

# *Algebra & Number Theory*

Volume 7

2013

No. 8

**Essential  $p$ -dimension of algebraic groups whose  
connected component is a torus**

Roland Löttscher, Mark MacDonald, Aurel Meyer and Zinovy Reichstein





# Essential $p$ -dimension of algebraic groups whose connected component is a torus

Roland Löttscher, Mark MacDonald, Aurel Meyer and Zinovy Reichstein

Following up on our earlier work and the work of N. Karpenko and A. Merkurjev, we study the essential  $p$ -dimension of linear algebraic groups  $G$  whose connected component  $G^0$  is a torus.

## 1. Introduction

Let  $p$  be a prime integer and  $k$  a base field of characteristic not equal to  $p$ . In this paper, we will study the essential  $p$ -dimension of linear algebraic  $k$ -groups  $G$  whose connected component  $G^0$  is an algebraic torus. This is a natural class of groups; for example, normalizers of maximal tori in reductive linear algebraic groups are of this form. This paper is a sequel to [Löttscher et al. 2013], where  $G$  was assumed to be of multiplicative type. For background material and further references on the notion of essential dimension, see [Reichstein 2011].

For the purpose of computing  $\text{ed}(G; p)$ , we may replace the base field  $k$  by any field extension whose degree is finite and prime to  $p$ . (We will sometimes refer to such field extensions as *prime-to- $p$  extensions*.) In particular, after passing to a suitable prime-to- $p$  extension of  $k$ , we may assume that  $k$  contains a primitive  $p$ -th root of unity  $\zeta_p$  and that there is a field extension  $l/k$  whose degree is a power of  $p$  such that (i) the torus  $T := G^0$  becomes split and (ii) the étale group  $G/G^0$  becomes constant over  $l$ . In this situation, the finite group  $G/G^0$  has a Sylow  $p$ -subgroup  $F$  defined over  $k$ ; see [Löttscher et al. 2013, Remark 7.2]. Since  $G$  is smooth, we may replace  $G$  by the preimage of  $F$  without changing its essential  $p$ -dimension; see [Meyer and Reichstein 2009, Lemma 4.1]. It is thus natural to restrict our attention to the case where  $F := G/G^0$  is a finite  $p$ -group. In view of this, we will make the

---

Löttscher is partially supported by the Deutsche Forschungsgemeinschaft, GI 706/2-1. MacDonald is partially supported by a postdoctoral fellowship from the Canadian National Science and Engineering Research Council (NSERC). Meyer is supported by a postdoctoral fellowship from the Swiss National Science Foundation. Reichstein is partially supported by a Discovery grant from the Canadian NSERC.

*MSC2010:* 20G15, 11E72.

*Keywords:* essential dimension, algebraic torus, twisted finite group, generically free representation.

following assumptions on  $k$  and  $G$  for the remainder of this section and throughout much of the rest of the paper:

**Notational conventions 1.1.** Unless otherwise specified,  $k$  will denote a field of characteristic not equal to  $p$  containing a primitive  $p$ -th root of unity  $\zeta_p$ , and  $G$  will denote an algebraic  $k$ -group that fits into an exact sequence

$$1 \rightarrow T \rightarrow G \xrightarrow{\pi} F \rightarrow 1 \quad (1-1)$$

of  $k$ -groups, where  $T := G^0$  is a torus and  $F := G/G^0$  is a finite  $p$ -group. Moreover, we will assume that there is a field extension of  $k$  of  $p$ -power degree over which  $T$  becomes split and  $F$  becomes constant. Note that  $F$  may be twisted (i.e., nonconstant) and  $T$  may be nonsplit over  $k$ . The extension (1-1) is not assumed to be split (not even over the algebraic closure of  $k$ ).

To state our main result, we recall that a linear representation  $\rho : G \rightarrow \mathrm{GL}(V)$  is called *generically free* if there exists a  $G$ -invariant dense open subset  $U \subseteq V$  such that the scheme-theoretic stabilizer of every point of  $U$  is trivial. We will say that  $\rho$  is  *$p$ -faithful* if  $\ker \rho$  is finite of order prime to  $p$ . We will say that  $\rho$  is  *$p$ -generically free* if it is  $p$ -faithful and gives rise to a generically free representation of  $G/\ker \rho$ .

A generically free representation is faithful, but a faithful representation may not be generically free. This phenomenon is not well understood; there is no classification of such representations, and we do not even know for which groups  $G$  they occur.<sup>1</sup> It is, however, the source of many of the subtleties we will encounter.

**Theorem 1.2.** *Let  $G$  be an algebraic  $k$ -group satisfying Conventions 1.1. Then*

$$\min \dim \rho - \dim G \leq \mathrm{ed}(G; p) \leq \min \dim \mu - \dim G,$$

where the minima are taken respectively over all  $p$ -faithful representations  $\rho$  of  $G$  and  $p$ -generically free representations  $\mu$  of  $G$ .

As a simple example, let  $k = \mathbb{C}$ ,  $p = 2$  and  $G = \mathrm{O}_2 \simeq \mathrm{SO}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$  be the group of  $2 \times 2$  orthogonal matrices, where  $G^0 = \mathrm{SO}_2 \simeq \mathbb{G}_m$  is a one-dimensional torus. The natural representation  $i : G \hookrightarrow \mathrm{GL}_2$  is faithful but not generically free: if  $a^2 + b^2 \neq 0$ , then the stabilizer of  $v = (a, b) \in \mathbb{C}^2$  is the subgroup of  $G = \mathrm{O}_2$  of order 2 generated by the reflection in the line spanned by  $v$ . It is easy to see that no two-dimensional representation of  $\mathrm{O}_2$  is 2-generically free, but the three-dimensional representation  $i \oplus \det$  is generically free. (Here  $\det : \mathrm{O}_2 \rightarrow \mathrm{GL}_1$  is the determinant.) Theorem 1.2 thus yields  $1 \leq \mathrm{ed}(\mathrm{O}_2; 2) \leq 2$ . The true value of  $\mathrm{ed}(\mathrm{O}_2; 2)$  is 2; see [Reichstein 2000, Theorem 10.3].

In general, let us denote the difference between the upper and lower bounds of Theorem 1.2 by  $\mathrm{gap}(G; p)$ . If  $G = G^0$  is a torus or  $G = F$  is a finite  $p$ -group, then

<sup>1</sup>Faithful representations that are not generically free are better understood for connected semisimple groups; see [Vinberg and Popov 1994, Section 7].

$\text{gap}(G; p) = 0$  (see [Löttscher et al. 2013, Lemma 2.5; Meyer and Reichstein 2009, Remark 2.1]), and Theorem 1.2 reduces to [Löttscher et al. 2013, Theorems 1.1 and 7.1], respectively. (The case where  $G = F$  is a constant finite  $p$ -group is due to Karpenko and Merkurjev [2008], whose work was the starting point for both [Löttscher et al. 2013] and the present paper.) We will show that the upper and lower bounds of Theorem 1.2 coincide for a larger class of groups, which we call *tame*; see Definition 7.3 and Corollary 7.4. More generally, we will show:

**Theorem 1.3.** *Let  $G$  be an algebraic  $k$ -group satisfying Conventions 1.1. Then  $\text{gap}(G; p) \leq \dim T - \dim T^{C(F)}$ .*

Here  $C(F)$  is the central  $p$ -subgroup of  $F$  defined in Section 4, the  $F$ -action on  $T$  is induced by conjugation in  $G$ , and  $T^{C(F)} \subseteq T$  denotes the subgroup of elements fixed by  $C(F)$ .

Our second main result about  $\text{gap}(G; p)$  is the following “additivity theorem”:

**Theorem 1.4.** *Let  $G_1$  and  $G_2$  be algebraic  $k$ -groups satisfying Conventions 1.1. If  $\text{gap}(G_1; p) = \text{gap}(G_2; p) = 0$ , then  $\text{gap}(G_1 \times G_2; p) = 0$ , and  $\text{ed}(G_1 \times G_2; p) = \text{ed}(G_1; p) + \text{ed}(G_2; p)$ .*

The rest of this paper is structured as follows. In Section 2, we discuss the notion of  $p$ -special closure  $k^{(p)}$  of a field  $k$  and show that passing from  $k$  to  $k^{(p)}$  does not change the essential  $p$ -dimension of any  $k$ -group. In Section 3, we show that if  $A \rightarrow B$  is an isogeny of degree prime to  $p$ , then  $A$  and  $B$  have the same essential  $p$ -dimension. Sections 4, 5 and 6 are devoted to the proof of our main Theorem 1.2. In Section 7, we introduce the class of tame groups and show that for these groups the upper and the lower bounds of Theorem 1.2 coincide. In Section 8, we prove Theorem 1.3, and in Section 9, we prove Theorem 1.4. In Section 10, we classify central extensions (1-1) with  $G$  of small essential  $p$ -dimension.

## 2. The $p$ -special closure of a field

Let  $K$  be an arbitrary field and  $p$  be a prime integer. We will denote the algebraic and separable closures of  $K$  by  $K_{\text{alg}}$  and  $K_{\text{sep}}$ , respectively. Recall that  $K$  is called  *$p$ -special* if the degree of every finite extension of  $K$  is a power of  $p$ .

**Lemma 2.1.** *A field  $K$  is  $p$ -special if and only if it has no nontrivial prime-to- $p$  extensions.*

*Proof.* We need to show that if  $K$  has no nontrivial prime-to- $p$  extensions, then the degree of every finite extension  $L/K$  is a power of  $p$ . After passing to the normal closure, we may assume that  $L$  is normal over  $K$ . Now  $L/K$  is generated by a separable extension  $L_s/K$  and a purely inseparable extension  $L_i/K$ ; see [Lang 1965, Proposition VII.7.12]. Hence, it suffices to show that  $[L : K]$  is a power of  $p$  if (i)  $L/K$  is separable or (ii)  $L/K$  is purely inseparable.

(i) As above, we may assume that  $L/K$  is normal, i.e., Galois. Let  $\Gamma_p$  be a  $p$ -Sylow subgroup of  $\Gamma = \text{Gal}(L/K)$ . Then  $L^{\Gamma_p}/K$  is a prime-to- $p$  extension. Hence,  $L^{\Gamma_p} = K$ , i.e.,  $\Gamma = \Gamma_p$ , and  $[L : K] = |\Gamma|$  is a power of  $p$ .

(ii) If  $\text{char}(K) \neq p$ , a purely inseparable extension  $L/K$  is prime-to- $p$  and hence trivial. If  $\text{char}(K) = p$ , then  $[L : K]$  is a power of  $p$ . □

By [Elman et al. 2008, Proposition 101.16] for every field  $K$ , there exists an algebraic field extension  $L/K$  such that  $L$  is  $p$ -special and every finite subextension of  $L/K$  has degree prime to  $p$ . Such a field  $L$  is called a  $p$ -special closure of  $K$  and will be denoted by  $K^{(p)}$ .

The following properties of  $p$ -special closures will be important for us in the sequel:

**Lemma 2.2.** *Let  $K$  be a field and  $K_{\text{alg}}$  an algebraic closure of  $K$  containing  $K^{(p)}$ .*

- (a)  $K^{(p)}$  is a direct limit of prime-to- $p$  extensions  $K_i/K$ .
- (b) The field  $K^{(p)}$  is perfect if  $\text{char } K \neq p$ .
- (c) Suppose  $\text{char } K \neq p$ . For any prime  $q \neq p$ , the cohomological  $q$ -dimension of  $\Psi = \text{Gal}(K_{\text{alg}}/K^{(p)})$  is  $\text{cd}_q(\Psi) = 0$ .

