



Algebra

Essential dimension of finite groups in prime characteristic [☆]*Dimension essentielle des groupes finis en caractéristique positive*Zinovy Reichstein ^{a,1}, Angelo Vistoli ^{b,2}^a Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2, Canada^b Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy

ARTICLE INFO

Article history:

Received 10 January 2018

Accepted after revision 27 March 2018

Available online 11 April 2018

Presented by Jean-Pierre Serre

ABSTRACT

Let F be a field of characteristic $p > 0$ and G be a smooth finite algebraic group over F . We compute the essential dimension $\text{ed}_F(G; p)$ of G at p . That is, we show that

$$\text{ed}_F(G; p) = \begin{cases} 1, & \text{if } p \text{ divides } |G|, \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

© 2018 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

R É S U M É

Soit F un corps de caractéristique $p > 0$, et soit G un groupe algébrique fini étale sur F . On calcule la dimension essentielle de G en p , que l'on note $\text{ed}_F(G; p)$. Plus précisément, on démontre que

$$\text{ed}_F(G; p) = \begin{cases} 1, & \text{si } p \text{ divise } |G|, \\ 0, & \text{sinon.} \end{cases}$$

© 2018 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

1. Introduction

Let F be a field and G be an algebraic group over F . We begin by recalling the definition of the essential dimension of G .

[☆] The authors are grateful to the Collaborative Research Group in Geometric and Cohomological Methods in Algebra at the Pacific Institute for the Mathematical Sciences for their support of this project.

E-mail addresses: reichst@math.ubc.ca (Z. Reichstein), angelo.vistoli@sns.it (A. Vistoli).

¹ Partially supported by Natural Sciences and Engineering Research Council of Canada Discovery grant 253424-2017.

² Partially supported by grant SNS16_B_VISTOLI from the Scuola Normale Superiore, Pisa, Italy.

Let K be a field containing F and $\tau : T \rightarrow \text{Spec}(K)$ be a G -torsor. We will say that τ descends to an intermediate subfield $F \subset K_0 \subset K$ if τ is the pull-back of some G -torsor $\tau_0 : T_0 \rightarrow \text{Spec}(K_0)$, i.e. if there exists a Cartesian diagram of the form

$$\begin{array}{ccccc} T & \longrightarrow & T_0 & & \\ \downarrow \tau & & \downarrow \tau_0 & & \\ \text{Spec}(K) & \longrightarrow & \text{Spec}(K_0) & \longrightarrow & \text{Spec}(F). \end{array}$$

The essential dimension of τ , denoted by $\text{ed}_F(\tau)$, is the smallest value of the transcendence degree $\text{trdeg}(K_0/F)$ such that τ descends to K_0 . The essential dimension of G , denoted by $\text{ed}_F(G)$, is the maximal value of $\text{ed}_F(\tau)$, as K ranges over all fields containing F and τ ranges over all G -torsors $T \rightarrow \text{Spec}(K)$.

Now let p be a prime integer. A field K is called p -closed if the degree of every finite extension L/K is a power of p . Equivalently, $\text{Gal}(K^s/K)$ is a pro- p -group, where K^s is a separable closure of K . For example, the field of real numbers is 2-closed. The essential dimension $\text{ed}_F(G; p)$ of G at p is the maximal value of $\text{ed}_F(\tau)$, where K ranges over p -closed fields K containing F , and τ ranges over the G -torsors $T \rightarrow \text{Spec}(K)$. For an overview of the theory of essential dimension, we refer the reader to the surveys [19] and [16].

The case where G is a finite group (viewed as a constant group over F) is of particular interest. A theorem of N.A. Karpenko and A.S. Merkurjev [10] asserts that, in this case,

$$\text{ed}_F(G; p) = \text{ed}_F(G_p; p) = \text{ed}_F(G_p) = \text{rdim}_F(G_p), \tag{1}$$

provided that F contains a primitive p -th root of unity ζ_p . Here G_p is any Sylow p -subgroup of G , and $\text{rdim}_F(G_p)$ denotes the minimal dimension of a faithful representation of G_p defined over F . For example, assuming that $\zeta_p \in F$, $\text{ed}_F(G) = \text{ed}(G; p) = r$ if $G = (\mathbb{Z}/p\mathbb{Z})^r$, and $\text{ed}(G) = \text{ed}(G; p) = p$ if G is a non-abelian group of order p^3 . Further examples can be found in [18].

