Algebraic Geometry 8 (6) (2021) 749–769
doi:10.14231/AG-2021–23

Essential dimension of extensions of finite groups by tori

Zinovy Reichstein and Federico Scavia

Abstract

Let p be a prime, k be a p-closed field of characteristic different from p, and $1 \to T \to G \to F \to 1$ be an exact sequence of algebraic groups over k, where T is a torus and F is a finite p-group. In this paper, we study the essential dimension $\mathrm{ed}(G;p)$ of G at p. R. Lötscher, M. MacDonald, A. Meyer, and the first author showed that

$$\min \dim(V) - \dim(G) \leqslant \mathrm{ed}(G;p) \leqslant \min \dim(W) - \dim(G)\,,$$

where V and W range over the p-faithful and p-generically free k-representations of G, respectively. In the special case where $G = F$, one recovers the formula for $\mathrm{ed}(F;p)$ proved earlier by N. Karpenko and A. Merkurjev. In the case where $F = T$, one recovers the formula for $\mathrm{ed}(T;p)$ proved earlier by R. Lötscher et al. In both of these cases, the upper and lower bounds on $\mathrm{ed}(G;p)$ given above coincide. In general, there is a gap between them. Lötscher et al. conjectured that the upper bound is, in fact, sharp; that is, $\mathrm{ed}(G;p) = \min \dim(W) - \dim(G)$, where W ranges over the p-generically free representations. We prove this conjecture in the case where F is diagonalizable.

1. Introduction

Let p be a prime integer and k be a p-closed field of characteristic different from p. That is, the degree of every finite extension l/k is a power of p. Consider an algebraic group G defined over k which fits into the exact sequence

$$1 \longrightarrow T \longrightarrow G \xrightarrow{\ \pi\ } F \longrightarrow 1\,, \tag{1.1}$$

where T is a (not necessarily split) torus and F is a (not necessarily constant) finite p-group defined over k. We say that a linear representation $G \to \mathrm{GL}(V)$ is p-faithful if its kernel is a finite subgroup of G of order prime to p and p-generically free if the isotropy subgroup G_v is a finite group of order prime to p for $v \in V(\overline{k})$ in general position. We denote by $\eta(G)$ (respectively, $\rho(G)$) the smallest dimension of a p-faithful (respectively, p-generically free) representation of G defined over k. R. Lötscher, M. MacDonald, A. Meyer, and the first author [LMMR13b, Theorem 1.1]

Received 30 March 2020, accepted in final form 12 April 2021.
2020 Mathematics Subject Classification 20G15, 14L30, 14E05.
Keywords: essential dimension, algebraic torus, stabilizer in general position.

Zinovy Reichstein was partially supported by National Sciences and Engineering Research Council of Canada Discovery grant 253424-2017. Federico Scavia was partially supported by a graduate fellowship from the University of British Columbia.

have shown that the essential p-dimension $\operatorname{ed}(G;p)$ of G over k satisfies the inequalities

$$\eta(G) - \dim(G) \leqslant \operatorname{ed}(G;p) \leqslant \rho(G) - \dim(G)\,. \tag{1.2}$$

For the definition of $\operatorname{ed}(G;p)$, see Section 4.

The inequalities (1.2) represent a common generalization of the formulas for the essential p-dimension of a finite constant p-group, due to N. Karpenko and A. Merkurjev [KM08, Theorem 4.1] (where $T = \{1\}$), and of an algebraic torus, due to R. Lötscher et al. [LMMR13a] (where $F = \{1\}$). In both of these cases, every p-faithful representation of G is p-generically free, and thus $\eta(G) = \rho(G)$. In general, $\eta(G)$ can be strictly smaller than $\rho(G)$. Lötscher et al. conjectured that the upper bound of (1.2) is, in fact, sharp.

Conjecture 1.1. Let p be a prime integer, k be a p-closed field of characteristic different from p, and G be an affine algebraic group defined over k. Assume that the connected component $G^0 = T$ is a k-torus and the component group $G/G^0 = F$ is a finite p-group. Then

$$\operatorname{ed}(G;p) = \rho(G) - \dim G\,,$$

where $\rho(G)$ is the minimal dimension of a p-generically free k-representation of G.

Informally speaking, the lower bound of (1.2) is the strongest lower bound on $\operatorname{ed}(G;p)$ one can hope to prove by the methods of [KM08, LMMR13a] and [LMMR13b]. In the case where the upper and lower bounds of (1.2) diverge, Conjecture 1.1 calls for a new approach.

Conjecture 1.1 appeared in print in [Rei10, Section 7.9] on the list of open problems in the theory of essential dimension. The only bit of progress since then has been a proof in the special case where G is a semi-direct product of a cyclic group $F = \mathbb{Z}/p\mathbb{Z}$ of order p and a split torus $T = \mathbb{G}_{\mathrm{m}}^n$, due to M. Huruguen (unpublished). Huruguen's argument relies on the classification of integral representations of $\mathbb{Z}/p\mathbb{Z}$ due to F. Diederichsen and I. Reiner [CR62, Theorem 74.3]. So far, this approach has resisted all attempts to generalize it beyond the case where $G \simeq \mathbb{G}_{\mathrm{m}}^n \rtimes (\mathbb{Z}/p\mathbb{Z})$.

Note that $\eta(G)$ is often accessible by cohomological and/or combinatorial techniques; see Section 6 and Lemma 9.3, as well as the remarks after this lemma. Computing $\rho(G)$ is usually a more challenging problem. The purpose of this paper is to establish Conjecture 1.1 in the case where F is a diagonalizable abelian p-group. Moreover, our main result also gives a way of computing $\rho(G)$ in this case.

Theorem 1.2. *Let p be a prime integer, k be a p-closed field of characteristic different from p, and G be an extension of a (not necessarily constant) diagonalizable p-group F by a (not necessarily split) torus T, as in (1.1).*

(a) *We have $\operatorname{ed}(G;p) = \rho(G) - \dim G$.*
(b) *Moreover, suppose that V is a p-faithful representation of G of minimal dimension, $\overline{k}$ is the algebraic closure of k, and $S_V \subset G_{\overline{k}}$ is a stabilizer in general position for the $G_{\overline{k}}$-action on $V_{\overline{k}}$. Then $\rho(G) = \eta(G) + \operatorname{rank}_p(S_V)$.*

Here $\operatorname{rank}_p(S_V)$ is the largest r such that S_V contains a subgroup isomorphic to μ_p^r. Note that S_V exists by Lemma 2.1. Most of the remainder of this paper (Sections 2–8) will be devoted to proving Theorem 1.2. A key ingredient in the proof is the resolution theorem (Theorem 7.2), which is based, in turn, on an old valuation-theoretic result of M. Artin and O. Zariski [Art86, Theorem 5.2]. In Section 9, we will use Theorem 1.2 to complete the computation of $\operatorname{ed}(N;p)$ initiated in [MR09] and [Mac11]. Here N is the normalizer of a split maximal torus in a split simple algebraic group.

2. Stabilizers in general position

In this section, we assume that the base field k is algebraically closed. Let G be a linear algebraic group defined over k. A G-variety X is called primitive if G transitively permutes the irreducible components of X.

Let X be a primitive G-variety. A subgroup $S \subset G$ is called a stabilizer in general position for the G-action on X if there exists an open G-invariant subset $U \subset X$ such that $\mathrm{Stab}_G(x)$ is conjugate to S for every $x \in U(k)$. Note that a stabilizer in general position does not always exist. See [PV94, Example 7.1.1] for an easy example where G is unipotent; further examples, with $G = \mathrm{SL}_n$, can be found in [Ric72, Section 12.4]. When a stabilizer in general position $S \subset G$ exists, it is unique up to conjugacy.

Lemma 2.1. *Let G be a linear algebraic group over k and X be a primitive quasi-projective G-variety. Assume that the connected component $T = G^0$ is a torus and the component group $F = G/G^0$ is finite of order prime to* $\mathrm{char}(k)$. *Then there exists a stabilizer in general position $S \subset G$.*

Proof. After replacing G with $\overline{G} := G/(K \cap T)$, where K is the kernel of the G-action on X, we may assume that the T-action on X is faithful and, hence, generically free. In other words, for $x \in X(k)$ in general position, $\mathrm{Stab}_G(x) \cap T = 1$; in particular, $\mathrm{Stab}_G(x)$ is a finite p-group. Since $\mathrm{char}(k) \neq p$, Maschke's theorem tells us that $\mathrm{Stab}_G(x)$ is linearly reductive. Hence, for $x \in X(k)$ in general position, $\mathrm{Stab}_G(x)$ is G-completely reducible; see [Jan04, Lemma 11.24]. The lemma now follows from [Mar15, Corollary 1.5]. □

Remark 2.2. The condition that X is quasi-projective can be dropped if $k = \mathbb{C}$; see [Ric72, Theorem 9.3.1]. With a bit more effort, this condition can also be removed for any algebraically closed base field k of characteristic different from p. Since we shall not need this more general variant of Lemma 2.1, we leave its proof as an exercise for the reader.

We define the (geometric) p-rank $\mathrm{rank}_p(G)$ of an algebraic group G to be the largest integer r such that G contains a subgroup isomorphic to $\mu_p^r = \mu_p \times \cdots \times \mu_p$ (r times).

Lemma 2.3. *Let X be a normal G-variety and $Y \subset X$ be a G-invariant prime divisor of X. Let S_X and S_Y be stabilizers in general position of the G-actions on X and Y, respectively. Assume that p is a prime and* $\mathrm{char}(k) \neq p$.

(a) *We have* $\mathrm{rank}_p(S_Y) \leqslant \mathrm{rank}_p(S_X) + 1$.

(b) *Assume that the G-action on X is p-faithful. Denote the kernel of the G-action on Y by N. Then there is a group homomorphism $\alpha\colon N \to \mathbb{G}_{\mathrm{m}}$ such that* $\mathrm{Ker}(\alpha)$ *does not contain a subgroup of order p.*

Proof. Let $U \subset X$ be a G-invariant dense open subset of X such that $\mathrm{Stab}_G(x)$ is conjugate to S_X for every $x \in U(k)$. If $Y \cap U \neq \emptyset$, then $S_Y = S_X$, and we are done. Thus we may assume that Y is contained in $Z = X \setminus U$. Since Y is a prime divisor in X, it is an irreducible component of Z. After removing all other irreducible components of Z from X, we may assume that $Z = Y$. Since X is normal, Y intersects the smooth locus of X non-trivially. Choose a k-point $y \in Y$ such that both X and Y are smooth at y and $\mathrm{Stab}_G(y)$ is conjugate to S_Y. After replacing S_Y with a conjugate, we may assume that $\mathrm{Stab}_G(y) = S_Y$. The group $\mathrm{Stab}_G(y)$ acts on the tangent spaces $T_y(X)$ and $T_y(Y)$, hence on the 1-dimensional normal space $T_y(X)/T_y(Y)$. This gives rise to a character $\alpha\colon S_Y \to \mathbb{G}_{\mathrm{m}}$.

