$ is cut out by $m-1$ homogeneous polynomials in $\mathbb{A}^n$, every irreducible component of it has dimension $\geq n-m+1$; cf., e.g., [Ha, Proposition I.7.1]. We conclude that every component of $X_{m,n}$ has dimension exactly $n-m+1$ and the restriction of π to any component of $X_{m,n}$ is dominant. Since S_n acts transitively on the fibers of π, its action on the set of the irreducible components of $X_{m,n}$ is also transitive.

Let X_1 be an irreducible component of $X_{m,n}$ and let H be the subgroup of S_n preserving X_1. Since S_n transitively permutes the components of $X_{m,n}$, it is enough to show that $H = \mathrm{S}_n$. We will do this by proving that H contains every transposition (i,j) for $1 \leq i < j \neq n$.

We claim that $\mathrm{Stab}(x) \subset H$ for every $0 \neq x \in X_1$. Indeed, assume to the contrary that $g \in \mathrm{Stab}(x)$ but $g(X_1) \neq X_1$. Then $g(X_1)$ and X_1 are distinct irreducible components of $X_{m,n}$ passing through x. Hence, x is a singular point of $X_{m,n}$, contradicting Lemma 9.3. This proves the claim.

It is now sufficient to show that for every transposition $g = (i,j)$ there exists a point $0 \neq x \in X_1$ such that $g(x) = x$. In other words, we want to show that there is a non-zero point $x = (x_1, \dots, x_n) \in X_1$ with $x_i = x_j$.

To prove the last assertion, we pass to the projective space $\mathbb{P}^{n-1}$. Let $\mathbb{P}(X_{m,n})$ be the projectivization of $X_{m,n}$, i.e., the subvariety of $\mathbb{P}^{n-1}$ given by (9.1). Then the irreducible components of $X_{m,n}$ are affine cones over the irreducible components of $\mathbb{P}(X_{m,n})$; in particular, X_1 is an affine cone over $\mathbb{P}(X_1)$, where $\dim(\mathbb{P}(X_1)) = \dim(X_1) - 1 = n - m$. Thus our assumption that $m \leq n-1$ translates into $\dim(\mathbb{P}(X_1)) \geq 1$. This implies that $\mathbb{P}(X_1)$ has a non-trivial intersection with any hyperplane. In particular, $\mathbb{P}(X_1) \cap \{x_i = x_j\} \neq \emptyset$ and, hence, X_1 contains a non-zero point preserved by (i,j). This completes the proof of Lemma 9.4. $\square$

Remark 9.5. The condition $m \leq n-1$ in Lemma 9.4 is essential. Indeed, the variety $X_{n,n}$ is a union of $(n-1)!$ lines given (in parametric form) by $(\zeta_1 t, \zeta_2 t, \dots, \zeta_n t)$, where $\zeta_1, \dots, \zeta_n$ are distinct n-th roots of unity. In other words, $\mathbb{P}(X_{m,n})$ is a union of the $(n-1)!$ projective points of the form $(\zeta_1 : \cdots : \zeta_n)$; note that none of these points lies on the hyperplane $x_i = x_j$ for any choice of $1 \leq i < j \leq n$.

Proof of Theorem 9.1. To prove the inequality $\tau(E/F) \leq n - m$, let $z = \dfrac{a_{n-1}}{a_n} x$. (Note that here we are using the assumption $m \leq n-1$.) Substituting $x = \dfrac{a_n}{a_{n-1}} z$ into the equation $f(x) = 0$, we see that the minimal polynomial of z over F is of the form

$$f_z(t) = t^n + b_m t^m + \cdots + b_{n-1} t + b_n \ ,$$

where $b_n = b_{n-1} = \dfrac{a_{n-1}^n}{a_n^{n-1}}$. Thus

$$\tau(E/F) \leq \mathrm{trdeg}_k\, k(b_m, \dots, b_{n-1}, b_n) = \mathrm{trdeg}_k\, k(b_m, \dots, b_{n-1}) \leq n - m \ ,$$

as claimed.

