J. reine angew. Math. **677** (2013), 1—13
DOI 10.1515/crelle.2012.010

Journal für die reine und
angewandte Mathematik

Essential dimension of algebraic tori

By *Roland Lötscher* at München, *Mark MacDonald* at Vancouver,
Aurel Meyer at Orsay and *Zinovy Reichstein* at Vancouver

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 an affine algebraic group (i.e., an affine group scheme of finite type) over k. We do not assume that G is smooth. Unless otherwise specified, all fields are assumed to contain k and all morphisms between them are assumed to be k-homomorphisms. Morphisms between algebraic k-groups 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 $\mathrm{Spec}(K)$. 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 $H^1(K_0, G) \to H^1(K, G)$. The minimal transcendence degree $\mathrm{trdeg}_k(K_0)$, where α descends to K_0, is called the *essential dimension of* α and is denoted by the symbol $\mathrm{ed}(\alpha)$. The *essential dimension of the group* G is the supremum of $\mathrm{ed}(\alpha)$, as K ranges over all field extensions of k and α ranges over $H^1(K, G)$. This numerical invariant of G has been extensively studied in recent years; see, e.g., [BuR], [R1], [R2], [BF], [Me1].

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

First author partially supported by the Swiss National Science Foundation (Schweizerischer Nationalfonds). Second author partially supported by an NSERC post-doctoral fellowship. Third author partially supported by a University Graduate Fellowship at the University of British Columbia. Fourth author (corresponding author) partially supported by NSERC Discovery and Accelerator Supplement grants.

p-dimension, $\mathrm{ed}(G;p)$, which is defined as follows. The *essential p-dimension* $\mathrm{ed}(\alpha;p)$ *of* $\alpha \in H^1(K,G)$ is the minimal value of $\mathrm{ed}(\alpha_L)$, as L ranges over all finite field extensions of K of degree prime to p. The *essential p-dimension* $\mathrm{ed}(G;p)$ *of G* is then the supremum of $\mathrm{ed}(\alpha;p)$ taken over all fields K containing k and all $\alpha \in H^1(K,G)$. For details on this notion, see [RY] or [Me1]. Clearly $0 \leqq \mathrm{ed}(G;p) \leqq \mathrm{ed}(G)$. It is also easy to check that if l/k is a finite extension of degree prime to p, then

$$\mathrm{ed}(G;p) = \mathrm{ed}(G_l;p); \tag{1}$$

see [Me1], Proposition 1.5. Here, as usual, $G_l := G \times_{\mathrm{Spec}\,k} \mathrm{Spec}(l)$ for any field extension l/k.

A representation $\psi : G \to \mathrm{GL}(V)$ 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 $U(k_{\mathrm{alg}})$ is trivial. Such a representation gives rise to an upper bound on the essential dimension,

$$\mathrm{ed}(G;p) \leqq \mathrm{ed}(G) \leqq \dim(V) - \dim(G); \tag{2}$$

see [Me1], Theorem 4.1, [R1], 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 pth root of unity (note that this implies $\mathrm{char}\,k \neq p$). The purpose of this paper is to establish a similar result for a large class of groups which includes all algebraic tori.

Let k_{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 $n \geqq 0$; G is said to be *of multiplicative type* if $G_{k_{\mathrm{sep}}}$ is diagonalizable, see, e.g., [V2], Section 3.4. Smooth connected groups of multiplicative type are precisely the algebraic tori. We will say that a k-group of multiplicative type is *split* over a field extension l/k if it is diagonalizable over l.

Recall that the *order* of an affine algebraic group F is defined as $|F| = \dim_k k[F]$. Affine algebraic groups of finite order are called *finite*. We will say that a representation $\psi : G \to \mathrm{GL}(V)$ 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*

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

where the minimum is taken over all p-faithful representations ψ of G. Moreover, if G is an extension of a p-group by a torus, then $\mathrm{ed}(G) = \mathrm{ed}(G;p)$.

The quantity $\min \dim(\psi)$ which appears in the statement of 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 Theorem 1.1 can be found in [Me2], [BM] and [M].

Note that Theorem 1.1 allows us to compute $\mathrm{ed}(G; p)$ 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),

$$\mathrm{ed}(G; p) = \mathrm{ed}(G_{k'}; p),$$

and the latter number is given by Theorem 1.1.

