ESSENTIAL p-DIMENSION OF ALGEBRAIC GROUPS WHOSE CONNECTED COMPONENT IS A TORUS

ROLAND LÖTSCHER[1], MARK MacDONALD[2], AUREL MEYER[3], AND ZINOVY REICHSTEIN[4]

Abstract. 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.

Contents

1. Introduction

Let p be a prime integer and k a base field of characteristic $\neq p$. In this paper we will study the essential 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. We will use the notational conventions of

2000 *Mathematics Subject Classification.* 20G15, 11E72.

Key words and phrases. Essential dimension, algebraic torus, twisted finite group, generically free representation.

[1] Supported by the Deutsche Forschungsgemeinschaft, GI 706/2-1.

[2] Partially supported by a postdoctoral fellowship from the Canadian National Science and Engineering Research Council (NSERC).

[3] Supported by a postdoctoral fellowship from the Swiss National Science Foundation.

[4] Partially supported by a Discovery grant from the Canadian National Science and Engineering Research Council (NSERC).

[LMMR]. For background material and further references on the notion of essential dimension, see [Re_2].

For the purpose of computing $\mathrm{ed}(G;p)$ we may replace the base field k by a p-special closure $k^{(p)}$. A p-special closure of k is a maximal directed limit of finite prime to p extensions over k; for details see Section 2. The resulting field $k = k^{(p)}$ is then *p-special*, i.e. every field extension of k has p-power degree. (Some authors use the term "p-closed" in place of "p-special".) Furthermore, the finite group G/G^0 has a Sylow p-subgroup F defined over $k = k^{(p)}$; see [LMMR, Remark 7.2]. Since G is smooth we may replace G by the preimage of F without changing the essential p-dimension; see [LMMR, Lemma 4.1]. It is thus natural to restrict our attention to the case where G/G^0 is a finite p-group, i.e., to those G which fit into an exact sequence of k-groups of the form

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

where T is a torus and F is a smooth finite p-group. Note that F may be twisted (i.e. non-constant) and T may be non-split over k. Moreover, the extension (1.1) is not assumed to be split either.

To state our main result, recall that a linear representation $\rho\colon G \to \mathrm{GL}(V)$ is called *generically free* if there exists a G-invariant dense open subset $U \subset V$ such that the scheme-theoretic stabilizer of every point of U is trivial. A generically free representation is clearly faithful but the converse does not always hold; see below. We will say that ρ is *p-generically free* (respectively, *p-faithful*) if $\ker \rho$ is finite of order prime to p, and ρ descends to a generically free (respectively, faithful) representation of $G/\ker\rho$.

Theorem 1.1. *Let G be an extension of a (possibly twisted) finite p-group F by an algebraic torus T defined over a p-special field k of characteristic $\neq p$. Then*

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

where the minima are taken over all p-faithful linear representations ρ of G and p-generically free representations μ of G, respectively.

If $G = G^0$ is a torus or $G = F$ is a finite p-group then the upper and lower bounds of Theorem 1.1 coincide (see, [LMMR, Lemma 2.5] and [MR_1, Remark 2.1], respectively). In these cases Theorem 1.1 reduces to [LMMR, Theorems 1.1 and 7.1], respectively. In the case of constant finite p-groups this result is due to N. Karpenko and A. Merkurjev, whose work [KM] was the starting point for both [LMMR] and the present paper. We will show that the upper and lower bounds of Theorem 1.1 coincide for a larger class of groups, which we call *tame*; see Definition 1.2 and Theorem 1.3(b) below.

In general, groups G of the form (1.1) may have faithful (respectively, p-faithful) representations which are not generically free (respectively, p-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 [1]. It is, however, the source of many of the subtleties we will encounter.

To give the reader a better feel for this phenomenon, let us briefly consider the following "toy" example. Let $k = \mathbb{C}$, $p = 2$ and $G = \mathrm{O}_2$, the group of 2×2 orthogonal matrices. It is well known that $G \simeq \mathbb{G}_m \rtimes \mathbb{Z}/2\mathbb{Z}$, where $G^0 = \mathrm{SO}_2 = \mathbb{G}_m$ is a 1-dimensional torus. It is easy to see that the natural representation $i\colon G \hookrightarrow \mathrm{GL}_2$ is the unique 2-dimensional faithful representation of G. However this representation is not generically free: the stabilizer $\mathrm{Stab}_G(v)$ of every anisotropic vector $v = (a, b) \in \mathbb{C}^2$ is a subgroup of $G = \mathrm{O}_2$ of order 2 generated by the reflection in the line spanned by v. Here "anisotropic" means $a^2 + b^2 \neq 0$; anisotropic vectors are clearly Zariski dense in $\mathbb{C}^2$. On the other hand, the 3-dimensional representation $i \oplus \det$ is easily seen to be generically free. Here det denotes the one-dimensional representation $\det\colon \mathrm{O}_2 \to \mathrm{GL}_1$. Since $\dim G = 1$, Theorem 1.1 yields $1 \leq \mathrm{ed}(\mathrm{O}_2; 2) \leq 2$. The true value of $\mathrm{ed}(\mathrm{O}_2; 2)$ is 2; see [Re$_1$, Theorem 10.3].

We now proceed to state our result about the gap between the upper and lower bounds of Theorem 1.1. The group $C(F)$ which appears in the definition below is the maximal split p-torsion subgroup of the center of F; for a precise definition, see Section 4.

Definition 1.2. Let G, $T := G^0$ and $\pi\colon G \to F := G/T$ be as in (1.1). Consider the natural (conjugation) action of F on T. 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 $\pi^{-1}(C(F))$.

For any group G as in (1.1) over a p-special field k, we define $\mathrm{gap}(G; p)$ to be the difference between the dimensions of a minimal p-faithful G-representation, and a minimal p-generically free G-representation. This is precisely the "gap" between the upper and lower bounds in Theorem 1.1.

Theorem 1.3. *Let k be a p-special field of characteristic $\neq p$ and G be as in* (1.1). *Then*

(a) $\mathrm{gap}(G; p) \leq \dim T - \dim T^{C(F)}$.

(b) If G is tame then $\mathrm{gap}(G; p) = 0$*, i.e.*

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

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

In many cases the lower bound of Theorem 1.1 is much larger than $\dim T$, so Theorem 1.3(a) may be interpreted as saying that the gap between the lower and upper bounds of Theorem 1.1 is not too wide, even if G is not tame.