It therefore remains to show that $\tau(E/F) \geq n - m$. Since

$$\tau(E \otimes_k \overline{k} / F \otimes_k \overline{k}) \geq \tau(E/F) \, ,$$

we may assume without loss of generality that $k = \overline{k}$ is algebraically closed; cf. Remark 6.2. Let $X_{m,n}$ be the S_n-variety defined by (9.1) and let $E^{\#}$ be the normal closure of E over F. Note that by [BR$_1$, Lemma 2.3] $\tau(E/F) = \tau(E^{\#}/F)$. Our strategy will thus be as follows: first we will show that

$$\tau(E^{\#}/F) = \mathrm{ed}(X_{m,n}) \ , \tag{9.4}$$

then

$$\mathrm{ed}(X_{m,n}) \geq n - m \ . \tag{9.5}$$

We now proceed to prove (9.4). By [BR$_1$, Lemma 2.7] it is enough to show that the field extensions $E^{\#}/F$ and $k(X_{m,n})/k(X_{m,n})^{\mathrm{S}_n}$ are isomorphic.

We claim that $k(X_{m,n})^{S_n} = k(s_m, \dots, s_n)$, where s_i is the ith symmetric polynomial of $x_1, \dots, x_n$, viewed as a regular function on $X_{m,n}$. Indeed, it is clear that $k(s_1, \dots, s_n) \subset k(X_{m,n})^{S_n}$. To prove equality, observe that the polynomial $f(x) = x^n + a_m x^{n-m} + \dots + a_{n-1}x + a_n$ has n distinct roots for a generic choice of $(a_m, a_{m+1}, \dots, a_n) \in \mathbb{A}^{n-m+1}$ (because $x^n - 1$ has n distinct roots). This means that the map

$$\pi \colon X_{m,n} \longrightarrow \mathbb{A}^{n-m+1}$$

given by (9.3), is generically $n! : 1$ and consequently, $[k(X_{m,n}) : k(s_m, \dots, s_n)] = n!$. Thus

$$[k(X_{m,n})^{S_n} : k(s_m, \dots, s_n)] = \frac{[k(X_{m,n}) : k(s_m, \dots, s_n)]}{[k(X_{m,n}) : k(X_{m,n})^{S_n}]} = \frac{n!}{n!} = 1 \ ,$$

as claimed.

Continuing with the proof of (9.4), note that the $s_m, \dots, s_n$ are algebraically independent over k. (This follows, e.g., from the fact that the map π defined in (9.3), is dominant.) Thus the fields $k(s_m, \dots, s_n)$ and $F = k(a_m, \dots, a_n)$ are isomorphic via a map that takes s_i to a_i for every i. Now observe that $k(X_{m,n})$ is the splitting field of the polynomial $g(x) = x^n + s_m x^{n-m} + \ldots + s_{n-1}x + s_n$ over $k(X_{m,n})^{\mathrm{S}_n} = k(s_m, \dots, s_n)$ and $E^{\#}$ is by definition the splitting field of $f(x)$ over $F = k(a_m, \dots, a_n)$. By the uniqueness of the splitting field, we see that the field extensions $k(X_{m,n})/k(X_{m,n})^{\mathrm{S}_n}$ and $E^{\#}/F$ are isomorphic, as claimed. This completes the proof of (9.4).

It remains to prove the inequality (9.5). In view of Theorem 7.2(2) it is sufficient to show that there exists a smooth point $x \in X_{m,n}$ such that $\mathrm{Stab}(x)$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{n-m}$. We shall thus look for a point of the form

$$x = (\alpha_1, \alpha_1, \alpha_2, \alpha_2, \dots, \alpha_{n-m}, \alpha_{n-m}, \alpha_{n-m+1}, \alpha_{n-m+2}, \dots, \alpha_{m-1}, \alpha_m) \ , \tag{9.6}$$

where at least one α_i is non-zero. (Here we are using the assumption that $m \geq n/2$ and thus $2(n-m) \leq n$.) By Lemma 9.3 any non-zero point x

of $X_{m,n}$ is smooth; moreover, if x is as in (9.6) then $\mathrm{Stab}(x)$ contains the subgroup

$$<(1,2)\,,\ (3,4)\,,\ \dots\,,\ (2n-2m-1,2n-2m)> \simeq (\mathbb{Z}/2\mathbb{Z})^{n-m}\,.$$

Thus we only need to show that a non-zero point of the form (9.6) exists on $X_{m,n}$. Substituting x into the defining equations $p_1(x) = \ldots = p_{m-1}(x) = 0$ of $X_{m,n}$ (see (9.2)), we obtain a system of $m-1$ homogeneous equations in $\alpha_1, \dots, \alpha_m$. Since the number of variables is greater than the number of equations, this system has a non-trivial solution, which gives us the desired point. This completes the proof of the inequality (9.5) and, hence, of Theorem 9.1. □

Remark 9.6. The same argument (with part (3) of Theorem 7.2 used in place of part (2)) shows that $\tau(E;2) = n-m$ in the sense of Definition 8.3 (here, as before, E is viewed as an n-dimensional F-algebra). In particular, the polynomial $f(x)$ of Theorem 9.1 cannot be reduced to a form with $\leq n-m$ algebraically independent coefficients by a Tschirnhaus transformation, even if we allow auxiliary radicals of odd degree; cf. [BR$_2$, Theorem 7.1].