*Proof.* (a) The finite subextensions  $K'/K$  of  $K^{(p)}/K$  form a direct system with limit  $K^{(p)}$ . (b) Every finite extension of  $K^{(p)}$  has  $p$ -power degree and is therefore separable. (c) By construction,  $\Psi$  is a profinite  $p$ -group. The result follows from [Serre 2002, Corollary 2, I.3]. □

Let  $l$  be a base field,  $\text{Fields}/l$  be the category of field extensions of  $l$  and  $\text{Sets}$  be the category of sets. We call a covariant functor  $\mathcal{F} : \text{Fields}/l \rightarrow \text{Sets}$  *limit-preserving* if, for any directed system of fields  $\{K_i\}$ ,  $\mathcal{F}(\varinjlim K_i) = \varinjlim \mathcal{F}(K_i)$ . For example, if  $A$  is an algebraic group, the functor  $\mathcal{F}(K) = H^1(K, A)$  is limit-preserving; see [Margaux 2007, 2.1].

**Lemma 2.3.** *Let  $\mathcal{F}$  be limit-preserving and  $\alpha \in \mathcal{F}(K)$  an object. Denote the image of  $\alpha$  in  $\mathcal{F}(K^{(p)})$  by  $\alpha_{K^{(p)}}$ . Then:*

- (a)  $\text{ed}_{\mathcal{F}}(\alpha; p) = \text{ed}_{\mathcal{F}}(\alpha_{K^{(p)}}; p) = \text{ed}_{\mathcal{F}}(\alpha_{K^{(p)}})$ .
- (b)  $\text{ed}(\mathcal{F}; p) = \text{ed}(\mathcal{F}_{l^{(p)}}; p)$ , where  $\mathcal{F}_{l^{(p)}} : \text{Fields}/l^{(p)} \rightarrow \text{Sets}$  denotes the restriction of  $\mathcal{F}$  to  $\text{Fields}/l^{(p)}$ .

*Proof.* (a) It is clear that  $\text{ed}_{\mathcal{F}}(\alpha; p) \geq \text{ed}_{\mathcal{F}}(\alpha_{K^{(p)}}; p) = \text{ed}_{\mathcal{F}}(\alpha_{K^{(p)}})$  for any functor  $\mathcal{F}$ . It remains to prove  $\text{ed}_{\mathcal{F}}(\alpha; p) \leq \text{ed}_{\mathcal{F}}(\alpha_{K^{(p)}})$ . If  $L/K$  is finite of degree prime to  $p$ ,

$$\text{ed}_{\mathcal{F}}(\alpha; p) = \text{ed}_{\mathcal{F}}(\alpha_L; p); \tag{2-1}$$

cf. [Merkurjev 2009, Proposition 1.5] and its proof. For the  $p$ -special closure  $K^{(p)}$ , this is similar and uses (2-1) repeatedly.

Suppose there is a subfield  $K_0 \subseteq K^{(p)}$  and  $\alpha_{K^{(p)}}$  comes from an element  $\beta \in \mathcal{F}(K_0)$  so that  $\beta_{K^{(p)}} = \alpha_{K^{(p)}}$ . Write  $K^{(p)} = \varinjlim \mathcal{L}$ , where  $\mathcal{L}$  is a direct system of finite prime-to- $p$  extensions of  $K$ . Then  $K_0 = \varinjlim \mathcal{L}_0$  with  $\mathcal{L}_0 = \{L \cap K_0 \mid L \in \mathcal{L}\}$ , and by assumption on  $\mathcal{F}$ , we have  $\mathcal{F}(K_0) = \varinjlim_{L' \in \mathcal{L}_0} \mathcal{F}(L')$ .

Thus, there is a field  $L' = L \cap K_0$  ( $L \in \mathcal{L}$ ) and  $\gamma \in \mathcal{F}(L')$  such that  $\gamma_{K_0} = \beta$ . Since  $\alpha_L$  and  $\gamma_L$  become equal over  $K^{(p)}$ , after possibly passing to a finite extension, we may assume they are equal over  $L$ , which is finite of degree prime to  $p$  over  $K$ . Combining these constructions with (2-1), we see that

$$\text{ed}_{\mathcal{F}}(\alpha; p) = \text{ed}_{\mathcal{F}}(\alpha_L; p) = \text{ed}_{\mathcal{F}}(\gamma_L; p) \leq \text{ed}_{\mathcal{F}}(\gamma_L) \leq \text{trdeg}_l K_0.$$

This proves  $\text{ed}_{\mathcal{F}}(\alpha; p) \leq \text{ed}_{\mathcal{F}}(\alpha_{K^{(p)}})$  since  $K_0$  was an arbitrary field of definition for  $\alpha_{K^{(p)}}$ .

(b) This follows directly from (a) by taking  $\alpha$  of maximal essential  $p$ -dimension.  $\square$

**Proposition 2.4.** *Let  $l$  be an arbitrary field,*

$$\mathcal{F}, \mathcal{G} : \text{Fields} / l \rightarrow \text{Sets}$$

*be limit-preserving functors and  $\mathcal{F} \rightarrow \mathcal{G}$  be a natural transformation. If the map  $\mathcal{F}(K) \rightarrow \mathcal{G}(K)$  is bijective or surjective for any  $p$ -special field containing  $l$ , then, respectively,*

$$\text{ed}(\mathcal{F}; p) = \text{ed}(\mathcal{G}; p) \quad \text{or} \quad \text{ed}(\mathcal{F}; p) \geq \text{ed}(\mathcal{G}; p).$$

*Proof.* Assume the maps are surjective. By Lemma 2.2(a), the natural transformation is  $p$ -surjective in the terminology of [Merkurjev 2009], so we can apply [Merkurjev 2009, Proposition 1.5] to conclude  $\text{ed}(\mathcal{F}; p) \geq \text{ed}(\mathcal{G}; p)$ .

Now assume the maps are bijective. Let  $\alpha$  be in  $\mathcal{F}(K)$  for some  $K/l$  and  $\beta$  its image in  $\mathcal{G}(K)$ . We claim that  $\text{ed}(\alpha; p) = \text{ed}(\beta; p)$ . First by Lemma 2.3, we may assume that  $K$  is  $p$ -special. In this situation, it is enough to prove that  $\text{ed}(\alpha) \leq \text{ed}(\beta)$  (the opposite inequality is by functoriality).

Assume that  $\beta$  comes from  $\beta_0 \in \mathcal{G}(K_0)$  for some field  $l \subseteq K_0 \subseteq K$ . Let  $K'_0$  denote the algebraic closure of  $K_0$  in  $K$ . Any finite prime-to- $p$  extension of  $K'_0$  is isomorphic (over  $K'_0$ ) to a subfield of  $K$  (cf. [Merkurjev 2009, Lemma 6.1]) and hence coincides with  $K'_0$ . Thus,  $K'_0$  has no nontrivial prime-to- $p$  extensions. By Lemma 2.1, it follows that  $K'_0$  is  $p$ -special. Since  $K'_0$  is an algebraic extension of  $K_0$ , we may replace  $K_0$  by  $K'_0$  and thus assume that  $K_0$  is  $p$ -special. By assumption,  $\mathcal{F}(K_0) \rightarrow \mathcal{G}(K_0)$  and  $\mathcal{F}(K) \rightarrow \mathcal{G}(K)$  are bijective; therefore, the unique element  $\alpha_0 \in \mathcal{F}(K_0)$  that maps to  $\beta_0$  must map to  $\alpha$  under the natural restriction map. The claim follows.

We obtain  $\text{ed}(\mathcal{F}; p) = \text{ed}(\alpha; p) = \text{ed}(\beta; p) \leq \text{ed}(\mathcal{G}; p)$  by taking  $\alpha$  of maximal essential  $p$ -dimension.  $\square$

### 3. Isogenies

An isogeny of algebraic groups is a surjective morphism  $A \rightarrow B$  with finite kernel. The degree of an isogeny is the order of its kernel.

**Proposition 3.1.** *Suppose  $A \rightarrow B$  is an isogeny of degree prime to  $p$  of smooth algebraic groups over a field  $l$  of characteristic not equal to  $p$ . Then*

- (a) *for any  $p$ -special field  $K$  containing  $k$ , the natural map  $H^1(K, A) \rightarrow H^1(K, B)$  is bijective and*
- (b)  $\text{ed}(A; p) = \text{ed}(B; p)$ .

**Example 3.2.** Let  $E_6^{\text{sc}}$  and  $E_7^{\text{sc}}$  be simply connected simple groups of type  $E_6$  and  $E_7$ , respectively. In [Gille and Reichstein 2009, 9.4 and 9.6], it is shown that if  $k$  is an algebraically closed field of characteristic not equal to 2 and 3, respectively, then

$$\text{ed}(E_6^{\text{sc}}; 2) = 3 \quad \text{and} \quad \text{ed}(E_7^{\text{sc}}; 3) = 3.$$

For the adjoint groups  $E_6^{\text{ad}} = E_6^{\text{sc}}/\mu_3$  and  $E_7^{\text{ad}} = E_7^{\text{sc}}/\mu_2$ , we therefore have

$$\text{ed}(E_6^{\text{ad}}; 2) = 3 \quad \text{and} \quad \text{ed}(E_7^{\text{ad}}; 3) = 3.$$

For the proof of Proposition 3.1, we will need a lemma.

**Lemma 3.3.** *Let  $N$  be a finite algebraic group over a field  $l$  of characteristic not equal to  $p$ . The following are equivalent:*

- (a)  *$p$  does not divide the order of  $N$ .*
- (b)  *$p$  does not divide the order of  $N(l_{\text{alg}})$ .*

*Proof.* Let  $N^0$  be the connected component of  $N$  and  $N^{\text{ét}} = N/N^0$  the étale quotient. Recall that the order of a finite algebraic group  $N$  over  $l$  is defined as  $|N| = \dim_l l[N]$  and  $|N| = |N^0||N^{\text{ét}}|$ ; see, e.g., [Tate 1997]. If  $\text{char } l = 0$ ,  $N^0$  is trivial; if  $\text{char } l = q \neq p$  is positive,  $|N^0|$  is a power of  $q$ . Hence,  $N$  is of order prime to  $p$  if and only if the étale algebraic group  $N^{\text{ét}}$  is. Since  $N^0$  is connected and finite,  $N^0(l_{\text{alg}}) = \{1\}$ , so  $N(l_{\text{alg}})$  is of order prime to  $p$  if and only if the group  $N^{\text{ét}}(l_{\text{alg}})$  is. Then  $|N^{\text{ét}}| = \dim_l l[N^{\text{ét}}] = |N^{\text{ét}}(l_{\text{alg}})|$ ; cf. [Bourbaki 1990, V.29 Corollary].  $\square$

*Proof of Proposition 3.1.* (a) Let  $N$  be the kernel of the isogeny  $A \rightarrow B$  and  $K$  be a  $p$ -special field over  $l$ . Since  $K_{\text{sep}} = K_{\text{alg}}$  (see Lemma 2.2(b)), the sequence of  $K_{\text{sep}}$ -points  $1 \rightarrow N(K_{\text{sep}}) \rightarrow A(K_{\text{sep}}) \rightarrow B(K_{\text{sep}}) \rightarrow 1$  is exact. By Lemma 3.3, the order of  $N(K_{\text{sep}})$  is not divisible by  $p$  and therefore coprime to the order of any finite quotient of  $\Psi = \text{Gal}(K_{\text{sep}}/K)$ . By [Serre 2002, I.5, Exercise 2], this implies that  $H^1(K, N) = \{1\}$ . Similarly, if  ${}_cN$  is the group  $N$  twisted by a cocycle  $c : \Psi \rightarrow A$ , then  ${}_cN(K_{\text{sep}}) = N(K_{\text{sep}})$  is of order prime to  $p$ , and  $H^1(K, {}_cN) = \{1\}$ . It follows that  $H^1(K, A) \rightarrow H^1(K, B)$  is injective; cf. [Serre 2002, I.5.5].