Little is known about essential dimension of finite groups over a field F of characteristic $p > 0$. A. Ledet [12] conjectured that

$$\text{ed}_F(\mathbb{Z}/p^r\mathbb{Z}) = r \tag{2}$$

for every $r \geq 1$. This conjecture remains open for every $r \geq 3$. In this paper we will prove the following surprising result.

Theorem 1. *Let F be a field of characteristic $p > 0$ and G be a smooth finite algebraic group over F . Then*

$$\text{ed}_F(G; p) = \begin{cases} 1, & \text{if } p \text{ divides } |G|, \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

In particular, Ledet’s conjecture (2) fails dramatically if the essential dimension is replaced by the essential dimension at p . On the other hand, Theorem 1 fails if $\text{ed}(G; p)$ is replaced by $\text{ed}(G)$; see [13].

Before proceeding with the proof of Theorem 1, we remark that the condition that G is smooth cannot be dropped. Indeed, it is well known that $\text{ed}_F(\mu_p^r; p) = r$ for any $r \geq 0$. More generally, if G is a group scheme of finite type over a field F of characteristic p (not necessarily finite or smooth), then $\text{ed}_F(G; p) \geq \dim(\mathcal{G}) - \dim(G)$, where \mathcal{G} is the Lie algebra of G ; see [25, Theorem 1.2].

2. Versality

Let G be an algebraic group and X be an irreducible G -variety (i.e. a variety with a G -action) over F . We will say that the G -variety X is *generically free* if there exists a dense open subvariety U of X such that the scheme-theoretic stabilizer G_u of every geometric point u of X is trivial. Equivalently, there exists a G -invariant dense open subvariety U' of X , which is the total space of a G -torsor; see [23, Section 5].

Following [23, Section 5] and [6, Section 1], we will say that X is *weakly versal* (respectively, *weakly p -versal*) if, for every infinite field (respectively, every p -closed field) E , and every G -torsor $T \rightarrow \text{Spec}(E)$, there is a G -equivariant F -morphism $T \rightarrow X$. We will say that X is *versal* (respectively, *p -versal*), if every G -invariant dense open subvariety of X is weakly versal (respectively, weakly p -versal).

It readily follows from these definitions that $\text{ed}(G)$ (respectively, $\text{ed}(G; p)$) is the minimal dimension $\dim(X) - \dim(G)$, where the minimum is taken over all versal (respectively p -versal) generically free G -varieties X ; see [23, Section 5.7], [6, Remark 2.6 and Section 8]. Our proof of Theorem 1 will be based on the following facts.

- (i) ([6, Proposition 2.2]) Every G -variety X with a G -fixed F -point is weakly versal.
- (ii) ([6, Theorem 8.3]) Let X be a smooth geometrically irreducible G -variety. Then X is weakly p -versal if and only if X is p -versal.

Combining (i) and (ii), we obtain the following proposition.

Proposition 2. ([6, Corollary 8.6(b)]) *Let G be a finite smooth algebraic group over F . If there exists a faithful geometrically irreducible G -variety X with a smooth G -fixed F -point, then $\text{ed}(G; p) \leq \dim(X)$.*

If we replace “ p -versal” by “versal”, then (ii) fails: a weakly versal G -variety does not need to be versal. This is the underlying reason why both Proposition 2 and Theorem 1 fail if $\text{ed}(G; p)$ is replaced by $\text{ed}(G)$.

3. Proof of Theorem 1

In this section, we will prove Theorem 1, assuming Lemmas 3 and 4 below. We will defer the proofs of these lemmas to sections 4 and 5, respectively.