References

[A] J. F. Adams, *2-tori in E_8*, Math. Ann., 287 (1987), 29–39.

[BM$_1$] E. Bierstone, P. D. Milman, *A simple constructive proof of canonical resolution of singularities*, Effective methods in algebraic geometry, Progress in Mathematics, **94**, Birkhäuser, Boston 1991.

[BM$_2$] E. Bierstone, P. D. Milman, *Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant*, Invent. math. **128** (1997), no. 2, 207–302.

[Bo] A. Borel, *Sous groupes commutatifs et torsion des groupes de Lie compacts connexes*, Tôhoku Math. J. (2) **13** (1961), 216–240.

[BS] A. Borel, J.-P. Serre, *Sur certains sous groupes des groupes de Lie compacts*, Comment. Math. Helv. **27** (1953), 128–139.

[BR$_1$] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179.

[BR$_2$] J. Buhler, Z. Reichstein, *On Tschirnhaus transformations*, in "Number Theory", Proceedings of a conference held at Penn. State University, edited by S. Ahlgren, G. Andrews and K. Ono, Kluwer Acad. Publishers, 127–142. Preprint available at http://ucs.orst.edu/~reichstz/pub.html.

[CS] A. M. Cohen, G. M. Seitz, *The r-rank of the groups of exceptional Lie type*, Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen, Series A, vol. 90, no. 3 (1997), 251–259.

[Ga] R. S. Garibaldi, *Structurable algebras and groups of type E_6 and E_7*, preprint.

[Gri] R. L. Griess, Jr., *Elementary abelian p-subgroups of algebraic groups*, Geom. Dedicata **39** (1991), 253–305.

[Gro] A. Grothendieck, *La torsion homologique et les sections rationnelles*, Exposé 5, Séminaire C. Chevalley, Anneaux de Chow et applications, 2nd année, IHP, 1958.

[EGA I] A. Grothendieck. Éléments de géométrie algébrique, I. Le langage des schémas. Publications mathématiques de l'Institut des Hautes Études Scientifiques, **4**, 1960.

[Ha] R. Hartshorne. Algebraic geometry. Springer, 1977.

[Hi] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero: I, II*, Annals of Math. **79** (1964), 109–326.

[Hu] J. E. Humphreys. Linear Algebraic Groups. Springer-Verlag, 1975.

[J_1] N. Jacobson, The Theory of Rings, Math, Surveys, no. 2, Amer. Math. Soc., Provedence, RI, 1943.

[J_2] N. Jacobson, Structure and Representations of Jordan Algebras, Amer. Math. Soc., Provedence, RI, 1968.

[KMRT] M.-A.Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, AMS Colloquium Publications, vol. 44, 1998.

[Ko] V. E. Kordonsky, *On essential dimension and Serre's Conjecture II for exceptional groups*, preprint (in Russian).

[L] S. Lang, Algebra, Addison—Wesley, 1965.

[OV] A. L. Onishchik, E. B. Vinberg. Lie Groups and Algebraic Groups. Springer-Verlag, 1990.

[P] A. Parusiński, *Lipschitz properties of semianalytic sets*, Ann. Inst. Fourier, Grenoble 38 (1988), 189–213.

[Po] V. L. Popov, *Sections in Invariant Theory*, Proceedings of the Sophus Lie Memorial Conference, Scandinavian University Press, 1994, 315–362.

[PV] V. L. Popov, E. B. Vinberg, *Invariant Theory*, in Encyclopaedia of Math. Sciences **55**, Algebraic Geometry IV, edited by A. N. Parshin and I. R. Shafarevich, Springer-Verlag, 1994.

[Re_1] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canadian J. Math., **51** (1) (1999), 69–95.

[Re_2] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformation groups, **5**, no. 3 (2000), to appear.
Preprint available at http://ucs.orst.edu/~reichstz/pub.html .

[RY_1] Z. Reichstein, B. Youssin, *Splitting fields of G-varieties*, Pacific J. Math., to appear.
Preprint available at http://ucs.orst.edu/~reichstz/pub.html .