Surjectivity is a consequence of [Serre 2002, I, Proposition 46] and the fact that the  $q$ -cohomological dimension of  $\Psi$  is 0 for any divisor  $q$  of  $|N(K_{\text{sep}})|$  (Lemma 2.2(c)).

(b) This part follows from (a) and Proposition 2.4. □

#### 4. Proof of the main theorem: an overview

We now assume that Conventions 1.1 are valid. The upper bound in Theorem 1.2 is an easy consequence of Proposition 3.1. Indeed, suppose  $\mu : G \rightarrow \text{GL}(V)$  is a  $p$ -generically free representation. That is,  $\ker \mu$  is a finite group of order prime to  $p$ , and  $\mu$  descends to a generically free representation of  $G' := G / \ker \mu$ . By Proposition 3.1,  $\text{ed}(G; p) = \text{ed}(G'; p)$ . On the other hand,

$$\text{ed}(G'; p) \leq \text{ed}(G') \leq \dim \mu - \dim G' = \dim \mu - \dim G;$$

see [Berhuy and Favi 2003, Lemma 4.11; Merkurjev 2009, Corollary 4.2]. This completes the proof of the upper bound in Theorem 1.2.

The rest of this section will be devoted to outlining a proof of the lower bound of Theorem 1.2. The details (namely, the proofs of Propositions 4.2 and 4.3) will be supplied in the next two sections. The starting point of our argument is [Löttscher et al. 2013, Theorem 3.1], which we reproduce below for the reader's convenience:

**Theorem 4.1.** *Consider an exact sequence of algebraic groups over a field*

$$1 \rightarrow C \rightarrow H \rightarrow Q \rightarrow 1$$

*such that  $C$  is central in  $H$  and is isomorphic to  $\mu_p^r$  for some  $r \geq 0$ . Given a character  $\chi : C \rightarrow \mu_p$ , denote by  $\text{Rep}^\chi$  the class of irreducible representations  $\phi : H \rightarrow \text{GL}(V)$  such that  $\phi(c) = \chi(c) \text{Id}$  for every  $c \in C$ .*

*Assume further that*

$$\text{gcd}\{\dim \phi \mid \phi \in \text{Rep}^\chi\} = \min\{\dim \phi \mid \phi \in \text{Rep}^\chi\} \tag{4-1}$$

*for every character  $\chi : C \rightarrow \mu_p$ . Then*

$$\text{ed}(H; p) \geq \min \dim \psi - \dim H,$$

*where the minimum is taken over all finite-dimensional representations  $\psi$  of  $H$  such that  $\psi|_C$  is faithful.*

To prove the lower bound of Theorem 1.2, we will apply Theorem 4.1 to the exact sequence

$$1 \rightarrow C(G) \rightarrow G \rightarrow Q \rightarrow 1, \tag{4-2}$$

where  $C(G)$  is a central subgroup of  $G$  defined as follows. Recall from [Löttscher et al. 2013, Section 2] that if  $A$  is a  $k$ -group of multiplicative type,  $\text{Split}_k(A)$  is

defined as the maximal split  $k$ -subgroup of  $A$ . That is, if  $X(A)$  is the character  $\text{Gal}(k_{\text{sep}}/k)$ -module of  $A$ , then the character module of  $\text{Split}_k(A)$  is defined as the largest quotient of  $X(A)$  with trivial  $\text{Gal}(k_{\text{sep}}/k)$ -action.

We denote by  $Z(G)[p]$  the  $p$ -torsion subgroup of the center  $Z(G)$ . Note that  $Z(G)$  is a commutative group, which is an extension of a  $p$ -group by a group of multiplicative type. Since  $\text{char } k \neq p$ , it follows that  $Z(G)$  is of multiplicative type. We now define  $C(G) := \text{Split}_k(Z(G)[p])$ .

In order to show that Theorem 4.1 can be applied to the sequence (4-2), we need to check that condition (4-1) is satisfied. This is a consequence of the following proposition, which will be proved in the next section:

**Proposition 4.2.** *The dimension of every irreducible representation of  $G$  over  $k$  is a power of  $p$ .*

Applying Theorem 4.1 to the exact sequence (4-2) now yields

$$\text{ed}(G; p) \geq \min \dim \rho - \dim G,$$

where the minimum is taken over all representations  $\rho : G \rightarrow \text{GL}(V)$  such that  $\rho|_{C(G)}$  is faithful. This resembles the lower bound of Theorem 1.2; the only difference is that in the statement of Theorem 1.2 we take the minimum over  $p$ -faithful representations  $\rho$  and here we only ask that  $\rho|_{C(G)}$  should be faithful. The following proposition shows that the two bounds are, in fact, the same, thus completing the proof of Theorem 1.2:

**Proposition 4.3.** *A finite-dimensional representation  $\rho$  of  $G$  is  $p$ -faithful if and only if  $\rho|_{C(G)}$  is faithful.*

We will prove Proposition 4.3 in Section 6.

**Remark 4.4.** The inequality  $\min \dim \rho - \dim G \leq \text{ed}(G; p)$  of Theorem 1.2, where  $\rho$  ranges over all  $p$ -faithful representations of  $G$ , fails if we take the minimum over just the faithful (rather than  $p$ -faithful) representations, even in the case where  $G = T$  is a torus.

Indeed, choose  $T$  so that the  $\text{Gal}(k_{\text{sep}}/k)$ -character lattice  $X(T)$  of  $T$  is a direct summand of a permutation lattice, but  $X(T)$  itself is not permutation (see [Colliot-Thélène and Sansuc 1977, 8A] for an example of such a lattice).

In other words, there exists a  $k$ -torus  $T'$  such that  $T \times T'$  is quasisplit (but  $T$  is not). This implies that  $H^1(K, T \times T') = \{1\}$  and thus  $H^1(K, T) = \{1\}$  for any field extension  $K/k$ . Consequently,  $\text{ed}(T; p) = 0$  for every prime  $p$ .

On the other hand, we claim that the dimension of the minimal faithful representation of  $T$  is strictly bigger than  $\dim T$ . Assume the contrary. Then there exists a surjective homomorphism  $f : P \rightarrow X(T)$  of  $\text{Gal}(k_{\text{sep}}/k)$ -lattices, where  $P$  is permutation and  $\text{rank } P = \dim T$ ; see, e.g., [Lötscher et al. 2013, Lemma 2.6]. This

implies that  $f$  has finite kernel and hence is injective. We conclude that  $f$  is an isomorphism, so  $X(T)$  is a permutation  $\text{Gal}(k_{\text{sep}}/k)$ -lattice, a contradiction.  $\square$

### 5. Dimensions of irreducible representations

The purpose of this section is to prove Proposition 4.2.

**Lemma 5.1.** *Let  $H$  be a finite  $p$ -subgroup of  $G$  defined over  $k$ . Then  $H$  becomes constant after some field extension of  $k$  whose degree is a power of  $p$ .*

Recall that here  $G$  and  $k$  are subject to Conventions 1.1.

*Proof.* After passing to a suitable  $p$ -power field extension of  $k$ , the torus  $T$  becomes split, and  $F$  becomes constant. In other words, we may assume that  $T \cap H$  is split and the image  $\pi(H)$  of  $H$  in  $F$  is constant. Moreover, after adjoining a primitive root of unity of order  $p^m := |T \cap H|$ , we may assume that  $T \cap H$  is constant (note that  $[k(\zeta_{p^m}) : k]$  is a power of  $p$  since  $k$  is assumed to contain  $\zeta_p$ ). Thus,  $H$  is an extension of a constant  $p$ -group  $\pi(H)$  by a constant  $p$ -group  $T \cap H$ . The group  $H$  becomes constant after a  $p$ -power field extension if and only if the image of  $\Gamma$  in  $\text{Aut}(H(k_{\text{sep}}))$  is a  $p$ -group. Thus, it suffices to establish the following claim:

**Claim.** Let  $B$  be a  $p$ -group,  $S$  a finite subgroup of  $\text{Aut}(B)$  and  $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$  an  $S$ -equivariant exact sequence with  $S$  acting trivially on  $A$  and  $C$ . Then  $S$  is a  $p$ -group.

To prove the claim, assume the contrary. Then  $S$  contains a subgroup of prime order  $q \neq p$ . After replacing  $S$  by that subgroup, we may assume without loss of generality that  $|S| = q$ . Let  $b \in B$ . Then the image of  $b$  in  $C$  is fixed under  $S$ . Hence, the fiber  $Ab$  over this element is  $S$ -stable. Since the cardinality of  $Ab$  is a power of  $p$  and thus is not divisible by  $q$ ,  $S$  has to fix some elements of  $Ab$ . Denote one of these elements by  $b_0$ . Then  $b \in Ab_0$ , and since the elements of  $A$  are fixed by  $S$ , this implies that  $b$  is fixed by  $S$  as well. This shows that  $S$  acts trivially on  $B$ , a contradiction.  $\square$

The special case of Proposition 4.2, where  $T = \{1\}$ , i.e.,  $G = F$  is a finite  $p$ -group that becomes constant after a  $p$ -power field extension, is established in the course of the proof of [Löttscher et al. 2013, Theorem 7.1]. Our proof of Proposition 4.2 below is based on leveraging this case as follows.

**Lemma 5.2.** *Let  $H$  be a smooth algebraic group defined over a field  $l$  and*

$$H_1 \subseteq H_2 \subseteq \dots \subseteq H$$

*be an ascending sequence of smooth  $l$ -subgroups whose union  $\bigcup_{n \geq 1} H_n$  is Zariski dense in  $H$ . If  $\rho : H \rightarrow \text{GL}(V)$  is an irreducible representation of  $H$ , then  $\rho|_{H_i}$  is irreducible for sufficiently large integers  $i$ .*

*Proof.* For each  $d = 1, \dots, \dim V - 1$ , consider the  $H$ -action on the Grassmannian  $\text{Gr}(d, V)$  of  $d$ -dimensional subspaces of  $V$ . Let  $X^{(d)} = \text{Gr}(d, V)^H$  and  $X_i^{(d)} = \text{Gr}(d, V)^{H_i}$  be the subvarieties of  $d$ -dimensional  $H$ - and  $H_i$ -invariant subspaces of  $V$ , respectively. Then  $X_1^{(d)} \supseteq X_2^{(d)} \supseteq \dots$ , and since the union of the groups  $H_i$  is dense in  $H$ ,

$$X^{(d)} = \bigcap_{i \geq 0} X_i^{(d)}.$$

By the Noetherian property of  $\text{Gr}(d, V)$ , we have  $X^{(d)} = X_{m_d}^{(d)}$  for some  $m_d \geq 0$ .

Since  $V$  does not have any  $H$ -invariant  $d$ -dimensional  $l$ -subspaces, we know that  $X^{(d)}(l) = \emptyset$ . Thus,  $X_{m_d}^{(d)}(l) = \emptyset$ , i.e.,  $V$  does not have any  $H_{m_d}$ -invariant  $d$ -dimensional  $l$ -subspaces. Setting  $m := \max\{m_1, \dots, m_{\dim V - 1}\}$ , we see that  $\rho|_{H_i}$  is irreducible for any  $i \geq m$ . □

We now proceed with the proof of Proposition 4.2. By Lemmas 5.1 and 5.2, it suffices to construct a sequence of finite  $p$ -subgroups

$$F_1 \subseteq F_2 \subseteq \dots \subseteq G$$

defined over  $k$  whose union  $\bigcup_{n \geq 1} F_n$  is Zariski dense in  $G$ . In fact, it suffices to construct one  $p$ -subgroup  $F' \subseteq G$  defined over  $k$  such that  $F'$  surjects onto  $F$ . Once  $F'$  is constructed, we can define  $F_i \subseteq G$  as the subgroup generated by  $F'$  and  $T[p^i]$  for every  $i \geq 0$ . Here  $T[m]$  denotes the  $m$ -torsion subgroup of  $T$ . Since  $\bigcup_{n \geq 1} F_n$  contains both  $F'$  and  $T[p^i]$  for every  $i \geq 0$ , it is Zariski dense in  $G$ , as desired.