(a) Assume the contrary: S_Y contains μ_p^{r+2}, where $r = \mathrm{rank}_p(S_X)$. Then the kernel of α contains a subgroup $\mu \simeq \mu_p^{r+1}$. By Maschke's theorem, the natural projection $T_y(X) \to T_y(X)/T_y(Y)$ is μ-equivariantly split. Equivalently, there exists a μ-invariant tangent vector $v \in T_y(X)$ which does not belong to $T_y(Y)$. By the Luna slice theorem,

$$T_y(X)^{\mu} = T_y(X^{\mu})\,. \tag{2.1}$$

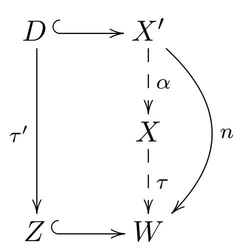
For a proof in characteristic 0, see [PV94, Section 6.5]. Generally speaking, Luna's theorem fails in prime characteristic, but (2.1) remains valid because μ is linearly reductive; see [BR85, Lemma 8.3]. Now observe that since μ does not fit into any conjugate of S_X, the subvariety X^{μ} is contained in $Y = X \setminus U$. Thus $v \in T_y(X)^{\mu} = T_y(X^{\mu}) \subset T_y(Y)$, which gives a contradiction.

(b) Let $y \in Y$ be a smooth k-point of X and Y, and $S_y = \mathrm{Stab}_G(y)$ as in part (a). Then N is contained in S_Y, and α restricts to a character $N \to \mathbb{G}_{\mathrm{m}}$. It suffices to show that the kernel of α in S_Y does not contain a subgroup of order p. Assume the contrary: a subgroup H of order p lies in the kernel of α. Then H fixes a smooth point y of X and acts trivially on both $T_y(Y)$ and $T_y(X)/T_y(Y)$ and hence (since H is linearly reductive) on $T_y(X)$. It is well known that this implies that H acts trivially on X; see, for example, the proof of [GR09, Lemma 4.1]. This contradicts our assumption that the G-action on X is p-faithful. □

3. Covers

Let k be an arbitrary field, and let G be a linear algebraic group defined over k. As usual, we will denote the algebraic closure of k by $\overline{k}$. A G-variety X is called primitive if the $G_{\overline{k}}$-variety $X_{\overline{k}}$ is primitive. A dominant G-equivariant rational map $X \dashrightarrow Y$ of primitive G-varieties is called a cover of degree d if $[k(X) : k(Y)] = d$. Here if $X_1, \ldots, X_n$ are the irreducible components of X, then $k(X)$ is defined as $k(X_1) \oplus \cdots \oplus k(X_n)$.

Lemma 3.1. *Let p be a prime integer, G be a smooth algebraic group such that G/G^0 is a finite p-group, W be an irreducible G-variety, $Z \subset W$ be an irreducible G-invariant divisor in W, and $\tau\colon X \dashrightarrow W$ be a G-equivariant cover of degree prime to p. Then there exists a commutative diagram of G-equivariant maps*



such that X' is normal, α is a birational isomorphism, D is an irreducible divisor in X', and τ' is a cover of Z of degree prime to p.

Proof. Let X' be the normalization of W in the function field $k(X)$. Since G acts compatibly on W and X, there is a G-action on X' such that the normalization map $n\colon X' \to W$ is G-equivariant. Over the dense open subset of W where τ is finite, n factors through X. Thus n factors into a composition of a birational isomorphism $\alpha\colon X' \dashrightarrow X$ and $\tau\colon X \dashrightarrow W$. This gives us the right column in the diagram.

To construct D, we argue as in the proof of [RY00, Proposition A.4]. Denote the irreducible components of the preimage of Z under n by $D_1, \ldots, D_r \subset X'$. These components are permuted by G. Denote the orbits of this permutation action by $\mathcal{O}_1, \ldots, \mathcal{O}_m$. After renumbering $D_1, \ldots, D_r$, we may assume that $D_i \in \mathcal{O}_i$ for $i = 1, \dots, m$. By the ramification formula (see, for example, [Lan02, XII, Corollary 6.3]),

$$d = \sum_{i=1}^{m} |\mathcal{O}_i| \cdot [D_i : Z] \cdot e_i \,,$$

where $[D_i : Z]$ denotes the degree of the cover $n_{|D_i} \colon D_i \to Z$ and e_i is the ramification index of n at the generic point of D_i. Since d is prime to p and each $|\mathcal{O}_i|$ is a power of p, we conclude that there exists an $i \in \{1, \dots, m\}$ such that $|\mathcal{O}_i| = 1$ (that is, D_i is G-invariant) and $[D_i : Z]$ is prime to p. We now set $D = D_i$ and $\tau' = n_{|D_i}$. □

Lemma 3.2. *Let G be a linear algebraic group over an algebraically closed field k, $p \neq \mathrm{char}(k)$ be a prime number, and $\tau \colon X \dashrightarrow W$ be a cover of G-varieties of degree d. Assume that stabilizers in general position for the G-actions on X and W exist; denote them by S_X and S_W, respectively. Assume that d is prime to p.*

(a) *If H is a finite p-subgroup of S_W, then S_X contains a conjugate of H.*

(b) *We have $\mathrm{rank}_p(S_X) = \mathrm{rank}_p(S_W)$.*

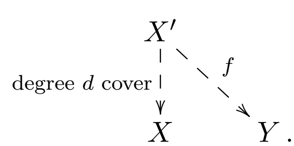
Proof. (a) After replacing W with a dense open subvariety, we may assume that the stabilizer of every point in W is a conjugate of S_W. Furthermore, after replacing X with the normal closure of W in $k(X)$, we may assume that τ is a finite morphism. We claim that $W^{S_W} \subset \tau(X^H)$. Indeed, suppose $w \in W^{S_W}$. Then H acts on $\tau^{-1}(w)$, which is a zero-cycle on X of degree d. Since H is a p-group, it fixes a k-point in $\tau^{-1}(w)$. Hence, $X^H \cap \tau^{-1}(w) \neq \emptyset$ or, equivalently, $w \in \tau\big(X^H\big)$. This proves the claim.

Since the stabilizer of every point of W is conjugate to S_W, we have $G \cdot W^{S_W} = W$. By the claim, $\tau\big(G \cdot X^H\big) = G \cdot \tau\big(X^H\big) = W$. Since G acts transitively on the irreducible components of X, this implies that $G \cdot X^H$ contains a dense open subset $X_0 \subset X$. In other words, the stabilizer of every point of X_0 contains a conjugate of H, and part (a) follows.

(b) Clearly $S_X \subset S_W$ and thus $\mathrm{rank}_p(S_X) \leqslant \mathrm{rank}_p(S_W)$. On the other hand, if S_W contains $H = \mu_p^r$ for some $r \geqslant 0$, then by part (a), the group S_X also contains a copy of μ_p^r. This proves the opposite inequality, $\mathrm{rank}_p(S_X) \geqslant \mathrm{rank}_p(S_W)$. □

4. Essential p-dimension

Let X and Y be G-varieties. Assume that X is primitive. By a G-equivariant correspondence $X \rightsquigarrow Y$ of degree d, we mean a diagram of rational maps



Here we require X' to be primitive. We say that this correspondence is dominant if f is dominant. A rational map may be viewed as a correspondence of degree 1.

The *essential dimension* $\mathrm{ed}(X)$ of a generically free G-variety X is the minimal value of $\dim(Y) - \dim(G)$, where the minimum is taken over all generically free G-varieties Y admitting a dominant rational map $X \dashrightarrow Y$. For a prime integer p, the essential dimension $\mathrm{ed}(X; p)$ of X at p is defined in a similar manner, as $\dim(Y) - \dim(G)$, where the minimum is taken over all generically free G-varieties X admitting a G-equivariant dominant correspondence $X \rightsquigarrow Y$ of degree prime to p. Note that these numbers depend on the base field k, which we assume to be fixed throughout.

It follows from [LMMR13b, Propositions 2.4 and 3.1] that this minimum does not change if we allow the G-action on Y to be p-generically free rather than generically free; we shall not need this fact. We will, however, need the following lemma.

Lemma 4.1. *Requiring Y to be projective in the above definitions does not change the values of* $\mathrm{ed}(X)$ *and* $\mathrm{ed}(X;p)$. *That is, for any primitive generically free G-variety X,*

(a) *there exists a G-equivariant dominant rational map $X \dashrightarrow Z$ where Z is projective, the G-action on Z is generically free, and* $\dim(Z) = \mathrm{ed}(X;G) + \dim(G)$*;*
(b) *there exists a G-equivariant dominant correspondence $X \rightsquigarrow Z'$ of degree prime to p where Z' is projective, the G-action on Z' is generically free, and* $\dim(Z') = \mathrm{ed}(X;p) + \dim(G)$.

Proof. Let Y be a generically free G-variety and V be a generically free linear representation of G. It is well known that the G-action on V is versal; see, for example, [Mer13, Proposition 3.10]. Consequently, there exist a G-invariant subvariety $Y_1 \subset V$ and a G-equivariant dominant rational map $Y \dashrightarrow Y_1$ such that the G-action on Y_1 is generically free. After replacing Y_1 with its Zariski closure Z in $\mathbb{P}(V \oplus k)$, where G acts trivially on k, we obtain a G-equivariant dominant rational map $\alpha\colon Y \dashrightarrow Z$ such that Z is projective and the G-action on Z is generically free.

To prove part (a), choose a dominant G-equivariant rational map $f\colon X \dashrightarrow Y$ such that the G-action on Y is generically free and $\dim(Y)$ is the smallest possible, that is, $\dim(Y) = \mathrm{ed}(X)+\dim(G)$. Now compose f with the map $\alpha\colon Y \dashrightarrow Z$ constructed above. By the minimality of $\dim(Y)$, we have $\dim(Z) = \dim(Y)$, and part (a) follows. The proof of part (b) is the same, except that the rational map f is replaced by a correspondence of degree prime to p. □

The essential dimension $\mathrm{ed}(G)$ (respectively, the essential dimension $\mathrm{ed}(G;p)$ at p) of the group G is the maximal value of $\mathrm{ed}(X)$ (respectively, of $\mathrm{ed}(X;p)$) taken over all generically free G-varieties X.

5. The groups G_n

Let G be an algebraic group over k such that the connected component $T = G^0$ is a torus and the component group $F = G/T$ is a finite p-group, as in (1.1). By [LMMR13b, Lemma 5.3], there exists a finite p-subgroup $F' \subset G$ such that $\pi|_{F'} : F' \to F$ is surjective. We will refer to F' as a "quasi-splitting subgroup" for G. We will denote the subgroup generated by F' and $T[n]$ by G_n. Here $T[n]$ denotes the n-torsion subgroup of T, that is, the kernel of the homomorphism $T \xrightarrow{\times\, n} T$. Note that our definition of G_n depends on the choice of the quasi-splitting subgroup F'. We will assume that F' is fixed throughout. We will be particularly interested in the subgroups

$$G_1 \subset G_p \subset G_{p^2} \subset G_{p^3} \subset \cdots . \tag{5.1}$$

Informally speaking, we will show that these groups approximate "p-primary behavior" of G in various ways; see Lemma 5.2 and Proposition 6.2(b) below.