[RY_2] Z. Reichstein, B. Youssin, *Parusiński's lemma via algebraic geometry*, Electronic Research Announcements of the AMS, **5** (1999), 136–145, http://www.ams.org/era/home-1999.html.

[RY_3] Z. Reichstein, B. Youssin, *Equivariant resolution of points of indeterminacy*, preprint, available at http://ucs.orst.edu/~reichstz/pub.html .

[Ro_1] M. Rosenlicht, *Some basic theorems on algebraic groups*, American Journal of Math., **78** (1956), 401–443.

[Ro_2] M. Rosenlicht, *A remark on quotient spaces*, Anais da Academia Brasileira de Ciências **35** (1963), 487–489.

[$Rost_1$] M. Rost, *Notes on 16-dimensional trace forms*, preprint, November 1998, http://www.physik.uni-regensburg.de/~rom03516.

[$Rost_2$] M. Rost, *On Galois cohomology of Spin(14)*, preprint, March 1999, http://www.physik.uni-regensburg.de/~rom03516.

[RST] M. Rost, J.-P. Serre, J.-P. Tignol, *The trace form of a central siple algebra of degree four*, in preparation.

[Row] L. H. Rowen, Polynomial Identities in Ring Theory. Academic Press, 1980.

[Se_1] J.-P. Serre, *Espaces fibrés algébriques*, Exposé 1, Séminaire C. Chevalley, Anneaux de Chow et applications, 2nd année, IHP, 1958.

[Se_2] J.-P. Serre, *Cohomologie galoisienne: progrès et problèmes*, in "Séminaire Bourbaki, Volume 1993/94, Exposés 775–789", Astérisque **227** (1995), 229–257.

[Se_3] J.-P. Serre, *Galois Cohomology*, Springer, 1997.

[Se_4] J.-P. Serre, letter from October 1, 1998.

[Se_5] J.-P. Serre, letter from November 16, 1998.

[St] R. Steinberg, *Generators, relations, and coverings of algebraic groups, II*, J. Algebra **71** (1981), 527–543.
[Su] H. Sumihiro, *Equivariant completion*, J. Math. Kyoto Univ. **14**-1 (1974), 1–28.
[V_1] O. E. Villamayor U., *Constructiveness of Hironaka's resolution,* Ann. scient. Éc. Norm. Sup., 4e série, **22** (1989), 1–32.
[V_2] O. E. Villamayor U., *Patching local uniformizations,* Ann. scient. Éc. Norm. Sup., 4e série, **25** (1992), 629–677.
[Wo] J. A. Wood, *Spinor groups and algebraic coding theory*, J. Combin. Theory, Series A **51** (1989), 277–313.

Department of Mathematics, Oregon State University, Corvallis, OR 97331-4506, USA
email: zinovy@math.orst.edu

Department of Mathematics, University of the Negev, Be'er Sheva', Israel
Current address: Hashofar 26/3, Ma'ale Adumim, Israel.
email: youssin@math.bgu.ac.il

A. Appendix

Fixed Points of Group Actions and Rational Maps

by

János Kollár

(Department of Mathematics, Princeton University, Princeton, NJ 08544-1000, USA, kollar@math.utah.edu)

and

Endre Szabó

(Mathematical Institut, Budapest, PO.Box 127, 1364 Hungary, endre@math-inst.hu)

The aim of this note is to give simple proofs of the results in Section 5 about the behaviour of fixed points of finite group actions under rational maps. Our proofs work in any characteristic.

Lemma A.1. *Let K be an algebraically closed field and H a (not necessarily connected) linear algebraic group over K. The following are equivalent.*

1. *Every representation $H \longrightarrow GL(n, K)$ has an H-eigenvector.*
2. *There is a (not necessarily connected) unipotent, normal subgroup $U < H$ such that H/U is abelian.*

Proof. Let $H \longrightarrow GL(n, K)$ be a faithful representation. If (1) holds then H is conjugate to an upper triangular subgroup, this implies (2).

Conversely, any representation of a unipotent group has fixed vectors (cf. [Borel91, I.4.8]) and the subspace of all fixed vectors is an H/U-representation. □

Proposition A.2 (Going down). *Let K be an algebraically closed field, H a linear algebraic group over K and $f : X \dashrightarrow Y$ an H-equivariant rational map of K-schemes. Assume that*

1. *H satisfies the equivalent conditions of Lemma A.1,*
2. *H has a smooth fixed point on X, and*
3. *Y is proper.*

Then H has a fixed point on Y.

Proof. The proof is by induction on $\dim X$. The case $\dim X = 0$ is clear.

