ESSENTIAL p-DIMENSION OF ALGEBRAIC TORI

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

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 broader class of groups, which includes all algebraic tori.

CONTENTS

2000 *Mathematics Subject Classification.* 20G15.

Key words and phrases. Essential dimension, algebraic torus, twisted finite group, lattice.

[1] Roland Lötscher was partially supported by the Swiss National Science Foundation (Schweizerischer Nationalfonds).

[2] Aurel Meyer was partially supported by a University Graduate Fellowship at the University of British Columbia.

[3] Zinovy Reichstein was partially supported by NSERC Discovery and Accelerator Supplement grants.

1. Introduction

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

We begin by recalling the notion of essential dimension of a functor from [BF]. Let Fields_k be the category of field extensions K/k, Sets be the category of sets, and $F\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor. As usual, given a field extension $k \subset K_0 \subset K$, we will denote the image of $\alpha \in F(K)$ under the natural map $F(K) \to F(L)$ by α_L.

An object $\alpha \in F(K)$ is said to *descend* to an intermediate field $k \subseteq K_0 \subseteq K$ if α is in the image of the induced map $F(K_0) \to F(K)$. The *essential dimension* $\mathrm{ed}_k(\alpha)$ is defined as the minimum of the transcendence degrees $\mathrm{trdeg}_k(K)$ taken over all fields $k \subseteq K_0 \subseteq K$ such that α descends to K_0. The essential dimension $\mathrm{ed}_k(F)$ of the functor F is defined as the maximal value of $\mathrm{ed}_k(\alpha)$, where the maximum is taken over all fields K/k and all $\alpha \in F(K)$.

Of particular interest to us will be the Galois cohomology functor $F_G := H^1(*, G)$, which associates to every K/k the set of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$. The essential dimension of this functor is usually called the *essential dimension of* G and is denoted by the symbol $\mathrm{ed}_k(G)$. Informally speaking, this number may be thought of a measure of complexity of G-torsors over fields. For example, if k is an algebraically closed field of characteristic 0 then groups G of essential dimension 0 are precisely the so-called *special groups*, i.e., algebraic groups G/k with the property that every G-torsor over $\mathrm{Spec}(K)$ is split, for every field K/k. These groups were classified by A. Grothendieck [Gro].

For many groups the essential dimension is hard to compute, even over the field $\mathbb{C}$ of complex numbers. The following related notion is often more accessible. Let $F\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor and p be a prime integer, as above. The *essential p-dimension* of $\alpha \in F(K)$, denoted $\mathrm{ed}_k(\alpha; p)$, is defined as the minimal value of $\mathrm{ed}_k(\alpha_{K'})$, where K' ranges over all finite field extensions of K whose degree is prime to p. The essential p-dimension of F, $\mathrm{ed}_k(F; p)$ of F is once again, defined as the maximal value of $\mathrm{ed}_k(\alpha; p)$, where the maximum is taken over all fields K/k and all $\alpha \in F(K)$, and once again we will write $\mathrm{ed}_k(G; p)$ in place of $\mathrm{ed}_k(F_G; p)$, where $F_G := H^1(*, G)$ is the Galois cohomology functor.

Note that $\mathrm{ed}_k(\alpha)$, $\mathrm{ed}_k(F)$, $\mathrm{ed}_k(G)$, $\mathrm{ed}_k(\alpha; p)$, etc., depend on k. We will write ed instead of ed_k if the reference to k is clear from the context. For background material on essential dimension we refer the reader to [BR, Re, RY, BF, Me_1].

We also remark that in the case of the Galois cohomology functor F_G, the maximal value of $\mathrm{ed}_k(\alpha)$ and $\mathrm{ed}_k(\alpha; p)$ in the above definitions is attained in the case where α is a versal G-torsor in the sense of [GMS, Section I.5].

Since every generically free linear representation $\rho\colon G \to \mathrm{GL}(V)$ gives rise to a versal G-torsor (see [GMS, Example I.5.4]), we obtain the inequality

$$\mathrm{ed}_k(G;p) \le \mathrm{ed}_k(G) \le \dim(V) - \dim(G)\,; \tag{1}$$

see [Re, Therem 3.4] or [BF, Lemma 4.11]. (Recall that ρ 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.)

N. Karpenko and A. Merkurjev [KM] recently showed that the inequality (1) is in fact sharp for finite constant p-groups.

Theorem 1.1. *Let G be a constant p-group and k be a field containing a primitive pth root of unity. Then*

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

where the minimum is taken over all faithful k-representations $G \hookrightarrow \mathrm{GL}(V)$.

The goal of this paper is to prove similar formulas for a broader class of groups G. To state our first result, let

$$1 \to C \to G \to Q \to 1 \tag{2}$$

be an exact sequence of algebraic groups over k such that C is central in G and isomorphic to μ_p^r for some $r \ge 0$. Given a character $\chi\colon C \to \mu_p$, we will, following [KM], denote by Rep^{χ} the set of irreducible representations $\phi\colon G \to \mathrm{GL}(V)$, defined over k, such that $\phi(c) = \chi(c)\,\mathrm{Id}_V$ for every $c \in C$.

Theorem 1.2. *Assume that k is a field of characteristic $\ne p$ containing a primitive pth root of unity. Suppose a sequence of k-groups of the form* (2) *satisfies the following condition:*

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

for every character $\chi\colon C \to \mu_p$. (Here, as usual, gcd *stands for the greatest common divisor.) Then*

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

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

Of particular interest to us will be extensions of finite p-groups by algebraic tori, i.e., k-groups G which fit into an exact sequence of the form

$$1 \to T \to G \to F \to 1\,, \tag{3}$$

where F is a finite p-group and T is a torus over k. Note that in this paper we will view finite groups F as algebraic groups over k, and will not assume they are constant, which is to say, the absolute Galois group of k may act non-trivially on the separable points of G. For the sake of computing $\mathrm{ed}_k(G;p)$ we may assume that k is a p-closed field (as in Definition 3.1); see Lemma 3.3. In this situation we will show that

(i) there is a natural choice of a split central subgroup $C \subset G$ in the sequence (2) such that

(ii) the conditions of Theorem 1.2 are always satisfied.

(iii) Moreover, if G is isomorphic to the direct product of a torus and a finite twisted p-group, then a variant of (1) yields an upper bound, matching the lower bound of Theorem 1.2.

This brings us to the main result of this paper. We will say that a representation $\rho\colon G \to \mathrm{GL}(V)$ of an algebraic group G is p-faithful if its kernel is finite and of order prime to p.

Theorem 1.3. *Let G be an extension of a (twisted) finite p-group F by an algebraic torus T defined over a field k (of characteristic not p). In other words, we have an exact sequence*

$$1 \to T \to G \to F \to 1\,.$$

Denote a p-closure of k by $k^{(p)}$ (see Definition 3.1). Then

(a) $\mathrm{ed}_k(G;p) \geq \min \dim(\rho) - \dim G$, *where the minimum is taken over all p-faithful linear representations ρ of $G_{k^{(p)}}$ over $k^{(p)}$.*

Now assume that G is the direct product of T and F. Then

(b) equality holds in (a), and

(c) over $k^{(p)}$ the absolute essential dimension of G and the essential p-dimension coincide:

$$\mathrm{ed}_{k^{(p)}}(G_{k^{(p)}}) = \mathrm{ed}_{k^{(p)}}(G_{k^{(p)}};p) = \mathrm{ed}_k(G;p).$$

If G is a p-group, a representation ρ is p-faithful if and only if it is faithful. However, for an algebraic torus, "p-faithful" cannot be replaced by "faithful"; see Remark 10.3.

Theorem 1.3 appears to be new even in the case where G is a twisted cyclic p-group, where it extends earlier work of Rost [Ro], Bayarmagnai [Ba] and Florence [Fl]; see Corollary 9.3 and Remark 9.4.

If G a direct product of a torus and an abelian p-group, the value of $\mathrm{ed}_k(G;p)$ given by Theorem 1.3 can be rewritten in terms of the character module $X(G)$; see Corollary 9.2. In particular, we obtain the following formula for the essential dimension of a torus.

Theorem 1.4. *Let T be an algebraic torus defined over a p-closed field $k = k^{(p)}$ of characteristic $\neq p$. Suppose $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ acts on the character lattice $X(T)$ via a finite quotient $\overline{\Gamma}$. Then*

$$\mathrm{ed}_k(T) = \mathrm{ed}_k(T;p) = \min \mathrm{rank}(L)\,,$$

where the minimum is taken over all exact sequences of $\mathbb{Z}_{(p)}\overline{\Gamma}$-lattices of the form

$$(0) \to L \to P \to X(T)_{(p)} \to (0)\,,$$

where P is permutation and $X(T)_{(p)}$ stands for $X(T) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$.

In many cases Theorem 1.4 renders the value of $\mathrm{ed}_k(T)$ computable by known representation-theoretic methods, e.g., from [CR]. We will give several examples of such computations in Sections 11 and 12. Another application was recently given by Merkurjev (unpublished), who used Theorem 1.4, in combination with techniques from [Me$_2$], to show that

$$\mathrm{ed}_k(\mathrm{PGL}_{p^r}; p) \geq (r-1)p^r + 1$$

for any $r \geq 1$. (For $r = 2$ the above inequality is the main result of [Me$_2$].) This represents dramatic improvement over the best previously known lower bounds on $\mathrm{ed}_k(\mathrm{PGL}_{p^r})$. The question of computing $\mathrm{ed}_k(\mathrm{PGL}_{p^r})$ is a long-standing open problem; for an overview, see [MR$_1$, MR$_2$].