From here on, we denote the center of G by $Z(G)$.

Lemma 5.1. (a) *Let $z \in Z(G)(\overline{k})$ be a central element of G of order p^n for some $n \geqslant 0$. Then $z \in G_{p^m}(\overline{k})$ for $m \gg 0$.*

(b) *For every $n \geqslant 0$, we have $Z(G)[p^n] = Z(G_{p^r})[p^n]$ as group schemes for all $r \gg 0$.*

Proof. (a) By the definition of F', there exist a $g \in F'(\overline{k})$ and a $t \in T(\overline{k})$ such that $g = zt$. Since F' is a p-group, $g^N = 1$, where N is a sufficiently high power of p. Taking $N \geqslant p^n$, we also have $z^N = 1$. Since z is central, $1 = g^N = (zt)^N = z^N t^N = t^N$. Thus $t \in T[N](\overline{k}) \subset G_N(\overline{k})$, and, consequently, $z = gt^{-1}$ is a $\overline{k}$-point of $F' \cdot T[N] = G_N$.

(b) Let $n \geqslant 0$ be fixed. Since both $Z(G)[p^n]$ and G_{p^r} are finite p-groups and we are assuming that $\mathrm{char}(k) \neq p$, part (a) tells us that there exists an $m \geqslant 0$ such that $Z(G)[p^n] \subset Z(G_{p^r})[p^n]$ as group schemes for all $r \geqslant m$.

Let $r \geqslant 0$, and let $x \in Z(G_{p^r})[p^n](\overline{k})$. Let $f_x \colon T_{\overline{k}} \to T_{\overline{k}}$ be the homomorphism of conjugation by x. Passing to character lattices, we obtain a homomorphism $\langle x \rangle \to \mathrm{GL}_d(\mathbb{Z})$, where $d = \operatorname{rank} X(T_{\overline{k}})$. By a theorem of Jordan, in $\mathrm{GL}_d(\mathbb{Z})$ there are at most finitely many finite subgroups up to conjugacy. In particular, we may find an integer $N \gg 0$ such that the restriction of $\mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/p^N\mathbb{Z})$ to every finite subgroup is injective.

Thus, if $r \geqslant N$, then f_x is the identity for every $x \in Z(G_{p^r})[p^n](\overline{k})$. Since F' is contained in G_{p^r}, every $x \in Z(G_{p^r})[p^n](\overline{k})$ commutes with F'. Since G^0 and F' generate G, we deduce that $x \in Z(G)[p^n](\overline{k})$. This shows that $Z(G_{p^r})[p^n] \subset Z(G)[p^n]$ for $r \geqslant N$. We conclude that for $r \geqslant \max(N, m)$, we have $Z(G_{p^r})[p^n] = Z(G)[p^n]$. □

Lemma 5.2. *Let K be a p-closed field containing k. Then every class $\alpha \in H^1(K, G)$ lies in the image of the map $H^1(K, G_{p^r}) \to H^1(K, G)$ for sufficiently high r.*

Proof. Let $\alpha \in H^1(K, G)$. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T[n] & \longrightarrow & G_n & \longrightarrow & F & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & T & \longrightarrow & G & \longrightarrow & F & \longrightarrow & 1 \end{array}$$

and the associated diagram in Galois cohomology. Let $\overline{\alpha} \in H^1(K, F)$ be the image of α under the natural morphism $H^1(K, G) \to H^1(K, F)$. Since T is abelian, the conjugation actions of G on T and of G_n on $T[n]$ descend to F. Twisting the bottom sequence by $\overline{\alpha}$ and setting $U = {}^{\overline{\alpha}}T$, we see that the fiber of $\overline{\alpha}$ equals the image of $H^1(K, U)$; see [Ser97, Section I.5.5]. Similarly twisting the top sequence by $\overline{\alpha}$, we see that the fiber of $H^1(K, G_n) \to H^1(K, F)$ over $\overline{\alpha}$ equals the image of $H^1(K, U[n])$. Here n is a power of p. Thus it suffices to prove the following:

Claim. *Let K be a p-closed field and U be a torus defined over K. Then the natural map $H^1(K, U[p^r]) \to H^1(K, U)$ is surjective for r sufficiently large.*

To prove the claim, note that since K is p-closed, the torus U is split by an extension L/K of degree n, where n is a power of p. By a restriction-corestriction argument, it follows that $H^1(K, U)$ is n-torsion. Now consider the short exact sequence

$$1 \longrightarrow U[n] \longrightarrow U \xrightarrow{\times\ n} U \longrightarrow 1\,.$$

The associated exact cohomology sequence

$$H^1(K, U[n]) \longrightarrow H^1(K, U) \xrightarrow{\times\ n} H^1(K, U)$$

shows that $H^1(K, U[n])$ surjects onto $H^1(K, U)$. This completes the proof of the claim and thus of the Lemma 5.2. □

6. The index

Let μ be a diagonalizable abelian p-group and

$$1 \longrightarrow \mu \longrightarrow G \longrightarrow \overline{G} \longrightarrow 1 \tag{6.1}$$

be a central exact sequence of affine algebraic groups defined over k. This sequence gives rise to the exact sequence of pointed sets

$$H^1(K,G) \longrightarrow H^1\big(K,\overline{G}\big) \xrightarrow{\partial_K} H^2(K,\mu)$$

for any field extension K of the base field k. Any character $x\colon \mu \to \mathbb{G}_{\mathrm{m}}$ induces a homomorphism $x_*\colon H^2(K,\mu) \to H^2(K,\mathbb{G}_{\mathrm{m}})$. We define $\operatorname{ind}^x(G,\mu)$ as the maximal index of $x_* \circ \partial_K(E) \in H^2(K,\mu)$, where the maximum is taken over all field extensions K/k and over all $E \in H^1\big(K,\overline{G}\big)$. This number is finite for every character $x\colon \mu \to \mathbb{G}_{\mathrm{m}}$; see [Mer13, Theorem 6.1].

Remark 6.1. Since μ is a finite p-group, the index of $x_* \circ \partial_K(E)$ does not change when K is replaced by a finite extension K'/K whose degree is prime to p and E is replaced by its image under the natural restriction map $H^1\big(K,\overline{G}\big) \to H^1\big(K',\overline{G}\big)$. Equivalently, we may replace K with its p-closure $K^{(p)}$. In other words, the maximal value of $x_* \circ \partial_K(E)$ will be attained if we only allow K to range over p-closed fields extensions of k.

Set $\operatorname{ind}(G,\mu) := \min \sum_{i=1}^r \operatorname{ind}^{x_i}(G,\mu)$, where the minimum is taken over all generating sets $x_1,\dots,x_r$ of the group $X(\mu)$ of characters of μ.

Now suppose that $G^0 = T$ is a torus and $G/G^0 = F$ is a p-group, as in (1.1). In this case, there is a particularly convenient choice of $\mu \subset G$. Following [LMMR13b, Section 4], we denote this central subgroup of G by $C(G)$. If k is algebraically closed, $C(G)$ is simply the p-torsion subgroup of the center of G, that is, $C(G) = Z(G)[p]$. If k is only assumed to be p-closed, then we set $C(G) = \operatorname{Split}_k(Z(G)[p])$ to be the largest k-split subgroup of $Z(G)[p]$ in the sense of [LMMR13a, Section 2].

Proposition 6.2. *Let G be as in (1.1). Denote by $\eta(G)$ the smallest dimension of a p-faithful G-representation.*

(a) *We have $\operatorname{ind}(G,C(G)) = \eta(G)$.*

(b) *If r is sufficiently large, then $\eta(G) = \eta(G_{p^r}) = \operatorname{ed}(G_{p^r}) = \operatorname{ed}(G_{p^r};p)$.*

Proof. (a) Let $\operatorname{Rep}^x(G)$ be the set of irreducible G-representations $\nu\colon G \to \operatorname{GL}(V)$ such that $\nu(z) = x(z)\operatorname{Id}_V$ for every $z \in \mu(\overline{k})$. By the index formula [Mer13, Theorem 6.1], we have $\operatorname{ind}^x(G) = \gcd\dim(\nu)$, where ν ranges over $\operatorname{Rep}^x(G)$ and gcd stands for the greatest common divisor. By [LMMR13b, Proposition 4.2], the dimension $\dim(\nu)$ is a power of p for every irreducible representation ν of G defined over k. Thus one can replace $\gcd\dim(\nu)$ with $\min\dim(\nu)$ in the index formula. Decomposing an arbitrary representation of G as a direct sum of irreducible subrepresentations, we see that $\operatorname{ind}(G,C(G))$ equals the minimal dimension of a k-representation $\nu\colon G \to \operatorname{GL}(V)$ such that the restriction $\nu_{|C(G)}\colon C(G) \to \operatorname{GL}(V)$ is faithful. Finally, by [LMMR13b, Proposition 4.3], the restriction $\nu_{|C(G)}$ is faithful if and only if ν is p-faithful.

(b) Since G_{p^r} is a (not necessarily constant) finite p-group and k is p-closed, the identities $\eta(G_{p^r}) = \operatorname{ed}(G_{p^r}) = \operatorname{ed}(G_{p^r};p)$ follow from [LMMR13a, Theorem 7.1]. It thus remains to show that

$$\eta(G) = \eta(G_{p^r}) \quad \text{for } r \gg 0\,. \tag{6.2}$$

By Lemma 5.1(b), we have $Z(G)[p] = Z(G_{p^r})[p]$ and thus $C(G) = C(G_{p^r})$ for $r \gg 0$. In view of part (a), the identity (6.2) is thus equivalent to

$$\operatorname{ind}(G, C(G)) = \operatorname{ind}(G_{p^r}, C(G)) \quad \text{for } r \gg 0\,. \tag{6.3}$$

Let h be the natural projection $G \to \overline{G} = G/C(G)$. Note that the group $\overline{G}$ is of the same type as G. That is, the connected component $\overline{G}^0$ is the torus $\overline{T} := h(T)$, and since the homomorphism $F = G/T \to \overline{G}/\overline{T}$ is surjective, $\overline{F} := \overline{G}/\overline{G}^0$ is a p-group. Moreover, if F' is a quasi-splitting subgroup for G (as defined at the beginning of Section 5), then $\overline{F}' := h(F')$ is a quasi-splitting subgroup for $\overline{G}$. We will use this subgroup to define the finite subgroups $\overline{G}_n$ of $\overline{G}$ for every integer n in the same way as we defined G_n:

$$\overline{G}_n \text{ is the subgroup of } \overline{G} \text{ generated by } \overline{F}' \text{ and the torsion subgroup } \overline{T}[n]\,.$$