As a consequence of Theorem 1.1, we will also prove the following "Additivity Theorem".

[1] More is known about faithful representations which are not generically free in the case where G is connected semisimple. For an overview of this topic, see [PV, Section 7].

Theorem 1.4. *Let k a p-special field of characteristic $\neq p$ and G_1, G_2 be groups such that* $\operatorname{gap}(G_1;p) = \operatorname{gap}(G_2;p) = 0$. *Then* $\operatorname{gap}(G_1 \times G_2;p) = 0$ *and* $\operatorname{ed}(G_1 \times G_2;p) = \operatorname{ed}(G_1;p) + \operatorname{ed}(G_2;p)$.

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 $G \to Q$ is an isogeny of degree prime to p then the essential p-dimensions of G and Q coincide. Sections 4, 5 and 6 are devoted to the proof of our Main Theorem 1.1. In Sections 7 and 8 we prove Theorem 1.3 and in Section 9 we prove the Additivity Theorem 1.4. In Section 10 we classify central extensions G of p-groups by tori of small essential p-dimension.

2. The p-special closure of a field

A field L is called *p-special* if every finite extension of L has degree a power of p. By [EKM, Proposition 101.16] there exists for every field K an algebraic field extension L/K such that L is p-special and every finite sub-extension of L/F 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 2.1. *Let K be a field with* $\operatorname{char} K \neq p$ *and let K_{alg} be an algebraic closure of K containing $K^{(p)}$.*

(a) *$K^{(p)}$ is a direct limit of finite extensions K_i/K of degree prime to p.*
(b) *The field $K^{(p)}$ is perfect.*
(c) *The cohomological q-dimension of* $\Psi = \operatorname{Gal}(K_{\mathrm{alg}}/K^{(p)})$ *is* $\operatorname{cd}_q(\Psi) = 0$ *for any prime $q \neq p$.*

Proof. (a)The finite sub-extensions K'/K of $K^{(p)}/K$ form a direct system with limit $K^{(p)}$. Moreover the degrees $[K' : K]$ are all prime to p. (b) Every finite extension of $K^{(p)}$ has p-power degree. Since $\operatorname{char} K \neq p$ it is separable. (c) By construction Ψ is a profinite p-group. The result follows from [Se, Cor. 2, I. 3]. □

We call a covariant functor $\mathcal{F}\colon \text{Fields}/k \to \text{Sets}$ *limit-preserving* if for any directed system of fields $\{K_i\}$, $\mathcal{F}(\varinjlim K_i) = \varinjlim \mathcal{F}(K_i)$. For example if G is an algebraic group, the functor $F_G = H^1(*, G)$ is limit-preserving; see [Ma, 2.1].

Lemma 2.2. *Let $\mathcal{F}$ be limit-preserving and $\alpha \in \mathcal{F}(K)$ an object. Denote the image of α in $\mathcal{F}(K^{(p)})$ by $\alpha_{K^{(p)}}$.*

(a) $\operatorname{ed}_{\mathcal{F}}(\alpha;p) = \operatorname{ed}_{\mathcal{F}}(\alpha_{K^{(p)}};p) = \operatorname{ed}_{\mathcal{F}}(\alpha_{K^{(p)}})$.
(b) $\operatorname{ed}(\mathcal{F};p) = \operatorname{ed}(\mathcal{F}_{k^{(p)}};p)$, *where* $\mathcal{F}_{k^{(p)}}\colon \text{Fields}/k^{(p)} \to \text{Sets}$ *denotes the restriction of $\mathcal{F}$ to* $\text{Fields}/k^{(p)}$.

Proof. (a) The inequalities $\mathrm{ed}_{\mathcal{F}}(\alpha; p) \geq \mathrm{ed}_{\mathcal{F}}(\alpha_{K^{(p)}}; p) = \mathrm{ed}_{\mathcal{F}}(\alpha_{K^{(p)}})$ are clear from the definition and since $K^{(p)}$ has no finite extensions of degree prime to p. It remains to prove $\mathrm{ed}_{\mathcal{F}}(\alpha; p) \leq \mathrm{ed}_{\mathcal{F}}(\alpha_{K^{(p)}})$. If L/K is finite of degree prime to p,

$$\mathrm{ed}_{\mathcal{F}}(\alpha; p) = \mathrm{ed}_{\mathcal{F}}(\alpha_L; p), \tag{2.1}$$

cf. [Me$_1$, 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 $K_0 \subset K^{(p)}$ and $\alpha_{K^{(p)}}$ comes from an element $\beta \in \mathcal{F}(K_0)$, so that $\beta_{K^{(p)}} = \alpha_{K^{(p)}}$. Write $K^{(p)} = \lim \mathcal{L}$, where $\mathcal{L}$ is a direct system of finite prime to p extensions of K. Then $K_0 = \lim \mathcal{L}_0$ with $\mathcal{L}_0 = \{L \cap K_0 \mid L \in \mathcal{L}\}$ and by assumption on $\mathcal{F}$, $\mathcal{F}(K_0) = \lim\limits_{L' \in \mathcal{L}_0} \mathcal{F}(L')$. 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 α_L and γ_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

$$\mathrm{ed}_{\mathcal{F}}(\alpha; p) = \mathrm{ed}_{\mathcal{F}}(\alpha_L; p) = \mathrm{ed}_{\mathcal{F}}(\gamma_L; p) \leq \mathrm{ed}_{\mathcal{F}}(\gamma_L) \leq \mathrm{ed}_{\mathcal{F}}(\alpha_{K^{(p)}}).$$

(b) This follows immediately from (a), taking α of maximal essential p-dimension. □

Proposition 2.3. *Let* $\mathcal{F}, \mathcal{G}\colon$ Fields $/k \to$ Sets *be limit-preserving functors and* $\mathcal{F} \to \mathcal{G}$ *a natural transformation. If the map*

$$\mathcal{F}(K) \to \mathcal{G}(K)$$

is bijective (resp. surjective) for any p-special field containing k then

$$\mathrm{ed}(\mathcal{F}; p) = \mathrm{ed}(\mathcal{G}; p) \quad (\textit{resp.}\ \ \mathrm{ed}(\mathcal{F}; p) \geq \mathrm{ed}(\mathcal{G}; p)).$$

Proof. Assume the maps are surjective. By Lemma 2.1(a), the natural transformation is p-surjective, in the terminology of [Me$_1$], so we can apply [Me$_1$, Prop. 1.5] to conclude $\mathrm{ed}(\mathcal{F}; p) \geq \mathrm{ed}(\mathcal{G}; p)$.