By [17, Lemma 4.1], if $G' \subset G$ is a subgroup of index prime to p , then

$$\text{ed}_F(G; p) = \text{ed}_F(G'; p). \tag{3}$$

In particular, if p does not divide $|G|$, then taking $G' = \{1\}$, we conclude that $\text{ed}_F(G; p) = 0$. On the other hand, if p divides $|G|$, then $\text{ed}_F(G; p) \geq 1$; see [15, Proposition 4.4] or [14, Lemma 10.1]. Our goal is thus to show that $\text{ed}_F(G; p) \leq 1$.

First let us consider the case where G is a finite group, viewed as a constant algebraic group over F . After replacing G by a Sylow p -subgroup, we may assume that G is a p -group. Let \mathbb{F}_p be the field of p elements. Since $\mathbb{F}_p \subset F$, we have $\text{ed}_F(G; p) \leq \text{ed}_{\mathbb{F}_p}(G; p)$. Thus, for the purpose of proving the inequality $\text{ed}_F(G; p) \leq 1$, we may assume that $F = \mathbb{F}_p$. In view of Proposition 2, it suffices to prove the following.

Lemma 3. *For every finite constant p -group G there exists a faithful G -curve defined over \mathbb{F}_p with a smooth G -fixed \mathbb{F}_p -point.*

Now consider the general case where G is a smooth finite algebraic group over F . In other words, $G = {}^\tau \Gamma$, where Γ is a constant finite group, $A = \text{Aut}_{\text{grp}}(\Gamma)$ is the group of automorphisms of Γ and τ is a cocycle representing a class in $H^1(F, A)$.

Lemma 4. (a) $\text{ed}_F(G) \leq \text{ed}_F(\Gamma \rtimes A)$, (b) $\text{ed}_F(G; p) \leq \text{ed}(\Gamma \rtimes A; p)$.

The semidirect product $\Gamma \rtimes A$ is a constant finite group. Hence, as we showed above, $\text{ed}_F(\Gamma \rtimes A; p) \leq 1$. Theorem 1 now follows from Lemma 4(b).

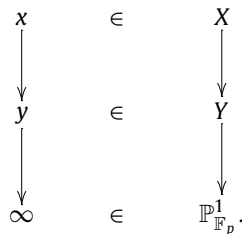
4. Proof of Lemma 3

We will give two proofs: our original proof, extracted from the literature, and a self-contained proof suggested to us by the referee.

Proof. Recall that the Nottingham group $\text{Aut}_0(\mathbb{F}_p[[t]])$ is the group of automorphisms σ of the algebra $\mathbb{F}_p[[t]]$ of formal power series such that $\sigma(t) = t + a_2 t^2 + a_3 t^3 + \dots$, for some $a_2, a_3, \dots \in \mathbb{F}_p$. By a theorem of Leedham–Green and Weiss [3, Theorem 3], every finite p -group G embeds into $\text{Aut}_0(\mathbb{F}_p[[t]])$. Fix an embedding $\phi: G \hookrightarrow \text{Aut}_0(\mathbb{F}_p[[t]])$. By [11, Theorem 1.4.1], there exists a smooth G -curve X over \mathbb{F}_p , with an \mathbb{F}_p -point $x \in X$ fixed by G , such that the G -action in the formal neighborhood of x is given by ϕ ; see also [9, Section 2] and [1, Theorem 4.8]. Since ϕ is injective, the G -action on X is faithful. \square

Alternative proof. First consider the case where $G = (\mathbb{Z}/p\mathbb{Z})^n$ is an elementary abelian p -group. Here we can construct X as the cover of \mathbb{P}^1 (with function field $\mathbb{F}_p(s)$) given by the compositum of n linearly disjoint Artin–Schreier extensions $\mathbb{F}_p(s, t_i)/\mathbb{F}_p(s)$ given by $t_i^p - t_i = f_i(s)$ (e.g., taking $f_i(s) = s^{pi+1}$).