Now observe that since $C(G)$ is p-torsion in G, we have $h(T[n]) \subset \overline{T}[n] \subset h(T[pn])$ and thus

$$h(G_n) \subset \overline{G}_n \subset h(G_{pn}) \tag{6.4}$$

for every n. We now proceed with the proof of (6.3). Consider the diagram of natural maps

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C(G) & \longrightarrow & G & \longrightarrow & \overline{G} & \longrightarrow & 1 \\
 & & \| & & \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle \bar{i}} & & \\
1 & \longrightarrow & C(G) & \longrightarrow & G_{p^r} & \longrightarrow & h(G_{p^r}) & \longrightarrow & 1
\end{array}$$

and the induced diagram in Galois cohomology

$$\begin{array}{ccccc}
H^1(K, G) & \longrightarrow & H^1\big(K, \overline{G}\big) & \xrightarrow{\partial_K} & H^2(K, C(G)) \\
\uparrow{\scriptstyle i_*} & & \uparrow{\scriptstyle \bar{i}_*} & & \| \\
H^1(K, G_{p^r}) & \longrightarrow & H^1(K, h(G_{p^r})) & \xrightarrow{\overline{\partial}_K} & H^2(K, C(G))\,.
\end{array}$$

In view of Remark 6.1, for the purpose of computing $\operatorname{ind}(G, C(G))$ and $\operatorname{ind}(G_{p^r}, C(G))$, we may assume that K is a p-closed field. We claim that for $r \gg 0$, the vertical map $\bar{i}_*\colon H^1(K, h(G_{p^r})) \to H^1\big(K, \overline{G}\big)$ is surjective for every p-closed field K/k. If we can prove this claim, then for $r \gg 0$, the image of $\overline{\partial}_K$ in $H^2(K, C(G))$ is the same as the image of ∂_K. Thus $\operatorname{ind}^x(G)$ and $\operatorname{ind}^x(G_{p^r})$ are the same for every $x \in X(C(G))$, and (6.3) will follow.

To prove the claim, note that $\overline{G}_{p^r} \subset h(G_{p^{r+1}})$ by (6.4). Consider the composition

$$H^1\big(K, \overline{G}_{p^{r-1}}\big) \longrightarrow H^1(K, h(G_{p^r})) \xrightarrow{\bar{i}_*} H^1\big(K, \overline{G}\big)\,.$$

By Lemma 5.2, the map $H^1\big(K, \overline{G}_{p^{r-1}}\big) \to H^1\big(K, \overline{G}\big)$ is surjective for $r \gg 0$. Hence, so is $\bar{i}_*$. This completes the proof of the claim and thus of (6.3) and of Proposition 6.2. □

7. A resolution theorem for rational maps

The following lemma is a minor variant of [BRV18, Lemma 2.1]. For the sake of completeness, we supply a self-contained proof.

Lemma 7.1. *Let $K \subset L$ be a field extension and $v\colon L^\times \to \mathbb{Z}$ be a discrete valuation. Assume that $v|_{K^\times}$ is non-trivial, and denote the residue fields of v and $v|_{K^\times}$ by L_v and K_v, respectively. Then $\operatorname{trdeg}_K L \geqslant \operatorname{trdeg}_{K_v} L_v$.*

Proof. Let $\overline{x}_1, \dots, \overline{x}_m \in L_v$. For every i, let x_i be a preimage of $\overline{x}_i$ in the valuation ring $\mathcal{O}_L$. It suffices to show that if $\overline{x}_1, \dots, \overline{x}_m$ are algebraically independent over K_v, then $x_1, \dots, x_m$ are algebraically independent over K. To prove this, we argue by contradiction. Suppose that there exists a non-zero polynomial $f \in K[t_1, \dots, t_m]$ such that $f(x_1, \dots, x_m) = 0$. Multiplying f by a suitable power of a uniformizing parameter for $v|_{K^\times}$, we may assume that $f \in \mathcal{O}_K[x_1, \dots, x_m]$ and that at least one coefficient of f has valuation equal to 0. Reducing modulo the maximal ideal of the valuation ring $\mathcal{O}_K$, we see that $\overline{x}_1, \dots, \overline{x}_m$ are algebraically dependent over K_v, which leads to a contradiction. □

Recall that if X_1 is normal and X_2 is complete, any rational map $f\colon X_1 \dashrightarrow X_2$ is regular in codimension 1. It follows that if $D \subset X_1$ is a prime divisor of X_1, the closure of the image $\overline{f(D)} \subset X_2$ is well defined.

Theorem 7.2. *Let G be a smooth linear algebraic group over k and $f\colon X \dashrightarrow Y$ be a dominant rational map of G-varieties. Assume that X is normal, Y is normal and complete, $D \subset X$ is a prime divisor, and $\overline{f(D)} \neq Y$. Then there exist a commutative diagram of G-equivariant dominant rational maps*

$$\begin{array}{ccc} & & Y' \\ & \overset{f'}{\nearrow} & \downarrow \pi \\ X & \overset{}{\underset{f}{\dashrightarrow}} & Y \end{array}$$

and a divisor $E \subset Y'$ such that Y' is complete, $\pi\colon Y' \to Y$ is a birational morphism, and $\overline{f'(D)} = E$.

Proof. Let $v\colon k(X)^\times \to \mathbb{Z}$ be the valuation given by the order of vanishing or pole along D. Since X is normal and Y is complete, f restricts to a rational map $D \dashrightarrow Y$. Denote the Zariski closure of the image of this map by C, and set

$$w\colon k(Y)^\times \xrightarrow{f^*} k(X)^\times \xrightarrow{v} \mathbb{Z}\,.$$

We claim that w is non-zero; that is, w is a discrete valuation on $k(Y)$. Indeed, choose $\varphi \in k(Y)^\times$ so that φ is regular in an open neighborhood U of the generic point of C and $\varphi|_{U\cap C} = 0$. It follows that $\varphi \circ f$ is zero on D, hence $w(f) = v(\varphi \circ f) > 0$. This proves the claim.

Since D maps dominantly onto C, we have an inclusion of local rings $f^*\colon \mathcal{O}_{Y,C} \hookrightarrow \mathcal{O}_{X,D}$. It follows that if $\varphi \in \mathcal{O}_{Y,C}$, then $w(\varphi) = v(\varphi \circ f) \geqslant 0$; that is, $\mathcal{O}_{Y,C}$ is contained in the valuation ring of w. In other words, C is the center of w.

Denote by $k(Y)_w$ the residue field of w. By Lemma 7.1, we have

$$\operatorname{trdeg}_k k(X) - \operatorname{trdeg}_k k(Y) \geqslant \operatorname{trdeg}_k k(D) - \operatorname{trdeg}_k k(Y)_w\,.$$

Since $\operatorname{trdeg}_k k(D) = \operatorname{trdeg}_k k(X) - 1$, this can be rewritten as

$$\operatorname{trdeg}_k k(Y)_w \geqslant \operatorname{trdeg}_k k(Y) - 1\,.$$

On the other hand, we have $\operatorname{trdeg}_k k(Y)_w \leqslant \operatorname{trdeg}_k k(Y) - 1$ by the Zariski–Abhyankar inequality [Bou89, Section VI.10.3, Corollary 1], hence

$$\operatorname{trdeg}_k k(Y)_w = \operatorname{trdeg}_k k(Y) - 1\,.$$

By [Art86, Theorem 5.2], there exists a sequence of proper birational morphisms

$$Y' = Y_n \to Y_{n-1} \to \cdots \to Y_1 \to Y_0 = Y$$

such that each $Y_{i+1} \to Y_i$ is a blow-up at the center of w on Y_i, the center E' of w on Y' is a prime divisor, and Y' is normal at the generic point of E'. Since C is G-invariant, by the universal property of the blow-up, the G-action on Y lifts to every Y_i, and the maps $Y_{i+1} \to Y_i$ are G-equivariant.

We let $\pi\colon Y' \to Y$ be the composition of the maps $Y_{i+1} \to Y_i$ and $f'\colon X \dashrightarrow Y'$ be the composition of f with the birational inverse of π. By construction, f' is G-equivariant. It suffices to show that $\overline{f'(D)} = E$. Since the center of w is the divisor $E \subset Y'$, the valuation w is given by the order of vanishing or pole along E. If we identify $k(Y)$ with $k(Y')$ via π, we also have $w = (f')^*v$. It follows that $\varphi \in k(Y')^\times$ is regular and vanishes at the generic point of E if and only if $w(\varphi) > 0$ if and only if $v(\varphi \circ f') > 0$ if and only if φ vanishes at the generic point of $f'(D)$. We conclude that $\overline{f'(D)} = E$, as desired.

Since G is smooth, the G-action on Y' lifts to the normalization $(Y')^{\mathrm{norm}}$, so that the normalization map $(Y')^{\mathrm{norm}} \to Y'$ is G-equivariant. After replacing Y' with $(Y')^{\mathrm{norm}}$ and E' with its preimage in $(Y')^{\mathrm{norm}}$, we may assume that Y' is normal everywhere (and not just at the generic point of E'). □

8. Proof of Theorem 1.2

Let G be an algebraic group as in (1.1). Let $\nu\colon G \to \mathrm{GL}(V)$ be a p-faithful representation of G of minimal dimension $\eta(G)$. By Lemma 2.1, there exists a stabilizer in general position S_V for the $G_{\overline{k}}$-action on $V_{\overline{k}}$. Since $V(k)$ is dense in V, we may assume without loss of generality that S_V is the stabilizer of a k-point of V. In particular, we may assume that S_V is a closed subgroup of G defined over k. Since T acts p-faithfully on V, we have $S_V \cap T = \{1\}$.

Reduction 8.1. To prove Theorem 1.2, it suffices to construct a G-representation V' such that $\dim(\tilde{V}) = \mathrm{rank}_p(S_V)$, $W := V \oplus \tilde{V}$ is p-generically free, and

$$\mathrm{ed}(W;p) = \dim(W) - \dim(G)\,. \tag{8.1}$$

Here when we write $\mathrm{ed}(W;p)$, we are viewing W as a generically free $G/\operatorname{Ker}(\varphi)$-variety, where $\varphi\colon G \to \mathrm{GL}(W)$ denotes the representation of G on W. The kernel $\operatorname{Ker}(\varphi)$ of this representation is a finite normal subgroup of G of order prime to p.

Proof. Suppose that we manage to construct $\tilde{V}$ so that (8.1) holds. Then

$$\mathrm{ed}(W;p) \overset{\text{(i)}}{=} \mathrm{ed}(G/\operatorname{Ker}(\varphi);p) \overset{\text{(ii)}}{=} \mathrm{ed}(G;p) \overset{\text{(iii)}}{\leqslant} \rho(G) - \dim(G) \overset{\text{(iv)}}{\leqslant} \dim(W) - \dim(G)\,,$$

where

(i) follows from the fact that W is a versal $G/\operatorname{Ker}(\varphi)$-variety; see, for example, [Mer13, Propositions 3.10 and 3.11];

(ii) follows by [LMMR13b, Proposition 2.4];

(iii) is the right-hand side of (1.2); and

(iv) is immediate from the definition of $\rho(G)$.

