Invent. math. 171, 175–189 (2008)
DOI: 10.1007/s00222-007-0079-5

Inventiones mathematicae

On the essential dimension of cyclic p-groups*

Mathieu Florence

Ecole Polytechnique Fédérale de Lausanne, FSB-MA, CH-1015 Lausanne, Switzerland
(e-mail: mathieu.florence@gmail.com)

Oblatum 21-XII-2006 & 13-VIII-2007
Published online: 22 September 2007 – © Springer-Verlag 2007

A la mémoire de mon père.

Abstract. Let p be a prime number, let K be a field of characteristic not p, containing the p-th roots of unity, and let $r \geq 1$ be an integer. We compute the essential dimension of $\mathbb{Z}/p^r\mathbb{Z}$ over K (Theorem 4.1). In particular,

i) We have $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/8\mathbb{Z}) = 4$, a result which was conjectured by Buhler and Reichstein in 1995 (unpublished).
ii) We have $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/p^r\mathbb{Z}) \geq p^{r-1}$.

Acknowledgements. We thank Jean Fasel and Giordano Favi for fruitful discussions about essential dimension. We are also grateful to the referee for numerous comments which helped improve the clarity of the paper.

1. Introduction

The notion of essential dimension was first introduced by Buhler and Reichstein for finite groups in [BR]. It was later generalized by Reichstein to arbitrary linear algebraic groups [Re]. Throughout this paper, we shall assume that the reader is somewhat familiar with this concept. A convenient and comprehensive reference on this subject is [BF].

Definition 1.1. *Let k be a field, and G a (smooth) linear algebraic k-group. Let K/k be a field extension, and let T be a G_K-torsor. The essential dimension of T (over k), denoted by* $\mathrm{ed}_k(T)$*, is the smallest nonnegative integer n with the following property.*

* The author gratefully acknowledges support from the Swiss National Science Fundation, grant no. 200020-109174/1 (project leader: E. Bayer-Fluckiger)

There exists a subfield K' of K, containing k, and a $G_{K'}$-torsor $T' \longrightarrow \mathrm{Spec}(K')$, such that

i) The G_K-torsors T and T'_K are isomorphic.
ii) The transcendence degree of K'/k is n.

The essential dimension of G over k, which we denote by $\mathrm{ed}_k(G)$, is the maximal value of $\mathrm{ed}_k(T)$, where K/k ranges through all field extensions, and T ranges through all G_K-torsors.

Thus, $\mathrm{ed}_k(G)$ is the smallest number of algebraically independent parameters required to define G-torsors. It is finite, as it readily follows from the existence of versal (or classifying) torsors (see [BF, Definition 6.1]). More precisely, $\mathrm{ed}_k(G) = \mathrm{ed}_k(T)$, where T/K is any versal G-torsor. It turned out that essential dimension, even in apparently simple cases, is extremely difficult to compute. Focusing on finite abelian groups, let us mention some known results. Over fields containing all roots of unity, the essential dimension of a finite abelian group G equals its rank (i.e. the minimal cardinality of a set of generators of G), at least if the characteristic does not divide the order of the group under consideration ([BR, Theorem 6.1]). Note that the inequality $\mathrm{ed}_k(G) \leq \mathrm{rank}(G)$ follows at once from Kummer theory. Over general fields, the answer was known only for cyclic groups of small order. To the author's knowledge, the results obtained so far over the field of rational numbers may be summarized as follows. The number $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/n\mathbb{Z})$ equals 1 for $n = 2, 3$ (easy exercise); it is 2 for $n = 4$ (Lenstra, Serre, see also [BF, Theorem 7.6] for an alternate proof); it is 2 for $n = 5$ ([JLY], see also [BF, Corollary 7.9]); it is 2 for $n = 7$ ([Le]). For n odd, Jensen, Ledet and Yui proved that $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/2n\mathbb{Z}) = 1 + \mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/n\mathbb{Z})$ ([JLY]). This settles the cases $n = 6$, 10 and 14. Let us also mention the following result of Rost ([Ros]): let k be a field of characteristic not 2, and G/k a linear algebraic group, geometrically isomorphic to μ_4. Then $\mathrm{ed}_k(G) = 1$ if G is isomorphic to μ_4, and $\mathrm{ed}_k(G) = 2$ otherwise. For arbitrary $n \geq 4$, it seems that the best known lower bound for $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/n\mathbb{Z})$ is 2 (this follows from the fact that a finite group of essential dimension 1 is isomorphic to a subgroup of PGL_2, see [BF], Proposition 6.21). The best upper bound is given by a result of Ledet ([Le], see also [FF], Theorem 4.1): for a prime number p and a positive integer r, we have $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/p^r\mathbb{Z}) \leq \phi(p-1)p^{r-1}$, where ϕ denotes Euler's function. A major part of the proof of this theorem consists in finding a k-torus T, of minimal possible dimension, together with an injection $\mathbb{Z}/p^r\mathbb{Z} \longrightarrow T$, factoring through a quasi-trivial torus (in other words, a torus whose character module admits a Galois stable $\mathbb{Z}$-basis). The less precise bound $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/p^r\mathbb{Z}) \leq \phi(p^r)$ may be obtained quickly as follows: consider the torus $T = R_{\mathbb{Q}(\mu_{p^r})/\mathbb{Q}}(\mathbb{G}_m)$ (Weil scalar restriction). The choice of a primitive p^r-th root of 1 in $\mathbb{Q}(\mu_{p^r})$ gives an injection $\mathbb{Z}/p^r\mathbb{Z} \longrightarrow T$. Hilbert's theorem 90 now implies that T has trivial H^1, hence the quotient map $T \longrightarrow T/(\mathbb{Z}/p^r\mathbb{Z})$ is a versal $\mathbb{Z}/p^r\mathbb{Z}$-torsor. Therefore, $\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z}) \leq \dim(T/(\mathbb{Z}/p^r\mathbb{Z})) = \phi(p^r)$.