It is natural to try to extend the formula of Theorem 1.3(b) to all k-groups G, whose connected component G^0 is a torus. For example, the normalizer of a maximal torus in any reductive k-group is of this form. For the purpose of computing $\mathrm{ed}_k(G; p)$ we may assume that k is p-closed and G/G^0 is a p-group; in other words, G is as in Theorem 1.3(a). Then

$$\min \dim \mu - \dim(G) \leq \mathrm{ed}(G; p) \leq \min \dim \rho - \dim G\,, \tag{4}$$

where the two minima are taken over all p-faithful representations μ, and p-generically free representations ρ, respectively. Here we say that a representation ρ of G is *p-generically free* if the $\ker(\rho)$ is finite of order prime to p, and ρ descends to a generically free representation of $G/\ker(\rho)$. The upper bound in (4) follows from (1), in combination with Theorem 6.1; the lower bound is Theorem 1.3(a). If G is a direct product of a torus and a p-group, then every p-generically free representation is p-faithful (see Lemma 7.1). In this case the lower and upper bounds of (4) coincide, yielding the exact value of $\mathrm{ed}_k(G; p)$ of Theorem 1.3(b). However, if we only assume G is a p-group extended by a torus, then faithful G-representations no longer need to be generically free. We do not know how to bridge the gap between the upper and the lower bound in (4) in this generality; however, in all of the specific examples we have considered, the upper bound turned out to be sharp. We thus put forward the following conjecture.

Conjecture 1.5. *Let G be an extension of a p-group by a torus, defined over a field k of characteristic $\neq p$. Then*

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

where the minimum is taken over all p-generically free representations ρ of $G_{k^{(p)}}$ over $k^{(p)}$.

The rest of the paper is structured as follows. Theorem 1.2 is proved in Section 2. Section 3 is devoted to preliminary material on the p-closure of a field. Theorem 1.3(a) is proved in Sections 4 and 5. In Section 6 we will show that if $G \to Q$ is a p-isogeny then $\mathrm{ed}_k(G; p) = \mathrm{ed}_k(Q; p)$. This result playes a key role in the proof of Theorem 1.3(b) in Section 7. At the end of Section 7 we prove a formula for the essential p-dimension of any finite group G by passing to a Sylow p-subgroup defined over k; see Corollory 7.2.

In Section 8 we prove the following Additivity Theorem 8.1: If G_1 and G_2 are direct products of tori and p-groups, then

$$\operatorname{ed}_k(G_1 \times G_2; p) = \operatorname{ed}_k(G_1; p) + \operatorname{ed}_k(G_2; p)\,.$$

In Section 9 we restate and amplify Theorem 1.3(b) (with G abelian) in terms of $\operatorname{Gal}(k_{\mathrm{sep}}/k)$-modules; in particular, Theorem 1.4 stated above is a special case of Corollary 9.2 which is proved there. In Section 10 we prove Theorem 1.3(c) by using Theorem 1.3(b), additivity, and the lattice perspective from Section 9. The last two sections are intended to illustrate our results by computing essential dimensions of specific algebraic tori. In Section 11 we classify algebraic tori T of essential p-dimension 0 and 1; see Theorems 11.1 and 11.5. In Section 12 we compute the essential p-dimension of all tori T over a p-closed field k, which are split by a cyclic extension l/k of degree dividing p^2.

2. Proof of Theorem 1.2

Denote by $C^* := \operatorname{Hom}(C, \mu_p)$ the character group of C. Let $E \to \operatorname{Spec} K$ be a versal Q-torsor [GMS, Example 5.4], where K/k is some field extension, and let $\beta\colon C^* \to \operatorname{Br}_p(K)$ denote the homomorphism that sends $\chi \in C^*$ to the image of $E \in H^1(K, Q)$ in $\operatorname{Br}_p(K)$ under the map

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

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

$$\operatorname{ed}_k(G; p) \geq \sum_{i=1}^{r} \operatorname{ind} \beta(\chi_i) - \dim G, \tag{5}$$

see [Me_1, Theorem 4.8, Example 3.7]. Moreover, by [KM, Theorem 4.4, Remark 4.5]

$$\operatorname{ind} \beta(\chi_i) = \gcd \dim(\rho)\,,$$

where the greatest common divisor is taken over all (finite-dimensional) representations ρ of G such that $\rho_{|C}$ 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 ρ_i of G with

$$\operatorname{ind} \beta(\chi_i) = \dim(\rho_i)$$

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

Set $\rho := \rho_1 \oplus \dots \oplus \rho_r$. The inequality (5) can be written as

$$\operatorname{ed}_k(G; p) \geq \dim(\rho) - \dim G. \tag{6}$$

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

3. The p-closure of a field

Let K be a field extension of k and K_{alg} an algebraic closure. We will construct a field $K^{(p)}/K$ in K_{alg} with all finite subextensions of $K^{(p)}/K$ of degree prime to p and all finite subextensions of $K_{\text{alg}}/K^{(p)}$ of degree a power of p.

Fix a separable closure $K_{\text{sep}} \subset K_{\text{alg}}$ of K and denote $\Gamma = \text{Gal}(K_{\text{sep}}/K)$. Recall that Γ is profinite and has Sylow-p subgroups which enjoy similar properties as in the finite case, see for example [RZ] or [Wi]. Let Φ be a Sylow-p subgroup of Γ and K_{sep}^{Φ} its fixed field.

Definition 3.1. We call the field

$$K^{(p)} = \{a \in K_{\text{alg}} | a \text{ is purely inseparable over } K_{\text{sep}}^{\Phi}\}$$

a *p-closure* of K. A field K will be called *p-closed* if $K{=}K^{(p)}$.

Note that $K^{(p)}$ is unique in K_{alg} only up to the choice of a Sylow-p subgroup Φ in Γ. The notion of being p-closed does not depend on this choice.

Proposition 3.2.

(a) $K^{(p)}$ is a direct limit of finite extensions K_i/K of degree prime to p.
(b) Every finite extension of $K^{(p)}$ is separable of degree a power of p; in particular, $K^{(p)}$ is perfect.
(c) The cohomological dimension of $\Psi = \text{Gal}(K_{\text{alg}}/K^{(p)})$ is $\text{cd}_q(\Psi) = 0$ for any prime $q \neq p$.

Proof. (a) First note that K_{sep} is the limit of the directed set $\{K_{\text{sep}}^N\}$ over all normal subgroups $N \subset \Gamma$ of finite index. Let

$$\mathcal{L} = \{K_{\text{sep}}^{N\Phi} | N \text{ normal with finite index in } \Gamma\}.$$

This is a directed set, and since Φ is Sylow, the index of $N\Phi$ in Γ is prime to p. Therefore $\mathcal{L}$ consists of finite separable extensions of K of degree prime to p. Moreover, K_{sep}^{Φ} is the direct limit of fields L in $\mathcal{L}$.

If $\text{char}\, k = 0$, $K^{(p)} = K_{\text{sep}}^{\Phi}$ and we are done. Otherwise suppose $\text{char}\, k = q \neq p$. Let

$$\mathcal{E} = \{E \subset K_{\text{alg}} | E/L \text{ finite and purely inseparable for some } L \in \mathcal{L}\}.$$

$\mathcal{E}$ consists of finite extensions of K of degree prime to p, because a purely inseparable extension has degree a power of q. One can check that $\mathcal{E}$ forms a directed set.

Finally note that if a is purely inseparable over K_{sep}^{Φ} with minimal polynomial $x^{q^n} - l$ (so that $l \in K_{\text{sep}}^{\Phi}$), then l is already in some $L \in \mathcal{L}$ since K_{sep}^{Φ} is the limit of $\mathcal{L}$. Thus $a \in E = L(a)$ which is in $\mathcal{E}$ and we conclude that $K^{(p)}$ is the direct limit of $\mathcal{E}$.

(b) $K^{(p)}$ is the purely inseparable closure of K_{sep}^{Φ} in K_{alg} and $K_{\text{alg}}/K^{(p)}$ is separable, see [Win, 2.2.20]. Moreover, $\text{Gal}(K_{\text{alg}}/K^{(p)}) \simeq \text{Gal}(K_{\text{sep}}/K_{\text{sep}}^{\Phi}) =$

Φ is a pro-p group and so every finite extension of $K^{(p)}$ is separable of degree a power of p.

(c) See [Se$_2$, Cor. 2, I. 3]. □

We call a covariant functor $\mathcal{F}\colon \mathrm{Fields}/k \to \mathrm{Sets}$ *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 Galois cohomology functor $H^1(*, G)$ is limit-preserving; see [Ma, 2.1].

Lemma 3.3. *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) $\mathrm{ed}_k(\alpha; p) = \mathrm{ed}_k(\alpha_{K^{(p)}}; p) = \mathrm{ed}_k(\alpha_{K^{(p)}})$.
(b) $\mathrm{ed}_k(\mathcal{F}; p) = \mathrm{ed}_{k^{(p)}}(\mathcal{F}; p)$.

Proof. (a) The inequalities $\mathrm{ed}(\alpha; p) \geq \mathrm{ed}(\alpha_{K^{(p)}}; p) = \mathrm{ed}(\alpha_{K^{(p)}})$ are clear from the definition and Proposition 3.2(b) since $K^{(p)}$ has no finite extensions of degree prime to p. It remains to prove $\mathrm{ed}(\alpha; p) \leq \mathrm{ed}(\alpha_{K^{(p)}})$. If L/K is finite of degree prime to p,

$$\mathrm{ed}(\alpha; p) = \mathrm{ed}(\alpha_L; p), \tag{7}$$

cf. [Me$_1$, Proposition 1.5] and its proof. For the p-closure $K^{(p)}$ this is similar and uses (7) 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 $\mathcal{L}_0 = \{L \cap K_0 | L \in \mathcal{L}\}$ and by assumption on $\mathcal{F}$, $\mathcal{F}(K_0) = \varinjlim_{L' \in \mathcal{L}_0} \mathcal{F}(L')$. Thus there is a field $L' = L \cap K_0$ ($L \in \mathcal{L}$) and $\gamma \in \mathcal{F}(L')$ such that $\gamma_{K_0} = \beta$. Since 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 (7) we see that

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

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

Proposition 3.4. *Let $\mathcal{F}, \mathcal{G}\colon \mathrm{Fields}/k \to \mathrm{Sets}$ 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-closed field extension K/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 Proposition 3.2(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 $\operatorname{ed}(\alpha;p) = \operatorname{ed}(\beta;p)$. First, by Lemma 3.3 we can assume that K is p-closed and it is enough to prove that $\operatorname{ed}(\alpha) = \operatorname{ed}(\beta)$.