If we know that (8.1) holds, then the inequalities (iii) and (iv) are, in fact, equalities. Equality in (iii) yields Theorem 1.2(a). On the other hand, since

$$\dim(W) = \dim(V) + \dim(\tilde{V}) = \eta(G) + \mathrm{rank}_p(S_V)\,,$$

equality in (iv) tells us that $\eta(G) + \mathrm{rank}_p(S_V) = \rho(G)$, thus proving Theorem 1.2(b). □

We now proceed with the construction of W. From now on, we replace G with $\overline{G} = G/\operatorname{Ker}(\nu)$. All other G-actions we will construct (including the linear G-action on W) will factor through $\overline{G}$. In the end, we will show that $\operatorname{ed}(W;p) = \operatorname{ed}\left(\overline{G};p\right)$; once again, this is enough because $\operatorname{ed}(G;p) = \eta(G) = \eta(\overline{G}) = \operatorname{ed}\left(\overline{G};p\right)$ by [LMMR13b, Proposition 2.4]. In other words, from now on we may (and will) assume that the G-action on V is faithful.

Recall that S_V denotes the stabilizer in general position for the G-action on V and that we have chosen S_V (which is a priori a closed subgroup of $G_{\overline{k}}$ defined up to conjugacy) so that it is defined over k. Since T is a torus and T acts faithfully on V, this action is automatically generically free. That is, $S_V \cap T = 1$ or, equivalently, the natural projection $\pi|_{S_V} \colon S_V \to F$ is injective. In particular, $\pi(S_V)$ is diagonalizable. By our assumption, F is isomorphic to the product $\mu_{p^{i_1}} \times \cdots \times \mu_{p^{i_R}}$ for some integers $R \geqslant 0$ and $i_1, \ldots, i_R \geqslant 1$. Moreover, this isomorphism can be chosen so that

$$\pi(S_V) = \mu_{p^{j_1}} \times \cdots \times \mu_{p^{j_r}}$$

for some $0 \leqslant r \leqslant R$ and some integers j_m with $1 \leqslant j_m \leqslant i_m$ for every $m = 1, \ldots, r$. Let χ_m be the composition of $\pi \colon G \to F$ with the projection map $F \to \mu_{p^{i_m}}$ to the mth component and V_m be a 1-dimensional vector space on which G acts by χ_m. Set $W_d = V$ and $W_{d+m} = V \oplus V_1 \oplus \cdots \oplus V_m$ for $m = 1, \ldots, r$. A stabilizer in general position for the G-action on W_{d+m} is

$$S_{W_{d+m}} = S_V \cap \operatorname{Ker}(\chi_1) \cap \cdots \cap \operatorname{Ker}(\chi_m)\,;$$

equivalently,

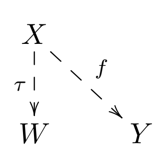
$$S_{W_{d+m}} \simeq \pi(S_{W_{d+m}}) = \{1\} \times \cdots \times \{1\} \times \mu_{p^{j_{m+1}}} \times \cdots \times \mu_{p^{j_r}} \qquad (8.2)$$

for any $0 \leqslant m \leqslant r$. In particular, $S_{W_{d+r}} = \{1\}$; in other words, the G-action on W_{d+r} is generically free. We now set

$$W = W_{d+r} = V \oplus V_1 \oplus \cdots \oplus V_r\,.$$

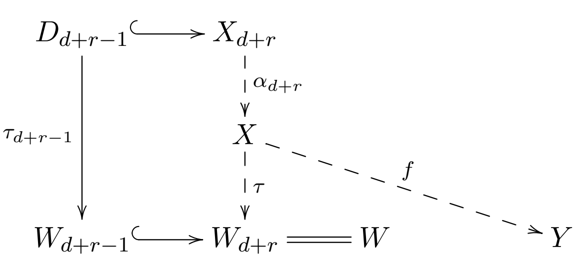
Having defined W, we now proceed with the proof of (8.1). In view of Lemma 4.1(b), it suffices to establish the following.

Proposition 8.2. *Let W be as above. Consider a dominant G-equivariant correspondence*



of degree prime to p, where Y is a p-generically free projective G-variety. Then $\dim(Y) = \dim(W) = d + r$.

We now proceed with the proof of the proposition. By Lemma 3.1 (with $Z = W_{d+r-1}$), there exists a commutative diagram of G-equivariant maps



such that X_{d+r} is normal, α_{d+r} is a birational isomorphism, D_{d+r-1} is an irreducible divisor in X_{d+r}, and τ_{d+r-1} is a cover of W_{d+r-1} of degree prime to p. Let $S_{D_{d+r-1}} \subset G$ be a stabilizer in general position for the G-action on D_{d+r-1}; it exists by Lemma 2.1. In view of (8.2), Lemma 3.2 tells us that

$$\operatorname{rank}_p(S_{D_{d+r-1}}) = 1\,. \tag{8.3}$$

On the other hand, by our assumption, the G-action on Y is p-generically free. Thus the restriction[1] of the dominant rational map $f \circ \alpha_{d+r} \colon X_{d+r} \dashrightarrow Y$ to D_{d+r-1} cannot be dominant, and Theorem 7.2 applies: there exists a commutative diagram

$$\begin{array}{ccc} X_{d+r} & \overset{f_{d+r}}{\dashrightarrow} & Y_{d+r} \\ {\scriptstyle \alpha_{d+r}} \downarrow & & \downarrow {\scriptstyle \sigma_{d+r}} \\ X & \overset{f}{\dashrightarrow} & Y \end{array}$$

of dominant G-equivariant rational maps, where σ_{d+r} is a birational morphism, Y_{d+r} is normal and complete, and f_{d+r} restricts to a dominant G-equivariant rational map $D_{d+r-1} \dashrightarrow E_{d+r-1}$ for some G-invariant irreducible divisor E_{d+r-1} of Y_{d+r}. We will denote this dominant rational map by $f_{d+r-1} \colon D_{d+r-1} \dashrightarrow E_{d+r-1}$. We now iterate this construction with f_{d+r} replaced by f_{d+r-1}.

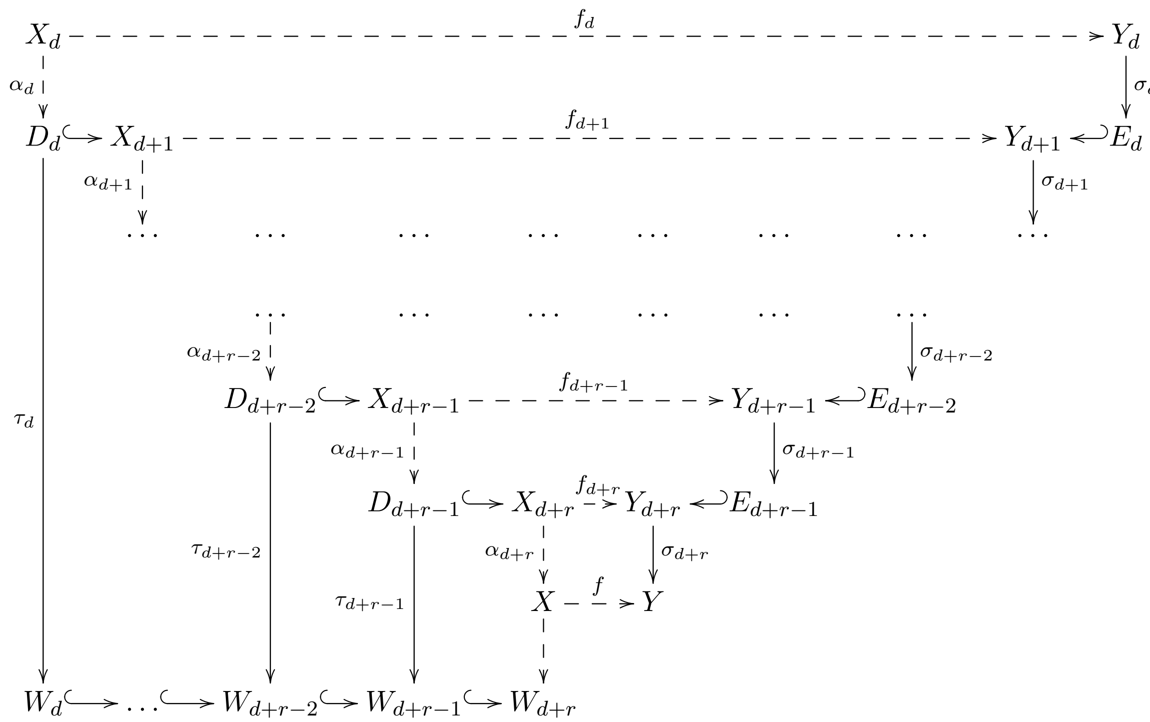
By Lemma 3.1, there exists a commutative diagram of G-equivariant maps

$$\begin{array}{ccc} D_{d+r-2} & \hookrightarrow & X_{d+r-1} \\ & & \downarrow {\scriptstyle \alpha_{d+r-1}} \\ {\scriptstyle \tau_{d+r-2}} \downarrow & & D_{d+r-1} \\ & & \downarrow {\scriptstyle \tau_{d+r-1}} \\ W_{d+r-2} & \hookrightarrow & W_{d+r-1} \end{array}$$

such that X_{d+r-1} is normal, α_{d+r-1} is a birational isomorphism, D_{d+r-2} is an irreducible divisor in X_{d+r-1}, and τ_{d+r-2} is a cover of W_{d+r-2} of degree prime to p.