2. Preliminaries on groups of multiplicative type

Throughout this section, A will denote an algebraic group of multiplicative type over a field k, $X(A) := \mathrm{Hom}_{k_{\mathrm{sep}}}(A_{k_{\mathrm{sep}}}, \mathbb{G}_{m,k_{\mathrm{sep}}})$ the character group of $A_{k_{\mathrm{sep}}}$, and $\Gamma := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ the absolute Galois group of k. Here $X(A)$ 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., [W], §7.3. Let Diag denote the inverse of X, so that $\mathrm{Diag}(X(A)) \simeq A$.

Given a field extension l/k, A is *split* over l if and only if the absolute Galois group $\mathrm{Gal}(l_{\mathrm{sep}}/l)$ acts trivially on $X(A)$. If a torsion-free $\mathbb{Z}\Gamma$-module P has a basis which is permuted by Γ, then it is called a *permutation* module, and $\mathrm{Diag}(P)$ 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 [W], §7.4. The following is a variant of this construction for algebraic groups of multiplicative type. Set

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

where $X(A)_\Gamma$ is the module of co-invariants, defined as the largest quotient of $X(A)$ with trivial Γ-action. Clearly $\mathrm{Split}_k(A)$ 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* $\mathrm{Split}_k(A) \neq \{1\}$.

Proof. If B is a k-subgroup of A, then $\mathrm{Split}_k(B) \subset \mathrm{Split}_k(A)$, so it suffices to show that $\mathrm{Split}_k(A[p]) \neq \{1\}$. 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 $\mathrm{Gal}(l/k)$ 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., [S], 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 $\gamma \in \mathrm{Gal}(l/k)$. The quotient of $X(A)$ by the linear span of $e_2, \dots, e_n$ has trivial Γ-action. Hence the module of co-invariants $X(A)_\Gamma$ is non-trivial. We conclude that $\mathrm{Split}_k(A) = \mathrm{Diag}\big(X(A)_\Gamma\big)$ is non-trivial as well. □

Let G be an algebraic group whose centre $Z(G)$ is of multiplicative type. Then we define $C(G) := \mathrm{Split}_k\big(Z(G)[p]\big)$. 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,

$$\{1\} \neq \mathrm{Split}_k(N[p]) \subseteq \mathrm{Split}_k(A[p]) = C(A),$$

as desired. □

Now suppose l/k is a Galois splitting field of A and $\psi : A \to \mathrm{GL}(V)$ 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 $V(\chi) \subset V_l$ is the weight space associated to $\chi \in \Lambda$, i.e., the subspace of V_l, where A acts via χ. The Galois group $\Gamma = \mathrm{Gal}(l/k)$ permutes Λ and the 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 $e_j^\chi \in V(\chi)$ and $\gamma e_j^\chi = e_j^{\gamma\chi}$ for every $\gamma \in \Gamma$.

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

Choose a weight $\chi_0 \in \Lambda$. The stabilizer Γ_0 of χ_0 in Γ 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 Γ_0. Now for $\chi \in \Lambda$ and $j = 1, \dots, d$, set $e_j^\chi := \gamma(e_j)$, where $\gamma \in \Gamma$ takes χ_0 to χ. It is now easy to see that the e_j^χ are well defined and form an l-basis of V_l with the desired property. □

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

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

Let Δ be as in Lemma 2.3 and consider the k-torus $T := \mathrm{Diag}(\mathbb{Z}[\Delta])$, which is split over l and quasi-split over k. By our construction T is equipped with a representation

$$\rho : T \hookrightarrow \mathrm{GL}(V).$$

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

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

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

Proof. As we saw above, $\psi = \rho \circ \hat{\psi}$, where $\rho : T \to \mathrm{GL}(V)$ is generically free. If ψ is faithful, then $\hat{\psi} : A \to T$ is injective, and hence, ψ is generically free. □