Now assume the maps are bijective. Let α be in $\mathcal{F}(K)$ for some K/k and β its image in $\mathcal{G}(K)$. We claim that $\mathrm{ed}(\alpha; p) = \mathrm{ed}(\beta; p)$. First, by Lemma 2.2 we can assume that K is p-special and it is enough to prove that $\mathrm{ed}(\alpha) = \mathrm{ed}(\beta)$.

Assume that β comes from $\beta_0 \in \mathcal{G}(K_0)$ for some field $K_0 \subset K$. Any finite prime to p extension of K_0 is isomorphic to a subfield of K (cf. [Me$_1$, Lemma 6.1]) and so also any p-special closure of K_0 (which has the same transcendence degree over k). We may therefore assume that K_0 is p-special. By assumption $\mathcal{F}(K_0) \to \mathcal{G}(K_0)$ and $\mathcal{F}(K) \to \mathcal{G}(K)$ are bijective. The unique element $\alpha_0 \in \mathcal{F}(K_0)$ which maps to β_0 must therefore map to α under the natural restriction map. This shows that $\mathrm{ed}(\alpha) \leq \mathrm{ed}(\beta)$. The other inequality always holds and the claim follows.

Taking α of maximal essential dimension, we obtain $\mathrm{ed}(\mathcal{F}; p) = \mathrm{ed}(\alpha; p) = \mathrm{ed}(\beta; p) \leq \mathrm{ed}(\mathcal{G}; p)$. □

3. p-isogenies

An isogeny of algebraic groups is a surjective morphism $G \to Q$ with finite kernel. If the kernel is of order prime to p we say that the isogeny is a p-isogeny. In this section we will prove Proposition 3.1 which says that p-isogenous groups have the same essential p-dimension.

Proposition 3.1. *Suppose $G \to Q$ is a p-isogeny of algebraic groups over a field k of characteristic $\neq p$. Then*

(a) For any p-special field K containing k the natural map $H^1(K, G) \to H^1(K, Q)$ is bijective.

(b) $\operatorname{ed}(G; p) = \operatorname{ed}(Q; p)$.

Example 3.2. Let E_6^{sc}, E_7^{sc} be simply connected simple groups of type E_6, E_7 respectively. In [GR, 9.4, 9.6] it is shown that if k is an algebraically closed field of characteristic $\neq 2$ and 3 respectively, then

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

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

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

For the proof of Proposition 3.1 will need two lemmas.

Lemma 3.3. *Let N be a finite algebraic group over a field k of characteristic $\neq p$. The following are equivalent:*

(a) p does not divide the order of N.

(b) p does not divide the order of $N(k_{\text{alg}})$.

If N is also assumed to be abelian, denote by $N[p]$ the p-torsion subgroup of N. The following are equivalent to the above conditions.

(a′) $N[p](k_{\text{alg}}) = \{1\}$.

(b′) $N[p](k^{(p)}) = \{1\}$.

Proof. (a) $\iff$ (b): Let N^0 be the connected component of N and $N^{et} = N/N^0$ the étale quotient. Recall that the order of a finite algebraic group N over k is defined as $|N| = \dim_k k[N]$ and $|N| = |N^0||N^{et}|$, see, for example, [Ta]. If $\operatorname{char} k = 0$, N^0 is trivial, if $\operatorname{char} k = q \neq p$ 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^{et} is. Since N^0 is connected and finite, $N^0(k_{\text{alg}}) = \{1\}$ and so $N(k_{\text{alg}})$ is of order prime to p if and only if the group $N^{et}(k_{\text{alg}})$ is. Then $|N^{et}| = \dim_k k[N^{et}] = |N^{et}(k_{\text{alg}})|$, cf. [Bou, V.29 Corollary].

(b) $\iff$ (a′) $\Rightarrow$ (b′) are clear.

(a′) $\Leftarrow$ (b′): Suppose $N[p](k_{\text{alg}})$ is nontrivial. The Galois group $\Gamma = \operatorname{Gal}(k_{\text{alg}}/k^{(p)})$ is a pro-p group and acts on the p-group $N[p](k_{\text{alg}})$. The image of Γ in $\operatorname{Aut}(N[p](k_{\text{alg}}))$ is again a (finite) p-group and the size of every Γ-orbit in $N[p](k_{\text{alg}})$ is a power of p. Since Γ fixes the identity in $N[p](k_{\text{alg}})$, this is only possible if it also fixes at least $p-1$ more elements. It follows that $N[p](k^{(p)})$ is non-trivial. □

Remark 3.4. Part (b$'$) could be replaced by the slightly stronger statement that $N[p](k^{(p)} \cap k_{\text{sep}}) = \{1\}$, but we will not need this in the sequel.

Proof of Proposition 3.1. (a) Let N be the kernel of $G \to Q$ and K be a p-special field over k. Since $K_{\text{sep}} = K_{\text{alg}}$ (see Lemma 2.1(b)), the sequence of K_{sep}-points $1 \to N(K_{\text{sep}}) \to G(K_{\text{sep}}) \to Q(K_{\text{sep}}) \to 1$ 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 [Se, I.5, ex. 2] this implies that $H^1(K, N) = \{1\}$. Similarly, if ${}_cN$ is the group N twisted by a cocycle $c : \Psi \to G$, ${}_cN(K_{\text{sep}}) = N(K_{\text{sep}})$ is of order prime to p and $H^1(K, {}_cN) = \{1\}$. It follows that $H^1(K, G) \to H^1(K, Q)$ is injective, cf. [Se, I.5.5].

Surjectivity is a consequence of [Se, I. Proposition 46] and the fact that the q-cohomological dimension of Ψ is 0 for any divisor q of $|N(K_{\text{sep}})|$ (Lemma 2.1(c)).