Let $x \in X$ be a smooth H-fixed point and consider the blow up $B_x X$ with exceptional divisor $E \cong \mathbb{P}^{n-1}$. The H-action lifts to $B_x X$ and so we get an H-action on E which has a fixed point by (1). Since Y is proper, the induced rational map $B_x X \longrightarrow X \dashrightarrow Y$ is defined outside a subset of codimension at least 2. Thus we get an H-equivariant rational map $E \dashrightarrow Y$. By induction, there is a fixed point on Y. □

Remark A.3. If H does not satisfy the conditions of Lemma A.1 then Proposition A.2 fails for some actions. Indeed, let $H \longrightarrow GL(n, K)$ be a representation without an H-eigenvector. This gives an H-action on $\mathbb{P}^n$ with a single fixed point $Q \in \mathbb{P}^n$. The corresponding action on $B_Q\mathbb{P}^n$ has no fixed points.

Proposition A.4 (Going up). *Let K be an algebraically closed field and H a finite abelian group of prime power order q^n (q is allowed to coincide with $\operatorname{char} K$). Let $p : X \dashrightarrow Z$ be an H-equivariant rational map of irreducible K-schemes. Assume that*

1. *p is generically finite, dominant and $q \nmid \deg(X/Z)$,*
2. *H has a smooth fixed point on Z, and*
3. *X is proper.*

Then H has a fixed point on X. Moreover, if $X \dashrightarrow Y$ is an H-equivariant rational map to a proper K-scheme then H has a fixed point on Y.

Proof. The proof is by induction on $\dim Z$. The case $\dim Z = 0$ is clear.

Let $z \in Z$ be a smooth fixed point and $E \subset B_z Z$ the exceptional divisor. Let $\bar{p} : \bar{X} \longrightarrow B_z Z$ denote the normalization of $B_z Z$ in the field of rational functions of X and $F_i \subset \bar{X}$ the divisors lying over E. H acts on the set $\{F_i\}$. Let $\mathcal{F}_j$ denote the H-orbits and in each pick a divisor $F_j^* \in \mathcal{F}_j$. By the ramification formula (see [Lang65, Corollary XII.6.2])

$$\deg(X/Z) = \sum_j |\mathcal{F}_j| \cdot \deg(F_j^*/E) \cdot e(\bar{p}, F_j^*)$$

where $e(\bar{p}, F_j^*)$ denotes the ramification index of $\bar{p}$ at the generic point of F_j^*. Since $\deg(X/Z)$ is not divisible by q, there is an orbit $\mathcal{F}_0$ consisting of a single element F_0^* such that $\deg(F_0^*/E)$ is not divisible by q.

We have H-equivariant rational maps $F_0^* \dashrightarrow E$, $F_0^* \dashrightarrow X$ and $F_0^* \dashrightarrow Y$. By induction H has a fixed point on F_0^*, X and Y. □

Remark A.5. We see from the proof that Proposition A.4 also holds if H is abelian and only one of the prime divisors of $|H|$ is less than $\deg(X/Z)$.

The method also gives a simpler proof of a result of [Nishimura55]. One can view this as a version of Proposition A.2 where H is the absolute Galois group of K.

Proposition A.6 (Nishimura lemma). *Let K be a field and $f : X \dashrightarrow Y$ a rational map of K-schemes. Assume that*

1. *X has a smooth K-point, and*
2. *Y is proper.*

Then Y has a K-point.

Proof. The proof is by induction on $\dim X$. The case $\dim X = 0$ is clear.

Let $x \in X$ be a smooth K-point and consider the blow up $B_x X$ with exceptional divisor $E \cong \mathbb{P}^{n-1}$. The divisor E has smooth K-points. Since Y is proper, the induced rational map $B_x X \longrightarrow X \dashrightarrow Y$ is defined outside a subset of codimension at least 2 and we get a rational map $E \dashrightarrow Y$. By induction, there is a K-point on Y. $\square$

Remark A.7. One can combine Propositions A.2 and A.6 if we know that any H-representation has an eigenvector defined over K. There are two interesting cases where this condition holds:

1. H is Abelian of order n and K contains all nth roots of unity.
2. H is nilpotent and its order is a power of $\operatorname{char} K$.

References

[Borel91] A. Borel, Linear algebraic groups, second ed. Springer, 1991

[Lang65] S. Lang, Algebra, Addison—Wesley, 1965.

[Nishimura55] H. Nishimura, Some remarks on rational points, Mem. Coll. Sci. Univ. Kyoto 29 (1955) 189-192