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-closure of K_0 (which has the same transcendence degree over k). We may therefore assume that K_0 is p-closed. 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 $\operatorname{ed}(\alpha) \leq \operatorname{ed}(\beta)$. The other inequality always holds and the claim follows.

Taking α maximal with respect to its essential dimension, we obtain $\operatorname{ed}(\mathcal{F};p) = \operatorname{ed}(\alpha;p) = \operatorname{ed}(\beta;p) \leq \operatorname{ed}(\mathcal{G};p)$. □

4. The group $C(G)$

As we indicated in the Introduction, our proof of Theorem 1.3(a) will rely on Theorem 1.2. To apply Theorem 1.2, we need to construct a split central subgroup C of G. In this section, we will explain how to construct this subgroup (we will call it $C(G)$) and discuss some of its properties.

Recall that an algebraic group G over a field k is said to be *of multiplicative type* if $G_{k_{\mathrm{sep}}}$ is diagonalizable over the separable closure k_{sep} of k; cf., e.g., [Vo, Section 3.4]. Here, as usual, $G_{k'} := G \times_{\operatorname{Spec} k} \operatorname{Spec}(k')$ for any field extension k'/k. Connected groups of multiplicative type are precisely the algebraic tori.

We will use the following common conventions in working with an algebraic group A of multiplicative type over k.

- We will denote the character group of A by $X(A)$.
- Given a field extension l/k, A is split over l if and only if the absolute Galois group $\operatorname{Gal}(l_{\mathrm{sep}}/l)$ acts trivially on $X(A)$.
- 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.

Let T be an algebraic torus. It is well known how to construct a maximal split subtorus of T, see for example [Bo, 8.15] or [Wa, 7.4]. The following definition is a variant of this.

Definition 4.1. Let A be an algebraic group of multiplicative type over k. Let $\Delta(A)$ be the Γ-invariant subgroup of $X(A)$ generated by elements of the form $x - \gamma(x)$, as x ranges over $X(A)$ and γ ranges over Γ. Define

$$\operatorname{Split}_k(A) = \operatorname{Diag}(X(A)/\Delta(A))\,.$$

Here Diag denotes the anti-equivalence between continuous $\mathbb{Z}\Gamma$-modules and algebraic groups of multiplicative type, cf. [Wa, 7.3].

Definition 4.2. Let G be an extension of a finite p-group by a torus, defined over a field k, as in (3). Then

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

where $Z(G)$ denotes the centre of G.

Lemma 4.3. *Let A be an algebraic group of multiplicative type over k.*

(a) $\mathrm{Split}_k(A)$ *is split over k,*
(b) $\mathrm{Split}_k(A) = A$ *if and only if A is split over k,*
(c) If B is a k-subgroup of A then $\mathrm{Split}_k(B) \subset \mathrm{Split}_k(A)$.
(d) For $A = A_1 \times A_2$, $\mathrm{Split}_k(A_1 \times A_2) = \mathrm{Split}_k(A_1) \times \mathrm{Split}_k(A_2)$,
(e) If $A[p] \neq \{1\}$ and A is split over a Galois extension l/k, such that $\overline{\Gamma} = \mathrm{Gal}(l/k)$ is a p-group, then $\mathrm{Split}_k(A) \neq \{1\}$.

Proof. Parts (a), (b), (c) and (d) easily follow from the definition.

Proof of (e): By part (c), 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 $\overline{\Gamma}$ acts. Any such action is upper-triangular, relative to some $\mathbb{F}_p$-basis $e_1, \dots, e_n$ of $X(A)$; see, e.g., [Se_1, 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 $\gamma \in \overline{\Gamma}$. Our goal is to show that $\Delta(A) \neq X(A)$. Indeed, every element of the form $x - \gamma(x)$ is contained in the Γ-invariant submodule $\mathrm{Span}(e_2, \dots, e_n)$. Hence, these elements cannot generate all of $X(A)$. □

Proposition 4.4. *Suppose G is an extension of a p-group by a torus, defined over a p-closed field k. Suppose N is a normal subgroup of G defined over k. 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 Lemma 4.3

$$\{1\} \neq C(A) \subset N \cap C(Z(G)[p]) = N \cap C(G)\,,$$

contradicting (ii).

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

Claim: Let M be a non-trivial normal finite p-subgroup of G such that the commutator $(G^0, M) = \{1\}$. 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 $(M\cap Z(G))(k_{\rm sep})$ 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

$$1\to N\cap T\to N\to\overline{N}\to 1\,, \tag{8}$$

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 $(N,T)=\{1\}$ by Zariski density. 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 $k_{\rm sep}$ 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 (8) splits, i.e., $N\simeq(N\cap T)\times\overline{N}$. This turns $\overline{N}$ into a subgroup of G satisfying the conditions of the claim. Therefore $\overline{N}$ is trivial and $N=N\cap T$ is a finite group of order prime to p, as claimed. □

For future reference, we record the following obvious consequence of the equivalence of conditions (i) and (ii) in Proposition 4.4.

Corollary 4.5. *Let $k=k^{(p)}$ be a p-closed field and G be an extension of a p-group by a torus, defined over k, as in* (3)*. A finite-dimensional representation ρ of G defined over k is p-faithful if and only $\rho_{|\,C(G)}$ is faithful.* □

5. Proof of Theorem 1.3(a)

The key step in our proof will be the following proposition.

Proposition 5.1. *Let k be a p-closed field, and G be an extension of a p-group by a torus, as in* (3)*. Then the dimension of every irreducible representation of G over k is a power of p.*

Assuming Proposition 5.1 we can easily complete the proof of Theorem 1.3(a). Indeed, by Proposition 3.4 we may assume that $k=k^{(p)}$ is p-closed. In particular, since we are assuming that $\mathrm{char}(k)\neq p$, this implies that k contains a primitive pth root of unity. (Indeed, if ζ is a p-th root of unity in $k_{\rm sep}$ then $d=[k(\zeta):k]$ is prime to p; hence, $d=1$.) Proposition 5.1 tells us that Theorem 1.2 can be applied to the exact sequence

$$1\to C(G)\to G\to Q\to 1\,. \tag{9}$$

This yields

$$\operatorname{ed}(G;p) \geq \min \, \dim(\rho) - \dim(G)\,, \tag{10}$$

where the minimum is taken over all representations $\rho\colon G \to \mathrm{GL}(V)$ such that $\rho_{|C(G)}$ is faithful. Corollary 4.4 now tells us that $\rho_{|C(G)}$ is faithful if and only if ρ is p-faithful, and Theorem 1.3(a) follows. □

The rest of this section will be devoted to the proof of Proposition 5.1. We begin by settling it in the case where G is a finite p-group.

Lemma 5.2. *Proposition 5.1 holds if G is a finite p-group.*

Proof. Choose a finite Galois field extension l/k such that (i) G is constant over l and (ii) every irreducible linear representation of G over l is absolutely irreducible. Since k is assumed to be p-closed, $[l : k]$ is a power of p.

Let $A := k[G]^*$ be the dual Hopf algebra of the coordinate algebra of G. By [Ja, Section 8.6] a G-module structure on a k-vector space V is equivalent to an A-module structure on V. Now assume that V is an irreducible A-module and let $W \subseteq V \otimes_k l$ be an irreducible $A \otimes_k l$-submodule. Then by [Ka, Theorem 5.22] there exists a divisor e of $[l : k]$ such that

$$V \otimes l \simeq e\left(\bigoplus_{i=1}^{r} {}^{\sigma_i}W\right)\,,$$

where $\sigma_i \in \mathrm{Gal}(l/k)$ and $\{{}^{\sigma_i}W \mid 1 \leq i \leq r\}$ are the pairwise non-isomorphic Galois conjugates of W. By our assumption on k, e and r are powers of p and by our choice of l, $\dim_l W = \dim_l({}^{\sigma_1}W) = \ldots = \dim_l({}^{\sigma_r}W)$ is also a power of p, since it divides the order of G_l. Hence, so is $\dim_k(V) = \dim_l V \otimes l = e(\dim_l {}^{\sigma_1}W + \cdots + \dim_l {}^{\sigma_r}W)$. □

Our proof of Proposition 5.1 in full generality will based on leveraging Lemma 5.2 as follows.

Lemma 5.3. *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 defined over k 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, $X^{(d)}_{m_d}(k) = \emptyset$, i.e., V does not have any F_{m_d}-invariant d-dimensional k-subspaces. Setting $m := \max\{m_1, \dots, m_{\dim(V)-1}\}$, we see that $\rho_{|F_m}$ is irreducible. □

We now proceed with the proof of Proposition 5.1. By Lemmas 5.2 and 5.3, 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.

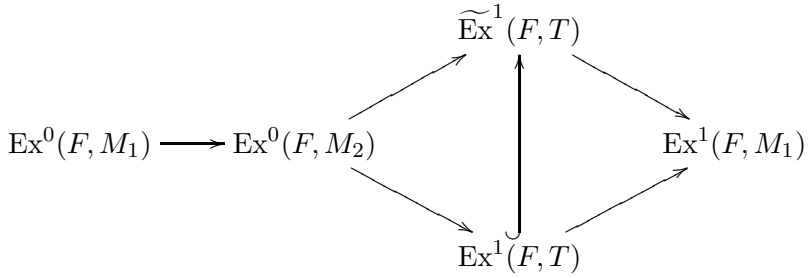
The following lemma, which establishes the existence of F', is thus the final step in our proof of Proposition 5.1 (and hence, of Theorem 1.3(a)).