In the present paper, we compute the essential dimension of cyclic p-groups, over fields of characteristic not p containing the p-th roots of unity (with an extra condition on the field if $p = 2$).

This paper is organized as follows. The second paragraph contains material about generically free representations and essential dimension. The process of twisting varieties by torsors, and its functorial properties, are also recalled. In the third paragraph, we prove two theorems which are key ingredients in the proof of our main result: a theorem of Karpenko about Severi–Brauer varieties (Theorem 3.2), which we derive here from Rost's degree formula, and Theorem 3.6, which generalizes the construction, due to Brauer and Rowen, of 'generic' division algebras. The last paragraph is devoted to the proof of our main theorem.

In the sequel, the letter k will denote an arbitrary field. We adopt the following conventions: a k-variety is a k-scheme which is separated and of finite type. An algebraic k-group is a smooth k-variety endowed with the structure of a k-group scheme (the smoothness assumption may be dropped in most of the general results we will state; however, we will always assume it for simplicity). Unless otherwise stated, all torsors are right torsors.

2. Some auxiliary results

Let us briefly recall the notion of *friendly open subset* (cf. [BF], Definition 4.8).

Let G/k be an algebraic group, and X/k an integral G-variety, on which G acts generically freely (on the right), in the sense that there is a G-invariant dense open subvariety $V \subset X$ such that the scheme-theoretic stabilizer of any point of V is trivial. By a theorem of Gabriel, there exists a G-invariant dense open subset $U \subset X$ such that the categorical quotient $U \longrightarrow U/G$ exists, and is a G-torsor for the *fppf* topology (*loc. cit.*, Theorem 4.7).

Definition 2.1. *Such an open subset $U \subset X$ is called a friendly open subset (for the action of G on X).*

In the sequel, we will often consider G-equivariant rational maps between integral G-varieties. The following lemma asserts that, under some hypothesis, the induced quotient rational map is then well-defined.

Lemma 2.2. *Let G/k be an algebraic group (not necessarily linear). Let S be a k-variety, and let $T \xrightarrow{\pi} S$ be a G-torsor. We assume that T (and hence S) is an integral k-variety. Let X be a k-variety on which G acts trivially. Then, given a rational G-equivariant map $\phi : T \dashrightarrow X$, there exists a unique rational map $\psi : S \dashrightarrow X$ such that $\phi = \psi \circ \pi$. It is regular if ϕ is regular.*

Proof. Let $\tilde{T} \subset T$ be the maximal open subset on which ϕ is defined. It is not hard to see that $\tilde{T}$ is G-invariant; this follows from the fact that ϕ is

G-equivariant. Note that π is an open morphism, since it is flat and of finite type. We can therefore speak about the open subvariety $\tilde{S} := \pi(\tilde{T}) \subset S$. Consider the pullback

$$\begin{array}{ccc} \tilde{S} \times_S T & \longrightarrow & T \\ \downarrow & & \downarrow \\ \tilde{S} & \longrightarrow & S. \end{array}$$

We have a canonical morphism $\tilde{T} \xrightarrow{i} \tilde{S} \times_S T$ arising from the open immersion $\tilde{T} \longrightarrow T$ and the morphism $\pi_{|\tilde{T}} : \tilde{T} \longrightarrow \tilde{S}$. The projection $\tilde{S} \times_S T \longrightarrow T$ and the composite $\tilde{T} \xrightarrow{i} \tilde{S} \times_S T \longrightarrow T$ are both open immersions, hence i is also an open immersion. Moreover, each fiber of the G-torsor $\tilde{S} \times_S T \longrightarrow \tilde{S}$ contains a point of $\tilde{T}$, which is G-stable. Therefore, i is in fact an isomorphism. Replacing $T \longrightarrow S$ by $\tilde{T} \longrightarrow \tilde{S}$, we may therefore assume that ϕ is regular. The existence and uniqueness of ψ is then obvious if the G-torsor $T \longrightarrow S$ is trivial. The general case now follows from faithfully flat descent theory (for morphisms). □

Definition 2.3. *Let V be a finite-dimensional vector space over k. We denote by $\mathbb{A}_k(V)$ the k-variety representing the functor $A \mapsto V \otimes_k A$ where A runs through all k-algebras.*

Definition 2.4. *Let X be an integral k-variety and Y a k-variety. Let $\phi : X \dashrightarrow Y$ be a k-rational map. Let η be the generic point of X. We denote by $\overline{\phi(X)}$ the closure of $\phi(\eta)$, together with its (reduced) induced scheme structure. It is an integral subvariety of Y.*

The following proposition seems to be well known; as we lack a suitable reference, we include a proof.