The following lemma, which establishes the existence of  $F'$ , is thus the final step in our proof of Proposition 4.2:

**Lemma 5.3.** *Let  $1 \rightarrow T \rightarrow G \xrightarrow{\pi} F \rightarrow 1$  be an extension of a  $p$ -group  $F$  by a torus  $T$  over an arbitrary field  $k$ . Then  $G$  has a  $p$ -subgroup  $F'$  with  $\pi(F') = F$ .*

Here  $G$  and  $k$  are not subject to Conventions 1.1. In the case where  $F$  is split and  $k$  is algebraically closed, the above lemma is proved in [Chernousov et al. 2006, page 564]; cf. also the proof of [Borel and Serre 1964, Lemme 5.11].

*Proof.* Denote by  $\widetilde{\text{Ex}}^1(F, T)$  the group of equivalence classes of extensions of  $F$  by  $T$ . We claim that  $\widetilde{\text{Ex}}^1(F, T)$  is torsion. Let  $\text{Ex}^1(F, T) \subseteq \widetilde{\text{Ex}}^1(F, T)$  be the classes of extensions that have a scheme-theoretic section (i.e.,  $G(K) \rightarrow F(K)$  is surjective for all  $K/k$ ). There is a natural isomorphism  $\text{Ex}^1(F, T) \simeq H^2(F, T)$ , where  $H^2$  denotes Hochschild cohomology; see [Demazure and Gabriel 1970, III.6.2, Proposition]. By [Schneider 1981], the usual restriction-corestriction arguments can be applied in Hochschild cohomology, and in particular,  $m \cdot H^2(F, T) = 0$ , where  $m$  is the order of  $F$ . Now recall that  $M \mapsto \widetilde{\text{Ex}}^i(F, M)$  and  $M \mapsto \text{Ex}^i(F, M)$  are both derived functors of the crossed homomorphisms  $M \mapsto \text{Ex}^0(F, M)$ , where

in the first case  $M$  is in the category of  $F$ -module sheaves and in the second  $F$ -module functors, cf. [Demazure and Gabriel 1970, III.6.2]. Since  $F$  is finite and  $T$  an affine scheme, by [Schneider 1980b, Sätze 1.2 and 3.3] there is an exact sequence of  $F$ -module schemes  $1 \rightarrow T \rightarrow M_1 \rightarrow M_2 \rightarrow 1$  and an exact sequence  $\text{Ex}^0(F, M_1) \rightarrow \text{Ex}^0(F, M_2) \rightarrow \widetilde{\text{Ex}}^1(F, T) \rightarrow H^2(F, M_1) \simeq \text{Ex}^1(F, M_1)$ . The  $F$ -module sequence also induces a long exact sequence on  $\text{Ex}(F, *)$ , and we have

$$\begin{array}{ccccc}
 & & \widetilde{\text{Ex}}^1(F, T) & & \\
 & & \nearrow & & \searrow \\
 \text{Ex}^0(F, M_1) & \longrightarrow & \text{Ex}^0(F, M_2) & & \text{Ex}^1(F, M_1) \\
 & & \searrow & & \nearrow \\
 & & \text{Ex}^1(F, T) & & 
 \end{array}$$

An element in  $\widetilde{\text{Ex}}^1(F, T)$  can thus be killed first in  $\text{Ex}^1(F, M_1)$ , so it comes from  $\text{Ex}^0(F, M_2)$ . Then kill its image in  $\text{Ex}^1(F, T) \simeq H^2(F, T)$ , so it comes from  $\text{Ex}^0(F, M_1)$  and hence is zero in  $\widetilde{\text{Ex}}^1(F, T)$ . In particular, multiplying twice by the order  $m$  of  $F$ , we see that  $m^2 \cdot \widetilde{\text{Ex}}^1(F, T) = 0$ . This proves the claim.

Now let us consider the exact sequence  $1 \rightarrow N \rightarrow T \xrightarrow{\times m^2} T \rightarrow 1$ , where  $N$  is the kernel of multiplication by  $m^2$ . Clearly  $N$  is finite, and we have an induced exact sequence

$$\widetilde{\text{Ex}}^1(F, N) \rightarrow \widetilde{\text{Ex}}^1(F, T) \xrightarrow{\times m^2} \widetilde{\text{Ex}}^1(F, T),$$

which shows that the given extension  $G$  comes from an extension  $F'$  of  $F$  by  $N$ . Then  $G$  is the pushout of  $F'$  by  $N \rightarrow T$ , and we can identify  $F'$  with a subgroup of  $G$ . □

### 6. Proof of Proposition 4.3

We will prove Proposition 6.1 below; Proposition 4.3 is an immediate consequence with  $N = \ker \rho$ . Once again, please note that Conventions 1.1 are in force.

**Proposition 6.1.** *Let  $N$  be a normal  $k$ -subgroup of  $G$ . The following conditions are equivalent:*

- (a)  $N$  is finite of order prime to  $p$ .
- (b)  $N \cap C(G) = \{1\}$ .
- (c)  $N \cap Z(G)[p] = \{1\}$ .

In particular, taking  $N = G$ , we see that  $C(G) \neq \{1\}$  if  $G \neq \{1\}$ .

*Proof.* (a)  $\implies$  (b) This is obvious since  $C(G)$  is a  $p$ -group.

(b)  $\implies$  (c) Assume the contrary:  $A := N \cap Z(G)[p] \neq \{1\}$ . By Lemma 5.1,  $Z(G)[p]$  becomes constant over a field extension  $k'/k$  of  $p$ -power degree. Since  $k$  contains  $\zeta_p$ ,

the group  $Z(G)[p]$  splits over  $k'$  as a group of multiplicative type. It is shown in [Löttscher et al. 2013, Section 2] that  $C(A) \neq \{1\}$ . Thus,

$$\{1\} \neq C(A) \subseteq N \cap C(G),$$

contradicting (b).

(c)  $\implies$  (a) Our proof of this implication will rely on the following assertion:

**Claim.** Let  $M$  be a nontrivial normal finite  $p$ -subgroup of  $G$  such that the commutator  $(T, M)$  is trivial. Then  $M \cap Z(G)[p] \neq \{1\}$ .

To prove the claim, note that  $M(k_{\text{sep}})$  is nontrivial and the conjugation action of  $G(k_{\text{sep}})$  on  $M(k_{\text{sep}})$  factors through an action of the  $p$ -group  $F(k_{\text{sep}})$ . Thus, each orbit has  $p^n$  elements for some  $n \geq 0$ ; consequently, the number of fixed points is divisible by  $p$ . The intersection  $(M \cap Z(G))(k_{\text{sep}})$  is precisely the fixed point set for this action; hence,  $M \cap Z(G)[p] \neq \{1\}$ . This proves the claim.

We now continue with the proof of the implication (c)  $\implies$  (a). Assume that  $N \triangleleft G$  and  $N \cap Z(G)[p] = \{1\}$ . Applying the claim to the normal subgroup  $M := (N \cap T)[p]$  of  $G$ , we see that  $(N \cap T)[p] = \{1\}$ , i.e.,  $N \cap T$  is a finite group of order prime to  $p$ . The exact sequence

$$1 \rightarrow N \cap T \rightarrow N \rightarrow \bar{N} \rightarrow 1, \tag{6-1}$$

where  $\bar{N}$  is the image of  $N$  in  $F := G/T$ , shows that  $N$  is finite. Now observe that for every  $r \geq 1$ , the commutator  $(N, T[p^r])$  is a  $p$ -subgroup of  $N \cap T$ . Thus,  $(N, T[p^r]) = \{1\}$  for every  $r \geq 1$ . We claim that this implies  $(N, T) = \{1\}$ . If  $N$  is smooth, this is straightforward; see [Borel 1969, Proposition 2.4, page 59]. If  $N$  is not smooth, note that the map  $c : N \times T \rightarrow G$  sending  $(n, t)$  to the commutator  $ntn^{-1}t^{-1}$  descends to  $\bar{c} : \bar{N} \times T \rightarrow G$  (indeed,  $N \cap T$  clearly commutes with  $T$ ). Since  $|\bar{N}|$  is a power of  $p$  and  $\text{char}(k) \neq p$ ,  $\bar{N}$  is smooth over  $k$ , and we can pass to the separable closure  $k_{\text{sep}}$  and apply the usual Zariski density argument to show that the image of  $\bar{c}$  is trivial.

We thus conclude that  $N \cap T$  is central in  $N$ . Since  $\gcd(|N \cap T|, |\bar{N}|) = 1$ , by [Schneider 1980a, Corollary 5.4] the extension (6-1) splits, i.e.,  $N \simeq (N \cap T) \times \bar{N}$ . This turns  $\bar{N}$  into a finite  $p$ -subgroup of  $G$  with  $(T, \bar{N}) = \{1\}$ . The claim implies that  $\bar{N}$  is trivial. Hence,  $N = N \cap T$  is a finite group of order prime to  $p$ , as claimed.

This completes the proof of Proposition 6.1 and thus of Theorem 1.2. □

### 7. Tame groups

As we have seen in Section 1, some groups  $G$  satisfying Conventions 1.1 have faithful linear representations that are not generically free. In this section, we take a closer look at this phenomenon.

If  $F'$  is a subgroup of  $F$ , then we will use the notation  $G_{F'}$  to denote the subgroup  $\pi^{-1}(F')$  of  $G$ . Here  $\pi$  is the natural projection  $G \rightarrow G/T = F$  as in (1-1).

**Lemma 7.1.** *Suppose  $T$  is central in  $G$ . Then*

- (a)  $G$  has only finitely many  $k$ -subgroups  $S$  such that  $S \cap T = \{1\}$ , and
- (b) every faithful action of  $G$  on a geometrically irreducible variety  $X$  is generically free.

*Proof.* After replacing  $k$  by its algebraic closure  $k_{\text{alg}}$ , we may assume without loss of generality that  $k$  is algebraically closed.

(a) Since  $F$  has finitely many subgroups, it suffices to show that for every subgroup  $F_0 \subseteq F$ , there are only finitely many  $S \subseteq G$  such that  $\pi(S) = F_0$  and  $S \cap T = \{1\}$ .

After replacing  $G$  by  $G_{F_0}$ , we may assume that  $F_0 = F$ . In other words, we will show that  $\pi$  has at most finitely many sections  $s : F \rightarrow G$ . Fix one such section,  $s_0 : F \rightarrow G$ . Denote the exponent of  $F$  by  $e$ . Suppose  $s : F \rightarrow G$  is another section. Then for every  $f \in F(k)$ , we can write  $s(f) = s_0(f)t$  for some  $t \in T(k)$ . Since  $T$  is central in  $G$ ,  $t$  and  $s_0(f)$  commute. Since  $s(f)^e = s_0(f)^e = 1$ , we see that  $t^e = 1$ . In other words,  $t \in T(k)$  is an  $e$ -torsion element, and there are only finitely many  $e$ -torsion elements in  $T(k)$ . We conclude that there are only finitely many choices of  $s(f)$  for each  $f \in F(k)$ . Hence, there are only finitely many sections  $F \rightarrow G$ , as claimed.

(b) The restriction of the  $G$ -action on  $X$  to  $T$  is faithful and hence generically free; cf., e.g., [Lötischer 2010, Proposition 3.7(A)]. Hence, there exists a dense open  $T$ -invariant subset  $U \subseteq X$  such that  $\text{Stab}_T(u) = \{1\}$  for all  $u \in U$ . In other words, if  $S = \text{Stab}_G(u)$ , then  $S \cap T = \{1\}$ . By (a),  $G$  has finitely many nontrivial subgroups  $S$  with this property. Denote them by  $S_1, \dots, S_n$ . Since  $G$  acts faithfully,  $X^{S_i}$  is a proper closed subvariety of  $X$  for any  $i = 1, \dots, n$ . Since  $X$  is irreducible,

$$U' = U \setminus (X^{S_1} \cup \dots \cup X^{S_n})$$

is a dense open  $T$ -invariant subset of  $X$ , and the stabilizer  $\text{Stab}_G(u)$  is trivial for every  $u \in U'$ . Replacing  $U'$  by the intersection of its (finitely many)  $G(k_{\text{alg}})$ -translates, we may assume that  $U'$  is  $G$ -invariant. This shows that the  $G$ -action on  $X$  is generically free. □

**Proposition 7.2.** (a) *A faithful action of  $G$  on a geometrically irreducible variety  $X$  is generically free if and only if the action of the subgroup  $G_{C(F)} \subseteq G$  on  $X$  is generically free.*

- (b) *A  $p$ -faithful action of  $G$  on a geometrically irreducible variety  $X$  is  $p$ -generically free if and only if the action of the subgroup  $G_{C(F)} \subseteq G$  on  $X$  is  $p$ -generically free.*

*Proof.* (a) The (faithful)  $T$ -action on  $X$  is necessarily generically free; cf. [Lötscher 2010, Proposition 3.7(A)]. Thus, by [Gabriel 2011, Exposé V, Théorème 10.3.1] or [Berhuy and Favi 2003, Theorem 4.7],  $X$  has a dense open  $T$ -invariant subvariety  $U$  defined over  $k$ , which is the total space of a  $T$ -torsor,  $U \rightarrow Y := U/T$ , where  $Y$  is also smooth and geometrically irreducible. Since  $G/T$  is finite, after replacing  $U$  by the intersection of its (finitely many)  $G(k_{\text{alg}})$ -translates, we may assume that  $U$  is  $G$ -invariant.

The  $G$ -action on  $U$  gives rise to an  $F$ -action on  $Y$  (by descent). Now it is easy to see (cf. [Lorenz and Reichstein 2000, Lemma 2.1]) that the following conditions are equivalent:

- (i) The  $G$ -action on  $X$  is generically free.
- (ii) The  $F$ -action on  $Y$  is generically free.

Since  $F$  is finite, (ii) is equivalent to

- (iii)  $F$  acts faithfully on  $Y$ .

Proposition 6.1 tells us that the kernel of the  $F$ -action on  $Y$  is trivial if and only if the kernel of the  $C(F)$ -action on  $Y$  is trivial. In other words, (iii) is equivalent to

- (iv)  $C(F)$  acts faithfully (or equivalently, generically freely) on  $Y$

and consequently to

- (v) the  $G_{C(F)}$ -action on  $U$  (or, equivalently, on  $X$ ) is generically free.

Note that (iv) and (v) are the same as (ii) and (i), respectively, except that  $F$  is replaced by  $C(F)$  and  $G$  by  $G_{C(F)}$ . Thus, the equivalence of (iv) and (v) follows like the equivalence of (i) and (ii). We conclude that (i) and (v) are equivalent, as desired.

(b) Let  $K$  be the kernel of the  $G$ -action on  $X$ , which is contained in  $T$  by assumption. Note that  $(G/K)/(T/K) = G/T = F$ , so (a) says the  $G/K$ -action on  $X$  is generically free if and only if the  $G_{C(F)}/K$ -action on  $X$  is generically free, and (b) follows.  $\square$

The following definition is natural in view of Proposition 7.2:

**Definition 7.3.** Consider the action of  $F$  on  $T$  induced by conjugation in  $G$ . We say that  $G$  is *tame* if  $C(F)$  lies in the kernel of this action. Equivalently,  $G$  is tame if  $T$  is central in  $G_{C(F)}$ .

Recall in Section 1 we defined  $\text{gap}(G; p)$  as the difference between the minimal dimension of a  $p$ -generically free representation and the minimal dimension of a  $p$ -faithful representation of  $G$  (all representations are assumed to be defined over  $k$ ).

**Corollary 7.4.** *Let  $G$  be a tame  $k$ -group and  $X$  be a geometrically irreducible  $k$ -variety  $X$ .*



- (a) Every faithful  $G$ -action on  $X$  is generically free.
- (b) Every  $p$ -faithful  $G$ -action on  $X$  is  $p$ -generically free.
- (c) We have  $\text{gap}(G; p) = 0$ . In other words,

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

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

*Proof.* (a) Since  $G$  is tame,  $T$  is central in  $G_{C(F)}$ . Hence, the  $G_{C(F)}$ -action on  $X$  is generically free by Lemma 7.1(b). By Proposition 7.2(a), the  $G$ -action on  $X$  is generically free.

(b) Let  $K$  be the kernel of the action. Note that  $G/K$  is also tame. Now apply (a) to  $G/K$ .

(c) This follows immediately from (b) and Theorem 1.2.  $\square$

### 8. Proof of Theorem 1.3

In this section, we will prove the following proposition, which implies Theorem 1.3:

**Proposition 8.1.** *Let  $\rho : G \rightarrow \text{GL}(V)$  be a linear representation of  $G$ .*

- (a) *If  $\rho$  is faithful, then  $G$  has a generically free representation of dimension at most  $\dim \rho + \dim T - \dim T^{C(F)}$ .*
- (b) *If  $\rho$  is  $p$ -faithful, then  $G$  has a  $p$ -generically free representation of dimension at most  $\dim \rho + \dim T - \dim T^{C(F)}$ .*

*Proof.* (a) The subgroup  $T^{C(F)}$  is preserved by the conjugation action of  $G$ , so the adjoint representation of  $G$  decomposes as  $\text{Lie}(T) = \text{Lie}(T^{C(F)}) \oplus W$  for some  $G$ -representation  $W$ . Since the  $G$ -action on  $\text{Lie}(T)$  factors through  $F$ , the existence of  $W$  follows from Maschke's theorem. Let  $\mu$  be the  $G$ -representation on  $V \oplus W$ . Since  $\dim \text{Lie}(T^{C(F)}) \geq \dim T^{C(F)}$ , we have  $\dim \mu \leq \dim \rho + \dim T - \dim T^{C(F)}$ . It thus remains to show that  $\mu$  is a generically free representation of  $G$ .

Let  $K$  be the kernel of the  $G_{C(F)}$ -action on  $\text{Lie}(T)$ . We claim  $T$  is central in  $K$ . The finite  $p$ -group  $K/T$  acts on  $T$  (by conjugation), and it fixes the identity. By construction,  $K/T$  acts trivially on the tangent space at the identity, which implies  $K/T$  acts trivially on  $T$  since the characteristic is not equal to  $p$ ; cf. [Gille and Reichstein 2009, Proof of Lemma 4.1]. This proves the claim.

By Lemma 7.1, the  $K$ -action on  $V$  is generically free. Now  $G_{C(F)}$  acts trivially on  $\text{Lie}(T^{C(F)})$ , so  $G_{C(F)}/K$  acts faithfully on  $W$ . Since  $G_{C(F)}/K$  is finite, this action is also generically free. Therefore,  $G_{C(F)}$  acts generically freely on  $V \oplus W$  [Meyer and Reichstein 2009, Lemma 3.2]. Finally, by Proposition 7.2(a),  $G$  acts generically freely on  $V \oplus W$ , as desired.

(b) By our assumption,  $\ker \rho \subseteq T$ . Set  $\bar{T} := T/\ker \rho$ . It is easy to see that  $\dim T^{C(F)} \leq \dim \bar{T}^{C(F)}$ . Hence, by (a) there exists a generically free representation of  $G/\ker \rho$  of dimension at most

$$\dim \bar{T} - \dim \bar{T}^{C(F)} \leq \dim T - \dim T^{C(F)}.$$

We may now view this representation as a  $p$ -generically free representation of  $G$ . This completes the proof of Theorem 1.3.  $\square$

**Remark 8.2.** A similar argument shows that for any tame normal subgroup  $H \subseteq G$  over  $k$ ,  $\text{gap}(G; p) \leq \text{ed}(G/H; p)$ .

### 9. Additivity

Our proof of the additivity Theorem 1.4 relies on the following lemma. Let  $G$  be an algebraic group defined over a field  $k$  and  $C$  be a  $k$ -subgroup of  $G$ . Denote the minimal dimension of a representation  $\rho$  of  $G$  such that  $\rho|_C$  is faithful by  $f(G, C)$ .

**Lemma 9.1.** *Let  $k$  be an arbitrary field. For  $i = 1, 2$ , let  $G_i$  be an arbitrary (linear) algebraic group defined over  $k$ , and let  $C_i$  be a central  $k$ -subgroup of  $G_i$ . Assume that  $C_i$  is isomorphic to  $\mu_p^{r_i}$  over  $k$  for some  $r_1, r_2 \geq 0$ . Then*

$$f(G_1 \times G_2; C_1 \times C_2) = f(G_1; C_1) + f(G_2; C_2).$$

Our argument below is a variant of the proof of [Karpenko and Merkurjev 2008, Theorem 5.1], where  $G$  is assumed to be a (constant) finite  $p$ -group and  $C = C(G)$  (recall that  $C(G)$  is defined at the beginning of Section 4).

*Proof.* For  $i = 1, 2$ , let  $\pi_i : G_1 \times G_2 \rightarrow G_i$  be the natural projection, and let  $\epsilon_i : G_i \rightarrow G_1 \times G_2$  be the natural inclusion.

If  $\rho_i$  is a  $d_i$ -dimensional representation of  $G_i$  whose restriction to  $C_i$  is faithful, then clearly  $\rho_1 \circ \pi_1 \oplus \rho_2 \circ \pi_2$  is a  $(d_1 + d_2)$ -dimensional representation of  $G_1 \times G_2$  whose restriction to  $C_1 \times C_2$  is faithful. This shows that

$$f(G_1 \times G_2; C_1 \times C_2) \leq f(G_1; C_1) + f(G_2; C_2).$$

To prove the opposite inequality, let  $\rho : G_1 \times G_2 \rightarrow \text{GL}(V)$  be a representation such that  $\rho|_{C_1 \times C_2}$  is faithful and of minimal dimension

$$d = f(G_1 \times G_2; C_1 \times C_2)$$

with this property. Let  $\rho_1, \rho_2, \dots, \rho_n$  denote the irreducible decomposition factors in a Jordan–Hölder series for  $\rho$ . (Note that since  $G_1$  and  $G_2$  are arbitrary linear algebraic groups,  $\rho$  may not be completely reducible.) Since  $C_1 \times C_2$  is central in  $G_1 \times G_2$ , each  $\rho_i$  restricts to a multiplicative character of  $C_1 \times C_2$ , which we will denote by  $\chi_i$ . Moreover, since  $C_1 \times C_2 \simeq \mu_p^{r_1+r_2}$  is linearly reductive,  $\rho|_{C_1 \times C_2}$

is a direct sum  $\chi_1^{\oplus d_1} \oplus \cdots \oplus \chi_n^{\oplus d_n}$ , where  $d_i = \dim \rho_i$ . It is easy to see that the following conditions are equivalent:

- (i)  $\rho|_{C_1 \times C_2}$  is faithful.
- (ii)  $\chi_1, \dots, \chi_n$  generate  $(C_1 \times C_2)^*$  as an abelian group.

In particular, we may replace  $\rho$  by the direct sum  $\rho_1 \oplus \cdots \oplus \rho_n$ . Since  $C_i$  is isomorphic to  $\mu_p^{r_i}$ , we will think of  $(C_1 \times C_2)^*$  as an  $\mathbb{F}_p$ -vector space of dimension  $r_1 + r_2$ . Since (i)  $\iff$  (ii) above, we know that  $\chi_1, \dots, \chi_n$  span  $(C_1 \times C_2)^*$ . In fact, they form a basis of  $(C_1 \times C_2)^*$ , i.e.,  $n = r_1 + r_2$ . Indeed, if they were not linearly independent, we would be able to drop some of the terms in the irreducible decomposition  $\rho_1 \oplus \cdots \oplus \rho_n$  so that the restriction of the resulting representation to  $C_1 \times C_2$  would still be faithful, contradicting the minimality of  $\dim \rho$ .

We claim that it is always possible to replace each  $\rho_j$  by  $\rho'_j$ , where  $\rho'_j$  is either  $\rho_j \circ \epsilon_1 \circ \pi_1$  or  $\rho_j \circ \epsilon_2 \circ \pi_2$  such that the restriction of the resulting representation  $\rho' = \rho'_1 \oplus \cdots \oplus \rho'_n$  to  $C_1 \times C_2$  remains faithful. Since  $\dim \rho_i = \dim \rho'_i$ , we see that  $\dim \rho' = \dim \rho$ . Moreover,  $\rho'$  will then be of the form  $\alpha_1 \circ \pi_1 \oplus \alpha_2 \circ \pi_2$ , where  $\alpha_i$  is a representation of  $G_i$  whose restriction to  $C_i$  is faithful. Thus, if we can prove the above claim, we will have

$$f(G_1 \times G_2; C_1 \times C_2) = \dim \rho = \dim \rho' = \dim \alpha_1 + \dim \alpha_2 \geq f(G_1, C_1) + f(G_2, C_2),$$

as desired.

To prove the claim, we will define  $\rho'_j$  recursively for  $j = 1, \dots, n$ . Suppose  $\rho'_1, \dots, \rho'_{j-1}$  have already be defined so that the restriction of

$$\rho'_1 \oplus \cdots \oplus \rho'_{j-1} \oplus \rho_j \oplus \cdots \oplus \rho_n$$

to  $C_1 \times C_2$  is faithful. For notational simplicity, we assume  $\rho_1 = \rho'_1, \dots, \rho_{j-1} = \rho'_{j-1}$ . Note that

$$\chi_j = (\chi_j \circ \epsilon_1 \circ \pi_1) \oplus (\chi_j \circ \epsilon_2 \circ \pi_2).$$

Since  $\chi_1, \dots, \chi_n$  form a basis of  $(C_1 \times C_2)^*$  as an  $\mathbb{F}_p$ -vector space, we see that (a)  $\chi_j \circ \epsilon_1 \circ \pi_1$  or (b)  $\chi_j \circ \epsilon_2 \circ \pi_2$  does not lie in  $\text{Span}_{\mathbb{F}_p}(\chi_1, \dots, \chi_{j-1}, \chi_{j+1}, \dots, \chi_n)$ . Set

$$\rho'_j := \begin{cases} \rho_j \circ \epsilon_1 \circ \pi_1 & \text{in case (a),} \\ \rho_j \circ \epsilon_2 \circ \pi_2 & \text{otherwise.} \end{cases}$$

Using the equivalence of (i) and (ii) above, we see that the restriction of

$$\rho_1 \oplus \cdots \oplus \rho_{j-1} \oplus \rho'_j \oplus \rho_{j+1} \oplus \cdots \oplus \rho_n$$

to  $C$  is faithful. This completes the proof of the claim and thus of Lemma 9.1.  $\square$

*Proof of Theorem 1.4.* The groups  $G_1$  and  $G_2$  in the statement of Theorem 1.4 are assumed to satisfy Conventions 1.1 and hence so does  $G := G_1 \times G_2$ .

Recall also that  $C(G)$  is defined as the maximal split  $p$ -torsion subgroup of the center of  $G$ ; see Section 4. It follows from this definition that

$$C(G) = C(G_1) \times C(G_2).$$

By Lemma 9.1 and Proposition 4.3, the minimal dimension of a  $p$ -faithful representation is

$$f(G, C(G)) = f(G_1, C(G_1)) + f(G_2, C(G_2)),$$

which is the sum of the minimal dimensions of  $p$ -faithful representations of  $G_1$  and  $G_2$ . For  $i \in \{1, 2\}$  since  $\text{gap}(G_i; p) = 0$ , there exists a  $p$ -generically free representation  $\rho_i$  of  $G_i$  of dimension  $f(G_i, C(G_i))$ . The direct sum  $\rho_1 \oplus \rho_2$  is a  $p$ -generically free representation of  $G$ , and its dimension is  $f(G, C(G))$ . It follows that  $\text{gap}(G; p) = 0$ . By Theorem 1.2,

$$\text{ed}(G; p) = f(G, C(G)) - \dim G$$

and similarly for  $G_1$  and  $G_2$ ; cf. Proposition 4.3. Hence, as desired, we have  $\text{ed}(G; p) = \text{ed}(G_1; p) + \text{ed}(G_2; p)$ . □

**Example 9.2.** Let  $T$  be a torus over a field  $k$  of characteristic not equal to 2. Suppose there exists an element  $\tau$  in the absolute Galois group  $\text{Gal}(k_{\text{sep}}/k)$  that acts on the character lattice  $X(T)$  via multiplication by  $-1$ . Then  $\text{ed}(T; 2) \geq \dim T$ .

*Proof.* Let  $n := \dim T$ . Over the fixed field  $K := (k_{\text{sep}})^\tau$ , the torus  $T$  becomes isomorphic to a direct product of  $n$  copies of a nonsplit one-dimensional torus  $T_1$ . Using [Löttscher et al. 2013, Theorem 1.1], it is easy to see that  $\text{ed}(T_1; 2) = 1$ . By Theorem 1.4, we conclude that

$$\text{ed}(T; 2) \geq \text{ed}(T_K; 2) = \text{ed}((T_1)^n; 2) = n \text{ed}(T_1; 2) = \dim T. \quad \square$$

We end this section with an example that shows that the property  $\text{gap}(G; p) = 0$  is not preserved under base field extensions.

**Example 9.3.** Let  $k$  be as in Conventions 1.1,  $T$  be an algebraic  $k$ -torus that splits over a field extension of  $k$  of  $p$ -power degree and  $F$  be a nontrivial  $p$ -subgroup of the constant group  $S_n$ . Form the wreath product

$$T \wr F := T^n \rtimes F,$$

where  $F$  acts on  $T^n$  by permutations.

Then  $\text{gap}(T \wr F; p) = 0$  if and only if  $\text{ed}(T; p) > 0$ . Moreover,

$$\text{ed}(T \wr F; p) = \begin{cases} \text{ed}(T^n; p) = n \text{ed}(T; p) & \text{if } \text{ed}(T; p) > 0, \\ \text{ed}(F; p) & \text{otherwise.} \end{cases}$$

*Proof.* Let  $W$  be a  $p$ -faithful  $T$ -representation of minimal dimension. By [Lötscher et al. 2013, Theorem 1.1],  $\text{ed}(T; p) = \dim W - \dim T$ .

Then  $W^{\oplus n}$  is naturally a  $p$ -faithful  $(T \wr F)$ -representation. Lemma 9.1 and Proposition 4.3 applied to  $T^n$  tell us that  $W^{\oplus n}$  has minimal dimension among all  $p$ -faithful representations of  $T \wr F$ .

Suppose  $\text{ed}(T; p) > 0$ , i.e.,  $\dim W > \dim T$ . The group  $F$  acts faithfully on the rational quotient  $W^{\oplus n}/T^n = (W/T)^n$  since  $\dim W/T = \dim W - \dim T > 0$ . It is easy to see that the  $(T \wr F)$ -action on  $W^{\oplus n}$  is  $p$ -generically free; cf., e.g, [Meyer and Reichstein 2009, Lemma 3.3]. In particular,  $\text{gap}(T \wr F; p) = 0$  and

$$\text{ed}(T \wr F; p) = \dim W^{\oplus n} - \dim(T \wr F) = n(\dim W - \dim T) = n \text{ed}(T; p) = \text{ed}(T^n; p),$$

where the last equality follows from the additivity Theorem 1.4.

Now assume that  $\text{ed}(T; p) = 0$ , i.e.,  $\dim W = \dim T$ . The group  $T \wr F$  cannot have a  $p$ -generically free representation  $V$  of dimension  $\dim W^{\oplus n} = \dim T \wr F$  since  $T^n$  would then have a dense orbit in  $V$ . It follows that  $\text{gap}(T \wr F; p) > 0$ . In order to compute its essential  $p$ -dimension of  $T \wr F$ , we use the fact that the natural projection  $T \wr F \rightarrow F$  has a section. Hence, the map  $H^1(*, T \wr F) \rightarrow H^1(*, F)$  also has a section and is consequently a surjection. This implies  $\text{ed}(T \wr F; p) \geq \text{ed}(F; p)$ . Let  $W'$  be a faithful  $F$ -representation of dimension  $\text{ed}(F; p)$ . The direct sum  $W^{\oplus n} \oplus W'$  considered as a  $T \wr F$  representation is  $p$ -generically free, so  $\text{ed}(T \wr F; p) = \text{ed}(F; p)$ .  $\square$

### 10. Groups of low essential $p$ -dimension

In [Lötscher et al. 2013], we have identified tori of essential dimension 0 as those tori whose character lattice is invertible, i.e., a direct summand of a permutation module; see [Lötscher et al. 2013, Example 5.4]. The following lemma (with  $H = G$ ) shows that among the algebraic groups  $G$  studied in this paper, i.e., extensions of  $p$ -groups by tori, there are no other examples of groups of  $\text{ed}(G; p) = 0$ :

**Lemma 10.1.** *Let  $H$  be an algebraic group over a field  $l$  such that  $H/H^0$  is a  $p$ -group. If  $\text{ed}(H; p) = 0$ , then  $H$  is connected.*

*Proof.* Assume the contrary:  $F := H/H^0 \neq \{1\}$ . Let  $X$  be an irreducible  $H$ -torsor over some field  $K/l$ . For example, we can construct  $X$  as follows. Start with a faithful linear representation  $H \hookrightarrow \text{GL}_n$  for some  $n \geq 0$ . The natural projection  $\text{GL}_n \rightarrow \text{GL}_n/H$  is an  $H$ -torsor. Pulling back to the generic point  $\text{Spec}(K) \rightarrow \text{GL}_n/H$ , we obtain an irreducible  $H$ -torsor over  $K$ .

Now  $X/H^0 \rightarrow \text{Spec}(K)$  is an irreducible  $F$ -torsor. Since  $F \neq \{1\}$  is not connected, this torsor is nonsplit. As  $F$  is a  $p$ -group,  $X/H^0$  remains nonsplit over every prime-to- $p$  extension  $L/K$ . It follows that the degree of every closed point of  $X$  is divisible by  $p$ ; hence,  $p$  is a torsion prime of  $H$ . Therefore,  $\text{ed}(H; p) > 0$  by

[Merkurjev 2009, Proposition 4.4]. This contradicts the assumption  $\text{ed}(H; p) = 0$ , so  $F$  must be trivial.  $\square$

**Proposition 10.2.** *Let  $G$  be a central extension of a  $p$ -group  $F$  by a torus  $T$  over a field  $k$  of characteristic not  $p$ . If  $\text{ed}(G; p) \leq p - 2$ , then  $G$  is of multiplicative type.*

*Proof.* Without loss of generality, assume  $k = k_{\text{alg}}$ . By Theorem 1.2, there is a  $p$ -faithful representation  $V$  of  $G$  with  $\dim V \leq \dim T + p - 2$ .

First consider the case where  $V$  is faithful. By the theorem of Nagata [1961],  $G$  is linearly reductive; hence, we can write  $V = \bigoplus_{i=1}^r V_i$  for some nontrivial irreducible  $G$ -representations  $V_i$ . Since  $T$  is central and diagonalizable, it acts by a fixed character on  $V_i$  for every  $i$ . Hence,  $r \geq \dim T$  by faithfulness of  $V$ . It follows that  $1 \leq \dim V_i \leq p - 1$  for each  $i$ . But every irreducible  $G$ -representation has dimension a power of  $p$  (Proposition 4.2), so each  $V_i$  is one-dimensional. In other words,  $G$  is of multiplicative type.

Now consider the general case, where  $V$  is only  $p$ -faithful, and let  $K \subseteq G$  be the kernel of that representation. Then  $G/K$  is of multiplicative type, so it embeds into a torus  $T_1$ . Since  $T$  is central in  $G$ , a subgroup  $F'$  as in Lemma 5.3 is normal, so let  $T_2 = G/F'$ , which is also a torus. The kernel of the natural map  $G \rightarrow T_1 \times T_2$  is contained in  $K \cap F'$ . On the other hand,  $K \cap F' = \{1\}$  because  $p$  does not divide the order of  $K$ . This shows that  $G$  embeds into the torus  $T_1 \times T_2$  and hence is of multiplicative type.  $\square$

**Example 10.3.** Proposition 10.2 does not generalize to tame groups. For a counterexample, assume that the field  $k$  contains a primitive root of unity of order  $p^2$ , and consider the group  $G = \mathbb{G}_m^p \rtimes \mathbb{Z}/p^2\mathbb{Z}$ , where a generator in  $\mathbb{Z}/p^2\mathbb{Z}$  acts by cyclically permuting the  $p$  copies of  $\mathbb{G}_m$ . The group  $G$  is tame since  $C(\mathbb{Z}/p^2\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} = \mu_p$  acts trivially on  $\mathbb{G}_m^p$ . On the other hand,  $G$  is not abelian and hence is not of multiplicative type.

We claim that  $\text{ed}(G; p) = 1$  and hence  $\text{ed}(G; p) \leq p - 2$  for every odd prime  $p$ . There is a natural  $p$ -dimensional faithful representation  $\rho$  of  $G$ ;  $\rho$  embeds  $\mathbb{G}_m^p$  into  $\text{GL}_p$  diagonally in the standard basis  $e_1, \dots, e_p$ , and  $\mathbb{Z}/p^2\mathbb{Z}$  cyclically permutes  $e_1, \dots, e_p$ . Taking the direct sum of  $\rho$  with the one-dimensional representation  $\chi : G \rightarrow \mathbb{Z}/p^2\mathbb{Z} = \mu_{p^2} \hookrightarrow \mathbb{G}_m = \text{GL}_1$ , we obtain a faithful  $(p + 1)$ -dimensional representation  $\rho \oplus \chi$ , which is therefore generically free by Corollary 7.4 (this can also be verified directly). Hence,  $\text{ed}(G; p) \leq (p + 1) - \dim(G) = 1$ . On the other hand, by Lemma 10.1, we see that  $\text{ed}(G; p) \geq 1$  and thus  $\text{ed}(G; p) = 1$ , as claimed.  $\square$

Let  $\Gamma_p$  be a finite  $p$ -group, and let  $\phi : P \rightarrow X$  be a map of  $\mathbb{Z}[\Gamma_p]$ -modules. As in [Lötscher et al. 2013], we will call  $\phi$  a  $p$ -presentation if  $P$  is permutation and the cokernel is finite of order prime to  $p$ . We will denote by  $I$  the augmentation ideal of  $\mathbb{Z}[\Gamma_p]$  and by  $\bar{X} := X/(pX + IX)$  the largest  $p$ -torsion quotient with trivial  $\Gamma_p$ -action. The induced map on quotient modules will be denoted by  $\bar{\phi} : \bar{P} \rightarrow \bar{X}$ .

**Lemma 10.4.** *Let  $\phi : P \rightarrow X$  be a map of  $\mathbb{Z}[\Gamma_p]$ -modules. Then the cokernel of  $\phi$  is finite of order prime to  $p$  if and only if  $\bar{\phi}$  is surjective.*

*Proof.* This is shown in [Merkurjev 2010, Proof of Theorem 4.3] and from a different perspective in [Lötscher et al. 2013, Lemma 2.2].  $\square$

In the sequel, for  $G$  a group of multiplicative type over  $k$ , the group  $\Gamma_p$  in the definition of “ $p$ -presentation” is understood to be a Sylow  $p$ -subgroup of  $\Gamma = \text{Gal}(\ell/k)$ , where  $\ell/k$  is a Galois splitting field of  $G$ .

**Proposition 10.5.** *Let  $G$  be a central extension of a  $p$ -group  $F$  by a torus  $T$ , and let  $0 \leq r \leq p - 2$ . The following statements are equivalent:*

- (a)  $\text{ed}(G; p) \leq r$ .
- (b)  $G$  is of multiplicative type, and there is a  $p$ -presentation  $P \rightarrow X(G)$  whose kernel is isomorphic to the trivial  $\mathbb{Z}[\Gamma_p]$ -module  $\mathbb{Z}^r$ .

*Proof.* (a)  $\implies$  (b) Assuming (a) by Proposition 10.2,  $G$  is of multiplicative type. By [Lötscher et al. 2013, Corollary 5.1], we know there is a  $p$ -presentation  $P \rightarrow X(G)$  whose kernel  $L$  is free of rank  $\text{ed}(G; p) \leq p - 2$ . By [Abold and Plesken 1978, Satz],  $\Gamma_p$  must act trivially on  $L$ .

(b)  $\implies$  (a) This direction follows from [Lötscher et al. 2013, Corollary 5.1].  $\square$

**Proposition 10.6.** *Assume that  $G$  is of multiplicative type with a  $p$ -presentation  $\phi : P \rightarrow X(G)$  whose kernel is isomorphic to the trivial  $\mathbb{Z}[\Gamma_p]$ -module  $\mathbb{Z}^r$  for some  $r \geq 0$ . Then  $\text{ed}(G; p) \leq r$ , and the following conditions are equivalent:*

- (a)  $\text{ed}(G; p) = r$ .
- (b)  $\ker \phi$  is contained in  $pP + IP$ .
- (c)  $\ker \phi$  is contained in

$$\left\{ \sum_{\lambda \in \Lambda} a_\lambda \lambda \in P \mid a_\lambda \equiv 0 \pmod{p}, \forall \lambda \in \Lambda^{\Gamma_p} \right\}.$$

Here  $I$  denotes the augmentation ideal in  $\mathbb{Z}[\Gamma_p]$ , and  $\Lambda$  is a  $\Gamma_p$ -invariant basis of  $P$ .

*Proof.* (a)  $\iff$  (b) We have a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbb{Z}^r & \longrightarrow & P & \xrightarrow{\phi} & X(G) \\ & & \downarrow & & \downarrow & \searrow & \downarrow \\ & & (\mathbb{Z}/p\mathbb{Z})^r & \longrightarrow & \bar{P} & \xrightarrow{\bar{\phi}} & \bar{X}(G) \end{array}$$

with exact rows. By Lemma 10.4,  $\bar{\phi}$  is a surjection. Therefore,  $\ker \phi \subseteq pP + IP$  if and only if  $\bar{\phi}$  is an isomorphism.

Write  $P$  as a direct sum  $P \simeq \bigoplus_{j=1}^m P_j$  of transitive permutation  $\mathbb{Z}[\Gamma_p]$ -modules  $P_1, \dots, P_m$ . Then  $P/(pP + IP) \simeq \bigoplus_{j=1}^m P_j/(pP_j + IP_j) \simeq (\mathbb{Z}/p\mathbb{Z})^m$ . If  $\bar{\phi}$  is not an isomorphism, we can replace  $P$  by the direct sum  $\hat{P}$  of only  $m - 1$   $P_j$ s without losing surjectivity of  $\bar{\phi}$ . The composition  $\hat{P} \hookrightarrow P \rightarrow X(G)$  is then still a  $p$ -presentation of  $X(G)$  by Lemma 10.4, so  $\text{ed}(G; p) \leq \text{rank } \hat{P} - \dim G < \text{rank } P - \dim G = r$ .

Conversely, assume that  $\bar{\phi}$  is an isomorphism. Let  $\psi : P' \rightarrow X(G)$  be a  $p$ -presentation such that  $\text{ed}(G; p) = \text{rank ker } \psi$ . Let  $d$  be the index  $[X(G) : \phi(P)]$ , which is finite and prime to  $p$ . Since the map  $X(G) \rightarrow d \cdot X(G), x \mapsto dx$  is an isomorphism, we may assume that the image of  $\psi$  is contained in  $\phi(P)$ . We have an exact sequence  $\text{Hom}_{\mathbb{Z}[\Gamma_p]}(P', P) \rightarrow \text{Hom}_{\mathbb{Z}[\Gamma_p]}(P', \phi(P)) \rightarrow \text{Ext}_{\mathbb{Z}[\Gamma_p]}^1(P', \mathbb{Z}^r)$ , and the last group is zero by [Lorenz 2005, Lemma 2.5.1]. Therefore,  $\psi = \phi \circ \psi'$  for some map  $\psi' : P' \rightarrow P$  of  $\mathbb{Z}[\Gamma_p]$ -modules. Since  $\bar{\phi}$  is an isomorphism and  $\psi$  is a  $p$ -presentation, it follows from Lemma 10.4 that  $\psi'$  is a  $p$ -presentation as well and in particular that  $\text{rank } P' \geq \text{rank } P$ . Thus,  $\text{ed}(G; p) = \text{rank ker } \psi \geq \text{rank ker } \phi = r$ .

(b)  $\iff$  (c). It suffices to show that  $P^{\Gamma_p} \cap (pP + IP)$  consists precisely of the elements of  $P^{\Gamma_p}$  of the form  $\sum_{\lambda \in \Lambda} a_\lambda \lambda$  with  $a_\lambda \equiv 0 \pmod{p}$  for all  $\lambda \in \Lambda$  for any permutation  $\mathbb{Z}[\Gamma_p]$ -module  $P$ . One easily reduces to the case where  $P$  is a transitive permutation module. Then  $P^{\Gamma_p}$  consists precisely of the  $\mathbb{Z}$ -multiples of  $\sum_{\lambda \in \Lambda} \lambda$ , and  $pP + IP$  are the elements  $\sum_{\lambda \in \Lambda} a_\lambda \lambda$  with  $\sum_{\lambda \in \Lambda} a_\lambda \equiv 0 \pmod{p}$ . Thus, for  $n \in \mathbb{Z}$ , the element  $n \sum_{\lambda \in \Lambda} \lambda$  lies in  $pP + IP$  if and only if  $n \cdot |\Lambda| \equiv 0 \pmod{p}$  if and only if  $n \equiv 0 \pmod{p}$  or  $|\Lambda| \equiv 0 \pmod{p}$ . Since  $|\Lambda|$  is a power of  $p$ , the claim follows.  $\square$

**Example 10.7.** Let  $E$  be an étale algebra over  $k$ . We can write  $E = \ell_1 \times \dots \times \ell_m$  with some separable field extensions  $\ell_i/k$ . The kernel of the norm map

$$n : \mathbb{R}_{E/k}(\mathbb{G}_m) \rightarrow \mathbb{G}_m$$

is denoted by  $\mathbb{R}_{E/k}^{(1)}(\mathbb{G}_m)$ . Let  $G = n^{-1}(\mu_{p^r})$  for some  $r \geq 0$ . It is a group of multiplicative type fitting into an exact sequence

$$1 \rightarrow \mathbb{R}_{E/k}^{(1)}(\mathbb{G}_m) \rightarrow G \rightarrow \mu_{p^r} \rightarrow 1.$$

Let  $\ell$  be a finite Galois extension of  $k$  containing  $\ell_1, \dots, \ell_m$  (so  $\ell$  splits  $G$ ), let  $\Gamma = \text{Gal}(\ell/k)$  and  $\Gamma_{\ell_i} = \text{Gal}(\ell/\ell_i)$ , and let  $\Gamma_p$  be a  $p$ -Sylow subgroup of  $\Gamma$ . The character module of  $G$  has a  $p$ -presentation

$$P := \bigoplus_{i=1}^m \mathbb{Z}[\Gamma/\Gamma_{\ell_i}] \rightarrow X(G)$$

with kernel generated by the element  $(p^r, \dots, p^r) \in P$ . This element is fixed by  $\Gamma_p$ , so  $\text{ed}(G; p) \leq 1$ . It satisfies condition (c) of Proposition 10.6 if and only if  $r > 0$  or every  $\Gamma_p$ -set  $\Gamma/\Gamma_{\ell_i}$  is fixed-point free. Note that  $\Gamma/\Gamma_{\ell_i}$  has  $\Gamma_p$ -fixed points if



and only if  $[\ell_i : k] = |\Gamma / \Gamma_{\ell_i}|$  is prime to  $p$ . We thus have

$$\text{ed}(G; p) = \begin{cases} 0 & \text{if } r = 0 \text{ and } [\ell_i : k] \text{ is prime to } p \text{ for some } i, \\ 1 & \text{otherwise.} \end{cases}$$

## References

- [Abold and Plesken 1978] H. Abold and W. Plesken, “Ein Sylowsatz für endliche  $p$ -Untergruppen von  $\text{GL}(n, \mathbf{Z})$ ”, *Math. Ann.* **232**:2 (1978), 183–186. MR 57 #16427 Zbl 0353.20033
- [Berhuy and Favi 2003] G. Berhuy and G. Favi, “Essential dimension: a functorial point of view (after A. Merkurjev)”, *Doc. Math.* **8** (2003), 279–330. MR 2004m:11056 Zbl 1101.14324
- [Borel 1969] A. Borel, *Linear algebraic groups*, W. A. Benjamin, New York, 1969. MR 40 #4273 Zbl 0186.33201
- [Borel and Serre 1964] A. Borel and J.-P. Serre, “Théorèmes de finitude en cohomologie galoisienne”, *Comment. Math. Helv.* **39** (1964), 111–164. MR 31 #5870 Zbl 0143.05901
- [Bourbaki 1990] N. Bourbaki, *Algebra. II. Chapters 4–7*, Springer, Berlin, 1990. MR 91h:00003 Zbl 0719.12001
- [Chernousov et al. 2006] V. Chernousov, P. Gille, and Z. Reichstein, “Resolving  $G$ -torsors by abelian base extensions”, *J. Algebra* **296**:2 (2006), 561–581. MR 2007k:20102 Zbl 1157.14311
- [Colliot-Thélène and Sansuc 1977] J.-L. Colliot-Thélène and J.-J. Sansuc, “La  $R$ -équivalence sur les tores”, *Ann. Sci. École Norm. Sup.* (4) **10**:2 (1977), 175–229. MR 56 #8576 Zbl 0356.14007
- [Demazure and Gabriel 1970] M. Demazure and P. Gabriel, *Groupes algébriques*, tome I: Géométrie algébrique, généralités, groupes commutatifs, North-Holland, Amsterdam, 1970. MR 46 #1800 Zbl 0203.23401
- [Elman et al. 2008] R. Elman, N. Karpenko, and A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, AMS Colloquium Publications **56**, Amer. Math. Soc., Providence, RI, 2008. MR 2009d:11062 Zbl 1165.11042
- [Gabriel 2011] P. Gabriel, “Construction de schémas quotients”, pp. 249–289 in *Schémas en groupes (SGA 3)*, tome I: Propriétés générales des schémas en groupes, edited by P. Gille and P. Polo, Documents Mathématiques **7**, Société Mathématique de France, Paris, 2011. MR 2867621 Zbl 1241.14002
- [Gille and Reichstein 2009] P. Gille and Z. Reichstein, “A lower bound on the essential dimension of a connected linear group”, *Comment. Math. Helv.* **84**:1 (2009), 189–212. MR 2009j:11066 Zbl 1173.11022
- [Karpenko and Merkurjev 2008] N. A. Karpenko and A. S. Merkurjev, “Essential dimension of finite  $p$ -groups”, *Invent. Math.* **172**:3 (2008), 491–508. MR 2009b:12009 Zbl 1200.12002
- [Lang 1965] S. Lang, *Algebra*, Addison-Wesley Publishing Co., Reading, MA, 1965. MR 33 #5416 Zbl 0193.34701
- [Lorenz 2005] M. Lorenz, *Multiplicative invariant theory*, Encyclopaedia of Mathematical Sciences **135**, Springer, Berlin, 2005. MR 2005m:13012 Zbl 1078.13003
- [Lorenz and Reichstein 2000] M. Lorenz and Z. Reichstein, “Lattices and parameter reduction in division algebras”, preprint, 2000. arXiv math/0001026
- [Lötscher 2010] R. Lötscher, *Contributions to the essential dimension of finite and algebraic groups*, Ph.D. thesis, Universität Basel, 2010, <http://edoc.unibas.ch/1147/1/DissertationEdocCC.pdf>.
- [Lötscher et al. 2013] R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein, “Essential dimension of algebraic tori”, *J. Reine Angew. Math.* **677** (2013), 1–13. MR 3039772 Zbl 06162480
- [Margaux 2007] B. Margaux, “Passage to the limit in non-abelian Čech cohomology”, *J. Lie Theory* **17**:3 (2007), 591–596. MR 2008j:14035 Zbl 1145.14018

- [Merkurjev 2009] A. S. Merkurjev, “Essential dimension”, pp. 299–325 in *Quadratic forms—algebra, arithmetic, and geometry*, edited by R. Baeza et al., Contemp. Math. **493**, Amer. Math. Soc., Providence, RI, 2009. MR 2010i:14014 Zbl 1188.14006
- [Merkurjev 2010] A. S. Merkurjev, “A lower bound on the essential dimension of simple algebras”, *Algebra Number Theory* **4**:8 (2010), 1055–1076. MR 2832634 Zbl 1231.16017
- [Meyer and Reichstein 2009] A. Meyer and Z. Reichstein, “The essential dimension of the normalizer of a maximal torus in the projective linear group”, *Algebra Number Theory* **3**:4 (2009), 467–487. MR 2010h:11065 Zbl 1222.11056
- [Nagata 1961] M. Nagata, “Complete reducibility of rational representations of a matrix group”, *J. Math. Kyoto Univ.* **1** (1961), 87–99. MR 26 #236 Zbl 0106.25201
- [Reichstein 2000] Z. Reichstein, “On the notion of essential dimension for algebraic groups”, *Transform. Groups* **5**:3 (2000), 265–304. MR 2001j:20073 Zbl 0981.20033
- [Reichstein 2011] Z. Reichstein, “Essential dimension”, pp. 162–188 in *Proceedings of the International Congress of Mathematicians* (Hyderabad, India, 2010), vol. 2, edited by R. Bhatia et al., Hindustan Book Agency, New Delhi, 2011. MR 2012g:11074 Zbl 1232.14030
- [Schneider 1980a] H.-J. Schneider, “Decomposable extensions of affine groups”, pp. 98–115 in *Séminaire d’Algèbre Paul Dubreil et Marie-Paule Malliavin, 32ème année* (Paris, 1979), Lecture Notes in Math. **795**, Springer, Berlin, 1980. MR 81m:14033 Zbl 0457.14021
- [Schneider 1980b] H.-J. Schneider, “Zerlegbare Erweiterungen affiner Gruppen”, *J. Algebra* **66**:2 (1980), 569–593. MR 82f:14044 Zbl 0452.20040
- [Schneider 1981] H.-J. Schneider, “Restriktion und Corestriktion für algebraische Gruppen”, *J. Algebra* **68**:1 (1981), 177–189. MR 82f:14045 Zbl 0464.20028
- [Serre 2002] J.-P. Serre, *Galois cohomology*, 2nd ed., Springer, Berlin, 2002. MR 2002i:12004 Zbl 1004.12003
- [Tate 1997] J. Tate, “Finite flat group schemes”, pp. 121–154 in *Modular forms and Fermat’s last theorem* (Boston, 1995), edited by G. Cornell et al., Springer, New York, 1997. MR 1638478 Zbl 0924.14024
- [Vinberg and Popov 1994] È. B. Vinberg and V. L. Popov, “Invariant theory”, pp. 123–284 in *Algebraic geometry*, vol. IV, edited by I. R. Shafarevich, Encyclopaedia of Mathematical Sciences **55**, Springer, Berlin, 1994. MR 95g:14002 Zbl 0788.00015

Communicated by Raman Parimala

Received 2012-02-24    Revised 2012-09-09    Accepted 2012-10-23

roland.loetscher@mathematik.uni-muenchen.de

*Mathematisches Institut, Ludwig-Maximilians-Universität  
München, D-80333 München, Germany*  
<http://www.mathematik.uni-muenchen.de/~lotscher/>

m.macdonald@lancaster.ac.uk

*Department of Mathematics and Statistics,  
Lancaster University, Lancaster, LA1 4YF, United Kingdom*  
<http://www.maths.lancs.ac.uk/~macdonam/>

aurel.meyer@gmail.com

*Département de Mathématiques, Université Paris-Sud,  
Bâtiment 425, 91405 Orsay, France*  
<http://www.math.u-psud.fr/~ameyer/>

reichst@math.ubc.ca

*Department of Mathematics, University of British Columbia,  
1984 Mathematics Road, Vancouver, BC V6T1Z2, Canada*  
<http://www.math.ubc.ca/~reichst>

# Algebra & Number Theory

msp.org/ant

## EDITORS

### MANAGING EDITOR

Bjorn Poonen  
Massachusetts Institute of Technology  
Cambridge, USA

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Bernd Sturmfels	University of California, Berkeley, USA
Ehud Hrushovski	Hebrew University, Israel	Richard Taylor	Harvard University, USA
Craig Huneke	University of Virginia, USA	Ravi Vakil	Stanford University, USA
Mikhail Kapranov	Yale University, USA	Michel van den Bergh	Hasselt University, Belgium
Yujiro Kawamata	University of Tokyo, Japan	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Efim Zelmanov	University of California, San Diego, USA
Barry Mazur	Harvard University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

## PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.


The subscription price for 2013 is US \$200/year for the electronic version, and \$350/year (+\$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

---

ANT peer review and production are managed by EditFlow<sup>®</sup> from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2013 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 7    No. 8    2013

---

The geometry and combinatorics of cographic toric face rings SEBASTIAN CASALAINA-MARTIN, JESSE LEO KASS and FILIPPO VIVIANI	1781
Essential $p$ -dimension of algebraic groups whose connected component is a torus ROLAND LÖTSCHER, MARK MACDONALD, AUREL MEYER and ZINOVY REICHSTEIN	1817
Differential characterization of Wilson primes for $\mathbb{F}_q[t]$ DINESH S. THAKUR	1841
Principal $W$ -algebras for $GL(m n)$ JONATHAN BROWN, JONATHAN BRUNDAN and SIMON M. GOODWIN	1849
Kernels for products of $L$ -functions NIKOLAOS DIAMANTIS and CORMAC O'SULLIVAN	1883
Division algebras and quadratic forms over fraction fields of two-dimensional henselian domains YONG HU	1919
The operad structure of admissible $G$ -covers DAN PETERSEN	1953
The $p$ -adic monodromy theorem in the imperfect residue field case SHUN OHKUBO	1977
On the Manin–Mumford and Mordell–Lang conjectures in positive characteristic DAMIAN RÖSSLER	2039



1937-0652(2013)7:8;1-5