Lemma 5.4. *Let $1 \to T \to G \xrightarrow{\pi} F \to 1$ be an extension of a p-group F by a torus T over k. Then G has a finite 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



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 we see that multiplying twice by the order m of F, $m^2 \cdot \widetilde{\mathrm{Ex}}^1(F,T) = 0$. 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. 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 Theorem 6.1 which says that p-isogenous groups have the same essential p-dimension. This result will play a key role in the proof of Theorem 1.3(b) in Section 7.

Theorem 6.1. *Suppose $G \to Q$ is a p-isogeny of algebraic groups over k. Then*

(a) For any p-closed field K containing k the natural map $H^1(K,G) \to H^1(K,Q)$ is bijective.
(b) $\mathrm{ed}_k(G;p) = \mathrm{ed}_k(Q;p)$.

Example 6.2. 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

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

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

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

We will need two lemmas.

Lemma 6.3. *Let N be a finite algebraic group over k ($\operatorname{char} k \neq p$). The following are equivalent:*

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

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

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′) $N[p](k_{\mathrm{alg}}) = \{1\}$.

(b′) $N[p](k^{(p)}) = \{1\}$.

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

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

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

Remark 6.4. Part (b′) could be replaced by the slightly stronger statement that $N[p](k^{(p)} \cap k_{\mathrm{sep}}) = \{1\}$, but we won't need this in the sequel.

Lemma 6.5. *Let Γ be a profinite group, G an (abstract) finite Γ-group and $|\Gamma|, |G|$ coprime. Then $H^1(\Gamma, G) = \{1\}$.*

The case where Γ is finite and G abelian is classical. In the generality we stated, this lemma is also known [Se_2, I.5, ex. 2].

Proof of Theorem 6.1. (a) Let N be the kernel of $G \to Q$ and $K = K^{(p)}$ be a p-closed field over k. Since $K_{\mathrm{sep}} = K_{\mathrm{alg}}$ (see Proposition 3.2(b)), the sequence of K_{sep}-points $1 \to N(K_{\mathrm{sep}}) \to G(K_{\mathrm{sep}}) \to Q(K_{\mathrm{sep}}) \to 1$ is exact. By Lemma 6.3, the order of $N(K_{\mathrm{sep}})$ is not divisible by p and therefore coprime to the order of $\Psi = \mathrm{Gal}(K_{\mathrm{sep}}/K)$. Thus $H^1(K, N) = \{1\}$ (Lemma 6.5). Similarly, if ${}_cN$ is the group N twisted by a cocycle $c : \Psi \to G$, ${}_cN(K_{\mathrm{sep}}) = N(K_{\mathrm{sep}})$ 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_2, I.5.5].

Surjectivity is a consequence of [Se_2, I. Proposition 46] and the fact that the q-cohomological dimension of Ψ is 0 for any divisor q of $|N(K_{\mathrm{sep}})|$ (Proposition 3.2).

This concludes the proof of part (a). Part (b) immediately follows from (a) and Proposition 3.4. □

7. Proof of Theorem 1.3(b)

Let k be a closed field and $G = T \times F$, where T is a torus and F is a finite p-group, defined over k. Our goal is to show that

$$\operatorname{ed}_k(G; p) \leq \dim(\rho) - \dim G\,, \tag{11}$$

where ρ is a p-faithful representation of G defined over k.

Lemma 7.1. *If a representation $\rho\colon G \to \mathrm{GL}(V)$ is p-faithful, then $G/\ker(\rho) \to \mathrm{GL}(V)$ is generically free. In other words, ρ is p-generically free.*

Proof. Since $\ker(\rho)$ has order prime to p, its image under the projection map $G = T \times F \to F$ is trivial. Hence $\ker(\rho) \subset T$ and T/N is again a torus. So without loss of generality, we may assume ρ is faithful.

Let $V_1 \subsetneq V$ be a closed subset of V such that T acts freely on $V \setminus V_1$. Let $n = p^r$ be the order of F and V_2 be the (finite) union of the fixed point sets of $1 \neq g \in T[n] \times F$. Here as usual, $T[n]$ denotes the n-torsion subgroup of T. Since ρ is faithful none of these fixed point sets are all of V, hence $U := V \setminus (V_1 \cup V_2)$ is a dense open subset of V.

We claim that $\mathrm{Stab}_G(v) = \{1\}$ for every $v \in U$. Indeed, assume $1 \neq g = (t, f) \in \mathrm{Stab}_G(v)$. Since $v \notin V_2$, $t^n \neq 1$. Then $1 \neq g^n = (t^n, 1)$ lies in both T and $\mathrm{Stab}_G(v)$. Since $v \notin V_1$, this is a contradiction. □

Now suppose ρ is any p-faithful representation of G. Then (1) yields

$$\operatorname{ed}_k(G/N; p) \leq \dim(\rho) - \dim(G/\ker(\rho)) = \dim(\rho) - \dim(G)\,.$$

By Theorem 6.1

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

as desired. This completes the proof of (11) and thus of Theorem 1.3(b). □

Corollary 7.2. *Let G be a finite algebraic group over a p-closed field $k = k^{(p)}$. Then G has a Sylow-p subgroup G_p defined over k and*

$$\operatorname{ed}_k(G; p) = \operatorname{ed}_k(G_p; p) = \operatorname{ed}_k(G_p) = \min \dim(\rho)$$

where the minimum is taken over all faithful representations of G_p over k.

Proof. By assumption, $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ is a pro-p group. It acts on the set of Sylow-p subgroups of $G(k_{\mathrm{sep}})$. Since the number of such subgroups is prime to p, Γ fixes at least one of them and by Galois descent one obtains a subgroup G_p of G. By Lemma 6.3, G_p is a Sylow-p subgroup of G. The first equality $\operatorname{ed}_k(G; p) = \operatorname{ed}_k(G_p; p)$ is shown in [MR$_1$, 4.1] (the reference is for smooth groups but can be generalized to the non-smooth case as well). The minimal G_p-representation ρ from Theorem 1.3(b) is faithful and thus $\operatorname{ed}_k(G_p) \leq \dim(\rho)$, see for example [BF, Prop. 4.11]. The Corollary follows. □

Remark 7.3. Two Sylow-p subgroups of G defined over $k = k^{(p)}$ do not need to be isomorphic over k.

8. An additivity theorem

The purpose of this section is to prove the following:

Theorem 8.1. *Let G_1 and G_2 be direct products of tori and p-groups over a field k. Then* $\operatorname{ed}_k(G_1 \times G_2; p) = \operatorname{ed}_k(G_1; p) + \operatorname{ed}_k(G_2; p)$.

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 (defined over k) such that $\rho_{|C}$ is faithful by $f(G, C)$.

Lemma 8.2. *For $i = 1, 2$ let G_i be an algebraic group defined over 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*

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

Our argument is a variant of the proof of [KM, Theorem 5.1], where G is assumed to be a (constant) finite p-group and C is the socle of G.

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 k-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 k-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 $\rho_1, \rho_2, \dots, \rho_n$ 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 $\chi_1^{\oplus d_1} \oplus \dots \oplus \chi_n^{\oplus d_n}$ 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 $\rho = \rho_1 \oplus \dots \oplus \rho_n$. 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 $\rho_1 \oplus \dots \oplus \rho_n$, 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 $\mathrm{Span}_{\mathbb{F}_p}(\chi_1, \dots, \chi_{j-1}, \chi_{j+1}, \dots, \chi_n)$. 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 8.2. □

Proof of Theorem 8.1. We can pass to a p-closure $k^{(p)}$ by Lemma 3.3. Let $C(G)$ be as in Definition 4.2. By Theorem 1.3(b)

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

cf. Corollary 4.5. Furthermore, we have $C(G_1 \times G_2) = C(G_1) \times C(G_2)$; cf. Lemma 4.3(d). Applying Lemma 8.2 finishes the proof. □

9. Modules and lattices

In this section we rewrite the value of $\mathrm{ed}_k(G; p)$ in terms of the character module $X(G)$ for an *abelian* group G which is an extension of a p-group and a torus. Moreover we show that tori with locally isomorphic character lattices have the same essential dimension. We need the following preliminaries.

Let R be a commutative ring (we use $R = \mathbb{Z}$ and $R = \mathbb{Z}_{(p)}$ mostly) and A an R-algebra. An A-module is called an *A-lattice* if it is finitely generated

and projective as an R-module. For $A = \mathbb{Z}\Gamma$ (Γ a group) this is as usual a free abelian group of finite rank with an action of Γ. Particular cases of $R\Gamma$-lattices are *permutation lattices* $L = R[\Lambda]$ where Λ is a Γ-set.

For $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ the absolute Galois group of k we tacitly assume that our $R\Gamma$-lattices are continuous, i.e. Γ acts through a finite quotient $\overline{\Gamma}$. Under the anti-equivalence Diag a $\mathbb{Z}\Gamma$-lattice corresponds to an algebraic k-torus. A torus S is called *quasi split* if it corresponds to a permutation lattice. Equivalently $S \simeq R_{E/k}(\mathbb{G}_m)$ where E/k is étale and $R_{E/k}$ denotes Weil restriction.

Recall that $\mathbb{Z}_{(p)}$ denotes the localization of the ring $\mathbb{Z}$ at the prime ideal (p). For a $\mathbb{Z}$-module M we also write $M_{(p)} := \mathbb{Z}_{(p)} \otimes M$.