Proposition 2.5. *Let G/k be a linear algebraic group and V a generically free finite-dimensional representation of G over k. Let $U \subset \mathbb{A}_k(V)$ be a friendly open subset. We then have*

$$\mathrm{ed}_k(G) + \dim(G) = \min(\dim(\overline{\phi(U)})),$$

where ϕ runs through all G-equivariant rational maps $U \dashrightarrow U$.

In particular, if every such ϕ is dominant, we have $\mathrm{ed}_k(G) = \dim(V) - \dim(G)$.

Proof. Throughout this proof, the action of G on V will be written on the right. By [BF, Proposition 4.11], we know that the G-torsor $U \longrightarrow U/G$ is versal. Let K be the function field of U/G, and $T = U \times_{U/G} \mathrm{Spec}(K)$. Assume there exists a k-subfield K' of K, of transcendence degree n over k, and a $G_{K'}$-torsor T' such that T is G_K-isomorphic to T'_K. By the definition

of a versal torsor, T' is isomorphic to the pullback of $U \longrightarrow U/G$ by a K'-point of U/G. The situation can then be summarized by the following commutative diagram:

$$\begin{array}{ccccccc} U & \xleftarrow{pr_U} & T & \xrightarrow{f} & T' & \xrightarrow{f'} & U \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ U/G & \longleftarrow & \mathrm{Spec}(K) & \longrightarrow & \mathrm{Spec}(K') & \longrightarrow & U/G, \end{array}$$

where the maps on the second line are k-morphisms, and the squares are pullbacks. Since U/k is of finite type, there exists a unique G-equivariant rational map $\phi : U \dashrightarrow U$ such that $f' \circ f$ equals the composite $T \xrightarrow{pr_U} U \overset{\phi}{\dashrightarrow} U$. Indeed, this is the geometric translation of the following algebraic fact: let U' be a nonempty affine open subvariety of U, and let A be the ring of regular functions on U'. It is a k-algebra of finite type. Hence the functor $B \mapsto \mathrm{Hom}_k(A, B)$, from the category of k-algebras to the category of sets, commutes with filtered direct limits.

One easily checks that $\dim(\overline{\phi(U)}) \leq n + \dim(G)$. Taking the minimal values of both sides yields the inequality $\mathrm{ed}_k(G) + \dim(G) \geq \min(\dim(\overline{\phi(U)}))$.

Let us prove the converse inequality. Let $\phi : U \dashrightarrow U$ be a G-equivariant rational map. We have a commutative square

$$\begin{array}{ccc} U & \overset{\phi}{\dashrightarrow} & U \\ \downarrow & & \downarrow \\ U/G & \overset{\psi}{\dashrightarrow} & U/G. \end{array}$$

Indeed, consider the composite $U \overset{\phi}{\dashrightarrow} U \longrightarrow U/G$. It is a rational G-equivariant map (G acting trivially on U/G). Therefore (see Lemma 2.2), it factors uniquely through the quotient map $U \longrightarrow U/G$, whence the existence of ψ. Let K' be the function field of $\overline{\psi(U/G)}$; it is a subfield of K of transcendence degree $n := \dim(\overline{\psi(U/G)})$. The preceding diagram implies that T is G_K-isomorphic to a torsor obtained from a $G_{K'}$-torsor by base change. Hence $\mathrm{ed}_k(G) \leq n$, i.e. $\dim(\overline{\phi(U)}) = n + \dim(G) \geq \mathrm{ed}_k(G) + \dim(G)$. □

Our next goal is to show that we may restrict our attention to a particular type of G-equivariant rational maps; namely, homogeneous ones. This is the content of Lemma 2.11. Its proof will require two definitions and an elementary general lemma.

Let V and W be two finite-dimensional vector spaces over k, and $\phi : \mathbb{A}_k(V) \dashrightarrow \mathbb{A}_k(W)$ be a nonzero rational map. Let $n \in \mathbb{Z}$ be an

integer. Consider the rational map

$$H_n(\phi) : \mathbb{A}_k(V) \times \mathbb{A}^1_k \dashrightarrow \mathbb{A}_k(W),$$
$$(v, t) \longmapsto t^n \phi\left(\frac{v}{t}\right).$$

Then, for n big enough, $H_n(\phi)$ is defined at the generic point of the hyperplane $t = 0$ of $\mathbb{A}_k(V) \times \mathbb{A}^1_k$.

Definition 2.6. *Let V, W, ϕ and $H_n(\phi)$ be as above. We denote by $n_0 = n_0(\phi)$ the smallest integer such that $H_n(\phi)$ is defined at the generic point of the hyperplane $t = 0$ of $\mathbb{A}_k(V) \times \mathbb{A}^1_k$. We denote by $H(\phi)$ the rational map $\mathbb{A}_k(V) \dashrightarrow \mathbb{A}_k(W)$ defined by the formula*

$$H(\phi)(v) = H_{n_0}(\phi)(v, 0).$$

Example 2.7. Let $W = k$, and let ϕ be regular. Then n_0 is the degree of ϕ, and $H(\phi)$ is the nonzero homogeneous component of degree n_0 of ϕ.