Now consider a general finite p -group G . Denote the Frattini subgroup of G by Φ and the quotient G/Φ by $(\mathbb{Z}/p\mathbb{Z})^n$. Let Y be the smooth curve and $Y \rightarrow \mathbb{P}^1$ be a $G/\Phi = (\mathbb{Z}/p\mathbb{Z})^n$ -cover constructed in the previous paragraph, totally ramified at a point $y \in Y(\mathbb{F}_p)$ above $\infty \in \mathbb{P}^1$. Let $E/\mathbb{F}_p(s)$ be the $(\mathbb{Z}/p\mathbb{Z})^n$ -Galois extension associated with this cover. By [21, Proposition II.2.2.3], the cohomological dimension of $\mathbb{F}_p(s)$ at p is ≤ 1 . Consequently, by [21, Propositions I.3.4.16], $E/\mathbb{F}_p(s)$ lifts to a G -Galois extension $K/\mathbb{F}_p(s)$ such that $K^\Phi = E$. Let X be the smooth curve associated with K and $x \in X(\overline{\mathbb{F}_p})$ is a point above y :



We claim that x is fixed by G ; in particular, this will imply that $x \in X(\mathbb{F}_p)$. Let H be the stabilizer of x in G . Since Φ acts transitively on the fiber above y in X , we have $\Phi \cdot H = G$. By Frattini’s theorem (see, e.g., [20, Theorem 5.2.12]), Φ is the set of non-generators of G . We conclude that $H = G$, as claimed. \square

5. Proof of Lemma 4

We will make use of the following description of $\text{ed}_F(G)$ and $\text{ed}_F(G; p)$ in the case where G is a finite algebraic group over F . Let $G \rightarrow \text{GL}(V)$ be a faithful representation. A compression (respectively, a p -compression) of V is a dominant G -equivariant rational map $V \dashrightarrow X$ (respectively, a dominant G -equivariant correspondence $V \rightsquigarrow X$ of degree prime to p), where G acts faithfully on X . Here, by a correspondence, we mean a G -equivariant subvariety V' of $V \times X$ such that the G transitively permutes the irreducible components of V' , and the dimension of each component equals the dimension of V . The degree of this correspondence is defined as the degree of the projection $V' \rightarrow V$ to the first factor.

Recall that $\text{ed}_F(G)$ (respectively, $\text{ed}_F(G; p)$) equals the minimal value of $\dim(X)$ taken over all compressions $V \dashrightarrow X$ (respectively all p -compressions $V \rightsquigarrow X$). In particular, these numbers depend only on G and F and not on the choice of the generically free representation V . For details, see [19].

We are now ready to proceed with the proof of Lemma 4. To prove part (a), let V be a generically free representation of $\Gamma \rtimes A$ and let $f: V \dashrightarrow X$ be a $\Gamma \rtimes A$ -compression, with X of minimal possible dimension. That is, $\dim_F(X) = \text{ed}_F(\Gamma \rtimes A)$. Twisting by τ , we obtain a $G = {}^\tau\Gamma$ -equivariant map ${}^\tau f: {}^\tau V \dashrightarrow {}^\tau X$; see, e.g., [7, Proposition 2.6(a)]. Now observe that by Hilbert’s Theorem 90, ${}^\tau V$ is a vector space with a linear action of $G = {}^\tau\Gamma$ and ${}^\tau f: {}^\tau V \dashrightarrow {}^\tau X$ is a compression. (To see that the G -action on ${}^\tau V$ and ${}^\tau X$ are faithful, we may pass to the algebraic closure \bar{F} of F . Over \bar{F} , τ is split, so that $G = \Gamma$, ${}^\tau V = V$, ${}^\tau X = X$ and ${}^\tau f = f$, and it becomes obvious that the G -actions on ${}^\tau V$ and ${}^\tau X$ are faithful.) We conclude that $\text{ed}_F(G) \leq \dim_F({}^\tau X) = \dim_F(X) = \text{ed}_F(\Gamma \rtimes A)$, as desired.