When $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ we will often pass from $\mathbb{Z}\Gamma$-lattices to $\mathbb{Z}_{(p)}\Gamma$-lattices. This corresponds to identifying p-isogeneous tori:

Lemma 9.1. *Let $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ and let M, L be $\mathbb{Z}\Gamma$-lattices. Then the following statements are equivalent:*

(a) $L_{(p)} \simeq M_{(p)}$.
(b) There exists an injective map $\phi\colon L \to M$ of $\mathbb{Z}\Gamma$-modules with cokernel Q finite of order prime to p.
(c) There exists a p-isogeny $\mathrm{Diag}(M) \to \mathrm{Diag}(L)$.

Proof. The equivalence (b) $\Leftrightarrow$ (c) is clear from the anti-equivalence of Diag.

The implication (b) $\Rightarrow$ (a) follows from $Q_{(p)} = 0$ and that tensoring with $\mathbb{Z}_{(p)}$ is exact.

For the implication (a) $\Rightarrow$ (b) we use that L and M can be considered as subsets of $L_{(p)}$ (resp. $M_{(p)}$). The image of L under a map $\alpha\colon L_{(p)} \to M_{(p)}$ of $\mathbb{Z}_{(p)}\Gamma$-modules lands in $\frac{1}{m}M$ for some $m \in \mathbb{N}$ (prime to p) and the index of $\alpha(L)$ in $\frac{1}{m}M$ is finite and prime to p if α is surjective. Since $\frac{1}{m}M \simeq M$ as $\mathbb{Z}\Gamma$-modules the claim follows. □

Corollary 9.2. *Let G be an abelian group which is an extension of a p-group by a torus over k and $\Gamma := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ be the absolute Galois group of $k = k^{(p)}$. Let Γ act through a finite quotient $\overline{\Gamma}$ on $X(G)$. Then*

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

where the minimum is taken over all permutation $\mathbb{Z}\overline{\Gamma}$-lattices L which admit a map of $\mathbb{Z}\overline{\Gamma}$-modules to $X(G)$ with cokernel finite of order prime to p.

If G is a torus, then the minimum can also be taken over all $\mathbb{Z}_{(p)}\overline{\Gamma}$-lattices L which admit a surjective map of $\mathbb{Z}_{(p)}\overline{\Gamma}$-modules to $X(G)_{(p)}$.

Proof. Let us prove the first claim. In view of Theorem 1.3(a) it suffices to show that the least dimension of a p-faithful representation of $G_{k^{(p)}}$ over $k^{(p)}$ is equal to the least rank of a permutation $\mathbb{Z}\overline{\Gamma}$-module L which admits a map to $X(G)$ with cokernel finite of order prime to p.

Assume we have such a map $L \to X(G)$. Using the anti-equivalence Diag we obtain a p-isogeny $G \to \mathrm{Diag}(L)$. We can embed the quasi-split torus

$\mathrm{Diag}(L)$ in GL_n where $n = \operatorname{rk} L$ [Vo, Section 6.1]. This yields a p-faithful representation of G of dimension $\operatorname{rk} L$.

Conversely let $\rho\colon G \to \mathrm{GL}(V)$ be a p-faithful representation of G. Since G_{sep} is diagonalizable, there exist characters $\chi_1, \dots, \chi_n \in X(G)$ such that G acts on V_{sep} via diagonal matrices with entries $\chi_1(g), \dots, \chi_n(g)$ (for $g \in G$) with respect to a suitable basis of V_{sep}. Moreover $\overline{\Gamma}$ permutes the set $\Lambda := \{\chi_1, \dots, \chi_n\}$. Define a map $\phi\colon \mathbb{Z}[\Lambda] \to X(G)$ of $\mathbb{Z}\overline{\Gamma}$-modules by sending the basis element $\chi_i \in \Lambda$ of $L := \mathbb{Z}[\Lambda]$ to itself. Then the p-faithfulness of ρ implies that the cokernel of ϕ is finite and of order prime to p. Moreover $\operatorname{rk} L = |\Lambda| \leq n = \dim V$.

Now consider the case where G is a torus. Assume we have a surjective map $\alpha\colon L \to X(G)_{(p)}$ of $\mathbb{Z}_{(p)}\overline{\Gamma}$-modules where $L = \mathbb{Z}_{(p)}[\Lambda]$ is permutation, Λ a $\overline{\Gamma}$-set. Then $\alpha(\Lambda) \subseteq \frac{1}{m}X(G)$ for some $m \in \mathbb{N}$ prime to p (note that $\frac{1}{m}X(G)$ can be considered as a subset of $X(G)_{(p)}$ since $X(G)$ is torsion free). By construction the induced map $\mathbb{Z}[\Lambda] \to \frac{1}{m}X(G) \simeq X(G)$ becomes surjective after localization at p, hence its cokernel is finite of order prime to p. □

Corollary 9.3. *Let A be a finite (twisted) cyclic p-group over k. Let l/k be a minimal Galois splitting field of A, and $\Gamma := \mathrm{Gal}(l/k)$. Then*

$$\operatorname{ed}(A; p) = |\Gamma|.$$

Proof. Since $[l : k]$ is a power of p, $l^{(p)}/k^{(p)}$ is a Galois extension of the same degree and the same Galois group as l/k. So we can assume $k = k^{(p)}$.

By Corollary 9.2 $\operatorname{ed}(A; p)$ is equal to the least cardinality of a Γ-set Λ such that there exists a map $\phi\colon \mathbb{Z}[\Lambda] \to X(A)$ of $\mathbb{Z}\Gamma$-modules with cokernel finite of order prime to p. The group $X(A)$ is a (cyclic) p-group, hence ϕ must be surjective. Moreover Γ acts faithfully on $X(A)$. Surjectivity of ϕ implies that some element $\lambda \in \Lambda$ maps to a generator a of $X(A)$. Hence $|\Lambda| \geq |\Gamma\lambda| \geq |\Gamma a| = |\Gamma|$. Conversely we have a surjective homomorphism $\mathbb{Z}[\Gamma a] \to X(A)$ that sends a to itself. Hence the claim follows.

□

Remark 9.4. In the case of twisted cyclic groups of order 4 Corollary 9.3 is due to Rost [Ro] (see also [BF, Theorem 7.6]), and in the case of cyclic groups of order 8 to Bayarmagnai [Ba]. The case of constant groups of arbitrary prime power order is due to Florence [Fl]; it is now a special case of the Karpenko-Merkurjev Theorem 1.1.

10. Proof of Theorem 1.3(c)

We will prove Theorem 1.3(c) by using the lattice point of view from Section 9 and the additivity theorem from Section 8.

Let $\overline{\Gamma}$ be a finite group. Two $\mathbb{Z}\overline{\Gamma}$-lattices M, N are said to be in the same *genus* if $M_{(p)} \simeq N_{(p)}$ for all primes p, cf. [CR, 31A]. It is sufficient to check this condition for divisors p of the order of $\overline{\Gamma}$. By a theorem of A.V. Roĭter

[CR, Theorem 31.28] M and N are in the same genus if and only if there exists a $\mathbb{Z}\overline{\Gamma}$-lattice L in the genus of the free $\mathbb{Z}\overline{\Gamma}$-lattice of rank one such that $M \oplus \mathbb{Z}\overline{\Gamma} \simeq N \oplus L$. This has the following consequence for essential dimension:

Proposition 10.1. *Let T, T' be k-tori. If the lattices $X(T), X(T')$ belong to the same genus then*

$$\mathrm{ed}_k(T) = \mathrm{ed}_k(T) \text{ and } \mathrm{ed}_k(T;\ell) = \mathrm{ed}_k(T;\ell) \text{ for all primes } \ell.$$

Proof. Let $\mathrm{Gal}(k_{\mathrm{sep}}/k)$ act through a finite quotient $\overline{\Gamma}$ on $X(T)$ and $X(T')$. By assumption there exists a $\mathbb{Z}\overline{\Gamma}$-lattice L in the genus of $\mathbb{Z}\overline{\Gamma}$ such that $X(T) \oplus \mathbb{Z}\overline{\Gamma} \simeq X(T') \oplus L$. The torus $S = \mathrm{Diag}(\mathbb{Z}\overline{\Gamma})$ has a generically free representation of dimension $\dim S$, hence $\mathrm{ed}_k(S) = 0$. Since L is a direct summand of $\mathbb{Z}\overline{\Gamma} \oplus \mathbb{Z}\overline{\Gamma}$ the torus $S' := \mathrm{Diag}(L)$ has $\mathrm{ed}_k(S') \le \mathrm{ed}_k(S \times S) \le 0$ as well, where the first inequality follows from [BF, Remarks 1.16 (b)]. Therefore

$$\mathrm{ed}_k(T) \le \mathrm{ed}_k(T \times S) = \mathrm{ed}_k(T' \times S') \le \mathrm{ed}_k(T') + \mathrm{ed}_k(S') = \mathrm{ed}_k(T')$$

and similarly $\mathrm{ed}_k(T') \le \mathrm{ed}_k(T)$. Hence $\mathrm{ed}_k(T) = \mathrm{ed}_k(T')$.