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*

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

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

Proof. Given $\psi : A \to \mathrm{GL}(V)$ with kernel N, write $\psi : A \xrightarrow{\hat{\psi}} T \xhookrightarrow{\rho} \mathrm{GL}(V)$ as above, where T is a quasi-split k-torus of dimension $\dim T = \operatorname{rank} X(T) = \dim \psi$ which splits over l. Then $\ker \hat{\psi} = N$ and the cokernel of the induced map $X(\hat{\psi}) : X(T) \to X(A)$ 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 GL_n, where $n = \operatorname{rank} P$ ([V2], Section 6.1). A map $f : P \to X(A)$ of $\mathbb{Z}\Gamma$-modules with cokernel $X(N)$ then yields a representation $A \to \mathrm{Diag}(P) \hookrightarrow \mathrm{GL}_n$ with kernel N. □

3. A lower bound on essential p-dimension

Consider an exact sequence of algebraic groups over k

$$1 \to C \to G \to Q \to 1 \tag{3}$$

such that C is central in G and isomorphic to μ_p^r for some $r \geqq 0$. Given a character $\chi : C \to \mu_p$, we will, following [KM], denote by Rep^{χ} the set of irreducible representations

$$\phi : G \to \mathrm{GL}(V)$$

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*:

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

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

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

where the minimum is taken over all finite-dimensional representations ψ of G such that $\psi_{|C}$ is faithful.

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

$$H^1(K, Q) \to H^2(K, C) \xrightarrow{\chi_*} H^2(K, \mu_p) = \mathrm{Br}_p(K)$$

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

$$\mathrm{ed}(G; p) \geqq \sum_{i=1}^{r} \mathrm{ind}\, \beta(\chi_i) - \dim G, \tag{4}$$

see [Me1], Theorem 4.8, Example 3.7. Moreover, by [KM], Theorem 4.4, Remark 4.5,

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

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

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

such that $(\psi_i)_{|C}$ is scalar multiplication by χ_i.

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

$$\mathrm{ed}(G; p) \geqq \dim(\psi) - \dim G. \tag{5}$$

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

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 $B \subset A$ be a closed subgroup of (finite) index prime to p. Then* $\mathrm{ed}(A; p) = \mathrm{ed}(B; p)$.

Proof. The inequality $\mathrm{ed}(B; p) \leqq \mathrm{ed}(A; p)$ follows from [Me1], Corollary 4.3, since $\dim A = \dim B$.

To prove the opposite inequality, set $Q := A/B$ and let K/k be a field extension. In view of the exact sequence $H^1(K, B) \to H^1(K, A) \to H^1(K, Q)$, it suffices to show that every Q-torsor $X \to \mathrm{Spec}(K)$ splits over some finite field extension L/K whose degree is prime to p.

Since Q is a finite group, it follows that $K[X]$ is isomorphic to a direct product of local rings $(A_1, \mathfrak{m}_1), \dots, (A_r, \mathfrak{m}_r)$ each of which is finite-dimensional over K. Since

$$\sum_{i=1}^{r} \dim_K A_i = \dim_K K[X] = |Q|$$

is prime to p, after renumbering $A_1, \dots, A_r$ we may assume that $\dim_K A_1$ is prime to p. Note that $(\mathfrak{m}_1)^N = 0$ for some $N \geqq 1$. Let $L := A_1/\mathfrak{m}_1$ be the residue field. For each $i < N$ the quotient $(\mathfrak{m}_1)^i/(\mathfrak{m}_1)^{i+1}$ is an L-vector space and we have

$$\dim_K A_1 = \sum_{i=0}^{N-1} \dim_K (\mathfrak{m}_1)^i/(\mathfrak{m}_1)^{i+1}.$$

We conclude that the degree $[L : K]$ divides $\dim_K A_1$, hence is prime to p. Note that the projection $K[X] \to A_1 \to L$ yields an L-point of X. Thus X splits over L. □

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 $\pi : G \to G/N$ be the natural projection. Then*

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

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

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

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

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 $p_n : G \to G$ be given by $g \to g^n$. 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 are coprime, $(p_n)_*$ is an isomorphism. Moreover, N lies in the kernel of p_n and so $(p_n)_*$ factors through π_*:

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

In particular, π_* is injective. A similar argument shows that, composing these maps in the opposite order, we obtain an isomorphism

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

Therefore π_* is surjective and hence, bijective, as desired. □

Proof of Theorem 1.1. We will first prove $\mathrm{ed}(G;p) \geqq \min \dim(\psi) - \dim G$, 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 χ of $C(G)$ and any $\phi \in \mathrm{Rep}^{\chi}$, $\dim(\phi)$ is a power of p. By Theorem 3.1, $\mathrm{ed}(G;p) \geqq \min \dim(\psi) - \dim G$, where ψ 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 $\mathrm{ed}(G;p) \leqq \dim \psi - \dim G$ for any p-faithful representation ψ 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 $\mathrm{ed}(G) = \mathrm{ed}(G/N)$. Now ψ can be considered as a faithful representation of G/N. By Lemma 2.5, this representation of G/N is generically free. By (2),

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

as desired.