This concludes the proof of part (a). Part (b) follows from part (a) and Proposition 2.3. □

4. Proof of the Main Theorem: an overview

We will assume throughout this section that the field k is p-special of $\operatorname{char} k \neq p$, and G is a smooth affine k-group, such that $G^0 = T$ is a torus and $G/G^0 = F$ is a finite p-group, as in (1.1).

The upper bound in Theorem 1.1 is an easy consequence of Proposition 3.1. Indeed, suppose $\mu \colon G \to \text{GL}(V)$ is a p-generically free representation. That is, $\operatorname{Ker} \mu$ is a finite group of order prime to p and μ descends to a generically free representation of $G' := G/\operatorname{Ker} \mu$. 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 [BF, Lemma 4.11] or [Me$_1$, Corollary 4.2]. This completes the proof of the upper bound in Theorem 1.1.

The rest of this section will be devoted to outlining a proof of the lower bound of Theorem 1.1. 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 [LMMR, Theorem 3.1], which we reproduce as Theorem 4.1 below for the reader's convenience.

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

$$1 \to C \to G \to Q \to 1$$

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

Assume further that

$$\gcd\{\dim \phi \mid \phi \in \text{Rep}^\chi\} = \min\{\dim \phi \mid \phi \in \text{Rep}^\chi\} \tag{4.1}$$

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

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

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

To prove the lower bound of Theorem 1.1, we will apply Theorem 4.1 to the exact sequence

$$1 \to C(G) \to G \to Q \to 1\,. \tag{4.2}$$

where $C(G)$ is a central subgroup of G defined as follows. Recall from [LMMR, Section 2] that if A is a k-group of multiplicative type, $\operatorname{Split}_k(A)$ is defined as the maximal split k-subgroup of A. That is, if $X(A)$ is the character $\operatorname{Gal}(k_{\text{sep}}/k)$-lattice of A then the character lattice of $\operatorname{Split}_k(A)$ is defined as the largest quotient of $X(A)$ with trivial $\operatorname{Gal}(k_{\text{sep}}/k)$-action.

If G be an extension of a finite p-group by a torus, as in (1.1), 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 torus. Since $\operatorname{char} k \neq p$ it is smooth. Moreover $Z(G)(k_{\text{alg}})$ consists of semi-simple elements. It follows that $Z(G)$ is of multiplicative type. We now define $C(G) := \operatorname{Split}_k(Z(G)[p])$.

In order to show that Theorem 4.1 can be aplied 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. *Let*

$$1 \to T \to G \to F \to 1$$

be an exact sequence of (linear) algebraic k-groups, where F is a finite p-group and T a torus. Then 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

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

where the minimum is taken over all representations $\rho \colon G \to \operatorname{GL}(V)$ such that $\rho_{|\,C(G)}$ is faithful. This resembles the lower bound of Theorem 1.1; the only difference is that in the statement of Theorem 1.1 we take the minimum over p-faithful representations ρ, and here we 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 1.1.

Proposition 4.3. *A finite-dimensional representation ρ 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 $\min\dim\rho - \dim G \leq \mathrm{ed}(G;p)$ of Theorem 1.1, where ρ 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 $\mathrm{Gal}(k_{\mathrm{sep}}/k)$-character lattice $X(T)$ of T is a direct summand of a permutation lattice, but $X(T)$ itself is not permutation (see [CTS$_1$, 8A.] for an example of such a lattice).

In other words, there exists a k-torus T' such that $T \times T'$ is quasi-split. This implies that $H^1(K, T \times T') = \{1\}$ and thus $H^1(K,T) = \{1\}$ for any field extension K/k. Consequently $\mathrm{ed}(T;p) = 0$ 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 by [LMMR, Lemma 2.6] there exists a surjective homomorphism $f\colon P \to X(T)$ of $\mathrm{Gal}(k_{\mathrm{sep}}/k)$-lattices, where P is permutation and $\mathrm{rank}\, P = \dim T$. This implies that f has finite kernel and hence, is injective. We conclude that f is an isomorphism and thus $X(T)$ is a permutation $\mathrm{Gal}(k_{\mathrm{sep}}/k)$-lattice, a contradiction. □

5. Dimensions of irreducible representations

The purpose of this section is to prove Proposition 4.2. Recall that G^0 is a torus, which we denote by T and G/G^0 is a finite p-group which we denote by F. The case, where $T = \{1\}$, i.e., $G = F$ is an arbitrary (possibly twisted) finite p-group, is established in the course of the proof of [LMMR, Theorem 7.1]. Our proof of Proposition 4.2 below is based on leveraging this case as follows.

Lemma 5.1. *Let G be an algebraic group defined over a field k and*

$$F_1 \subseteq F_2 \subseteq \cdots \subset G$$

be an ascending sequence of finite k-subgroups whose union $\cup_{n\geq 1} F_n$ is Zariski dense in G. If $\rho\colon G \to \mathrm{GL}(V)$ is an irreducible representation of G then $\rho_{|\,F_i}$ is irreducible for sufficiently large integers i.

Proof. For each $d = 1, ..., \dim V - 1$ consider the G-action on the Grassmannian $\mathrm{Gr}(d,V)$ of d-dimensional subspaces of V. Let $X^{(d)} = \mathrm{Gr}(d,V)^G$ and $X_i^{(d)} = \mathrm{Gr}(d,V)^{F_i}$ be the subvariety of d-dimensional G- (resp. F_i-)invariant subspaces of V. Then $X_1^{(d)} \supseteq X_2^{(d)} \supseteq \ldots$ and since the union of the groups F_i is dense in G,

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

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

Since V does not have any G-invariant d-dimensional k-subspaces, we know that $X^{(d)}(k) = \emptyset$. Thus, $X_{m_d}^{(d)}(k) = \emptyset$, i.e., V does not have any F_{m_d}-invariant d-dimensional k-subspaces. Setting $m := \max\{m_1, \ldots, m_{\dim V - 1}\}$, we see that $\rho_{|\,F_m}$ is irreducible. □

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

$$F_1 \subseteq F_2 \subseteq \cdots \subset G$$

defined over k whose union $\cup_{n\geq 1} F_n$ is Zariski dense in G.