A similar argument shows that $\mathrm{ed}_k(T;\ell) = \mathrm{ed}_k(T';\ell)$ for any prime ℓ. This concludes the proof. □

Corollary 10.2. *Let $k = k^{(p)}$ be a p-closed field and T a k-torus. Then*

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

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

Proof. The second equality follows from Theorem 1.3(a) and the inequality $\mathrm{ed}_k(T;p) \le \mathrm{ed}_k(T)$ is clear. Hence it suffices to show $\mathrm{ed}_k(T) \le \mathrm{ed}_k(T;p)$. Let $\rho\colon T \to \mathrm{GL}(V)$ be a p-faithful representation of minimal dimension so that $\mathrm{ed}_k(T;p) = \dim \rho - \dim T$. The representation ρ can be considered as a faithful representation of the torus $T' = T/N$ where $N := \ker \rho$ is finite of order prime to p. By construction the character lattices $X(T)$ and $X(T')$ are isomorphic after localization at p. Since $\mathrm{Gal}(k_{\mathrm{sep}}/k)$ is a (profinite) p-group it follows that $X(T)$ and $X(T')$ belong to the same genus. Hence by Proposition 10.1 we have $\mathrm{ed}_k(T') = \mathrm{ed}_k(T)$. Moreover $\mathrm{ed}_k(T') \le \dim \rho - \dim T'$, since ρ is a generically free representation of T'. This finishes the proof. □

Proof of Theorem 1.3(b). The equality $\mathrm{ed}_{k^{(p)}}(G_{k^{(p)}};p) = \mathrm{ed}_k(G;p)$ follows from Lemma 3.3. Now we are assuming $G = T \times F$ for a torus T and a p-group F over k, which is p-closed. Notice that a minimal p-faithful representation of F from Theorem 1.3(a) is also faithful, and therefore $\mathrm{ed}_k(F;p) = \mathrm{ed}_k(F)$. Combining this with Corollary 10.2 and the additivity Theorem 8.1, we see

$$\mathrm{ed}(T \times F) \le \mathrm{ed}(T) + \mathrm{ed}(F) = \mathrm{ed}(T;p) + \mathrm{ed}(F;p) = \mathrm{ed}(T \times F;p) \le \mathrm{ed}(T \times F).$$

This completes the proof. □

Remark 10.3. The following example shows that "p-faithful" cannot be replaced by "faithful" in the statement of Theorem 1.3(a) (and Corollary 10.2), even in the case where G is a torus.

Let p be a prime number such that the ideal class group of $\mathbb{Q}(\zeta_p)$ is non-trivial (this applies to all but finitely many primes, e.g. to $p = 23$). This means that the subring $R = \mathbb{Z}[\zeta_p] \subseteq \mathbb{Q}(\zeta_p)$ of algebraic integers has non-principal ideals. Let k be a field which admits a Galois extension l of degree p and let $\Gamma := \mathrm{Gal}(k_{\mathrm{sep}}/k)$, $\overline{\Gamma} := \mathrm{Gal}(l/k) \simeq \Gamma/\Gamma_l \simeq C_p$ where $\Gamma_l = \mathrm{Gal}(k_{\mathrm{sep}}/l)$ and C_p denotes the cyclic group of order p.

We endow the ring R with a $\mathbb{Z}\Gamma$-module structure through the quotient map $\Gamma \to \overline{\Gamma}$ by letting a generator of $\overline{\Gamma}$ act on R via multiplication by ζ_p. The k-torus $Q := \mathrm{Diag}(R)$ is isomorphic to the Weil restriction $R_{l/k}(\mathbb{G}_m)$ and has a p-dimensional faithful representation. We will construct a k-torus G with a p-isogeny $G \to Q$, such that G does not have a p-dimensional faithful representation.

Let I be a non-principal ideal of R. We may consider I as a $\mathbb{Z}\Gamma$-module and set $G := \mathrm{Diag}(I)$. We first show that I and R become isomorphic as $\mathbb{Z}\Gamma$-modules after localization at p. For this purpose let $I^* = \{x \in \mathbb{Q}(\zeta_p) \mid xI \subseteq R\}$ denote the inverse fractional ideal. We have $I \oplus I^* \simeq R \oplus R$ by [CR, Theorem 34.31]. The Krull-Schmidt Theorem [CR, Theorem 36.1] for $\mathbb{Z}_{(p)}C_p$-lattices implies $I_{(p)} \simeq R_{(p)}$, hence the claim. Therefore by Lemma 9.1 there exists a p-isogeny $G \to Q$, which shows in particular that G has a p-faithful representation of dimension p.

Assume that G has a p-dimensional faithful representation. Similarly as in the proof of Corollary 9.2 this would imply the existence of a surjective map of $\mathbb{Z}\Gamma$-lattices $\mathbb{Z}\overline{\Gamma} \to I$. However such a map cannot exist since I is non-principal, hence non-cyclic as a $\mathbb{Z}\Gamma$-module.

11. Tori of essential dimension ≤ 1

Theorem 11.1. *Let T be a torus over k, $k^{(p)}$ a p-closure and $\Gamma = \mathrm{Gal}(k_{\mathrm{alg}}/k^{(p)})$. The following are equivalent:*

(a) $\mathrm{ed}_k(T; p) = 0$.
(b) $\mathrm{ed}_{k^{(p)}}(T; p) = 0$.
(c) $\mathrm{ed}_{k^{(p)}}(T) = 0$
(d) $H^1(K, T) = \{1\}$ *for any p-closed field K containing k.*
(e) $X(T)_{(p)}$ *is a $\mathbb{Z}_{(p)}\Gamma$-permutation module.*
(f) $X(T)$ *is an invertible $\mathbb{Z}\Gamma$-lattice (i.e a direct summand of a permutation lattice).*
(g) There is a torus S over $k^{(p)}$ and an isomorphism

$$T_{k^{(p)}} \times S \simeq \mathrm{R}_{E/k^{(p)}}(\mathbb{G}_m),$$

for some étale algebra E over $k^{(p)}$.

Remark 11.2. A prime p for which any of these statements fails is called a *torsion prime* of T.

Proof. (a) $\Leftrightarrow$ (b) is Lemma 3.3.

(a) $\Leftrightarrow$ (d) follows from [Me$_1$, Proposition 4.4].

(c) $\Rightarrow$ (b) is clear.

(b) $\Rightarrow$ (e): This follows from Corollary 9.2. Indeed, $\mathrm{ed}_k(T;p) = 0$ implies the existence of a $\mathbb{Z}_{(p)}\Gamma$-permutation lattice L together with a surjective homomorphism $\alpha : L \to X(T)_{(p)}$ and $\operatorname{rk} L = \operatorname{rk} X(T)_{(p)}$. It follows that α is injective and $X(T)_{(p)} \simeq L$.

(e) $\Rightarrow$ (f): Let L be a $\mathbb{Z}\Gamma$-permutation lattice such that $L_{(p)} \simeq X(T)_{(p)}$. Then by [CR, Corollary 31.7] there is a $\mathbb{Z}\Gamma$-lattice L' such that $L \oplus L \simeq X(T) \oplus L'$.

(g) $\Rightarrow$ (c): The torus $R = \mathrm{R}_{E/k^{(p)}}(\mathbb{G}_m)$ has a faithful representation of dimension $\dim R$ (over $k^{(p)}$) and hence $\mathrm{ed}_{k^{(p)}}(R) = 0$. Since $T_{k^{(p)}}$ is a direct factor of R we must have $\mathrm{ed}_{k^{(p)}}(T) \leq 0$ by [BF, Remarks 1.16 b)].

(f) $\Leftrightarrow$ (g): A permutation lattice P can be written as

$$P = \bigoplus_{i+1}^{m} \mathbb{Z}[\Gamma/\Gamma_{L_i}],$$

for some (separable) extensions $L_i/k^{(p)}$ and $\Gamma_{L_i} = \mathrm{Gal}(k_{\mathrm{alg}}/L_i)$. Set $E = L_1 \times \cdots \times L_m$. The torus corresponding to P is exactly $\mathrm{R}_{E/k^{(p)}}(\mathbb{G}_m)$, cf. [Vo, 3. Example 19]. □

Example 11.3. Let T be a torus over k of rank $< p-1$. Then $\mathrm{ed}_k(T;p) = 0$. This follows from the fact that there is no non-trivial integral representation of dimension $< p-1$ of any p-group, see for example [AP, Satz]. Thus any finite quotient of $\Gamma = \mathrm{Gal}(k_{\mathrm{alg}}/k^{(p)})$ acts trivially on $X(T)$ and so does Γ.

Remark 11.4. The equivalence of parts (d) and (f) in Theorem 11.1 can also be deduced from [CTS, Proposition 7.4].

Theorem 11.5. *Let p be an odd prime, T an algebraic torus over k, and $\Gamma = \mathrm{Gal}(k_{\mathrm{alg}}/k^{(p)})$.*

- *(a)* $\mathrm{ed}(T;p) \leq 1$ *iff there exists a Γ-set Λ and an $m \in \mathbb{Z}[\Lambda]$ fixed by Γ such that $X(T)_{(p)} \cong \mathbb{Z}_{(p)}[\Lambda]/\langle m\rangle$ as $\mathbb{Z}_{(p)}\Gamma$-lattices.*
- *(b)* $\mathrm{ed}(T;p) = 1$ *iff $m = \sum a_\lambda \lambda$ from part (a) is not* 0 *and for any $\lambda \in \Lambda$ fixed by Γ, $a_\lambda = 0 \mod p$.*
- *(c) If* $\mathrm{ed}(T;p) = 1$ *then $T_{k^{(p)}} \cong T' \times S$ where* $\mathrm{ed}_{k^{(p)}}(S;p) = 0$ *and $X(T')_{(p)}$ is an indecomposable $\mathbb{Z}_{(p)}\Gamma$-lattice, and* $\mathrm{ed}_{k^{(p)}}(T';p) = 1$.

Proof. (a) If $\mathrm{ed}(T;p) = 1$, then by Corollary 9.2 there is a map of $\mathbb{Z}\Gamma$-lattices from $\mathbb{Z}[\Lambda]$ to $X(T)$ which becomes surjective after localization at p and whose kernel is generated by one element. Since the kernel is stable under Γ, any element of Γ sends a generator m to either itself or its negative. Since p is odd, m must be fixed by Γ.

The $\mathrm{ed}(T;p) = 0$ case and the converse follows from Theorem 1.4 or Corollary 9.2.