Denote a stabilizer in general position for the G-action on E_{d+r-1} by $S_{E_{d+r-1}}$. Recall that the G-action on Y (and thus Y_{d+r}) is p-generically free. Since E_{d+r-1} is a G-invariant hypersurface in Y_{d+r}, Lemma 2.3(a) tells us that $\operatorname{rank}_p(S_{E_{d+r-1}}) \leqslant 1$. On the other hand, since X_{d+r-1} maps dominantly to E_{d+r-1}, the group $S_{E_{d+r-1}}$ contains (a conjugate of) $S_{X_{d+r-1}}$ and thus $\operatorname{rank}_p(S_{E_{d+r-1}}) \geqslant \operatorname{rank}_p(S_{X_{d+r-1}})$, where $\operatorname{rank}_p(S_{X_{d+r-1}}) = 1$ by (8.3). We conclude that $\operatorname{rank}_p(S_{E_{d+r-1}}) = 1$. Now observe that since $\operatorname{rank}_p(S_{E_{d+r-1}}) = 1$ and $\operatorname{rank}_p(S_{X_{d+r-2}}) = 2$ (see (8.2)), the image of X_{d+r-2} under f_{d+r-1} cannot be Zariski dense in E_{d+r-1}. Consequently, Theorem 7.2 can be applied to $f_{d+r-1} \colon X_{d+r-1} \dashrightarrow E_{d+r-1}$. It yields a birational morphism $\sigma_{d+r-1} \colon Y_{d+r-1} \to E_{d+r-1}$ such that Y_{d+r-1} is normal and complete, and the composition $\sigma_{d+r-1}^{-1} \circ f_{d+r-1}$ restricts to a dominant G-equivariant rational map $f_{d+r-2} \colon D_{d+r-2} \dashrightarrow E_{d+r-2}$ for some G-invariant prime divisor E_{d+r-2} of Y_{d+r-1}. Proceeding recursively, we obtain a commutative diagram of G-equivariant maps

[1] The restriction of $f \circ \alpha_{d+r}$ to D_{d+r-1} is well defined because X_{d+r} is normal and Y is complete.



such that for every m,

(i) D_{d+m} is an irreducible divisor in X_{d+m+1} and E_{d+m} is an irreducible divisor in Y_{d+m+1};

(ii) the vertical maps $\alpha_{d+m}\colon X_{d+m} \dashrightarrow D_{d+m}$ and $\sigma_{d+m}\colon Y_{d+m} \to E_{d+m}$ are birational isomorphisms;

(iii) X_{d+m} and Y_{d+m} are normal, and Y_{d+m} is complete;

(iv) $\operatorname{rank}_p(S_{X_{d+m}}) = \operatorname{rank}_p(S_{Y_{d+m}}) = r - m$;

(v) the vertical morphism $\tau_{d+m}\colon D_{d+m} \to W_{d+m}$ is a cover of degree prime to p.

Note that the subscripts are chosen so that $\dim(X_{d+m}) = \dim(W_{d+m}) = d + m$ for each $m = 0, \ldots, r$. We will eventually show that $\dim(Y_{d+m}) = d + m$ for each m as well, but we do not know what $\dim(Y_{d+m})$ is at this point.

LEMMA 8.3. *The G-action on Y_{d+m} (or, equivalently, on E_{d+m}) is p-faithful for every $m = 0, \ldots, r$.*

Assume, for a moment, that this lemma is established. By our construction, f_d may be viewed as a dominant G-equivariant correspondence $W_d \rightsquigarrow Y_d$ of degree prime to p. Now recall that $W_d = V$ is a p-faithful representation of G of minimal possible dimension $\eta(G)$. By Lemma 8.3, the G-action of Y_d is p-faithful. Restricting to the p-subgroup $G_n \subset G$, where n is a power of p, we obtain a dominant G_n-equivariant correspondence $f_d\colon V \rightsquigarrow Y_d$ of degree prime to p, where the G_n-action on Y is faithful. Thus $\dim(Y_d) \geqslant \operatorname{ed}(G_n; p)$. When n is a sufficiently high power of p, Proposition 6.2 tells us that

$$\operatorname{ed}(G_n; p) = \eta(G_n) = \eta(G) = \dim(V) = d\,.$$

By conditions (i) and (ii) above, $\dim(Y_{d+m+1}) = \dim(E_{d+m}) + 1 = \dim(Y_{d+m}) + 1$ for each $m = 0, 1, \ldots, r$. Thus $\dim(Y) = \dim(Y_{d+r}) = \dim(Y_d) + r = \dim(V) + r = d + r = \dim(W)$, as desired. This will complete the proof of Proposition 8.2 and thus of Theorem 1.2.

Proof of Lemma 8.3. For the purpose of this proof, we may replace k with its algebraic closure $\overline{k}$ and thus assume that k is algebraically closed. We argue by reverse induction on m. For the base case, where $m = r$, note that by our assumption, the G-action on Y is p-generically free and hence p-faithful. Since Y_{d+r} is birationally isomorphic to Y, the same is true of the G-action on Y_{d+r}.

For the induction step, assume that the G-action on Y_{d+m+1} is p-faithful for some m with $0 \leqslant m \leqslant r-1$. Our goal is to show that the G-action on Y_{d+m} is also p-faithful. Let N be the kernel of the G-action on Y_{d+m}. Recall that by Lemma 2.3(b), there is a homomorphism

$$\alpha\colon N \to \mathbb{G}_{\mathrm{m}} \tag{8.4}$$

where $\mathrm{Ker}(\alpha)$ has no elements of order p. Since $\mathrm{Ker}(\alpha)$ is a subgroup of G and we are assuming that $G^0 = T$ is a torus and $G/G^0 = F$ is a finite p-group, we conclude that

$$\mathrm{Ker}(\alpha) \text{ is a finite subgroup of } T \text{ of order prime to } p\,. \tag{8.5}$$

It remains to show that $\alpha(N)$ is a finite group of order prime to p. Assume the contrary: $\alpha(N)$ contains $\mu_p \subset \mathbb{G}_{\mathrm{m}}$.

Claim. *There exists a subgroup $\mu_p \simeq N_0 \subset N$ such that N_0 is central in G.*

First we observe that in order to prove the claim, it suffices to show that there exists a subgroup $\mu_p \simeq N_0 \subset N$ such that N_0 is normal in G. Indeed, since $G^0 = T$ is a torus and $G/G^0 = F$ is a p-group, if $N_0 \simeq \mu_p$ is normal in G, then the conjugation map $G \to \mathrm{Aut}(\mu_p) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ is trivial, so N_0 is automatically central. Now consider two cases.

Case 1: $G^0 = T$ does not act p-faithfully on Y_{d+m}. Then $\mu_p \subset N \cap T \triangleleft G$. In view of (8.4) and (8.5), the intersection $N \cap T$ contains exactly one copy of μ_p. This implies that μ_p is characteristic in $N \cap T$ and, hence, normal in G, as desired.

Case 2: The intersection $N \cap T$ does not contain μ_p; that is, $N \cap T$ is a finite group of order prime to p. Examining the exact sequence

$$1 \to N \cap T \to N \to F = G/T\,,$$

we see that N is a finite group of order pm, where m is prime to p. Let $\mathrm{Syl}_p(N)$ be the set of Sylow p-subgroups of N. By Sylow's theorem, we have[2] $|\mathrm{Syl}_p(N)| \equiv 1 \pmod{p}$. The group G acts on $\mathrm{Syl}_p(N)$ by conjugation. Clearly T acts trivially, and the p-group $F = G/T$ fixes a subgroup $N_0 \in \mathrm{Syl}_p$. In other words, $N_0 \simeq \mu_p$ is normal in G. This proves the claim.

We are now ready to finish the proof of Lemma 8.3. Let $S_{Y_{d+m}} \subset G$ be a stabilizer in general position for the G-action on Y_{d+m}, N be the kernel of this action, and N_0 be the central subgroup of N isomorphic to μ_p, as in the claim. Clearly $N_0 \subset N \subset S_{Y_{d+m}}$. Since $f_{d+m}\colon X_{d+m} \dashrightarrow Y_{d+m}$ is a dominant G-equivariant rational map, $S_{Y_{d+m}}$ contains (a conjugate of) $S_{X_{d+m}}$. By condition (iv),

$$\mathrm{rank}_p(S_{Y_{d+m}}) = r - m = \mathrm{rank}_p(S_{X_{d+m}})\,. \tag{8.6}$$

In particular, $S_{X_{d+m}}$ contains a subgroup A isomorphic to μ_p^{r-m}. Since $N_0 \simeq \mu_p$ is central in G, it has to be contained in A; otherwise, $S_{Y_{d+m}}$ would contain a subgroup isomorphic to $A \times \mu_p = (\mu_p)^{r-m+1}$, contradicting (8.6). Thus $\mu_p \simeq N_0 \subset S_{X_{d+m}}$. Moreover, since N_0 is central in G, it is contained in every conjugate of $S_{X_{d+m}}$. This implies that N_0 stabilizes every point

[2] Recall that we are assuming that k is an algebraically closed field of characteristic different from p. If $\mathrm{char}(k)$ does not divide $|N|$, then $\mathrm{Syl}_p(N)$ is the set of Sylow subgroups of the finite group $N(k)$. If $\mathrm{char}(k)$ divides $|N|$, then elements of $\mathrm{Syl}_p(N)$ can be identified with Sylow p-subgroups of the finite group $N_{\mathrm{red}}(k)$.

of X_{d+m}. In other words, N_0 acts trivially on X_{d+m}. Tracing to the above diagram, we see that N_0 acts trivially on D_{d+m-1}, hence on X_{d+m-1}, hence on D_{d+m-2}, etc. Finally, we conclude that N_0 acts trivially on X_d and hence on $\tau_d(X_d) = W_d = V$, contradicting our assumption that G acts p-faithfully on $W_d = V$.

This contradiction shows that our assumption that $\alpha(N)$ contains μ_p was false. Returning to (8.4) and (8.5), we deduce that the kernel N of the G-action on Y_{d+m} is a finite group of order prime to p. In other words, the G-action on Y_{d+m} is p-faithful. This completes the proof of Lemma 8.3 and thus of Proposition 8.2 and Theorem 1.2. □

Remark 8.4. Our proof of Theorem 1.2 goes through even if F is not abelian, provided that the stabilizer in general position S_V projects isomorphically to $F/[F,F]$. (If F is abelian, this is always the case.)

Remark 8.5. Theorem 1.2 implies that if V and V' are p-faithful representations of G of minimal dimension $\eta(G)$, then the stabilizers in general position, S_V and $S_{V'}$, have the same p-rank:

$$\mathrm{rank}_p(S_V) = \mathrm{rank}_p(S_{V'}) = \rho(G) - \eta(G) = \mathrm{ed}(G;p) + \dim(G) - \eta(G)\,.$$

In our proof of Theorem 1.2, this number is denoted by r.

9. Normalizers of maximal tori in split simple groups

In this section, Γ will denote a split simple algebraic group over k, T will denote a k-split maximal torus of Γ, N will denote the normalizer of T in Γ, and $W = N/T$ will denote the Weyl group. These groups fit into an exact sequence

$$1 \longrightarrow T \longrightarrow N \xrightarrow{\pi} W \longrightarrow 1\,. \tag{9.1}$$

A. Meyer and the first author [MR09] have computed $\mathrm{ed}(N;p)$ in the case where $\Gamma = \mathrm{PGL}_n$ for every prime number p. M. MacDonald [Mac11] subsequently found the exact value of $\mathrm{ed}(N;p)$ for most other split simple groups Γ. One reason this is of interest is that

$$\mathrm{ed}(N;p) \geqslant \mathrm{ed}(\Gamma;p)\,;$$

see, for example, [Mer13, Section 10a]. Let W_p denote a Sylow p-subgroup of W and N_p denote the preimage of W_p in N. Then

$$\mathrm{ed}(N;p) = \mathrm{ed}(N_p;p)\,;$$

see [MR09, Lemma 4.1]. The exact sequence

$$1 \longrightarrow T \longrightarrow N_p \xrightarrow{\pi} W_p \longrightarrow 1$$

is of the form of (1.1), and thus the inequalities (1.2) apply to N_p. MacDonald computed the exact value of $\mathrm{ed}(N;p) = \mathrm{ed}(N_p;p)$ for most split simple linear algebraic groups Γ by showing that the left-hand side and right-hand side of the inequalities (1.2) for N_p coincide. There are two families of groups Γ where the exact value of $\mathrm{ed}(N;p)$ remained inaccessible by this method, $\Gamma = \mathrm{SL}_n$ and $\Gamma = \mathrm{SO}_{4n}$.[3] As an application of Theorem 1.2, we will now compute $\mathrm{ed}(N;p)$ in these two remaining cases. Our main results are Theorems 9.1 and 9.2 below.