In fact, it suffices to construct one p-subgroup $F' \subset G$, defined over k such that F' surjects onto F. Indeed, once F' is constructed, we can define $F_i \subset G$ as the subgroup generated by F' and $T[p^i]$, for every $i \geq 0$. Since $\cup_{n\geq 1} F_n$ 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 5.2. *Let $1 \to T \to G \xrightarrow{\pi} F \to 1$ be an extension of a p-group F by a torus T over a field k, as in* (1.1)*. Then G has a p-subgroup F' with $\pi(F') = F$.*

In the case where F is split and k is algebraically closed this is proved in [CGR, p. 564]; cf. also the proof of [BS, Lemme 5.11].

Proof. Denote by $\widetilde{\mathrm{Ex}}^1(F,T)$ the group of equivalence classes of extensions of F by T. We claim that $\widetilde{\mathrm{Ex}}^1(F,T)$ is torsion. Let $\mathrm{Ex}^1(F,T) \subset \widetilde{\mathrm{Ex}}^1(F,T)$ be the classes of extensions which have a scheme-theoretic section (i.e. $G(K) \to F(K)$ is surjective for all K/k). There is a natural isomorphism $\mathrm{Ex}^1(F,T) \simeq H^2(F,T)$, where the latter one denotes Hochschild cohomology, see [DG, III. 6.2, Proposition]. By [Sch$_3$] 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 $M \mapsto \widetilde{\mathrm{Ex}}^i(F,M)$ and $M \mapsto \mathrm{Ex}^i(F,M)$ are both derived functors of the crossed homomorphisms $M \mapsto \mathrm{Ex}^0(F,M)$, where in the first case M is in the category of F-module sheaves and in the second, F-module functors, cf. [DG, III. 6.2]. Since F is finite and T an affine scheme, by [Sch$_1$, Satz 1.2 & Satz 3.3] there is an exact sequence of F-module schemes $1 \to T \to M_1 \to M_2 \to 1$ and an exact sequence $\mathrm{Ex}^0(F,M_1) \to \mathrm{Ex}^0(F,M_2) \to \widetilde{\mathrm{Ex}}^1(F,T) \to H^2(F,M_1) \simeq \mathrm{Ex}^1(F,M_1)$. The F-module sequence also induces a long exact sequence on $\mathrm{Ex}(F,*)$ and we have a diagram

$$\begin{tikzcd}
 & & \widetilde{\mathrm{Ex}}^1(F,T) \arrow[dr] & \\
\mathrm{Ex}^0(F,M_1) \arrow[r] & \mathrm{Ex}^0(F,M_2) \arrow[ur] \arrow[dr] & & \mathrm{Ex}^1(F,M_1) \\
 & & \mathrm{Ex}^1(F,T) \arrow[uu, hook] \arrow[ur] &
\end{tikzcd}$$

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

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

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

which shows that the given extension G comes from an extension F' of F by N. Then G is the pushout of F' by $N\to T$ 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 $N=\operatorname{Ker}\rho$. Recall that G is an algebraic group over a p-special field k of characteristic $\neq p$ such that G^0 is a torus, G/G^0 is a finite p-group, as in (1.1), and $C(G)$ is the split central p-subgroup of G defined in Section 4.

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

(i) N is finite of order prime to p,

(ii) $N\cap C(G)=\{1\}$,

(iii) $N\cap Z(G)[p]=\{1\}$,

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

Proof. (i)$\Longrightarrow$ (ii) is obvious, since $C(G)$ is a p-group.

(ii) $\Longrightarrow$ (iii). Assume the contrary: $A:=N\cap Z(G)[p]\neq\{1\}$. By [LMMR, Section 2]

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

contradicting (ii).

Our proof of the implication (iii) $\Longrightarrow$ (i) will rely on the following assertion:

Claim: Let M be a non-trivial normal finite p-subgroup of G such that the commutator (G^0,M) is trivial. Then $M\cap Z(G)[p]\neq\{1\}$.

To prove the claim, note that $M(k_{\mathrm{sep}})$ is non-trivial and the conjugation action of $G(k_{\mathrm{sep}})$ on $M(k_{\mathrm{sep}})$ factors through an action of the p-group $(G/G^0)(k_{\mathrm{sep}})$. Thus each orbit has p^n elements for some $n\geq 0$; consequently, the number of fixed points is divisible by p. The intersection $(M\cap Z(G))(k_{\mathrm{sep}})$ 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 (iii) $\Longrightarrow$ (i). For notational convenience, set $T := G^0$. Assume that $N \lhd G$ 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

$$1 \to N \cap T \to N \to \overline{N} \to 1\,, \tag{6.1}$$

where $\overline{N}$ is the image of N in 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 [Bo, Proposition 2.4, p. 59]. If N is not smooth, note that the map $c\colon N \times T \to G$ sending (n, t) to the commutator $ntn^{-1}t^{-1}$ descends to $\overline{c}\colon \overline{N} \times T \to G$ (indeed, $N \cap T$ clearly commutes with T). Since $|\overline{N}|$ is a power of p and $\mathrm{char}(k) \neq p$, $\overline{N}$ is smooth over k, and we can pass to the separable closure k_{sep} and apply the usual Zariski density argument to show that the image of $\overline{c}$ is trivial.

We thus conclude that $N \cap T$ is central in N. Since $\gcd(|N \cap T|, \overline{N}) = 1$, by [Sch$_2$, Corollary 5.4] the extension (6.1) splits, i.e., $N \simeq (N \cap T) \times \overline{N}$. This turns $\overline{N}$ into a finite p-subgroup of G with $(T, \overline{N}) = \{1\}$. The claim implies that $\overline{N}$ 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 1.1. □

7. Faithful versus generically free

Throughout this section we will assume that k is a p-special field of characteristic $\neq p$ and G is a (smooth) algebraic k-group such that $T := G^0$ is a torus and $F := G/G^0$ is a finite p-group, as in (1.1). As we have seen in the introduction, some groups of this type 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 π is the natural projection $G \to G/T = F$.

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

(a) G has only finitely many k-subgroups S such that $S \cap T = \{1\}$.

(b) Every faithful action of G on a geometrically irreducible variety X is generically free.