(b) Assume we are in the situation of (a), and say $\lambda_0 \in \Lambda$ is fixed by Γ and a_{λ_0} is not $0 \mod p$. Then $X(T)_{(p)} \cong \mathbb{Z}_{(p)}[\Lambda - \{\lambda_0\}]$, so by Theorem 11.1 we have $\mathrm{ed}(T;p) = 0$.

Conversely, assume $\mathrm{ed}(T;p) = 0$. Then by Theorem 11.1, we have an exact sequence $0 \to \langle m \rangle \to \mathbb{Z}_{(p)}[\Lambda] \to \mathbb{Z}_{(p)}[\Lambda'] \to 0$ for some Γ-set Λ' with one fewer element than Λ. We have

$$\mathrm{Ext}^1_\Gamma(\mathbb{Z}_{(p)}[\Lambda'], \mathbb{Z}_{(p)}) = (0)$$

by [CTS, Key Lemma 2.1(i)] together with the Change of Rings Theorem [CR, 8.16]; therefore this sequence splits. In other words, there exists a $\mathbb{Z}_{(p)}\Gamma$-module homomorphism $f\colon \mathbb{Z}_{(p)}[\Lambda] \to \mathbb{Z}_{(p)}[\Lambda]$ such that the image of f is $\langle m \rangle$ and $f(m) = m$. Then we can define $c_\lambda \in \mathbb{Z}_{(p)}$ by $f(\lambda) = c_\lambda m$. Note that $f(\gamma(\lambda)) = f(\lambda)$ and thus

$$c_{\gamma(\lambda)} = c_\lambda \tag{12}$$

for every $\lambda \in \Lambda$ and $\gamma \in \Gamma$. If $m = \sum_{\lambda\in\Lambda} a_\lambda \lambda$, as in the statement of the theorem, then $f(m) = m$ translates into

$$\sum_{\lambda\in\Lambda} c_\lambda a_\lambda = 1\,.$$

Since every Γ-orbit in Λ has a power of p elements, reducing modulo p, we obtain

$$\sum_{\lambda\in\Lambda^\Gamma} c_\lambda a_\lambda = 1 \pmod p\,.$$

This shows that $a_\lambda \neq 0$ modulo p, for some $\lambda \in \Lambda^\Gamma$, as claimed.

(c) Decompose $X(T)_{(p)}$ uniquely into a direct sum of indecomposable $\mathbb{Z}_{(p)}\Gamma$-lattices by the Krull-Schmidt theorem [CR, Theorem 36.1]. Since $\mathrm{ed}(T;p) = 1$, and the essential p-dimension of tori is additive (Thm. 8.1), all but one of these summands are permutation $\mathbb{Z}_{(p)}\Gamma$-lattices. Now by [CR, 31.12], we can lift this decomposition to $X(T) \cong X(T') \oplus X(S)$, where $\mathrm{ed}(T';p) = 1$ and $\mathrm{ed}(S;p) = 0$. □

Example 11.6. Let E be an étale algebra over k. It can be written as $E = L_1 \times \cdots \times L_m$ with some separable field extensions L_i/k. The kernel of the norm $\mathrm{R}_{E/k}(\mathbb{G}_m) \to \mathbb{G}_m$ is denoted by $\mathrm{R}^{(1)}_{E/k}(\mathbb{G}_m)$. It is a torus with lattice

$$\bigoplus_{i=1}^m \mathbb{Z}[\Gamma/\Gamma_{L_i}] \,/\, \langle 1, \cdots, 1\rangle,$$

where $\Gamma = \mathrm{Gal}(k_{\mathrm{sep}}/k)$ and $\Gamma_{L_i} = \mathrm{Gal}(k_{\mathrm{sep}}/L_i)$. Let Λ be the disjoint union of the cosets Γ/Γ_{L_i} Passing to a p-closure $k^{(p)}$ of k, $\Gamma_{k^{(p)}}$ fixes a λ in Λ iff $[L_i : k]$ is prime to p for some i. We thus have

$$\mathrm{ed}_k(\mathrm{R}^{(1)}_{E/k}(\mathbb{G}_m); p) = \begin{cases} 1, & [L_i : k] \text{ is divisible by } p \text{ for all } i = 1, ..., m \\ 0, & [L_i : k] \text{ is prime to } p \text{ for some } i. \end{cases}$$

12. Tori split by cyclic extensions of degree dividing p^2

In this section we assume $k = k^{(p)}$ is p-closed. Over $k = k^{(p)}$ every torus is split by a Galois extension of p-power order. We wish to compute the essential dimension of all tori split by a Galois extension with a (small) fixed Galois group G. The following theorem tells us for which G this is feasible:

Theorem 12.1 (A. Jones [Jo])**.** *For a p-group G there are only finitely many genera of indecomposable $\mathbb{Z}G$-lattices if and only if G is cyclic of order dividing p^2.*

Remark 12.2. For $G = C_2 \times C_2$ a classification of the (infinitely many) different genera of $\mathbb{Z}G$-lattices has been worked out by [NA]. In contrast for $G = C_{p^3}$ or $G = C_p \times C_p$ and p odd (in the latter case) no classification is known.

Hence in this section we consider tori T whose minimal splitting field is cyclic of degree dividing p^2. Its character lattice $X(T)$ is then a $\mathbb{Z}G$-lattice where $G = \langle g | g^{p^2} = 1 \rangle$ denotes the cylic group of order p^2. Heller and Reiner [HR], (see also [CR, 34.32]) classified all indecomposable $\mathbb{Z}G$-lattices. Our goal consists in computing the essential dimension of T. By Corollary 10.2 we have $\mathrm{ed}_k(T) = \mathrm{ed}_k(T; p)$, hence by the additivity Theorem 8.1 it will be enough to find the essential p-dimension of the tori corresponding to indecomposable $\mathbb{Z}G$-lattices. Recall that two lattices are in the same genus if their p-localization (or equivalently p-adic completion) are isomorphic. By Proposition 10.1 tori with character lattices in the same genus have the same essential p-dimension, which reduces the task to calculating the essential p-dimension of tori corresponding to the $4p + 1$ cases in the list [CR, 34.32].

Denote by $H = \langle h | h^p = 1 \rangle$ the group of order p. We can consider $\mathbb{Z}H$ as a G-lattice with the action $g \cdot h^i = h^{i+1}$. Let

$$\delta_G = 1 + g + \ldots + g^{p^2-1} \quad \delta_H = 1 + h + \ldots + h^{p-1}$$

be the "diagonals" in $\mathbb{Z}G$ and $\mathbb{Z}H$ and

$$\epsilon = 1 + g^p + \ldots + g^{p^2-p}.$$

The following $\mathbb{Z}G$-lattices represent all genera of indecomposable $\mathbb{Z}G$-lattices (by $\langle * \rangle$ we mean the $\mathbb{Z}G$-sublattice generated by $*$):

$$\begin{array}{lcll}
M_1 & = & \mathbb{Z} & \\
M_2 & = & \mathbb{Z}H & \\
M_3 & = & \mathbb{Z}H/\langle \delta_H \rangle & \\
M_4 & = & \mathbb{Z}G & \\
M_5 & = & \mathbb{Z}G/\langle \delta_G \rangle & \\
M_6 & = & \mathbb{Z}G \oplus \mathbb{Z}/\langle \delta_G - p \rangle & \\
M_7 & = & \mathbb{Z}G/\langle \epsilon \rangle & \\
M_8 & = & \mathbb{Z}G/\langle \epsilon - g\epsilon \rangle & \\
M_{9,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon - (1-h)^r \rangle & 1 \le r \le p-1 \\
M_{10,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon(1-g) - (1-h)^{r+1} \rangle & 1 \le r \le p-2 \\
M_{11,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon - (1-h)^r, \delta_H \rangle & 1 \le r \le p-2 \\
M_{12,r} & = & \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon(1-g) - (1-h)^{r+1}, \delta_H \rangle & 1 \le r \le p-2
\end{array}$$

In the sequel we will refer to the above list as ($\mathbb{L}$).

In ($\mathbb{L}$) we describe $\mathbb{Z}G$-lattices as quotients of permutation lattices of minimal possible rank, whereas [CR, 34.32] describes these lattices as certain extensions $1 \to L \to M \to N \to 1$ of $\mathbb{Z}[\zeta_{p^2}]$-lattices by $\mathbb{Z}H$-lattices. Therefore these two lists look differently. Nevertheless they represent the same $\mathbb{Z}G$-lattices. We show in the example of the lattice $M_{10,r}$ how one can translate from one list to the other.

Let $\mathbb{Z}x$ be a $\mathbb{Z}G$-module of rank 1 with trivial G-action. We have an isomorphism

$$M_{10,r} = \mathbb{Z}G \oplus \mathbb{Z}H/\langle \epsilon(1-g) - (1-h)^{r+1} \rangle \simeq \mathbb{Z}G \oplus \mathbb{Z}H \oplus \mathbb{Z}x/\langle \epsilon - (1-h)^r - x \rangle$$

induced by the inclusion $\mathbb{Z}G \oplus \mathbb{Z}H \hookrightarrow \mathbb{Z}G \oplus \mathbb{Z}H \oplus \mathbb{Z}x$.

This allows us to write $M_{10,r}$ as the pushout

$$\begin{array}{ccc}
\mathbb{Z}H & \xrightarrow{h \mapsto \epsilon} & \mathbb{Z}G \\
{\scriptstyle h \mapsto (1-h)^r + x}\downarrow & & \downarrow \\
\mathbb{Z}H \oplus \mathbb{Z}x & \longrightarrow & M_{10,r}
\end{array}$$

Completing both lines on the right we see that $M_{10,r}$ is an extension

$$0 \to \mathbb{Z}H \oplus \mathbb{Z}x \to M_{10,r} \to \mathbb{Z}G/\mathbb{Z}H \to 0$$

with extension class determined by the vertical map $h \mapsto (1-h)^r + x$ cf. [CR, 8.12] and we identify (the p-adic completion of) $M_{10,r}$ with one of the indecomposable lattices in the list [CR, 34.32].