[3] The omission of SL_n from [Mac11, Remark 5.11] is an oversight; we are grateful to Mark MacDonald for clarifying this point for us.

Theorem 9.1. *Let $n \geqslant 1$ be an integer, and let N be the normalizer of a k-split maximal torus T in SL_n. Then*

(a) $\mathrm{ed}(N;p) = n/p + 1$ *if $p \geqslant 3$ and n is divisible by p,*
(b) $\mathrm{ed}(N;p) = n/2 + 1$ *if $p = 2$ and n is divisible by 4,*
(c) $\mathrm{ed}(N;p) = \lfloor n/p \rfloor$ *if $p \geqslant 3$ and n is not divisible by p,*
(d) $\mathrm{ed}(N;p) = \lfloor n/2 \rfloor$ *if $p = 2$ and n is not divisible by 4.*

Theorem 9.2. *Let k be a field of characteristic different from 2 and $n \geqslant 1$ be an integer. Let N be the normalizer of a k-split maximal torus of SO_{4n}. Then $\mathrm{ed}(N;2) = 4n$.*

Our proofs of these theorems will rely on the following simple lemma, which is implicit in [MR09] and [Mac11]. Let F be a finite discrete p-group, and let M be an F-lattice. The symmetric p-rank of M is the minimal cardinality d of a finite H-invariant p-spanning subset $\{x_1, \ldots, x_d\} \subset M$. Here "$p$-spanning" means that the index of the $\mathbb{Z}$-module spanned by $x_1, \ldots, x_d$ in M is finite and prime to p. Following MacDonald, we will denote the symmetric p-rank of M by $\mathrm{SymRank}(M;p)$.

Lemma 9.3. *Consider an exact sequence $1 \to T \to G \to F \to 1$ of algebraic groups over k, as in* (1.1)*. Assume further that T is a split torus and F is a constant finite p-group. Denote the character lattice of T by $X(T)$, we will view it as an F-lattice. Then $\eta(G) \geqslant \mathrm{SymRank}(X(T);p)$.*

Here $\eta(G)$ denotes the minimal dimension of a p-faithful representation of G, as defined in the introduction, and $X(T)$ is viewed as an F-lattice. If we further assume that the sequence (1.1) in Lemma 9.3 is split, then, in fact, $\eta(G) = \mathrm{SymRank}(X(T);p)$. We shall not need this equality, so we leave its proof as an exercise for the reader.

Proof of Lemma 9.3. Let V be a p-faithful representation of G of minimal dimension $r = \eta(G)$. As a T-representation, V decomposes as the direct sum of characters $\chi_1, \ldots, \chi_r$. A simple calculation shows that the F-action permutes the χ_i. Let $S \subset \mathrm{GL}(V)$ be the diagonal torus generated by the images of the χ_i. By construction, the kernel of the F-equivariant homomorphism

$$(\chi_1, \ldots, \chi_r) \colon T \to S$$

is finite and of order prime to p. Passing to character lattices, we obtain an F-equivariant homomorphism $X(S) \to X(T)$ whose cokernel is finite and of order prime to p. In other words, the images of the χ_i in $X(T)$ form a p-spanning subset of $X(T)$ of size r. We conclude that $\mathrm{SymRank}(X(T);p) \leqslant r = \eta(G)$, as claimed. □

For the proof of Theorem 9.1 we will also need the following lemma. Let $\Gamma = \mathrm{SL}_n$, T be the diagonal maximal torus, N be the normalizer of T in SL_n, H be a subgroup of the Weyl group $W = N/T \simeq \mathrm{S}_n$, and N' be the preimage of H in N. Restricting (9.1) to N', we obtain an exact sequence

$$1 \longrightarrow T \longrightarrow N' \xrightarrow{\pi} H \longrightarrow 1\,.$$

Lemma 9.4. *Let V_n be the natural n-dimensional representation of SL_n and S be the stabilizer in general position for the restriction of this representation to N'. Then* (a) *$S \cap T = 1$ and* (b) *$\pi(S) = H \cap \mathrm{A}_n$.*

Here, as usual, A_n denotes the alternating subgroup of S_n.

Proof. Part (a) follows from the fact that the T-action on V_n is generically free. To prove part (b), note that $\pi(S)$ is the kernel of the action of H on V_n/T, where V_n/T is the rational quotient of V_n by the action of T; see, for example, the proof of [LMMR13b, Proposition 7.2]. Consider the dense open subset $\mathbb{G}_{\rm m}^n \subset V_n$ consisting of vectors of the form $(x_1, x_2, \dots, x_n)$, where $x_i \neq 0$ for any $i = 1, \dots, n$. We can identify $\mathbb{G}_{\rm m}^n$ with the diagonal maximal torus in GL_n. Now

$$V_n/T \overset{\cong}{\dashleftarrow\dashrightarrow} (\mathbb{G}_{\rm m})^n/T \xrightarrow[\det]{\simeq} \mathbb{G}_{\rm m}\,,$$

where S_n acts on $\mathbb{G}_{\rm m}$ by $\sigma \cdot t = \mathrm{sign}(\sigma)t$. Thus the kernel of the H-action on V_n/T is $H \cap \mathrm{A}_n$, as claimed. □

Proof of Theorem 9.1. We will assume that $\Gamma = \mathrm{SL}_n$ and T is the diagonal torus in Γ. The inequalities

$$\left\lfloor \frac{n}{p} \right\rfloor \leqslant \mathrm{ed}(N;p) \leqslant \left\lfloor \frac{n}{p} \right\rfloor + 1\,; \tag{9.2}$$

are known for every n and p; see [Mac11, Section 5.4]. We will write V_n for the natural n-dimensional representation of SL_n (which we will sometimes restrict to N or subgroups of N).

(a) Assume that p is an odd prime and n is divisible by p. Let $H \simeq (\mathbb{Z}/p\mathbb{Z})^{n/p}$ be the subgroup of $W = N/T \simeq \mathrm{S}_n$ generated by the commuting p-cycles $(1\ 2\ \dots\ p)$, $(p+1\ p+2\ \dots\ 2p)$, $\dots$, $(n-p+1\ \dots\ n)$. Since H is a p-group, it lies in a Sylow p-subgroup W_p of S_n. Denote the preimage of H in N by N'. Then N' is a subgroup of N of finite index, so

$$\mathrm{ed}(N;p) \geqslant \mathrm{ed}(N';p)\,; \tag{9.3}$$

see [BRV10, Lemma 2.2]. It thus suffices to show that $\mathrm{ed}(N';p) = n/p + 1$.

CLAIM. $\eta(N') = n$.

Suppose that the claim is established. Then V_n is a p-faithful representation of N' of minimal dimension. Since p is odd, H lies in the alternating group A_n. By Lemma 9.4(a), the stabilizer in general position for the N'-action on V is isomorphic to H. By Theorem 1.2,

$$\mathrm{ed}(N';p) = \dim(V_n) + \mathrm{rank}(H) - \dim(N') = n + \frac{n}{p} - (n-1) = \frac{n}{p} + 1\,,$$

and we are done.

To prove the claim, note that N' has a faithful representation V_n of dimension n. Hence, $\eta(N') \leqslant n$. To prove the opposite inequality, $\eta(N') \geqslant n$, it suffices to show that

$$\mathrm{SymRank}(X(T);p) \geqslant n\,; \tag{9.4}$$

see Lemma 9.3. Here we view $X(T)$ as an H-lattice. By definition, $\mathrm{SymRank}(X(T);p)$ is the minimal cardinality of a finite H-invariant p-spanning subset $\{x_1, \dots, x_d\} \subset X(T)$. The H-action on $\{x_1, \dots, x_d\}$ gives rise to a permutation representation $\varphi\colon H \to \mathrm{S}_d$.

The permutation representation φ is necessarily faithful. Indeed, assume the contrary: $1 \neq h$ lies in the kernel of φ. Then $x_1, \dots, x_d$ lie in $X(T)^h$. On the other hand, it is easy to see that $X(T)^h$ is of infinite index in $X(T)$. Hence, $\{x_1, \dots, x_d\}$ cannot be a p-spanning subset of $X(T)$. This contradiction shows that φ is faithful.

Now [AG89, Theorem 2.3(b)] tells us that the order of any abelian p-subgroup of S_d is at most $p^{d/p}$. In particular, $|H| \leqslant p^{d/p}$. In other words, $p^{n/p} \leqslant p^{d/p}$ or, equivalently, $n \leqslant d$. This completes the proof of (9.4) and thus of the claim and of part (a).

(b) When $p = 2$ and n is even, the argument in part (a) does not work as stated because it is no longer true that H lies in the alternating group A_n. However, when n is divisible by 4, we can redefine H as

$$H_1 \times \cdots \times H_{n/4} \hookrightarrow \underbrace{\mathrm{A}_4 \times \cdots \times \mathrm{A}_4}_{(n/4 \text{ times})} \hookrightarrow A_n\,,$$

where $H_i \simeq (\mathbb{Z}/2\mathbb{Z})^2$ is the unique normal subgroup of order 4 in the ith copy of A_4. With H defined this way, $H \simeq (Z/2\mathbb{Z})^{n/2}$ is a subgroup of A_n, and the rest of the proof of part (a) goes through unchanged.

(c) Write $n = pq+r$, where $1 \leqslant r \leqslant p-1$. The subgroup of S_n consisting of the permutations σ such that $\sigma(i) = i$ for any $i > pq$, is naturally identified with S_{pq}. Let P_{pq} be a p-Sylow subgroup of S_{pq}, and let N' be the preimage of P_{pq} in N. Then $[N : N'] = [\mathrm{S}_n : P_{pq}]$ is prime to p; hence, it suffices to show that $\mathrm{ed}(N'; p) = \lfloor n/p \rfloor$. In view of (9.2), it is enough to show that $\mathrm{ed}(N'; p) \leqslant \lfloor n/p \rfloor$. Since $r \geqslant 1$, as an N'-representation, V_n splits as $k^{pq} \oplus k^r$ in the natural way. Let us now write k^r as $k^{r-1} \oplus k$ and combine k^{r-1} with k^{pq}. This yields a decomposition $V_n = k^{n-1} \oplus k$, where the action of N' on k^{n-1} is faithful. Now recall that P_{pq} has a faithful q-dimensional representation; see, for example, the proof of [MR09, Lemma 4.2]. Denote this representation by V'. Viewing V' as a q-dimensional representation of N' via the natural projection $N' \to P_{pq}$, we obtain a generically free representation $k^{n-1} \oplus V'$ of N'. Thus

$$\mathrm{ed}(N'; p) \leqslant \dim\left(k^{n-1} \oplus V'\right) - \dim(N') = (n-1) + q - (n-1) = q = \left\lfloor \frac{n}{p} \right\rfloor,$$

as desired.