Taking ψ to be of minimal dimension, we also see that in this case we have

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

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 $\mathrm{Diag}\big(X(F)/Y\big)$, where Y is the submodule of elements of order prime to p.

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

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

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

5. Main theorem in the language of character modules

Let Γ be a finite group and X a $\mathbb{Z}\Gamma$-module. We will call a map of $\mathbb{Z}\Gamma$-modules $P \to X$ a *p-presentation* of X if P is a 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 type over k, l/k be a finite Galois splitting field of G, and Γ_p be a Sylow p-subgroup of* $\mathrm{Gal}(l/k)$. *Then*

$$\mathrm{ed}(G; p) = \min \mathrm{rank}(\ker \phi),$$

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

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

$$\mathrm{ed}(G_{k'}; p) = \min \dim(\psi) - \dim G,$$

where the minimum is taken over all p-faithful representations ψ of $G_{k'}$. By Lemma 2.6

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

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

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

Example 5.3. Let l/k be a Galois extension with Galois group the symmetric group $\Gamma = \mathscr{S}_{p^r}$ for some $r \geqq 1$. Let T be a torus with character lattice

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

where Γ naturally permutes $a_1, \ldots, a_{p^r}$. Let Γ_p be a Sylow p-subgroup of Γ. In [MR], Section 6 and Proposition 7.2, it is shown that the minimal rank of a permutation module with a p-presentation to $X(T)$, viewed as $\mathbb{Z}\Gamma_p$-module, is p^{2r-1}. Thus by Corollary 5.1,

$$\mathrm{ed}(T; p) = p^{2r-1} - p^r + 1.$$

For our next example, recall that an algebraic group G over k is called *special* if it satisfies $H^1(l, G) = 0$ for all field extensions l/k.

Example 5.4. Let T be an algebraic torus and let Γ be the Galois group of a Galois splitting field of T. It is a deep result of J.-L. Colliot-Thélène and J.-J. Sansuc (see [CTS], Proposition 7.4, and [BR], Theorem 1.1) that T is special iff $X(T)$ is an invertible $\mathbb{Z}\Gamma$-module (i.e., a direct summand of a permutation $\mathbb{Z}\Gamma$-module). The following local-global argument, which considers each prime separately, gives a new, shortened proof of this result.

Proof. Assume T is special. Then $\mathrm{ed}(T;p) = 0$ for all primes p. By Corollary 5.1 we know $X(T)_{(p)}$ is a permutation $\mathbb{Z}_{(p)}\Gamma_p$-lattice for each Sylow p-subgroup Γ_p of Γ. Here $\mathbb{Z}_{(p)}$ denotes the localization of the ring of integers at the prime ideal (p) and $X(T)_{(p)} := X(T) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. So by [CR], 31.7, $X(T)$ is an invertible $\mathbb{Z}\Gamma_p$-module for each Sylow p-subgroup Γ_p of Γ and all primes p. Thus by [CW], Lemma 1, $X(T)$ is an invertible $\mathbb{Z}\Gamma$-module. The converse argument is easy. □

6. Forms of μ_n

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

Proof. Let Γ_p be a Sylow p-subgroup of $\mathrm{Gal}(l/k)$ and $\phi : P \to X(A)$ be a p-presentation of $X(A)$, viewed as $\mathbb{Z}\Gamma_p$-module. Note that, on the one hand, $X(A)$ is a cyclic p-group, and on the other hand, the index $[X(A) : \phi(P)]$ is finite and prime to p. We thus conclude that ϕ is surjective.