Similarly, $M_1, \dots, M_{12,r}$ are representatives of the genera of indecomposable $\mathbb{Z}G$-lattices.

Theorem 12.3. *Every indecomposable torus T over k split by G has character lattice isomorphic to one of the $\mathbb{Z}G$-lattices M in the list* ($\mathbb{L}$) *after*

p-localization and $\mathrm{ed}(T) = \mathrm{ed}(T;p) = \mathrm{ed}(\mathrm{Diag}(M);p)$. *Their essential dimensions are given in the tables below.*

M	$\mathrm{rk}\, M$	$\mathrm{ed}(T)$
M_1	1	0
M_2	p	0
M_3	$p-1$	1
M_4	p^2	0
M_5	p^2-1	1
M_6	p^2	1

M	$\mathrm{rk}\, M$	$\mathrm{ed}(T)$
M_7	p^2-p	p
M_8	p^2-p+1	$p-1$
$M_{9,r}$	p^2	p
$M_{10,r}$	p^2+1	$p-1$
$M_{11,r}$	p^2-1	$p+1$
$M_{12,r}$	p^2	p

Proof of Proposition 12.3. We will assume $p > 2$ in the sequel. For $p = 2$ the Theoerem is still true but some easy additional arguments are needed which we leave out here.

The essential p-dimension of tori corresponding to $M_1 \dots, M_6$ easily follows from the discussion in section 11. Let M be one of the lattices $M_7, \dots, M_{12,r}$ and $T = \mathrm{Diag}\, M$ the corresponding torus. We will determine the minimal rank of a permutation $\mathbb{Z}G$-lattice P admitting a homomorphism $P \to M$ which becomes surjective after localization at p. Then we conclude $\mathrm{ed}(T;p) = \mathrm{rk}\, P - \mathrm{rk}\, M$ with Corollary 9.2.

We have the bounds

$$\mathrm{rk}\, M \le \mathrm{rk}\, P \le p^2 \text{ (or } p^2+p), \tag{13}$$

where the upper bound holds since every M is given as a quotient of $\mathbb{Z}G$ (or $\mathbb{Z}G \oplus \mathbb{Z}H$). Let $C = \mathrm{Split}_k(T[p])$ the finite constant group used in the proof of Theorem 1.3. The rank of C determines exactly the number of direct summands into which P decomposes. Moreover each indecomposable summand has rank a power of p.

As an example, we show how to find C for $M = M_{11,r}$: The relations $g^j \cdot (\epsilon - (1-h)^r); \delta_H$ are written out as

$$\sum_{i=0}^{p-1} g^{pi+j} - \sum_{\ell=0}^{r} \binom{r}{\ell} (-1)^\ell h^{\ell+j},\ 0 \le j \le p-1; \quad \sum_{i=0}^{p-1} h^i$$

and the k_{sep}-point of the torus are

$$T(k_{\mathrm{sep}}) = \Big\{ (t_0, \dots, t_{p^2-1}, s_0, \dots, s_{p-1}) \mid \prod_{i=0}^{p-1} t_{pi+j} = \prod_{\ell=0}^{r} s_{\ell+j}^{(-1)^\ell \binom{r}{\ell}},\ 0 \le j \le p-1; \quad \prod_{i=0}^{p-1} s_i = 1 \Big\}$$

and C is the constant group of fixed points of the p-torsion $T[p]$:

$$C(k) = \left\{ \left(\zeta_p^i, \dots, \zeta_p^i, \zeta_p^j, \dots, \zeta_p^j\right) \mid\ 0 \le i, j \le p-1 \right\} \simeq \mu_p^2.$$

(Note that the primitive pth root of unity ζ_p is in k by our assumption that k is p-closed). For other lattices this is similar: C is equal to $\mathrm{Split}_k(\mathrm{Diag}(P)[p]) \simeq \mu_p^r$ where M is presented as a quotient P/N of a permutation lattice P (of

minimal rank) as in (𝕃) and where r denotes the number of summands in a decomposition of P.

M	rank C	rank M	possible rk P
M_7	1	p^2-p	p^2
M_8	1	p^2-p+1	p^2
$M_{9,r}$	2	p^2	p^2+1 or p^2+p
$M_{10,r}$	2	p^2+1	p^2+1 or p^2+p
$M_{11,r}$	2	p^2-1	p^2+1 or p^2+p
$M_{12,r}$	2	p^2	p^2+1 or p^2+p

We need to exclude the possibility $\operatorname{rk} P = p^2+1$ for the lattices $M = M_{9,r}, \dots, M_{12,r}$. We can only have the value p^2+1 if there exists a character in M which is fixed under the Galois group and nontrivial on C. The following Lemma 12.4 tells us, that such characters do not exist in either case. Hence the minimal dimension of a p-faithful representation of all these tori is p^2+p. □

Lemma 12.4. *For $i = 9, \dots, 12$ and $r \geq 1$ every character $\chi \in M_{i,r}$ fixed under G has trivial restriction to C.*

Proof. By [Hi] the cohomology group $H^0(G, M_{i,r}) = M_{i,r}^G$ of G-fixed points in $M_{i,r}$ is trivial for $i = 11$, has rank 1 for $i = 9, 12$ and rank 2 for $i = 10$, respectively. They are represented by $\mathbb{Z}\delta_H$ in $M_{9,r}$, by $\mathbb{Z}(\epsilon - (1-h)^r)$ in $M_{12,r}$ and by $\mathbb{Z}(\epsilon - (1-h)^r) \oplus \mathbb{Z}\delta_H$ in $M_{10,r}$, respectively. Since all these characters are trivial on

$$C = \operatorname{Split}_k(\operatorname{Diag}(\mathbb{Z}G \oplus \mathbb{Z}H)[p]),$$

the claim follows. □

Acknowledgments

The authors are grateful to A. Auel, A. Merkurjev and A. Vistoli for helpful comments and conversations.

References

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

[Ba] G. Bayarmagnai, *Essential dimension of some twists of μ_{p^n}*, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 145–151, RIMS Kôkyûroku Bessatsu, B4, Res. Inst. Math. Sci. (RIMS), Kyoto (2007).

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

[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).

[BR] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica 106:159–179.(1997).

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

[CTS] J.-L. Colliot-Thélène, J. J. Sansuc, *Principal Homogeneous Spaces under Flasque Tori: Applications*, J. Algebra **106** (1087), 148–205.

[CR] C. W. Curtis, I. Reiner, *Methods of representation theory* ,vol. 1, Wiley (Interscience), 1981.

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

[Fl] M. Florence, *On the essential dimension of cyclic p-groups*, Inventiones Mathematicae, **171** (2007), 175-189.

[GMS] S. R. Garibaldi, A. Merkurjev, J.-P. Serre: *Cohomological Invariants in Galois Cohomology*, University Lecture Series, Vol. 28, American Mathematical Society, Providence, RI, (2003).

[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.

[Gro] A. Grothendieck, *La torsion homologique et les sections rationnelles*, Exposé 5, Séminaire C. Chevalley, Anneaux de Chow et applications, IHP, (1958).

[HR] A. Heller, I. Reiner: *Representations of cyclic groups in rings of integers I*, Annals of Math, **76** (1962), 73-92.

[Hi] H. Hiller, *Flat Manifolds with $\mathbb{Z}/p^2$ Holonomy*, L'Enseignement Mathématique, **31** (1985), 283–297.

[Ja] J. C. Jantzen, *Representations of Algebraic Groups*. Pure and Applied Mathematics, 131. Academic Press, Orlando, Florida, (1987).

[Jo] A. Jones, *Groups with a finite number of indecomposable integral representations*, Mich. Math. J, **10** (1963), 257-261.

[Ka] G. Karpilovsky, *Clifford Theory for Group Representations*. Mathematics Studies, 156. North-Holland, Netherlands, (1989).

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

[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 *Essential dimension of $PGL(p^2)$*, preprint, available at `http://www.math.ucla.edu/~merkurev/publicat.htm`.

[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.

[MR$_2$] A. Meyer, Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, to appear in Journal of Algebra, 10.1016/j.jalgebra.2009.09.019, preprint available at arXiv:0907.4496

[NA] L. A. Nazarova, *Unimodular representations of the four group*, Dokl. Akad. Nauk SSSR, **140** (1961), 1011–1014.

[Re] Z. Reichstein, *On the Notion of Essential Dimension for Algebraic Groups*, Transformation Groups, **5**, 3 (2000), 265-304.

[RY] Z. Reichstein, B. Youssin, *Essential Dimensions of Algebraic Groups and a Resolution Theorem for G-varieties*, with an appendix by J. Kollar and E. Szabo, Canadian Journal of Mathematics, **52**, 5 (2000), 1018–1056.

[RZ] L. Ribes, P. Zalesskii, *Profinite Groups*. Springer-Verlag, Berlin, 2000.

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

[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 fr algebraische Gruppen* J. Algebra, **68**, no. 1 (1981), 177–189.

[Se$_1$] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, **42**, Springer-Verlag, 1977.

[Se$_2$] 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.

[Vo] V. E. Voskresenskiĭ, *Algebraic Groups and Their Birational Invariants*, American Mathematical Society, Providence, RI, 1998.

[Wa] W. C. Waterhouse, *Introduction to affine group schemes*. Springer-Verlag, New York-Berlin, 1979.

[Wi] J. S. Wilson, *Profinite Groups*. London Math. Soc. Monographs 19, Oxford University Press, New York, 1998.

[Win] D. Winter, *The structure of fields*. Graduate Texts in Mathematics, no. 16. Springer-Verlag, New York-Heidelberg, 1974.