Proof. After replacing k by its algebraic closure k_{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 $F_0 \subset F$, there are only finitely many $S \subset G$ 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 π has at most finitely many sections $s\colon F \to G$. Fix one such section, $s_0\colon F \to G$. Denote the exponent of F by e. Suppose $s\colon F \to G$ is another section. Then for every $f \in F(k)$, we can write $s(f) = s_0(f)t$ for some $t \in T$. 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. We conclude that there are only finitely many choices of $s(f)$ for each $f \in F$. Hence, there are only finitely many sections $F \to G$, as claimed.

(b) The restriction of the G-action on X to T is faithful and hence, generically free; cf., e.g., [Lo, Proposition 3.7(A)]. Hence, there exists a dense open T-invariant subset $U \subset X$ such that $\mathrm{Stab}_T(u) = \{1\}$ for all $u \in U$. In other words, if $S = \mathrm{Stab}_G(u)$ then $S \cap T = \{1\}$. By part (a) G has finitely many non-trivial 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,

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

is a dense open T-invariant subset of X, and the stabilizer $\mathrm{Stab}_G(u)$ is trivial for every $u \in U'$. Replacing U' by the intersection of its (finitely many) $G(k_{\mathrm{alg}})$-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. [Lo, Proposition 3.7(A)]. Thus by [Ga, Exposé V, Théorème 10.3.1] (or [BF, Theorem 4.7]) X has a dense open T-invariant subvariety U defined over k, which is the total space of a T-torsor, $U \to Y := U/G$, where Y is also smooth and geometrically irreducible. Since G/T is finite, after replacing U by the intersection of its (finitely many) $G(k_{\mathrm{alg}})$-translates, we may assume that U is G-invariant.

The G-action on U descends to an F-action on Y (by descent). Now it is easy to see that the following conditions are equivalent:

(i) the G-action on X is generically free, and

(ii) the F-action on Y is generically free;

cf. [LR, Lemma 2.1]. Since F is finite, (ii) is equivalent to

(iii) F acts faithfully on Y.

Since k is p-special, Proposition 6.1 tells us that the kernel of the F-action on Y is trivial iff 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 from 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. Notice that $(G/K)/(T/K) = G/T = F$. So part (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 part (b) follows. □

Corollary 7.3. *Consider an action of a tame k-group G (see Definition 1.2) on a geometrically irreducible k-variety X.*

(a) If this action is faithful then it is generically free.

(b) If this action is p-faithful then it is is p-generically free.

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 part (a) to G/K. □

8. Proof of Theorem 1.3

In this section we will prove the following proposition, which implies Theorem 1.3(a). Theorem 1.3(b) is an immediate consequence of part (a) and Theorem 1.1 (or alternatively, of Corollary 7.3(b) and Theorem 1.1).

We continue to use the notational conventions and assumptions on k and G described at the beginning of Section 7.

Proposition 8.1. *Let $\rho\colon G \to \mathrm{GL}(V)$ be a linear representation of G.*

(a) If ρ is faithful then G has a generically free representation of dimension $\dim \rho + \dim T - \dim\ T^{C(F)}$.

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

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

Let K be the kernel of the $G_{C(F)}$ action on $\mathrm{Lie}(T)$. 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 $\neq p$; cf. [GR, Proof of 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 $\mathrm{Lie}(T^{C(F)})$, 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 $V \oplus W$ [MR$_1$, Lemma 3.2]. Finally, by Proposition 7.2(a), G acts generically freely on $V \oplus W$, as desired.

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

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

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

Remark 8.2. A similar argument shows that for any tame normal subgroup $H \subset G$ over a p-special field k, $\mathrm{gap}(G;p) \leq \mathrm{ed}(G/H;p)$.

9. Additivity

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

Lemma 9.1. *For $i = 1,2$ let G_i be an algebraic group defined over a field k and 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 [KM, 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 $\pi_i \colon G_1 \times G_2 \to G_i$ be the natural projection and $\epsilon_i \colon G_i \to G_1 \times G_2$ be the natural inclusion.

If ρ_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

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

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

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

with this property. Let $\rho_1, \rho_2, \ldots, \rho_n$ denote the irreducible decomposition factors in a decomposition series of ρ. Since $C_1 \times C_2$ is central in $G_1 \times G_2$, each ρ_i restricts to a multiplicative character of $C_1 \times C_2$ which we will denote by χ_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 $d_i = \dim V_i$. 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 assume that $\rho = \rho_1 \oplus \cdots \oplus \rho_n$. Since C_i is isomorphic to $\mu_p^{r_i}$, we will think of $(C_1 \times C_2)^*$ as a $\mathbb{F}_p$-vector space of dimension r_1 + r_2. Since (i) $\Leftrightarrow$ (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 ρ_j by ρ'_j, where ρ'_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, ρ' will then be of the form $\alpha_1 \circ \pi_1 \oplus \alpha_2 \circ \pi_2$, where α_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

$$\begin{aligned} f(G_1 \times G_1; C_1 \times C_2) = \dim \rho = \dim \rho' &= \dim \alpha_1 + \dim \alpha_2 \\ &\geq f(G_1, C_1) + f(G_2, C_2)\,, \end{aligned}$$

as desired.

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

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

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

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

Since $\chi_1, \dots, \chi_n$ form a basis $(C_1 \times C_2)^*$ 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 $\operatorname{Span}_{\mathbb{F}_p}(\chi_1, \dots, \chi_{j-1}, \chi_{j+1}, \dots, \chi_n)$. Set

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

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

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

to C is faithful. This completes the proof of the claim and thus of Lemma 9.1. □

Proof of Theorem 1.4. Clearly $G_1 \times G_2$ is again a p-group extended by a torus.

Reall 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

$$C(G_1 \times G_2) = C(G_1) \times C(G_2)\,;$$

cf. [LMMR, Lemma 2.1]. Lemma 9.1 and Proposition 4.3 show that 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 $\operatorname{gap}(G_i; p) = 0$, there exists a p-generically free representation ρ_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 $\operatorname{gap}(G_1 \times G_2; p) = 0$. By Theorem 1.1

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

cf. Proposition 4.3, and similarly for G_1 and G_2. Hence the equality $\operatorname{ed}(G; p) = \operatorname{ed}(G_1; p) + \operatorname{ed}(G_2; p)$ follows. This concludes the proof. □

Example 9.2. Let T be a torus over a field k. Suppose there exists an element τ in the absolute Galois group $\operatorname{Gal}(k_{\text{sep}}/k)$ which acts on the character lattice $X(T)$ via multiplication by -1. Then $\operatorname{ed}(T; 2) \geq \dim T$.