If Λ is a basis of P, permuted by Γ_p, then some element $\lambda \in \Lambda$ maps to a generator a of $X(A)$. Moreover, Γ_p acts faithfully on $X(A)$ and $|\Lambda| \geqq |\Gamma_p \lambda| \geqq |\Gamma_p a| = |\Gamma_p|$. Conversely we have a surjective homomorphism $\mathbb{Z}[\Gamma_p a] \to X(A)$ that sends a to itself. So the minimal value of $\mathrm{rank}(P)$ is $|\Gamma_p|$. Now apply Corollary 5.1. □

Remark 6.2. For $\mathrm{char}\, k \neq p$, 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 [B]. The case of constant cyclic groups of arbitrary prime power order is due to M. Florence [F].

Example 6.3. Let $\mathrm{char}\, k = p$. 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 $\leqq n$. The following example, with $n = 2$ and $p > 2$, answers this question in the negative.

Let l/k be a cyclic extension of degree p; set $\Gamma := \mathrm{Gal}(l/k)$. (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 Γ-module obtained by identifying Γ with the unique subgroup of

$$\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{Z}/p(p-1)\mathbb{Z}$$

of order p. By construction $G = \mathrm{Diag}(M)$ is a form of μ_{p^2} defined over k, whose minimal Galois splitting field is l. Proposition 6.1 now tells us that

$$\mathrm{ed}(G) = \mathrm{ed}(G; p) = [l : k] = p > 2. \quad \square$$

7. Twisted p-groups

In this section we will use Theorem 3.1 to extend the Karpenko–Merkurjev Theorem to arbitrary (possibly twisted) finite p-groups as follows.

Theorem 7.1. *Assume that* $\mathrm{char}\, k \neq p$ *and* k *contains a primitive* p*th root of unity. Let* G *be a finite* p*-group defined over* k, *which becomes constant over some Galois extension* l/k *such that* $[l : k]$ *is a power of* p. *Then*

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

where ψ *runs through all faithful* k*-representations of* G.

Proof. The inequalities $\mathrm{ed}(G; p) \leqq \mathrm{ed}(G) \leqq \min \dim \psi$ follow from (2), since by [BF], Proposition 4.13, every faithful representation of G is generically free. Hence it suffices to show that $\mathrm{ed}(G; p) \geqq \min \dim \psi$.

Since $\mathrm{char}\, k \neq p$ the centre of G is of multiplicative type, the subgroup

$$C(G) = \mathrm{Split}_k\big(Z(G)[p]\big)$$

is well-defined (as in Section 2) and is isomorphic to μ_p^r for some $r \geqq 1$.

We claim that the dimension of every irreducible k-representation ψ of G is a power of p. To prove this claim, denote by ζ a primitive root of unity of order equal to the exponent of $G(l)$. Since k contains a primitive pth root of unity, $l' := l(\zeta)$ is Galois over k and of p-power degree. Thus we may replace l by l', i.e., assume that l contains ζ.

Now ψ decomposes over l as a direct sum of absolutely irreducible representations of the abstract p-group $G(l)$. All direct summands in this decomposition have the same dimension, equal to a power of p. By [K], Theorem 5.22, the number of direct summands in this decomposition is also a power of p, and the claim follows.

Now Theorem 3.1 can be applied. It tells us that $\mathrm{ed}(G; p) \geqq \min \dim \psi$, where the minimum is taken over all representations ψ 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 pth 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 $\mathrm{ed}(G; p)$, at least in principle, for any étale algebraic group G over k, provided $\mathrm{char}(k) \neq p$.

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 pth 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 the field L. Indeed, the p-group $\mathrm{Gal}(E/L)$ permutes the Sylow subgroups of $G(E)$. By the Sylow Theorems, the number of such subgroups is prime to p. Thus at least one of them is fixed by the p-group $\mathrm{Gal}(E/L)$. This proves the claim.

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

Acknowledgement. The authors are grateful to A. Merkurjev and the referee for numerous constructive suggestions, including simplifying our earlier proofs of Proposition 4.2 and Lemma 4.1 respectively. The authors would also like to thank A. Auel and A. Vistoli for helpful discussions.

References

[AP] *H. Abold* and *W. Plesken*, Ein Sylowsatz für endliche p-Untergruppen von $\mathrm{GL}(n,Z)$, Math. Ann. **232** (1978), no. 2, 183–186.

[BM] *S. Baek* and *A. Merkurjev*, Essential dimension of central simple algebras, Acta Math., to appear.

[B] *G. Bayarmagnai*, Essential dimension of some twists of μ_{p^n}, RIMS Kôkyûroku Bessatsu **B4** (2007), 145–151.

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

[BR] *M. Borovoi* and *Z. Reichstein*, Toric-friendly groups, preprint 2010, http://arxiv.org/abs/1003.5894v2.

[BuR] *J. Buhler* and *Z. Reichstein*, On the essential dimension of a finite group, Compos. Math. **106** (1997), 159–179.

[CW] *G. Cliff* and *A. Weiss*, Summands of permutation lattices for finite groups, Proc. Amer. Math. Soc. **110** (1990), no. 1, 17–20.

[CTS] *J.-L. Colliot-Thélène* and *J.-J. Sansuc*, Principal homogeneous spaces under flasque tori: Applications, J. Alg. **106** (1087), 148–205.

[CR] *C. W. Curtis* and *I. Reiner*, Methods of representation theory, Volume 1, Wiley Interscience, New York 1981.

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

[KM] *N. Karpenko* and *A. Merkurjev*, Essential dimension of finite p-groups, Invent. Math. **172** (2008), 491–508.

[K] *G. Karpilovsky*, Clifford theory for group representations, North-Holland Math. Stud. **156**, North-Holland, Amsterdam 1989.

[M] *M. L. MacDonald*, Essential p-dimension of the normalizer of a maximal torus, Transform. Groups, to appear.

[Me1] *A. Merkurjev*, Essential dimension, in: Quadratic forms—Algebra, arithmetic, and geometry, R. Baeza, W. K. Chan, D. W. Hoffmann and R. Schulze-Pillot, eds., Contemp. Math. **493**, Amer. Math. Soc., Providence, RI, (2009), 299–326.

[Me2] *A. Merkurjev*, A lower bound on the essential dimension of simple algebras, Alg. Number Th. **4** (2010), no. 8, 1055–1076.

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

[R1] *Z. Reichstein*, On the notion of essential dimension for algebraic groups, Transform. Groups **5** (2000), no. 3, 265–304.

[R2] *Z. Reichstein*, Essential Dimension, Proc. Internat. Congr. Math. **2** (2010), World Scientific.

[RY] *Z. Reichstein* and *B. Youssin*, Essential dimensions of algebraic groups and a resolution theorem for G-varieties, with an appendix by J. Kollar and E. Szabo, Canad. J. Math. **52** (2000), no. 5, 1018–1056.

[Ro] *M. Rost*, Essential dimension of twisted C_4, preprint 2002, http://www.math.uni-bielefeld.de/~rost/ed.html.

[S] *J.-P. Serre*, Linear representations of finite groups, Grad. Texts Math. **42**, Springer-Verlag, Berlin 1977.

[Sh] *I. R. Shafarevich*, Basic algebraic geometry, Volume 1, Second edition, Springer-Verlag, Berlin 1994.
[TV] *D. Tossici* and *A. Vistoli*, On the essential dimension of infinitesimal group schemes, Amer. J. Math., to appear.
[V1] *V. E. Voskresenskiĭ*, Maximal tori without affect in semisimple algebraic groups, Mat. Zametki **44** (1988), no. 3, 309–318, 410; Trans. Math. Notes **44** (1988), no. 3, 651–655.
[V2] *V. E. Voskresenskiĭ*, Algebraic groups and their birational invariants, Amer. Math. Soc., Providence, RI, 1998.
[W] *W. C. Waterhouse*, Introduction to affine group schemes, Springer-Verlag, New York–Berlin 1979.

Mathematisches Institut, Universität München, 80333 München, Germany
e-mail: Roland.Loetscher@mathematik.uni-muenchen.de

Department of Mathematics, University of British Columbia, Vancouver V6T1Z2, Canada
e-mail: mlm@math.ubc.ca

Département de Mathématiques, Université Paris-Sud 11, 91405 Orsay, France
e-mail: aurel.meyer@math.u-psud.fr

Department of Mathematics, University of British Columbia, Vancouver V6T1Z2, Canada
e-mail: reichst@math.ubc.ca

Eingegangen 13. Juni 2010, in revidierter Fassung 24. Juni 2011