Remark 2.8. More generally, $H(\phi)$ can be described concretely as follows. Identify $\mathbb{A}_k(V)$ (resp. $\mathbb{A}_k(W)$) with $\mathbb{A}^n$ (resp. $\mathbb{A}^m$) by choosing a basis of V (resp. of W). Write $\phi = (\frac{P_1}{Q_1}, \dots, \frac{P_m}{Q_m})$, where the P_i's and the Q_i's are polynomials in n variables. Set

$$d := \max\{\deg(P_i) - \deg(Q_i),\ i = 1, \dots, m\},$$

the degree of the zero polynomial being $-\infty$. Denote by p_i (resp. q_i) the homogeneous component of highest degree of P_i (resp. Q_i). Then $n_0 = d$ and $H(\phi) = (r_1, \dots, r_n)$, where $r_i = p_i/q_i$ if $\deg(P_i) - \deg(Q_i) = d$, and $r_i = 0$ otherwise. This description shows that $n_0 > -\infty$ and that $H(\phi)$ is nonzero, but has the disadvantage of being non-canonical.

Definition 2.9. *Let V, W be two finite-dimensional vector spaces over k, and d an integer. A nonzero rational map $\mathbb{A}_k(V) \overset{\phi}{\dashrightarrow} \mathbb{A}_k(W)$ is said to be d-homogeneous if the following diagram commutes:*

$$\begin{array}{ccc} \mathbb{G}_m \times \mathbb{A}_k(V) & \xrightarrow{(\lambda, v) \mapsto \lambda v} & \mathbb{A}_k(V) \\ \downarrow{\scriptstyle Id \times \phi} & & \downarrow{\scriptstyle \phi} \\ \mathbb{G}_m \times \mathbb{A}_k(W) & \xrightarrow{(\lambda, v) \mapsto \lambda^d v} & \mathbb{A}_k(W). \end{array}$$

We shall also say that ϕ is homogeneous if it is d-homogeneous for some $d \in \mathbb{Z}$. The integer d is then well defined.

Lemma 2.10. *Notation being as in Definition 2.6, the map $H(\phi)$ is nonzero and n_0-homogeneous. Furthermore, for $f \in \mathrm{GL}_k(V)$ and $g \in \mathrm{GL}_k(W)$, we have $H(g \circ \phi \circ f) = g \circ H(\phi) \circ f$.*

Proof. It is not hard to see that $H(\phi)$ is nonzero (see for instance the remark above). We now compute, for $(v, t) \in \mathbb{A}_k(V) \times \mathbb{A}_k^1$ in general position:

$$H_{n_0}(\phi)(\lambda v, t) = t^{n_0}\phi\left(\frac{\lambda v}{t}\right) = \lambda^{n_0}\left(\frac{t}{\lambda}\right)^{n_0}\phi\left(v\frac{\lambda}{t}\right) = \lambda^{n_0}H_{n_0}(\phi)\left(v, \frac{t}{\lambda}\right).$$

Equality must then hold also for $t = 0$, whence the homogeneity of $H(\phi)$. The last assertion is proved in the same way. Indeed, we have that $H_{n_0}(g \circ \phi \circ f) = g \circ H_{n_0}(\phi) \circ f$. □

Lemma 2.11. *Let G/k be a linear algebraic group, and V a finite-dimensional linear representation of G over k. Assume there exists a G-equivariant rational map $\mathbb{A}_k(V) \overset{\phi}{\dashrightarrow} \mathbb{A}_k(V)$ which is not dominant and nonzero. Then there exists a homogeneous rational map $\mathbb{A}_k(V) \overset{\psi}{\dashrightarrow} \mathbb{A}_k(V)$ with the same properties.*

Proof. Set $\psi = H(\phi)$. By the first (resp. second) part of Lemma 2.10, it is an n_0-homogeneous (resp. G-equivariant) nonzero rational map. Let us show that ϕ is not dominant. By assumption, there exists a nonconstant polynomial map $f : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k^1$ such that $f \circ \phi = 0$. Assume first that $n_0 \geq 0$. Define a nonconstant polynomial map $g : \mathbb{A}_k(V) \times \mathbb{A}_k^1 \longrightarrow \mathbb{A}_k^1$ by the formula $g(v, t) = t^{n_0 d} f(\frac{v}{t^{n_0}})$, where d is the degree of f. For (v, t) in general position, we find that $g(H_{n_0}(\phi)(v, t), t) = t^{n_0 d} f(\phi(\frac{v}{t})) = 0$. Hence equality also holds for $t = 0$. Setting $h(v) = g(v, 0)$, this means that $h \circ \psi = 0$. But h is a nonzero polynomial map: it is the homogeneous component of degree d of f if $n_0 \geq 1$; it is the polynomial f if $n_0 = 0$. The case $n_0 \leq 0$ is dealt with along similar lines, replacing d by the lowest degree of a nonzero homogeneous component of f. □

In the sequel, we will repeatedly use an important process from descent theory: twisting varieties by torsors. Let us recall its definition.

Proposition 2.12. *Let X/k be a quasiprojective variety. Let G/k be an algebraic group (not necessarily linear). Assume we are given an action of G on X (on the left). Let P be a G-torsor over k. Let G act on the product $P \times_k X$ by the formula $(p, x).g = (pg, g^{-1}x)$. Then the categorical quotient $(P \times_k X)/G$ exists in the category of k-varieties. It is called the twist of X by P, denoted by ${}^P X$. Furthermore, the formation of ${}^P X$ commutes with base field extension, and ${}^P X$ is canonically isomorphic to X if $P = G$ is the trivial G-torsor.*

Proof. Existence (and of course uniqueness) is obvious if P is trivial. The general case now follows from faithfully flat descent theory for schemes, which is possible here since X is quasiprojective (see for instance [Se, Chap. V, §4.20, Corollary 2]). The proof of the last assertion is straightforward. □

Remark 2.13. The quotient map $(P \times_k X) \longrightarrow {}^P X$ is in fact a G-torsor. This follows from descent theory, since it is obviously true when P is trivial.