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 non-split one-dimensional torus T_1. Using [LMMR, Theorem 1.1] it is easy to see that $\operatorname{ed}(T_1; 2) = 1$. By the Additivity Theorem 1.4 we conclude that $\operatorname{ed}(T; 2) \geq \operatorname{ed}(T_K; 2) = \operatorname{ed}((T_1)^n; 2) = n \operatorname{ed}(T_1; 2) = \dim T$. □

We conclude this section with an example which shows, in particular, that the property $\operatorname{gap}(G; p) = 0$ is not preserved under base field extensions. Let T be an algebraic torus over a field p-special field k of characteristic $\neq p$ and F a non-trivial p-subgroup of the constant group S_n. Then we can form the wreath product

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

where F acts on T^n by permutations.

Example 9.3. $\operatorname{gap}(T \wr F; p) = 0$ if and only if $\operatorname{ed}(T; p) > 0$. Moreover,

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

Proof. Let W be a p-faithful T-representation of minimal dimension. By [LMMR, Theorems 1.1], $\operatorname{ed}(T; p) = \dim W - \dim T$.

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 $\operatorname{ed}(T; p) > 0$, 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, [MR$_1$, Lemma 3.3]. In particular, $\operatorname{gap}(T \wr F; p) = 0$ and

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

where the last equality follows from Theorem 1.4.

Now assume that $\operatorname{ed}(T; p) = 0$, 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 $\operatorname{gap}(T \wr F; p) > 0$. In order to compute its essential p-dimension of $T \wr F$ we use the fact that the natural projection $T \wr F \to F$ has a section. Hence, the map $H^1(-, T \wr F) \to H^1(-, F)$ also has a section and is, consequently, a surjection. This implies that $\operatorname{ed}(T \wr F; p) \geq \operatorname{ed}(F; p)$. Let W' be a faithful F-representation of dimension $\operatorname{ed}(F; p)$. The direct sum $W^{\oplus n} \oplus W'$ considered as a $T \wr F$ representation is p-generically free. So, $\operatorname{ed}(T \wr F; p) = \operatorname{ed}(F; p)$. □

10. Groups of low essential p-dimension

In [LMMR] 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 [LMMR, Example 5.4]. The following lemma 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 $\operatorname{ed}(G; p) = 0$.

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

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

Now $X/G^0 \to \operatorname{Spec}(K)$ is an irreducible F-torsor. Since $F \neq \{1\}$ is not connected, this torsor is non-split. As F is a p-group, X/G^0 remains non-split 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 G. Therefore $\operatorname{ed}(G; p) > 0$ by [Me$_1$, Proposition 4.4]. This contradicts the assumption $\operatorname{ed}(G; p) = 0$ and so F must be trivial. □

For the remainder of this section we will assume the base field k is of characteristic $\neq p$.

Proposition 10.2. *Let G be a central extension of a p-group F by a torus T. If $\operatorname{ed}(G; p) \leq p - 2$, then G is of multiplicative type.*

Proof. Without loss of generality, assume $k = k_{\mathrm{alg}}$. By Theorem 1.1, there is a p-faithful representation V of G, with $\dim V \leq \dim T + p - 2$.

First consider the case when V is faithful. By Nagata's theorem [Na] G is linearly reductive, hence we can write $V = \bigoplus_{i=1}^{r} V_i$ for some non-trivial 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 $K \subset G$ 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 5.2 is normal, so let $T_2 = G/F'$, which is also a torus. The kernel of the natural map $G \to T_1 \times T_2$ is contained in $K \cap F'$, which is trivial since p does not divide the order of K. In other words, G embeds into a torus, and hence is of multiplicative type. □

Example 10.3. Proposition 10.2 does not generalize to tame groups. For a counter-example, assume the p-special field k contains a primitive p^2-root of unity, and consider the group $G = \mathbb{G}_m^p \rtimes \mathbb{Z}/p^2$, where a generator in $\mathbb{Z}/p^2$ acts by cyclically permuting the p copies of $\mathbb{G}_m$. The group G is tame, because $C(\mathbb{Z}/p^2) = \mathbb{Z}/p = \mu_p$ 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 $\mathrm{ed}(G;p) = 1$ and hence, $\leq p-2$ for every odd prime p. There is a natural p-dimensional faithful representation ρ of G; ρ embeds $\mathbb{G}_m^p$ into GL_p diagonally, in the standard basis $e_1, \dots, e_p$, and $\mathbb{Z}/p^2$ cyclically permutes $e_1, \dots, e_p$. Taking the direct sum of ρ with the 1-dimensional representation $\chi \colon G \to \mathbb{Z}/p^2 = \mu_{p^2} \hookrightarrow \mathbb{G}_m = \mathrm{GL}_1$, we obtain a faithful $p+1$-dimensional representation $\rho \oplus \chi$ which is therefore generically free by Corollary 7.3 (this can also be verified directly). Hence, $\mathrm{ed}(G;p) \leq (p+1) - \dim(G) = 1$. On the other hand, by Lemma 10.1, we see that $\mathrm{ed}(G;p) \geq 1$ and thus $= 1$, as claimed. □

Let Γ_p a finite p-group, and let $\phi : P \to X$ be a map of $\mathbb{Z}\Gamma_p$-modules. As in [LMMR], we will call ϕ 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 $\overline{X} := X/(pX + IX)$ the largest p-torsion quotient with trivial Γ_p-action. The induced map on quotient modules will be denoted $\bar{\phi} : \overline{P} \to \overline{X}$.

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

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

Proof. This is shown in [Me$_2$, proof of Theorem 4.3], and from a different perspective in [LMMR, Lemma 2.2]. □

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) $\mathrm{ed}(G;p) \leq r$

(b) *G is of multiplicative type and there is a p-presentation $P \to X(G)$ whose kernel is isomorphic to the trivial $\mathbb{Z}\Gamma_p$-module $\mathbb{Z}^r$.*

Proof. Assuming (a), by Proposition 10.2 G is of multiplicative type. By [LMMR, Corollary 5.1] we know there is a p-presentation $P \to X(G)$, whose kernel L is of free of rank $\operatorname{ed}(G;p) \leq p-2$. By [AP, Satz], Γ_p must act trivially on L.

(b) ⇒ (a) follows from [LMMR, Corollary 5.1]. □

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

(a) $\operatorname{ed}(G;p) = r$,

(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 Λ is a Γ_p-invariant basis of P.

Proof. $(a) \Leftrightarrow (b)$: We have a commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}^r \arrow[r] \arrow[d] & P \arrow[r, "\phi"] \arrow[d] \arrow[dr] & X(G) \arrow[d] \\
 & (\mathbb{Z}/p\mathbb{Z})^r \arrow[r] & \overline{P} \arrow[r, "\bar{\phi}"] & \overline{X(G)}
\end{tikzcd}$$

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 $\hat{P} \hookrightarrow P \to X(G)$ is then still a p-presentation of $X(G)$, by Lemma 10.4. Hence $\operatorname{ed}(G;p) \leq \operatorname{rank} \hat{P} - \dim G < \operatorname{rank} P - \dim G = r$.

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

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

Example 10.7. Let E be an étale algebra over a field k. It can be written as $E = \ell_1 \times \cdots \times \ell_m$ with some separable field extensions ℓ_i/k. The kernel of the norm map $n\colon \mathrm{R}_{E/k}(\mathbb{G}_m) \to \mathbb{G}_m$ is denoted by $\mathrm{R}^{(1)}_{E/k}(\mathbb{G}_m)$. Let $G = n^{-1}(\mu_{p^r})$ for some $r \geq 0$. It is a group of multiplicative type fitting into an exact sequence

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

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

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

with kernel generated by the element $(p^r, \cdots, p^r) \in P$. This element is fixed by Γ_p, so $\mathrm{ed}(G;p) \leq 1$. It satisfies condition (c) of Proposition 10.6 iff $r > 0$ or every Γ_p-set Γ/Γ_{ℓ_i} is fixed-point free. Note that Γ/Γ_{ℓ_i} has Γ_p-fixed points if and only if $[\ell_i : k] = |\Gamma/\Gamma_{\ell_i}|$ is prime to p. We thus have

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

References

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

[BF] G. Berhuy, G. Favi, *Essential Dimension: A Functorial Point of View (after A. Merkurjev)*, Documenta Math. **8** (2003), 279–330.

[Bo] A. Borel *Linear Algebraic Groups*, Benjamin (1969).

[BS] A. Borel, J.-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comment. Math. Helv. **39** (1964), 111–164.

[Bou] N. Bourbaki, *Algebra. II. Chapters 4–7.* Translated from the French by P. M. Cohn and J. Howie. Elements of Mathematics. Springer-Verlag, Berlin, (1990).

[CGR] V. Chernousov, Ph. Gille, Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), no. 2, 561–581.

[CTS$_1$] J.-L. Colliot-Thélène, J. J. Sansuc, *R-équvalence sur les tores*, Ann. scient. ENS **4**, 10 (1977), 175–230.

[DG] M. Demazure, P. Gabriel, *Groupes algébriques. Tome I*, Masson & Cie, Paris; North-Holland Publishing Co., Amsterdam, 1970.

[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).

[Ga] P. Gabriel, *Construction de préschémas quotient*, SGA 3, Exposé V (1963), in Réédition de SGA 3, available at `http://people.math.jussieu.fr/~polo/SGA3/`.

[GR] Ph. Gille, Z. Reichstein, *A lower bound on the essential dimension of a connected linear group*, Comment. Math. Helv. **4**, no. 1 (2009), 189–212.

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

[Lo] R. Lötscher, *Contributions to the essential dimension of finite and algebraic groups*, Ph.D. thesis (2010), available at `edoc.unibas.ch/1147/1/DissertationEdocCC.pdf`.

[LMMR] R. Lötscher, M. MacDonald, A. Meyer, Z. Reichstein, *Essential dimension of algebraic tori*, to appear in Crelle.

[Lor] M. Lorenz, *Multiplicative Invariant Theory*, Encyclopaedia of Mathematical Sciences, Springer (2005).

[LR] M. Lorenz, Z. Reichstein *Lattices and parameter reduction in division algebras*, MSRI preprint 2000-001, (2000), arXiv:math/0001026

[Ma] B. Margaux, *Passage to the limit in non-abelian Čech cohomology.* J. Lie Theory **17**, no. 3 (2007), 591–596.

[Me$_1$] 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$_2$] A. Merkurjev, *A lower bound on the essential dimension of simple algebras*, Algebra and Number Theory, **4**, no. 8, (2010), 1055–1076.

[MR$_1$] 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.

[Na] M. Nagata, *Complete reducibility of rational representations of a matric group*, J. Math. Kyoto Univ. **1** (1961–1962), 87–99.

[PV] V. L. Popov, E. B. Vinberg, *Invariant Theory*, in: *Algebraic Geometry* IV, Encyclopaedia of Mathematical Sciences, Vol. 55, Springer-Verlag, Berlin, 1994, pp. 123–284.

[Re$_1$] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformation Groups, **5**, 3 (2000), 265-304.

[Re$_2$] Z. Reichstein, *Essential Dimension*, Proceedings of the International Congress of Mathematicians, Vol. II, 162–188, Hindustan Book Agency, New Delhi, 2010.

[Sch$_1$] H.-J. Schneider, *Zerlegbare Erweiterungen affiner Gruppen* J. Algebra **66**, no. 2 (1980), 569–593.

[Sch$_2$] H.-J. Schneider, *Decomposable Extensions of Affine Groups*, in Lecture Notes in Mathematics **795**, Springer Berlin/Heidelberg (1980), 98–115.

[Sch$_3$] H.-J. Schneider, *Restriktion und Corestriktion für algebraische Gruppen* J. Algebra, **68**, no. 1 (1981), 177–189.

[Se] J.-P. Serre, *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.

[Ta] J. Tate, *Finite flat group schemes.* Modular forms and Fermat's last theorem (Boston, MA, 1995), 121–154, Springer, New York, 1997.

Mathematisches Institut, Universität München, 80333 München, Germany
E-mail address: `roland.loetscher@mathematik.uni-muenchen.de`

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

Départment de Mathématiques, Université Paris-Sud 11, 91405 Orsay, France
E-mail address: `aurel.meyer@math.u-psud.fr`

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