The proof of part (b) proceeds along the same lines. The starting point is a p -compression $f: V \rightsquigarrow X$ with X of minimal possible dimension, $\dim_F(X) = \text{ed}_F(\Gamma \rtimes A; p)$. We twist f by τ to obtain a p -compression ${}^\tau f: {}^\tau V \rightsquigarrow {}^\tau X$ of the linear action of $G = {}^\tau\Gamma$ on ${}^\tau V$. The rest of the argument is the same as in part (a). This completes the proof of Lemma 4 and thus of Theorem 1. \square

6. An application

In this section, G will denote a connected reductive linear algebraic group over a field F . It is shown in [4, Theorem 1.1(c)] that there exists a finite F -subgroup $S \subset G$ such that every G -torsor over every field K/F admits reduction of structure to S ; see also [5, Corollary 1.4]. In other words, the map $H^1(K, S) \rightarrow H^1(K, G)$ is surjective for every field K containing F . If this happens, we will say that “ G admits reduction of structure to S ”.

We will now use Theorem 1 to show that if $\text{char}(F) = p > 0$ and p is a torsion prime for G , then S cannot be smooth. For the definition of torsion primes, a discussion of their properties and further references, see [22]. Note that by a theorem of A. Grothendieck [8], if G is not special (i.e. if $H^1(K, G) \neq \{1\}$ for some field K containing F), then G has at least one torsion prime; see also [22, 1.5.1].

Corollary 5. *Let G be a connected reductive linear algebraic group over an algebraically closed field F of characteristic $p > 0$.*

(a) *If S is a smooth finite subgroup of G defined over F , then the natural map*

$$f_K: H^1(K, S) \rightarrow H^1(K, G)$$

is trivial for any p -closed field K containing F . In other words, f_K sends every $\alpha \in H^1(K, S)$ to $1 \in H^1(K, G)$.

(b) *If p is a torsion prime for G , then G does not admit reduction of structure to any smooth finite subgroup.*

Proof. (a) Let $\alpha \in H^1(K, S)$ and $\beta = f_K(\alpha) \in H^1(K, G)$. By Theorem 1, α descends to $\alpha_0 \in H^1(K_0, S)$ for some intermediate field $F \subset K_0 \subset K$, where $\text{trdeg}(K_0/F) \leq 1$. Since F is algebraically closed, $\dim(K_0) \leq 1$; see [21, Sections II.3.1-3]. By Serre’s Conjecture I (proved by R. Steinberg [24] for a perfect field K_0 and by A. Borel and T. A. Springer [2, §8.6] for an arbitrary K_0 of dimension ≤ 1), $H^1(K_0, G) = \{1\}$. Tracing through the diagram

$$\begin{array}{ccc}
 H^1(K_0, S) & \xrightarrow{f_{K_0}} & H^1(K_0, G) = \{1\} \\
 \downarrow & & \downarrow \\
 H^1(K, S) & \xrightarrow{f_K} & H^1(K, G)
 \end{array}$$

$\begin{array}{ccc} \alpha_0 & \longrightarrow & 1 \\ \downarrow & & \downarrow \\ \alpha & \longrightarrow & \beta \end{array}$

we see that $\beta = 1$, as desired.

(b) If p is a torsion prime for G , then $H^1(K, G) \neq \{1\}$ for some p -closed field K containing F ; see [15, Proposition 4.4]. In view of part (a), this implies that f_K is not surjective. \square

Acknowledgements

We are grateful to the referee for a thorough reading of the paper and numerous constructive suggestions, including an alternate proof of Lemma 3. We would also like to thank D. Tossici and J.-P. Serre for helpful comments.