Twisting by torsors is functorial, in the sense of the next lemma.

Lemma 2.14. *Let X and Y be quasiprojective integral k-varieties, both endowed with a left action of an algebraic group G/k. Let P be a G-torsor, and let $\phi : X \dashrightarrow Y$ be a G-equivariant rational map. Then there exists a canonical rational map ${}^P\phi : {}^P X \dashrightarrow {}^P Y$ satisfying the following properties:*

i) If Z is another quasiprojective integral G-variety, and $\phi' : Y \dashrightarrow Z$ is a G-equivariant rational map such that ϕ and ϕ' are composable, then so are ${}^P\phi$ and ${}^P\phi'$, and ${}^P(\phi' \circ \phi) = {}^P\phi' \circ {}^P\phi$.
ii) The formation of ${}^P\phi$ commutes with base field extension.
iii) If $P = G$ is the trivial G-torsor, then ${}^P\phi = \phi$.

Proof. Consider the induced rational map $\psi : P \times_k X \overset{Id\times\phi}{\dashrightarrow} P \times_k Y$. Let G act on both sides as in Proposition 2.12. Then ψ is G-equivariant. Consider the composite map

$$P \times_k X \overset{\psi}{\dashrightarrow} P \times_k Y \longrightarrow (P \times_k Y)/G = {}^P Y.$$

It is G-equivariant, G acting trivially on ${}^P Y$. Lemma 2.2 (together with Remark 2.13) implies that it factors uniquely through the quotient $P \times_k X \longrightarrow {}^P X$, giving rise to a commutative diagram:

$$\begin{array}{ccc} P \times_k X & \overset{\psi}{\dashrightarrow} & P \times_k Y \\ \downarrow & & \downarrow \\ {}^P X & \overset{{}^P\phi}{\dashrightarrow} & {}^P Y. \end{array}$$

This proves the existence of ${}^P\phi$. The assertions i), ii) and iii) obviously follow from the definition. □

3. Central simple algebras and Severi–Brauer varieties

Let A/k be a central simple algebra of degree n. Recall that the functor

$$R \mapsto \left\{ \begin{array}{l} I \subset A \otimes_k R,\ I \text{ is a left ideal of } A \otimes_k R \text{ such that } (A \otimes_k R)/I \\ \text{is a projective } R\text{-module of constant rank } n \end{array} \right\},$$

from the category of k-algebras to the category of sets, is representable by a projective k-variety, called the Severi–Brauer variety associated to A, and which we denote by $SB(A)$. If $A = \mathrm{End}_k(V)$ for some k-vector space V of dimension n, then $SB(A)$ is canonically isomorphic to the projective

space $\mathbb{P}_k(V)$. On the level of k-points, a line l in V corresponds to the ideal $I = \{f \in \mathrm{End}_k(V) \text{ such that } f(l) = 0\}$. The following elementary lemma will be useful in the sequel.

Lemma 3.1. *Let V be a finite-dimensional k-vector space. We let the group $\mathrm{PGL}_k(V)$ act on $\mathbb{P}_k(V)$ in the obvious way, and on $\mathrm{End}_k(V)$ by inner conjugation. Let P be a $\mathrm{PGL}_k(V)$-torsor defined over k. Then the twist of $\mathbb{P}_k(V)$ by P is canonically isomorphic to the Severi–Brauer variety associated to the central simple k-algebra obtained by twisting $\mathrm{End}_k(V)$ by P.*

Proof. Let $G = \mathrm{PGL}_k(V)$. Assume first that P is trivial. Choose $p \in P(k)$. Consider the morphism

$$\Phi_p : P \times_k \mathbb{P}_k(V) \longrightarrow \mathbb{P}_k(V)$$

defined as follows: for any k-algebra R, and points $g \in G(R)$, $v \in \mathbb{P}_k(V)(R)$, we have

$$\Phi_p(pg, v) = gv.$$

The map Φ_p factors through the quotient $P \times_k \mathbb{P}_k(V) \longrightarrow {}^P\mathbb{P}_k(V)$ (here we do not need to use Lemma 2.2 since P is assumed to be trivial), giving rise to an isomorphism

$$\phi_p : {}^P\mathbb{P}_k(V) \longrightarrow \mathbb{P}_k(V).$$

Similarly, we define an isomorphism

$$\psi_p : SB\big({}^P\mathrm{End}_k(V)\big) \longrightarrow SB(\mathrm{End}_k(V)).$$

For $g \in G(k)$, we have that $\phi_{pg} = g^{-1}\phi_p$ and $\psi_{pg} = g^{-1}\psi_p$. Let $f : \mathbb{P}_k(V) \longrightarrow SB(\mathrm{End}_k(V))$ be the canonical G-equivariant isomorphism. The isomorphism

$$\psi_p^{-1} \circ f \circ \phi_p : {}^P\mathbb{P}_k(V) \longrightarrow SB\big({}^P\mathrm{End}_k(V)\big)$$

is independent of the choice of p. The case of an arbitrary P now follows from faithfully flat descent theory. □

The following theorem, due to Karpenko, plays a key rôle in the proof of our main theorem. It can be viewed as a consequence of Rost's degree formula. For the convenience of the reader, we outline such a proof below. It is not stated by Karpenko as it is here; however, it is straightforward to deduce it from [Ka, Theorem 2.1]. Note that Karpenko's proof does not make use of Rost's degree formula.

Theorem 3.2 [Ka]. *Let k be a field, p a prime number, and A/k a central division algebra of index p^n for some $n \geq 1$. Then any k-rational map $SB(A) \overset{f}{\dashrightarrow} SB(A)$ is dominant.*

Proof. Let $SB(A) \overset{f}{\dashrightarrow} SB(A)$ be a rational map. We want to apply Rost's rational degree formula ([Me], Theorem 3.3). To this end, we have to compute the numbers $I(SB(A))$ and $\eta_p(SB(A))$ (cf. [Me] for the definition of these numbers). The first one is easily seen to be p^n, as A is a division algebra. By [Me], Remark 6.5, the number $\eta_p(SB(A)) \in \mathbb{Z}/p^n\mathbb{Z}$ equals p^{n-1}. Hence, Rost's degree formula yields $p^{n-1} = \deg(f)p^{n-1}$ mod p^n. In particular, $\deg(f)$ is nonzero; that is to say, f is dominant. □

From now on, p will be a prime number. We shall use the following notation. The letter K will denote a field of characteristic not p, and $\bar{K}$ a separable closure of K. For any $n \geq 1$, let $G_n = \mu_{p^n}(\bar{K})$ (viewed as a finite abstract group) and $K_n = K(\mu_{p^n}(\bar{K}))$.

Definition 3.3. *Notation being as above, we set*

$$s(K) = \max\{n \in \mathbb{N}, \textit{ such that } K = K_n\}.$$

If the dependence in K is clear from the context, we will denote $s(K)$ simply by s.

We shall always assume that s is finite; if not, the question we are dealing with has a trivial answer. We will only consider fields K such that the following holds:

i) We have $s \geq 1$, i.e. $\mu_p(\bar{K}) \subset K$.
ii) If $p = 2$ and $s(K) = 1$, then $K_2 \neq K_3$.

Remark 3.4. Let ζ_s be a primitive p^s-th root of unity. It is easy to check that the polynomial $X^{p^n} - \zeta_s$ is irreducible over K for any $n \geq 0$ (in other words, K_{s+n}/K is a Galois field extension, of degree p^n). In particular, for any integer $s' \geq s(K)$, we have that $s' = s(K_{s'})$, and the field $K_{s'}$ still satisfies the Conditions i) and ii), with s replaced by s'.

Let $r \geq 1$ be any integer. Our goal is to compute the number $\mathrm{ed}_K(G_r) = \mathrm{ed}_K(\mathbb{Z}/p^r\mathbb{Z})$. It is 1 if $r \leq s$, so we assume $r > s$.

Consider $\mathbb{P}_K(K_r)$, the projective space of K_r viewed as a K-vector space. Multiplication by $\mu_{p^r}(\bar{K})$ induces a G_r/G_s-action on $\mathbb{P}_K(K_r)$, which is easily seen to be faithful. We identify G_r/G_s with G_{r-s} using the exact sequence

$$1 \longrightarrow G_s \longrightarrow G_r \overset{\theta}{\longrightarrow} G_{r-s} \longrightarrow 1,$$

where $\theta(x) = x^{p^s}$.

The following lemma will be useful in the sequel.

Lemma 3.5. *Let $\zeta_r \in \bar{K}$ be a primitive p^r-th root of unity. Set $\zeta_s = \zeta_r^{p^{r-s}}$ and $\zeta_{r-s} = \zeta_r^{p^s}$. Let L/K be any field extension, and M/L a cyclic field extension, with an isomorphism $G_{r-s} \simeq \mathrm{Gal}(M/L)$. Let $L_r = L \otimes_K K_r$.*

Then the twist of $\mathbb{P}_L(L_r)$ by the G_{r-s}-torsor associated to M/L is the Severi–Brauer variety corresponding to the cyclic algebra $(M/L, \sigma, \zeta_s)$, where $\sigma = \zeta_{r-s}^{-1} \in G_{r-s}$. In other words, this algebra is generated by M and an indeterminate X, with relations $X^{p^{r-s}} = \zeta_s$ and $XmX^{-1} = \sigma(m)$, for $m \in M$.

Proof. Using Lemma 3.1, we have to describe the algebra A obtained by twisting $\mathrm{End}_L(L_r)$ by the G_{r-s}-torsor T associated to M/L (recall that $T = \mathrm{Spec}(M)$, with the obvious G_{r-s}-action). By definition, the inner action of G_{r-s} on $\mathrm{End}_L(L_r)$ is given by the formula

$$(\lambda.f)(x) = \lambda f(\lambda^{-1}x),$$

where $\lambda \in G_r/G_s = G_{r-s}$, $f \in \mathrm{End}_L(L_r)$ and $x \in L_r$.

Let G_{r-s} act on $M \otimes_L \mathrm{End}_L(L_r)$ by the formula

$$g.(m \otimes f) = g(m) \otimes (g.f).$$

Then by definition $A = (M \otimes_L \mathrm{End}_L(L_r))^{G_{r-s}}$. With this description, it is obvious that A contains L_r as a maximal étale subalgebra (indeed, G_{r-s} acts trivially on $L_r \subset \mathrm{End}_L(L_r)$). Now consider the maximal (split) étale subalgebra $E = \bigoplus_{i=1}^{p^{r-s}} L$ of $\mathrm{End}_L(L_r)$ consisting of linear maps admitting $1, \zeta_r, \ldots, \zeta_r^{p^{r-s}-1}$ as eigenvectors. One easily sees that $\zeta_{r-s} \in G_{r-s} = G_r/G_s$ acts on E by cyclic permutation of the coordinates. Hence, the twist of E by T is a maximal subfield of A isomorphic to M. More precisely, let $e_0 \in E$ be the idempotent sending 1 to 1 and ζ_r^i to 0 for $i = 1, \ldots, p^{r-s} - 1$. Then the map

$$\begin{aligned} M &\longrightarrow (M \otimes E)^{G_{r-s}}, \\ m &\longmapsto \sum_{g \in G_{r-s}} g(m) \otimes g(e_0) \end{aligned}$$

is a field isomorphism. Let $X = \zeta_r \in L_r$. For $m \in M$ and $e \in E$, we have that $(1 \otimes X)(m \otimes e)(1 \otimes X)^{-1} = m \otimes \sigma^{-1}(e)$ by definition of σ and of the G_{r-s}-action on $\mathrm{End}_L(L_r)$. Via the preceding isomorphism, we see that σ acts by conjugation by X on M. It follows that A is presented as stated in the lemma. □

In the proof of Theorem 4.1, we shall apply Theorem 3.2 to some particular division algebras arising as a generalized version of the 'generic' division algebras of Brauer–Rowen. These algebras were first introduced by Brauer in the important paper [Bra]. They were used to show that the only relations between the index and the exponent of a central simple algebra are the 'obvious' ones (the exponent divides the index, and they have the same prime factors). Later, Rowen generalized Brauer's process to obtain a wider class of generic division algebras ([Row]). In the present paper, we shall need a slightly more general statement than [Row, Theorem 7.3.8]. Indeed,

we have to replace the field $\mathbb{Q}(\mu_{p^s})$ considered by Rowen by K as above. *Mutatis mutandis*, the proof of the next theorem is nevertheless the same as that of [Row, Theorem 7.3.8]. It relies on the existence of a graded order in the central simple algebra under consideration (this order is $W_{n,t}(K)$ in the proof); it is thus of valuative nature. We tried to harmonize our notation with that of Rowen, with some minor changes: for instance, the letters n and t used in [Row] correspond here to p^n and p^t, respectively.

Theorem 3.6. *Let K be a field of characteristic not p. We assume that $s = s(K)$ (cf. Definition 3.3) is finite and positive. If $p = 2$ and $s = 1$, assume moreover that $K(\mu_4) \neq K(\mu_8)$. Let $E_t(K) = K(x_1, \ldots, x_{p^t})$ be the purely transcendental field extension of K generated by indeterminates $x_1, \ldots, x_{p^t}$. Let σ be the K-automorphism of order p^t of $E_t(K)$ permuting the x_i's cyclically. Let $F_t(K)$ be the subfield of $E_t(K)$ fixed by σ. Then, for any primitive p^s-th root of unity $\zeta_s \in K$, the cyclic algebra $(E_t(K)/F_t(K), \sigma, \zeta_s)$ is a division algebra.*

Proof. We will prove more than the statement of the theorem. Let n be a nonnegative integer satisfying $n \leq t$, and let $K_{n,t}$ be the subfield of $E_t(K)$ fixed by σ^{p^n}. We will prove the following:

($\mathcal{P}(K, t, n)$) *Suppose $s(K) > t - n$. Then, for any primitive p^s-th root of unity $\zeta_s \in K$, the cyclic algebra $R_{n,t}(K) := (K_{n,t}/K_{0,t}, \sigma, \zeta_s)$ is a division algebra.*

The theorem follows by taking $n = t$. The proof is an induction on n. More precisely, we assume that $n \geq 1$ (indeed, it is obvious that $\mathcal{P}(K, t, 0)$ is true) and that $\mathcal{P}(K', t, n-1)$ holds for every field K' satisfying the assumptions of the theorem. We now proceed to show that $\mathcal{P}(K, t, n)$ holds as well.

Recall that K_n denotes the field $K(\mu_{p^n})$. For each integer $n \geq 1$, we denote by $\zeta_n \in K_n$ a primitive p^n-th root of unity, such that $\zeta_{n+1}^p = \zeta_n$. Let $H = K[x_1, \ldots, x_{p^t}]$ and $H_1 = \bigoplus_{i=1}^{p^t} Kx_i$. We shall consider H as a $K[\sigma]$-module; the submodule $H_1 \subset H$ is then free of rank 1. Write $R_{n,t}(K) = \bigoplus_{i=0}^{p^n-1} K_{n,t} z^i$ where $zaz^{-1} = \sigma(a)$ for each $a \in K_{n,t}$ and $z^{p^n} = \zeta_s$. Let $W_{n,t}(K) = \bigoplus_{i=0}^{p^n-1} (H \cap K_{n,t}) z^i$; it is an order in $R_{n,t}(K)$ since the field of fractions of $H \cap K_{n,t}$ equals $K_{n,t}$. Choose a decomposition