(d) The argument of part (c) is valid for any prime. In particular, if $p = 2$, it proves part (d) in the case where n is odd. Thus we may assume without loss of generality that $n \equiv 2 \pmod 4$. Let N' be the preimage of P_n in N, where P_n is a Sylow 2-subgroup of S_n. Then the index $[N : N'] = [\mathrm{S}_n : P_n]$ is finite and odd; hence, $\mathrm{ed}(N; 2) = \mathrm{ed}(N'; 2)$. In view of (9.2), it suffices to show that $\mathrm{ed}(N'; 2) \leqslant n/2$.

Since $n \equiv 2 \pmod 4$, we have $P_n = P_{n-2} \times P_2$, where $P_2 \simeq \mathrm{S}_2$ is the subgroup of S_n of order 2 generated by the 2-cycle $(n-1,\ n)$. Let V' be a faithful representation of P_{n-2} of dimension $(n-2)/2$. We may view V' as a representation of N' via the projection $N' \to P_n \to P_{n-2}$.

Claim. *The action of N' on $V_n \oplus V'$ is generically free.*

If this claim is established, then

$$\mathrm{ed}(N') \leqslant \dim(V_n \oplus V') - \dim(N') = n + \frac{n-2}{2} - (n-1) = \frac{n}{2}\,,$$

and we are done.

To prove the claim, let S the stabilizer in general position for the action of N' on V_n. Denote the natural projection $N' \to P_n$ by π. By Lemma 9.4(a), we have $S \cap T = 1$. In other words, π is an isomorphism between S and $\pi(S)$. Since $P_n = P_{n-2} \times P_2$, the kernel of the P_n-action on V' is P_2. It now suffices to show that S acts faithfully on V', that is, $\pi(S) \cap P_2 = 1$.

By Lemma 9.4, we have $\pi(S) \subset \mathrm{A}_n$; that is, every permutation in $\pi(S)$ is even. On the other hand, the non-trivial element of P_2, namely the transposition $(n-1,\ n)$, is odd. This shows that $\pi(S) \cap P_2 = 1$, as desired. □

Proof of Theorem 9.2. By [Mac11, Section 5.7], we have $\mathrm{ed}(N; 2) \leqslant 4n$. Thus it suffices to show that $\mathrm{ed}(N; 2) \geqslant 4n$.

Recall that a split maximal torus T of SO_{4n} is isomorphic to $(\mathbb{G}_\mathrm{m})^{2n}$ and the Weyl group W is a semi-direct product $A \rtimes \mathrm{S}_{2n}$. Here $A \simeq (\mathbb{Z}/2\mathbb{Z})^{2n-1}$ is the multiplicative group of $2n$-tuples $\epsilon = (\epsilon_1, \ldots, \epsilon_{2n})$, where each ϵ_i is ± 1 and $\epsilon_1\epsilon_2 \cdots \epsilon_{2n} = 1$. The symmetric group S_{2n} acts on A by permuting $\epsilon_1, \ldots, \epsilon_{2n}$. The action of W on $(t_1, \ldots, t_{2n}) \in T$ is as follows: S_{2n} permutes $t_1, \ldots, t_{2n}$, and ϵ takes each t_i to $t_i^{\epsilon_i}$. The normalizer N of T in SO_{4n} is the semidirect product of T and W with respect to this action.

Let H be the subgroup of W generated by elements $(\epsilon_1, \ldots, \epsilon_{2n}) \in A$ with $\epsilon_1 = \epsilon_2$, $\epsilon_3 = \epsilon_4$, $\ldots$, $\epsilon_{2n-1} = \epsilon_{2n}$ and the n disjoint 2-cycles $(1, 2), (3, 4), \ldots, (2n-1, 2n)$ in S_{2n}. It is easy to see that these generators are of order 2 and commute with each other, so that $H \simeq (\mathbb{Z}/2\mathbb{Z})^n$. Let N' be the preimage of H in N.

Note that H arises as a stabilizer in general position of the natural $4n$-representation V_{4n} of N (restricted from SO_{4n}). Here $(t_1, \ldots, t_{2n}) \in T$ acts on $(x_1, \ldots, x_{2n}, y_1, \ldots, y_{2n}) \in V_{4n}$ by $x_i \mapsto t_i x_i$ and $y_i \mapsto t_i^{-1} y_i$ for each i. The symmetric group S_{2n} simultaneously permutes $x_1, \ldots, x_{2n}$ and $y_1, \ldots, y_{2n}$; the $2n$-tuple $\epsilon \in A$ leaves x_i and y_i invariant if $\epsilon_i = 1$ and switches them if $\epsilon_i = -1$.

Note that N' is a subgroup of finite index in N. Hence, $\mathrm{ed}(N; 2) \geqslant \mathrm{ed}(N'; 2)$, and it suffices to show that $\mathrm{ed}(N'; 2) \geqslant 4n$.

Claim. $\eta(N') = 4n$.

Suppose for a moment that the claim is established. Then V_{4n} is a 2-faithful representation of N' of minimal dimension. As we mentioned above, a stabilizer in general position for this representation is isomorphic to H. By Theorem 1.2,

$$\mathrm{ed}(N'; 2) = \dim(V_{4n}) + \mathrm{rank}(H) - \dim(N') = 4n + 2n - 2n = 4n\,,$$

and we are done.

To prove the claim, note that $\eta(N') \leqslant 4n$ since N' has a faithful representation V_{4n} of dimension $4n$. By Lemma 9.4, in order to establish the opposite inequality, $\eta(N') \geqslant 4n$, it suffices to show that $\mathrm{SymRank}(X(T); 2) \geqslant 4n$. To prove this last inequality, we will use the same argument as in the proof of Theorem 9.1(a). Recall that $\mathrm{SymRank}(X(T); 2)$ is the minimal size of an H-invariant 2-generating set $x_1, \ldots, x_d$ of $X(T)$. The H-action on $x_1, \ldots, x_d$ induces a permutation representation $\varphi\colon H \to \mathrm{S}_d$. Once again, this representation has to be faithful. By [AG89, Theorem 2.3(b)], we have $|H| \leqslant 2^{d/2}$. In other words, $2^{2n} \leqslant 2^{d/2}$ or, equivalently, $d \geqslant 4n$, as claimed. ☐

Acknowledgements

We are grateful to Jerome Lefebvre, Mathieu Huruguen, and Mikhail Borovoi for stimulating discussions related to Conjecture 1.1 and to the anonymous referee for constructive comments.

References

AG89 M. Aschbacher and R. M. Guralnick, *On abelian quotients of primitive groups*, Proc. Amer. Math. Soc. **107** (1989), no. 1, 89–95; doi:10.2307/2048039.

Art86 M. Artin, *Néron models*, Arithmetic Geometry (Storrs, Conn., 1984) (Springer, New York, 1986), 213–230; doi:10.1007/978-1-4613-8655-1_8.

Bou89 N. Bourbaki, *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Springer-Verlag, Berlin, 1989).

BR85 P. Bardsley and R. W. Richardson, *Étale slices for algebraic transformation groups in characteristic p*, Proc. London Math. Soc. **51** (1985), no. 2, 295–317; doi:10.1112/plms/s3-51.2.295.

BRV10 P. Brosnan, Z. Reichstein, and A. Vistoli, *Essential dimension, spinor groups, and quadratic forms*, Ann. of Math. **171** (2010), no. 1, 533–544; doi:10.4007/annals.2010.171.533.

BRV18 ———, *Essential dimension in mixed characteristic*, Doc. Math. **23** (2018), 1587–1600; doi:10.25537/dm.2018v23.1587-1600.

CR62 C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure Appl. Math., vol. 11 (Interscience Publ., New York – London, 1962).

GR09 P. Gille and Z. Reichstein, *A lower bound on the essential dimension of a connected linear group*, Comment. Math. Helv. **84** (2009), no. 1, 189–212; doi:10.4171/CMH/158.

Jan04 J. C. Jantzen, *Nilpotent orbits in representation theory*, Lie Theory, Progr. Math., vol. 228 (Birkhäuser Boston, Boston, MA, 2004), 1–211; doi:10.1007/978-0-8176-8192-0_1.

KM08 N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508; doi:10.1007/s00222-007-0106-6.

Lan02 S. Lang, *Algebra*, 3rd ed., Grad. Texts in Math., vol. 211 (Springer-Verlag, New York, 2002); doi:10.1007/978-1-4613-0041-0.

LMMR13a R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein, *Essential dimension of algebraic tori*, J. reine angew. Math. **677** (2013), 1–13; doi:10.1515/crelle.2012.010.

LMMR13b ———, *Essential p-dimension of algebraic groups whose connected component is a torus*, Algebra Number Theory **7** (2013), no. 8, 1817–1840; doi:10.2140/ant.2013.7.1817.

Mac11 M. L. MacDonald, *Essential p-dimension of the normalizer of a maximal torus*, Transform. Groups **16** (2011), no. 4, 1143–1171; doi:10.1007/s00031-011-9157-2.

Mar15 B. Martin, *Generic stabilisers for actions of reductive groups*, Pacific J. Math. **279** (2015), no. 1-2, 397–422; doi:10.2140/pjm.2015.279.397.

Mer13 A. S. Merkurjev, *Essential dimension: a survey*, Transform. Groups **18** (2013), no. 2, 415–481; doi:10.1007/s00031-013-9216-y.

MR09 A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra Number Theory **3** (2009), no. 4, 467–487; doi:10.2140/ant.2009.3.467.

PV94 V. L. Popov and E. B. Vinberg, *Invariant theory*, Algebraic Geometry IV, Encyclopaedia Math. Sci., vol. 55 (Springer, Berlin – Heidelberg, 1994), 123–278; doi:10.1007/978-3-662-03073-8_2.

Rei10 Z. Reichstein, *Essential dimension*, Proceedings of the ICM (2010), vol. 2 (Hindustan Book Agency, New Delhi, 2010), 162–188; doi:10.1142/9789814324359_0045.

Ric72 R. W. Richardson, Jr., *Deformations of Lie subgroups and the variation of isotropy subgroups*, Acta Math. **129** (1972), 35–73; doi:10.1007/BF02392213.

RY00 Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties (with an appendix by János Kollár and Endre Szabó)*, Canad. J. Math. **52** (2000), no. 5, 1018–1056; doi:10.4153/CJM-2000-043-5.

Ser97 J.-P. Serre, *Galois cohomology* (Springer-Verlag, Berlin, 1997); doi:10.1007/978-3-642-59141-9.

Zinovy Reichstein reichst@math.ubc.ca
Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada

Federico Scavia scavia@math.ubc.ca
Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada