

# ESSENTIAL DIMENSION OF ALGEBRAIC TORI

ROLAND LÖTSCHER<sup>(1)</sup>, MARK MACDONALD, AUREL MEYER<sup>(2)</sup>,  
AND ZINOVY REICHSTEIN<sup>(3)</sup>

ABSTRACT. The essential dimension is a numerical invariant of an algebraic group  $G$  which may be thought of as a measure of complexity of  $G$ -torsors over fields. A recent theorem of N. Karpenko and A. Merkurjev gives a simple formula for the essential dimension of a finite  $p$ -group. We obtain similar formulas for the essential  $p$ -dimension of a broad class of groups, which includes all algebraic tori.

## 1. INTRODUCTION

Throughout this paper  $p$  will denote a prime integer,  $k$  an arbitrary base field and  $G$  a (not necessarily smooth) algebraic group defined over  $k$ . Unless otherwise specified, all fields are assumed to contain  $k$  and all morphisms between them are assumed to be  $k$ -homomorphisms. Morphisms of algebraic groups over  $k$  are assumed to be defined over  $k$ .

Let  $K$  be a field and  $H^1(K, G)$  be the nonabelian cohomology set with respect to the finitely presented faithfully flat (fppf) topology. Equivalently  $H^1(K, G)$  is the set of isomorphism classes of  $G$ -torsors over  $\text{Spec}(K)$ . If  $G$  is smooth then one may identify  $H^1(*, G)$  with the first Galois cohomology functor. We say that  $\alpha \in H^1(K, G)$  *descends* to an intermediate field  $k \subset K_0 \subset K$  if it lies in the image of the natural map  $H^1(K_0, G) \rightarrow H^1(K, G)$ . The minimal transcendence degree  $\text{trdeg}_k(K_0)$ , where  $\alpha$  descends to  $K_0$ , is called the essential dimension of  $\alpha$  and is denoted by the symbol  $\text{ed}(\alpha)$ . The *essential dimension* of the group  $G$  is the supremum of  $\text{ed}(\alpha)$ , as  $K$  ranges over all field extensions of  $k$  and  $\alpha$  ranges over  $H^1(K, G)$ . This numerical invariant of  $G$  has been extensively studied in recent years; see [BF, BR, Re, RY, Me<sub>1</sub>].

For many groups  $G$  the essential dimension  $\text{ed}(G)$  is hard to compute, even over the field  $k = \mathbb{C}$  of complex numbers. Given a prime  $p$ , it is often

---

2000 *Mathematics Subject Classification.* 20G15.

*Key words and phrases.* Essential dimension, group of multiplicative type, algebraic torus, twisted finite group, lattice, Galois-module.

<sup>(1)</sup> Roland Löttscher was partially supported by the Swiss National Science Foundation (Schweizerischer Nationalfonds).

<sup>(2)</sup> Aurel Meyer was partially supported by a University Graduate Fellowship at the University of British Columbia.

<sup>(3)</sup> Zinovy Reichstein was partially supported by NSERC Discovery and Accelerator Supplement grants.

easier to compute the essential  $p$ -dimension,  $\text{ed}(G; p)$ , which is defined as follows. The essential  $p$ -dimension  $\text{ed}(\alpha; p)$  of  $\alpha \in H^1(K, G)$  is the minimal value of  $\text{ed}(\alpha_L)$ , as  $L$  ranges over all finite field extensions of  $K$  of degree prime to  $p$ . The *essential  $p$ -dimension*  $\text{ed}(G; p)$  of  $G$  is then the supremum of  $\text{ed}(\alpha; p)$  taken over all fields  $K$  containing  $k$  and all  $\alpha \in H^1(K, G)$ . For details on this notion, see [RY] or [Me<sub>1</sub>]. Clearly  $0 \leq \text{ed}(G; p) \leq \text{ed}(G)$ . It is also easy to check that if  $L/K$  is a finite extension of degree prime to  $p$  then

$$(1) \quad \text{ed}(G; p) = \text{ed}(G_L; p);$$

see [Me<sub>1</sub>, Proposition 1.5].

A representation  $\psi: G \rightarrow \text{GL}(V)$  is called *generically free* if there exists a non-empty  $G$ -invariant open subset  $U \subset V$  such that the scheme-theoretic stabilizer of every point of  $U(k_{\text{alg}})$  is trivial. Such a representation gives rise to an upper bound on the essential dimension,

$$(2) \quad \text{ed}(G; p) \leq \text{ed}(G) \leq \dim(V) - \dim(G);$$

see [Me<sub>1</sub>, Theorem 4.1], [Re, Theorem 3.4], [BF, Lemma 4.11].

N. Karpenko and A. Merkurjev [KM] recently showed that the inequalities (2) are in fact sharp for finite constant  $p$ -groups, assuming that the base field  $k$  contains a primitive  $p$ th root of unity (note that this implies  $\text{char } k \neq p$ ). The purpose of this paper is to establish a similar result for a large class of groups which includes all algebraic tori.

For a field extension  $l/k$ , set  $G_l := G \times_{\text{Spec } k} \text{Spec}(l)$ . Let  $k_{\text{sep}}$  be a fixed separable closure of  $k$ . Recall that an algebraic group  $G$  over a field  $k$  is called *diagonalizable* if it is isomorphic to a closed subgroup of  $\mathbb{G}_m^n$  for some  $n \geq 0$ ;  $G$  is said to be *of multiplicative type* if  $G_{k_{\text{sep}}}$  is diagonalizable, see, e.g., [Vos<sub>2</sub>, Section 3.4]. Smooth connected groups of multiplicative type are precisely the algebraic tori.

Recall that the *order* of an algebraic group  $F$  is defined as  $|F| = \dim_k k[F]$ ; algebraic groups of finite order are called *finite*. We will say that a representation  $\psi: G \rightarrow \text{GL}(V)$  of an algebraic group  $G$  is  *$p$ -faithful* if its kernel is finite and of order prime to  $p$ .

**Theorem 1.1.** *Let  $G$  be a group of multiplicative type over an arbitrary field  $k$ . Assume that  $G$  has a Galois splitting field of  $p$ -power degree. Then*

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

where the minimum is taken over all  $p$ -faithful representations  $\psi$  of  $G$ . Moreover, if  $G$  is an extension of a  $p$ -group by a torus then

$$\text{ed}(G) = \text{ed}(G; p).$$

The quantity  $\min \dim(\psi)$  which appears in the statement of the Theorem 1.1 can be conveniently described in terms of character modules; see Corollary 5.1. We give several applications of these results in Sections 5 and 6. Further applications of the Theorem 1.1, to the classical problem

of computing essential dimensions of central simple algebras, can be found in [Me<sub>2</sub>] and [BM].

Note that Theorem 1.1 allows us to compute  $\text{ed}(G; p)$  for any group  $G$  of multiplicative type over  $k$ . Indeed, we can always choose a finite field extension  $k'/k$  of degree prime to  $p$  such that  $G_{k'}$  has a Galois splitting field of  $p$ -power degree. In view of (1),  $\text{ed}(G; p) = \text{ed}(G_{k'}; p)$ , and the latter number is given by Theorem 1.1.

In the last section we will prove analogous results for a finite (not necessarily abelian) algebraic group over  $k$ , assuming  $\text{char } k \neq p$ ; see Theorem 7.1 and Remark 7.2.

## 2. PRELIMINARIES ON GROUPS OF MULTIPLICATIVE TYPE

Throughout this section,  $A$  will denote an algebraic group of multiplicative type over a field  $k$ ,  $X(A)$  the character group of  $A$ , and  $\Gamma := \text{Gal}(k_{\text{sep}}/k)$  the absolute Galois group of  $k$ . Then  $X(A)$  is a continuous  $\mathbb{Z}\Gamma$ -module. Moreover,  $X(*)$  defines an anti-equivalence between algebraic  $k$ -groups of multiplicative type and continuous  $\mathbb{Z}\Gamma$ -modules; see, e.g., [Wa, 7.3]. Let  $\text{Diag}$  denote the inverse of  $X$ , so that  $\text{Diag}(X(A)) \simeq A$ .

Given a field extension  $l/k$ , recall that  $A$  is called *split* over  $l$  if and only if the absolute Galois group  $\text{Gal}(l_{\text{sep}}/l)$  acts trivially on  $X(A)$ . If a torsion-free  $\mathbb{Z}\Gamma$ -module  $P$  has a basis which is permuted by  $\Gamma$ , then it is called a *permutation* module, and  $\text{Diag}(P)$  is a *quasi-split* torus.

We will write  $A[p]$  for the  $p$ -torsion subgroup  $\{a \in A \mid a^p = 1\}$  of  $A$ . Clearly  $A[p]$  is defined over  $k$ . If  $A$  is a finite algebraic group of multiplicative type, then  $|A| = |X(A)|$  (by Cartier duality).

It is well known how to construct a maximal split subtorus of an algebraic torus, see for example [Wa, 7.4]. The following is a variant of this construction for algebraic groups of multiplicative type. Set

$$\text{Split}_k(A) := \text{Diag}(X(A)_\Gamma),$$

where  $X(A)_\Gamma$  is the module of co-invariants, defined as the largest quotient of  $X(A)$  with trivial  $\Gamma$ -action. Clearly  $\text{Split}_k(A)$  is split over  $k$ .

**Lemma 2.1.** *If  $A[p] \neq \{1\}$  and  $A$  is split over a Galois extension  $l/k$  of  $p$ -power degree, then  $\text{Split}_k(A) \neq \{1\}$ .*

*Proof.* If  $B$  is a  $k$ -subgroup of  $A$  then  $\text{Split}_k(B) \subset \text{Split}_k(A)$ , so it suffices to show that  $\text{Split}_k(A[p]) \neq \{1\}$ . Hence, we may assume that  $A = A[p]$  or equivalently, that  $X(A)$  is a finite-dimensional  $\mathbb{F}_p$ -vector space on which the  $p$ -group  $\text{Gal}(l/k)$  acts. Any such action is upper-triangular, relative to some  $\mathbb{F}_p$ -basis  $e_1, \dots, e_n$  of  $X(A)$ ; see, e.g., [Se<sub>1</sub>, Proposition 26, p. 64]. That is,

$$\gamma(e_i) = e_i + (\mathbb{F}_p\text{-linear combination of } e_{i+1}, \dots, e_n)$$

for every  $i = 1, \dots, n$  and every  $\gamma \in \text{Gal}(l/k)$ . The quotient of  $X(A)$  by the linear span of  $e_2, \dots, e_n$  has trivial  $\Gamma$ -action. Hence the module of co-invariants  $X(A)_\Gamma$  is non-trivial. Then  $\text{Split}_k(A) = \text{Diag}(X(A)_\Gamma)$  is non-trivial as well.  $\square$

Let  $G$  be an algebraic group whose centre  $Z(G)$  is of multiplicative type. Then we define  $C(G) := \text{Split}_k(Z(G)[p])$ . Note that this definition depends on the prime  $p$ , which we assume to be fixed throughout.

**Lemma 2.2.** *Let  $N$  be a subgroup of  $A$  defined over  $k$ . Assume that  $A$  has a Galois splitting field  $l/k$  of  $p$ -power degree. Then  $N \cap C(A) = \{1\}$  if and only if  $N$  is finite and its order is prime to  $p$ .*

*Proof.* If the order of  $N \subseteq A$  is finite and prime to  $p$  then clearly  $N \cap C(A) = \{1\}$ , because  $C(A)$  is a  $p$ -group. Conversely, suppose the order of  $N$  is either infinite or is finite but divisible by  $p$ . Then  $N[p] \neq \{1\}$ , and  $N[p]$  is split by  $l$ . By Lemma 2.1,  $\{1\} \neq \text{Split}_k(N[p]) \subseteq \text{Split}_k(A[p]) = C(A)$ , as desired.  $\square$

Now suppose  $l/k$  be a Galois splitting field of  $A$  and  $\psi: A \rightarrow \text{GL}(V)$  is a  $k$ -representation. Then we can decompose  $V_l = \bigoplus_{\chi \in \Lambda} V(\chi)$ , where  $\Lambda \subseteq X(A)$  is the set of weights and  $V(\chi) \subset V$  is the weight space associated to  $\chi \in \Lambda$ , i.e., the subspace of  $V$ , where  $A$  acts via  $\chi$ . The Galois group  $\Gamma = \text{Gal}(l/k)$  permutes  $\Lambda$  and weight spaces  $V(\chi)$ .

**Lemma 2.3.** *Let  $d_\chi = \dim_l V(\chi)$ . Then there exists an  $l$ -basis*

$$\Delta = \{e_j^\chi \mid \chi \in \Lambda, j = 1, \dots, d_\chi\}$$

*of  $V_l$  such that  $\gamma e_j^\chi = e_j^{\gamma\chi}$  for every  $\gamma \in \Gamma$ .*

*Proof.* We may assume that  $\Gamma$  acts transitively on  $\Lambda$ . Then  $d = \dim_l V(\chi)$  is independent of  $\chi \in \Lambda$ .

Choose a weight  $\chi_0 \in \Lambda$ . The stabilizer  $\Gamma_0$  of  $\chi_0$  in  $\Gamma$  acts semi-linearly on the  $l$ -vector space  $V(\chi_0)$ . By the no-name lemma [Sh, Appendix 3] there exists a basis  $e_1, \dots, e_d$  of  $V(\chi_0)$  such that each  $e_i$  is preserved by  $\Gamma_0$ . Now for  $\chi \in \Lambda$  and  $j = 1, \dots, d$ , set  $e_j^\chi := \gamma(e_j)$ , where  $\gamma \in \Gamma$  takes  $\chi_0$  to  $\chi$ . It is now easy to see that the  $e_j^\chi$  are well defined and form an  $l$ -basis of  $V_l$  with the desired property.  $\square$

**Corollary 2.4.** *Suppose  $A$  is split by a Galois extension  $l/k$  and  $\psi$  is an irreducible representation of  $A$ . Then  $\dim \psi$  divides  $[l : k]$ .*

*Proof.* By our construction  $\Gamma = \text{Gal}(l/k)$  permutes the  $l$ -basis  $\Delta$  of  $V_l$ . Since  $V$  is  $k$ -irreducible, this permutation action is transitive. Hence,  $|\Delta| = \dim \psi$  divides  $|\Gamma| = [l : k]$ .  $\square$

Now consider the  $k$ -torus  $T := \text{Diag}(\mathbb{Z}[\Delta])$ , which is split over  $l$  and quasi-split over  $k$ . By our construction  $T$  is equipped with a representation

$$\iota: T \hookrightarrow \text{GL}(V).$$

In the basis  $\Delta$  of  $V_l$ , this representation is given by  $\iota(t) \cdot e_j^\chi = \chi(t)e_j^\chi$ . Note that by Galois descent,  $\iota$  is defined over  $k$ . One easily checks that  $\iota$  is generically free (this can be done over  $l$ ).

We also remark that the original representation  $\psi: A \rightarrow \mathrm{GL}(V)$  can be written as a composition  $\psi = \iota \circ \hat{\psi}$ , where  $\hat{\psi}: A \rightarrow T$  is induced by the map  $\mathbb{Z}[\Delta] \rightarrow X(A)$  of  $\Gamma$ -modules, sending  $e_j^\chi$  to  $\chi$ .

**Lemma 2.5.** *Every faithful representation  $\psi: A \rightarrow \mathrm{GL}(V)$  of  $A$  is generically free.*

*Proof.* As we saw above,  $\psi = \iota \circ \hat{\psi}$ , where  $\iota: T \rightarrow \mathrm{GL}(V)$  is generically free. If  $\psi$  is faithful then  $\hat{\psi}: A \rightarrow T$  is faithful, and hence,  $\psi$  is generically free.  $\square$

**Lemma 2.6.** *Let  $N$  be a closed subgroup of  $A$ ,  $l/k$  be a Galois splitting field of  $A$  and  $\Gamma = \mathrm{Gal}(l/k)$ . Then*

$$\min \dim \psi = \min \mathrm{rank}(P)$$

where the minimum on the left hand side is taken over all  $k$ -representations  $\psi$  of  $A$  with kernel  $N$ , and the minimum on the right is taken over all homomorphisms  $f: P \rightarrow X(A)$  of  $\mathbb{Z}\Gamma$ -modules, with  $P$  permutation and  $\mathrm{cokernel}(f) = X(N)$ .

*Proof.* Given  $\psi: A \rightarrow \mathrm{GL}(V)$  with kernel  $N$ , write  $\psi: A \xrightarrow{\hat{\psi}} T \xrightarrow{\iota} \mathrm{GL}(V)$  as above, where  $T$  is a quasi-split  $k$ -torus of dimension  $\dim T = \mathrm{rank} X(T) = \dim \psi$  which splits over  $l$ . Then  $\ker \hat{\psi} = N$  and the cokernel of the induced map  $X(\hat{\psi}): X(T) \rightarrow X(A)$  of  $\mathbb{Z}\Gamma$ -modules is  $X(N)$ .

Conversely, if  $P$  is a permutation  $\mathbb{Z}\Gamma$ -module then we can embed the torus  $\mathrm{Diag}(P)$  in  $\mathrm{GL}_n$ , where  $n = \mathrm{rk} P$  [Vos<sub>2</sub>, Section 6.1]. A map  $f: P \rightarrow X(A)$  of  $\mathbb{Z}\Gamma$ -modules with cokernel  $X(N)$  then yields a representation  $A \rightarrow \mathrm{Diag}(P) \hookrightarrow \mathrm{GL}_n$  with kernel  $N$ .  $\square$

### 3. A LOWER BOUND ON ESSENTIAL $p$ -DIMENSION

Consider an exact sequence of algebraic groups over  $k$

$$(3) \quad 1 \rightarrow C \rightarrow G \rightarrow Q \rightarrow 1$$

such that  $C$  is central in  $G$  and isomorphic to  $\mu_p^r$  for some  $r \geq 0$ . Given a character  $\chi: C \rightarrow \mu_p$ , we will, following [KM], denote by  $\mathrm{Rep}^\chi$  the set of irreducible representations  $\phi: G \rightarrow \mathrm{GL}(V)$ , such that  $\phi(c) = \chi(c) \mathrm{Id}$  for every  $c \in C$ .

**Theorem 3.1.** *Suppose a sequence of  $k$ -groups of the form (3) satisfies the following condition:*

$$\mathrm{gcd}\{\dim(\phi) \mid \phi \in \mathrm{Rep}^\chi\} = \min\{\dim(\phi) \mid \phi \in \mathrm{Rep}^\chi\}$$

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

$$\mathrm{ed}(G; p) \geq \min \dim(\psi) - \dim G,$$

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

*Proof.* Denote by  $C^* := \text{Hom}(C, \mu_p)$  the character group of  $C$ . Let  $V$  be a generically free  $Q$ -module, and  $U \subseteq V$  an open dense  $Q$ -invariant subvariety such that  $U \rightarrow U/Q$  is a  $Q$ -torsor. Then let  $E \rightarrow \text{Spec } K$  be the generic fibre of this torsor, and let  $\beta: C^* \rightarrow \text{Br}_p(K)$  denote the homomorphism that sends  $\chi \in C^*$  to the image of  $E \in H^1(K, Q)$  in  $\text{Br}_p(K)$  under the map

$$H^1(K, Q) \rightarrow H^2(K, C) \xrightarrow{\chi^*} H^2(K, \mu_p) = \text{Br}_p(K)$$

given by composing the connecting map with  $\chi_*$ . Then there exists a basis  $\chi_1, \dots, \chi_r$  of  $C^*$  such that

$$(4) \quad \text{ed}(G; p) \geq \sum_{i=1}^r \text{ind } \beta(\chi_i) - \dim G,$$

see [Me<sub>1</sub>, Theorem 4.8, Example 3.7]. Moreover, by [KM, Theorem 4.4, Remark 4.5]

$$\text{ind } \beta(\chi_i) = \text{gcd } \dim(\psi),$$

where the greatest common divisor is taken over all (finite-dimensional) representations  $\psi$  of  $G$  such that  $\psi|_C$  is scalar multiplication by  $\chi_i$ . By our assumption, gcd can be replaced by min. Hence, for each  $i \in \{1, \dots, r\}$  we can choose a representation  $\psi_i$  of  $G$  with

$$\text{ind } \beta(\chi_i) = \dim(\psi_i)$$

such that  $(\psi_i)|_C$  is scalar multiplication by  $\chi_i$ .

Set  $\psi := \psi_1 \oplus \dots \oplus \psi_r$ . The inequality (4) can be written as

$$(5) \quad \text{ed}(G; p) \geq \dim(\psi) - \dim G.$$

Since  $\chi_1, \dots, \chi_r$  form a basis of  $C^*$  the restriction of  $\psi$  to  $C$  is faithful. This proves the theorem.  $\square$

#### 4. PROOF OF THE MAIN RESULT

The following lemma generalizes [MR, Lemma 4.1].

**Lemma 4.1.** *Let  $A$  be an algebraic group of multiplicative type over a field  $k$ , and let  $B \subset A$  a closed subgroup of (finite) index prime to  $p$ . Then  $\text{ed}(A; p) = \text{ed}(B; p)$ .*

*Proof.* The inequality  $\text{ed}(B; p) \leq \text{ed}(A; p)$  is clear, since  $\dim A = \dim B$ ; see [Me<sub>1</sub>, Corollary 4.3].

To prove the opposite inequality, set  $Q := A/B$ . In view of the exact sequence  $H^1(K, B) \rightarrow H^1(K, A) \rightarrow H^1(K, Q)$  it suffices to show that every  $Q$ -torsor  $X \rightarrow \text{Spec}(K)$  splits over a finite prime to  $p$  extension of  $K$ . (Here  $K$  is assumed to be an arbitrary field extension of  $k$ .)

First suppose  $\text{char } k = p$ . In this case  $X$  is étale over  $\text{Spec}(K)$  (since  $Q$  is étale over  $\text{Spec}(K)$ , see [Wa, 14.4]). The proof now proceeds as in [MR,

Lemma 4.1]. That is,  $X$  is  $K$ -isomorphic to a direct product  $\text{Spec}(K_1 \times \cdots \times K_n)$ , where each  $K_i/K$  is a finite separable field extension. One of the fields  $K_i$  has degree prime to  $p$  over  $K$ , and we get a  $K_i$ -point of  $X$  from the map  $\text{Spec}(K_i) \rightarrow X$ , induced by the projection  $K[X] \rightarrow K_i$ . This implies that  $X$  splits over  $K_i$ .

Now suppose  $\text{char } k \neq p$ . By [EKM, Prop 101.16] there exists an algebraic field extension  $K^{(p)}/K$  such that every finite extension of  $K^{(p)}$  has degree a power of  $p$  and every finite sub-extension  $L/K$  of  $K^{(p)}/K$  has degree prime to  $p$ . It is easy to see that  $K^{(p)}$  is a perfect field and  $\Gamma = \text{Gal}(K_{\text{alg}}/K^{(p)})$  is a profinite  $p$ -group. Since  $Q(K_{\text{alg}})$  has order prime to  $p$  the group  $H^1(K^{(p)}, Q) = H^1(\Gamma, Q(K_{\text{alg}}))$  is trivial by [Se2, I.5, ex. 2]. Thus  $X$  splits over  $K^{(p)}$  and hence over a finite sub-extension  $L/K$  of  $K^{(p)}/K$ .  $\square$

**Proposition 4.2.** *Let  $G$  be an algebraic group of multiplicative type over  $k$ ,  $T$  its maximal  $k$ -torus, and  $l/k$  a minimal Galois splitting field of  $T$ . Let  $N \subset G$  be a finite  $k$ -subgroup whose order is coprime to both  $[l : k]$  and  $|G/T|$ . Let  $\pi : G \rightarrow G/N$  be the natural projection. Then*

$$\pi_* : H^1(K, G) \rightarrow H^1(K, G/N)$$

*is bijective, for any field extension  $K/k$ . In particular,  $\text{ed}(G) = \text{ed}(G/N)$ .*

The following argument, simplifying our earlier proof, was suggested to us by Merkurjev.

*Proof.* We claim that  $H^1(K, G)$  is  $m$ -torsion, where  $m = [l : k] \cdot |G/T|$ . Indeed, since  $T_K$  is split by a Galois extension of degree dividing  $[l : k]$ , restricting and corestricting in Galois cohomology yields  $[l : k] \cdot H^1(K, T) = (0)$ . On the other hand, since  $|G/T| \cdot H^1(K, G/T) = (0)$ , the exact sequence

$$H^1(K, T) \rightarrow H^1(K, G) \rightarrow H^1(K, G/T)$$

shows that  $H^1(K, G)$  is  $m$ -torsion, as claimed. Note that  $N$  is contained in  $T$  and the quotient of  $G/N$  by its maximal torus  $T/N$  is isomorphic to  $G/T$ . So the group  $H^1(K, G/N)$  is  $m$ -torsion as well.

Now let  $n = |N|$  and  $p_n : G \rightarrow G$  be given by  $g \rightarrow g^n$ . The induced map  $H^1(K, G) \xrightarrow{(p_n)_*} H^1(K, G)$  is multiplication by  $n$ . Since  $H^1(K, G)$  is  $m$ -torsion and by assumption  $n$  and  $m$  coprime,  $(p_n)_*$  is an isomorphism. Moreover,  $N$  lies in the kernel of  $p_n$  and so  $(p_n)_*$  factors through  $\pi_*$ :

$$(p_n)_* : H^1(K, G) \xrightarrow{\pi_*} H^1(K, G/N) \rightarrow H^1(K, G).$$

In particular,  $\pi_*$  is injective. A similar argument shows that composing these maps in the opposite order,

$$H^1(K, G/N) \rightarrow H^1(K, G) \xrightarrow{\pi_*} H^1(K, G/N),$$

we get an isomorphism as well. This shows that  $\pi_*$  is surjective and hence, bijective, as desired.  $\square$

*Proof of the Theorem 1.1.* We will first prove  $\text{ed}(G; p) \geq \min \dim(\psi) - \dim G$ , where the minimum is over  $p$ -faithful representations. Since  $G$  is split by a Galois extension of  $p$ -power degree, Corollary 2.4 tells us that for any character  $\chi$  of  $C(G)$  and any  $\phi \in \text{Rep}^\chi$ ,  $\dim(\phi)$  is a power of  $p$ . By Theorem 3.1,  $\text{ed}(G; p) \geq \min \dim(\psi) - \dim G$ , where  $\psi$  ranges over representations of  $G$  whose restriction to  $C(G)$  is faithful. By Lemma 2.2 representations with this property are precisely the  $p$ -faithful representations.

We will now show that  $\text{ed}(G; p) \leq \dim \psi - \dim G$  for any  $p$ -faithful representation  $\psi$  of  $G$ . We will proceed in two steps.

Step 1. Suppose  $G$  is an extension of a  $p$ -group  $F$  by a torus  $T$ . Since  $N := \ker \psi$  is finite of order prime to  $p$ , Proposition 4.2 yields  $\text{ed}(G) = \text{ed}(G/N)$ . Now  $\psi$  can be considered as a faithful representation of  $G/N$ . By Lemma 2.5, this representation of  $G/N$  is generically free. By (2),

$$\text{ed}(G; p) \leq \text{ed}(G) = \text{ed}(G/N) \leq \dim \psi - \dim(G/N) = \dim \psi - \dim(G),$$

as desired.

Taking  $\psi$  to be of minimal dimension, we also see that in this case we have  $\text{ed}(G; p) = \text{ed}(G)$ , as asserted in the statement of the theorem.

Step 2. Let  $G$  be an arbitrary group of multiplicative type. Let  $T$  be the maximal torus of  $G$ , and  $F'$  be the Sylow  $p$ -subgroup of the multiplicative finite group  $F := G/T$ . Recall that  $F'$  is defined as  $\text{Diag}(X(F)/Y)$ , where  $Y$  is the submodule of elements of order prime to  $p$ .

Now denote the pre-image of  $F'$  under the projection  $G \rightarrow F = G/T$  by  $G'$ . Since  $G'$  is an extension of a  $p$ -group by a torus, we know from Step 1 that

$$\text{ed}(G'; p) \leq \dim \psi|_{G'} - \dim G' = \dim \psi - \dim G.$$

The index of  $G'$  in  $G$  is finite and prime to  $p$ , hence  $\text{ed}(G; p) = \text{ed}(G'; p)$  by Lemma 4.1 and the desired inequality,  $\text{ed}(G; p) \leq \dim \psi - \dim G$  follows.  $\square$

## 5. MAIN THEOREM IN THE LANGUAGE OF CHARACTER MODULES

Let  $G$  be of multiplicative type over  $k$  and let  $l/k$  be a Galois splitting field of  $G$ . We will call a map of  $\mathbb{Z} \text{Gal}(l/k)$ -modules  $P \rightarrow X(G)$  a  $p$ -presentation if  $P$  is permutation, and the cokernel is finite of order prime to  $p$ .

We now restate our Theorem 1.1 in a way that is often more convenient to use.

**Corollary 5.1.** *Let  $G$  be a group of multiplicative over  $k$ ,  $l/k$  be a finite Galois splitting field of  $G$ , and  $\Gamma_p$  be a Sylow  $p$ -subgroup of  $\text{Gal}(l/k)$ . Then*

$$\text{ed}(G; p) = \min \text{rk ker } \phi,$$

where the minimum is taken over all  $p$ -presentations  $\phi: P \rightarrow X(G)$  of  $X(G)$ , viewed as a  $\mathbb{Z}\Gamma_p$ -module.

*Proof.* Let  $k' = l^{\Gamma_p}$ . Then  $\text{Gal}(l/k') = \Gamma_p$ . Since  $[k' : k]$  is finite and prime to  $p$ , (1) tells us that  $\text{ed}(G; p) = \text{ed}(G_{k'}; p)$ . By Theorem 1.1  $\text{ed}(G_{k'}; p) =$

$\min \dim(\psi) - \dim G$ , where the minimum is taken over all  $p$ -faithful representations  $\psi$  of  $G_{k'}$ . By Lemma 2.6

$$\min \dim(\psi) - \dim G = \min \operatorname{rank}(P) - \dim G = \min \operatorname{rk} \ker \phi,$$

where the minimum on the right is taken over all  $p$ -presentations  $\phi: P \rightarrow X(G)$ , as in the statement of the theorem.  $\square$

**Example 5.2.** Let  $T$  be a torus of dimension  $< p - 1$ . Then  $\operatorname{ed}(T; p) = 0$ , because there is no non-trivial integral representation of dimension  $< p - 1$  of any  $p$ -group [AP, Satz].

**Example 5.3.** Assume  $\operatorname{char} k = 0$ , and let  $\Gamma = \mathcal{S}_{p^r}$  denote the symmetric group for some  $r \geq 1$ . The generic torus  $T$  of  $\operatorname{PGL}_n$ , defined in [Vos<sub>2</sub>, §4.1–4.2], is of dimension  $p^r - 1$  and has character lattice

$$X(T) = \{a \in \mathbb{Z}^{p^r} \mid a_1 + \cdots + a_{p^r} = 0\}$$

with the natural action of  $\Gamma$  on it; see [Vos<sub>1</sub>]. Let  $\Gamma_p$  be a Sylow  $p$ -subgroup of  $\Gamma$ . In [MR, Prop. 7.2] it is shown that the minimal rank of a permutation module with a  $p$ -presentation to  $X(T)$  is  $p^{2r-1}$ . Thus by Corollary 5.1,  $\operatorname{ed}(T; p) = p^{2r-1} - p^r + 1$ .

## 6. FORMS OF $\mu_n$

**Proposition 6.1.** *Let  $A$  be a twisted form of  $\mu_{p^n}$  over  $k$  and  $l/k$  a minimal Galois splitting field. Then  $\operatorname{ed}(A; p) = p^r$ , where  $p^r$  is the highest power of  $p$  dividing  $[l : k]$ .*

*Proof.* Let  $\Gamma_p$  be a Sylow  $p$ -subgroup of  $\operatorname{Gal}(l/k)$  and  $\phi: P \rightarrow X(A)$  be a  $p$ -presentation. Since  $\phi$  has prime to  $p$  cokernel and  $X(A)$  is a cyclic  $p$ -group,  $\phi$  must be surjective. Thus, if  $\Lambda$  is a basis of  $P$ , permuted by  $\Gamma_p$ , some element  $\lambda \in \Lambda$  maps to a generator  $a$  of  $X(A)$ . Moreover,  $\Gamma_p$  acts faithfully on  $X(A)$  and  $|\Lambda| \geq |\Gamma_p \lambda| \geq |\Gamma_p a| = |\Gamma_p|$ . Conversely we have a surjective homomorphism  $\mathbb{Z}[\Gamma_p a] \rightarrow X(A)$  that sends  $a$  to itself. So the minimal value of  $\operatorname{rk} P$  is  $|\Gamma_p|$ . Now apply Corollary 5.1.  $\square$

*Remark 6.2.* For  $\operatorname{char} k \neq p$ , Proposition 6.1 was previously known in the following special cases:

For twisted cyclic groups of order 4 it is due to M. Rost [Ro] and in the case of cyclic groups of order 8 to G. Bayarmagnai [Ba]. The case of constant cyclic groups of arbitrary prime power order is due to M. Florence [Fl].

**Example 6.3.** Let  $\operatorname{char} k = p$ . D. Tossici and A. Vistoli [TV, Question 4.1 (2)] asked if the essential dimension of every algebraic  $k$ -group of order  $p^n$  is  $\leq n$ . The following example, with  $n = 2$  and  $p > 2$ , answers this question in the negative.

Let  $l/k$  be a cyclic extension of order  $p$ ; set  $\Gamma := \operatorname{Gal}(l/k)$ . (For example, we can take  $k$  and  $l$  to be finite fields of orders  $p$  and  $p^p$ , respectively.) Now let  $M \simeq \mathbb{Z}/p^2\mathbb{Z}$  be the  $\Gamma$ -module obtained by identifying  $\Gamma$  with the unique subgroup of  $\operatorname{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{Z}/p(p-1)\mathbb{Z}$  of order  $p$ . By construction  $G =$

$\text{Diag}(M)$  is a form of  $\mu_{p^2}$  defined over  $k$ , whose minimal Galois splitting field is  $l$ . Proposition 6.1 now tells us that  $\text{ed}(G) = \text{ed}(G; p) = [l : k] = p > 2$ .  $\square$

## 7. TWISTED $p$ -GROUPS

In this section we will use Theorem 3.1 to generalize the Karpenko–Merkurjev theorem to arbitrary (possibly twisted) finite  $p$ -groups over a field  $k$ , assuming that  $\text{char } k \neq p$  and  $k$  contains a primitive  $p$ th root of unity.

**Theorem 7.1.** *Let  $G$  be an algebraic group over  $k$  such that  $G_L$  is a constant group of order  $p^n$  for some  $n \geq 1$  and some Galois extension  $L/k$  of  $p$ -power degree. Then*

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

where  $\psi$  runs through all faithful representations of  $G$ .

*Proof.* The inequalities  $\text{ed}(G; p) \leq \text{ed}(G) \leq \min \dim \psi$  follow from (2). Hence it suffices to show that  $\text{ed}(G; p) \geq \min \dim \psi$ .

Since  $\text{char } k \neq p$  the centre of  $G$  is of multiplicative type, the subgroup  $C(G) = \text{Split}_k(Z(G)[p])$  is well-defined (as in Section 2) and is isomorphic to  $\mu_p^r$  for some  $r \geq 1$ .

We claim that every irreducible representation  $\psi$  of  $G$  has dimension equal to a power of  $p$ . Denote by  $\zeta$  a primitive root of unity of order equal to the exponent of  $G(L)$ . Since  $k$  contains a primitive  $p$ th root of unity,  $L' := L(\zeta)$  is Galois over  $k$  and of  $p$ -power degree, and  $\psi$  decomposes over  $L'$  as a direct sum of absolutely irreducible representations of the abstract  $p$ -group  $G(L') = G(L)$ . All direct summands in this decomposition have the same dimension, equal to a power of  $p$ . By [Ka, Theorem 5.22] the number of direct summands in this decomposition is also a power of  $p$ , and the claim follows.

Therefore, Theorem 3.1 can be applied, i.e.,  $\text{ed}(G; p) \geq \min \dim \psi$  taken over all representations  $\psi$  of  $G$  whose restriction to  $C(G)$  is faithful. Let  $N$  be the kernel of such a representation. We claim that  $N \cap C(G) = \{1\}$  implies that  $N$  is trivial. If  $G$  is constant we have  $C(G) = Z(G)[p]$  since  $k$  contains a primitive  $p$ th root of unity and the claim is a standard elementary fact about  $p$ -groups. The general case follows from Lemma 2.1 applied to  $A = Z(G)[p] \cap N$ .  $\square$

*Remark 7.2.* Theorem 7.1 allows one to compute  $\text{ed}(G; p)$ , at least in principle, for any étale algebraic group  $G$  over  $k$ , provided  $\text{char}(k) \neq p$ .

To carry out this computation, we first pass to a suitable Galois extension  $L/k$  of degree prime to  $p$  such that  $L$  contains a primitive  $p$ th root of unity and  $G_L$  becomes constant over a Galois extension  $E/L$  of  $p$ -power degree.

We claim that  $G_L$  has a Sylow  $p$ -subgroup  $S$  defined over  $L$ . Indeed, the  $p$ -group  $\text{Gal}(E/L)$  permutes the Sylow subgroups of  $G(E)$ . By the Sylow theorems, the number of such subgroups is prime to  $p$ . Thus one of them is fixed by the  $p$ -group  $\text{Gal}(E/L)$ . This proves the claim.

Now we have  $\text{ed}(G;p) = \text{ed}(G_L;p) = \text{ed}(S;p)$ , and  $\text{ed}(S;p)$  is given by Theorem 7.1.

## ACKNOWLEDGMENTS

The authors are grateful to A. S. Merkurjev for numerous constructive comments on earlier versions of this paper, and to A. Auel and A. Vistoli for helpful discussions.

## REFERENCES

- [AP] H. Abold, W. Plesken, *Ein Sylowsatz für endliche  $p$ -Untergruppen von  $\text{GL}(n, Z)$* , Math. Ann. 232 (1978), no. 2, 183–186.
- [Ba] G. Bayarmagnai, *Essential dimension of some twists of  $\mu_{p^n}$* , Proc. Symp. Algebraic Number Theory and Related Topics, 145–151, RIMS Kôkyûroku Bessatsu, B4, Res. Inst. Math. Sci. (RIMS), Kyoto (2007).
- [BF] G. Berhuy, G. Favi, *Essential Dimension: A Functorial Point of View (after A. Merkurjev)*, Doc. Math. 8 (2003), 279–330.
- [BM] S. Baek, A. Merkurjev, *Essential dimension of central simple algebras*, preprint, <http://www.math.ucla.edu/~merkurev/publicat.htm>.
- [BR] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica 106:159–179 (1997).
- [EKM] R. Elman, N. Karpenko, A. Merkurjev: *The algebraic and geometric theory of quadratic forms*. Amer. Math. Soc. Coll. Publ. **56**, Providence, RI: Amer. Math. Soc. (2008).
- [Fl] M. Florence, *On the essential dimension of cyclic  $p$ -groups*, Inventiones Mathematicae, **171** (2007), 175–189.
- [Ka] G. Karpilovsky, *Clifford Theory for Group Representations*. Mathematics Studies, 156. North-Holland, Netherlands, (1989).
- [KM] N. Karpenko, A. Merkurjev, *Essential dimension of finite  $p$ -groups*, Inventiones Mathematicae, **172** (2008), 491–508.
- [Me<sub>1</sub>] A. Merkurjev, *Essential dimension*, in Quadratic forms – algebra, arithmetic, and geometry (R. Baeza, W.K. Chan, D.W. Hoffmann, and R. Schulze-Pillot, eds.), Contemporary Mathematics **493** (2009), 299–326.
- [Me<sub>2</sub>] A. Merkurjev, *A lower bound on the essential dimension of simple algebras*, preprint, <http://www.math.ucla.edu/~merkurev/publicat.htm>.
- [MR] A. Meyer, Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra and Number Theory, **3**, no. 4 (2009), 467–487.
- [Re] Z. Reichstein, *On the Notion of Essential Dimension for Algebraic Groups*, Transformation Groups, **5**, 3 (2000), 265–304.
- [RY] Z. Reichstein, B. Youssin, *Essential Dimensions of Algebraic Groups and a Resolution Theorem for  $G$ -varieties*, with an appendix by J. Kollar and E. Szabo, Canadian Journal of Mathematics, **52**, 5 (2000), 1018–1056.
- [Ro] M. Rost, *Essential dimension of twisted  $C_4$* , preprint, <http://www.math.uni-bielefeld.de/~rost/ed.html>
- [Se<sub>1</sub>] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, **42**, Springer-Verlag, 1977.
- [Se<sub>2</sub>] J.-P. Serre, *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.
- [Sh] I. R. Shafarevich, *Basic Algebraic Geometry*, vol. 1, 2nd edition, Springer-Verlag, 1994.

- [TV] D. Tossici, A. Vistoli, *On the essential dimension of infinitesimal group schemes*, preprint, <http://www.mathematik.uni-bielefeld.de/lag/man/377>
- [Vos<sub>1</sub>] V. E. Voskresenskiĭ, *Maximal tori without affect in semisimple algebraic groups*, *Mat. Zametki* **44** (1988), no. 3, 309–318, 410. English transl.: *Math. Notes* **44** (1988) (1989), no. 3–4, 651–655.
- [Vos<sub>2</sub>] V. E. Voskresenskiĭ, *Algebraic Groups and Their Birational Invariants*, American Mathematical Society, Providence, RI, 1998.
- [Wa] W. C. Waterhouse, *Introduction to affine group schemes*. Springer-Verlag, New York-Berlin, 1979.