References

- [1] F.M. Bleher, T. Chinburg, B. Poonen, P. Symonds, Automorphisms of Harbater–Katz–Gabber curves, *Math. Ann.* 368 (1–2) (2017) 811–836, MR3651589.
- [2] A. Borel, T.A. Springer, Rationality properties of linear algebraic groups. II, *Tohoku Math. J. (2)* 20 (1968) 443–497, MR0244259.
- [3] R. Camina, Subgroups of the Nottingham group, *J. Algebra* 196 (1) (1997) 101–113, MR1474165.
- [4] V. Chernousov, P. Gille, Z. Reichstein, Resolving G -torsors by abelian base extensions, *J. Algebra* 296 (2) (2006) 561–581, MR2201056.
- [5] V. Chernousov, P. Gille, Z. Reichstein, Reduction of structure for torsors over semilocal rings, *Manuscr. Math.* 126 (4) (2008) 465–480, MR2425436.
- [6] A. Duncan, Z. Reichstein, Versality of algebraic group actions and rational points on twisted varieties, *J. Algebraic Geom.* 24 (3) (2015) 499–530, MR3344763.
- [7] M. Florence, Z. Reichstein, The rationality problem for forms of moduli spaces of stable marked curves of positive genus, arXiv:1709.05696.
- [8] A. Grothendieck, Torsion homologique et sections rationnelles, in: *Anneaux de Chow et Applications*, in: *Séminaire Claude-Chevalley*, vol. 3, 1958, pp. 1–29, exposé 5.
- [9] D. Harbater, Moduli of p -covers of curves, *Commun. Algebra* 8 (12) (1980) 1095–1122, MR0579791.
- [10] N.A. Karpenko, A.S. Merkurjev, Essential dimension of finite p -groups, *Invent. Math.* 172 (3) (2008) 491–508, MR2393078.
- [11] N.M. Katz, Local-to-global extensions of representations of fundamental groups, *Ann. Inst. Fourier (Grenoble)* 36 (4) (1986) 69–106, MR0867916.
- [12] A. Ledet, On the essential dimension of p -groups, in: *Galois Theory and Modular Forms*, in: *Dev. Math.*, vol. 11, Kluwer Academic Publishers, Boston, MA, USA, 2004, pp. 159–172, MR2059762.
- [13] A. Ledet, Finite groups of essential dimension one, *J. Algebra* 311 (1) (2007) 31–37, MR2309876.
- [14] R. Lötscher, M. MacDonald, A. Meyer, Z. Reichstein, Essential p -dimension of algebraic groups whose connected component is a torus, *Algebra Number Theory* 7 (8) (2013) 1817–1840, MR3134035.
- [15] A.S. Merkurjev, Essential dimension, in: *Quadratic Forms—Algebra, Arithmetic, and Geometry*, in: *Contemp. Math.*, vol. 493, American Mathematical Society, Providence, RI, USA, 2009, pp. 299–325, MR2537108.
- [16] A.S. Merkurjev, Essential dimension: a survey, *Transform. Groups* 18 (2) (2013) 415–481.
- [17] A. Meyer, Z. Reichstein, The essential dimension of the normalizer of a maximal torus in the projective linear group, *Algebra Number Theory* 3 (4) (2009) 467–487.
- [18] A. Meyer, Z. Reichstein, Some consequences of the Karpenko–Merkurjev theorem, in: *Extra vol.: Andrei A. Suslin’s sixtieth birthday*, *Doc. Math.* (2010) 445–457, MR2804261.
- [19] Z. Reichstein, Essential dimension, in: *Proceedings of the International Congress of Mathematicians, Vol. II*, Hindustan Book Agency, New Delhi, 2010, pp. 162–188.
- [20] D.J.S. Robinson, *A Course in the Theory of Groups*, second edition, *Graduate Texts in Mathematics*, vol. 80, Springer-Verlag, New York, 1996, MR1357169.
- [21] J.-P. Serre, *Galois Cohomology*, translated from the French by Patrick Ion and revised by the author Springer-Verlag, Berlin, 1997, MR1466966.
- [22] J.-P. Serre, Sous-groupes finis des groupes de Lie, *Astérisque* 266 (2000) 415–430, Exp. No. 864, 5. MR1772682.
- [23] J.-P. Serre, Cohomological invariants, Witt invariants, and trace forms, in: *Cohomological Invariants in Galois Cohomology*, in: *Univ. Lecture Ser.*, vol. 28, American Mathematical Society, Providence, RI, USA, 2003, pp. 1–100, Notes by Skip Garibaldi.
- [24] R. Steinberg, Regular elements of semisimple algebraic groups, *Inst. Hautes Études Sci. Publ. Math.* 25 (1965) 49–80, MR0180554.
- [25] D. Tossici, A. Vistoli, On the essential dimension of infinitesimal group schemes, *Amer. J. Math.* 135 (1) (2013) 103–114, MR3022958.