$$K[\sigma] = K[X]/(X^{p^t} - 1) = L_1 \times \ldots \times L_u$$

(direct product of fields). Let $e_i \in K[\sigma]$ be the idempotent corresponding to L_i. Let $V_i = e_i H_1$; these are simple $K[\sigma]$-modules. Given $j = (j_1, \ldots, j_u) \in \mathbb{N}^u$, put $H_j = V_1^{j_1} \ldots V_u^{j_u}$. We say that $a \in W_{n,t}(K)$ is homogeneous if $a \in \bigoplus_{i=0}^{p^n-1} H_j z^i$ for some j. Let us prove the following two assertions:

i) Assume that $s > t - n$. Then, for any $j = (j_1, \ldots, j_u)$, there is a nonzero homogeneous element $b \in H_1$ such that $bH_j \subset K_{n-1,t}$.

ii) If $0 \leq d \leq n$, the centralizer of z^{p^d} in $R_{n,t}(K)$ is equal to $\bigoplus_{i=0}^{p^n-1} K_{d,t}z^i$ and is isomorphic to $R_{d,t}(K_{s+n-d})$.

We first prove i). Let $\tau = \sigma^{p^{n-1}}$. Then τ is of order $p^{t-n+1} \leq p^s$. Since $\mu_{p^{t-n+1}} \subset K$, it follows that the action of τ on V_i is diagonalizable. Because V_i is an irreducible $K[\sigma]$-module, τ must act by multiplication by some p^{t-n+1}-th root of unity $\zeta(i)$ on the whole space V_i. Let $\zeta = \zeta(1)^{j_1} \dots \zeta(u)^{j_u}$. Now τ acts by multiplication by ζ on H_j. One easily sees that all p^{t-n+1}-th roots of unity occur as eigenvalues of τ acting on H_1 (indeed, H_1 is a free $K[\tau]$-module). Hence we can pick a nonzero homogeneous $b \in H_1$ such that $\tau(b) = \zeta^{-1}b$. It is clear that τ acts trivially on bH_j, whence the claim.

We now prove ii). Let R' be the centralizer of z^d in $R_{n,t}(K)$. It is clear that $R' = \bigoplus_{i=0}^{p^n-1} K_{d,t}z^i$ since $K_{d,t}$ is the subfield of $K_{n,t}$ fixed by σ^d. The polynomial $X^{p^{n-d}} - \zeta_s$ is irreducible in $K_{d,t}[X]$. Indeed, this is the content of Remark 3.4, with K replaced by $K_{d,t}$ (note that K is algebraically closed in $K_{d,t}$). Therefore, it is the minimal polynomial of z^{p^d} over $K_{d,t}$. We then have $K_{d,t}(z^{p^d}) \simeq K_{d,t}(\zeta_{s+n-d})$. We can now compute:

$$R' = \bigoplus_{i=0}^{p^d-1} K_{d,t}(z^{p^d})z^i \simeq \bigoplus_{i=0}^{p^d-1} K_{d,t}(\zeta_{s+n-d})z^i \simeq R_{d,t}(K_{s+n-d}).$$

The last isomorphism follows from the fact that $K_{d,t}(\zeta_{s+n-d})$ is canonically isomorphic to $K(\zeta_{s+n-d})_{d,t} = (K_{s+n-d})_{d,t}$.

With i) and ii) at our disposal, the rest of the proof is straightforward. Since $W_{n,t}(K)$ is an order in $R_{n,t}(K)$, it suffices to show that $W_{n,t}(K)$ has no zero-divisors. Take $a, b \in W_{n,t}(K)$ such that $ab = 0$. Considering leading terms for the total degree on H, we may assume a, b are homogeneous (in the sense defined above). By i) there exist nonzero homogeneous elements a' and b' in H such that $a'a$ and bb' belong to $\bigoplus_{i=0}^{p^n-1} K_{n-1,t}z^i$, which is isomorphic to $R_{n-1,t}(K_{s+1})$ by ii) applied to $d = n-1$, and which is a division ring by $\mathcal{P}(K_{s+1}, t, n-1)$ (the induction step works since we have $n-1 \leq t < s+1+n-1$). But $(a'a)(bb') = 0$, so $a'a = 0$ or $bb' = 0$, implying $a = 0$ or $b = 0$. □

4. The main theorem

We are now ready to prove the theorem announced in the abstract.

Theorem 4.1. *Let K be a field, and p a prime number invertible in K. Let $s = \max\{n \in \mathbb{N}, \mu_{p^n} \subset K\}$. We assume that s is finite and positive, and that $K(\mu_8) \neq K(\mu_4)$ if $p = 2$ and $s = 1$. Let $r > s$ be an integer. We then have*

$$\mathrm{ed}_K(\mathbb{Z}/p^r\mathbb{Z}) = p^{r-s}.$$

Proof. We use the notation of the preceding section. The K-vector space K_r is a generically free representation of G_r, of dimension p^{r-s}. Let

$\mathbb{A}_K(K_r) - \{0\} \xrightarrow{\phi} \mathbb{A}_K(K_r) - \{0\}$ be a G_r-equivariant rational map. By Proposition 2.5, it is enough to show that ϕ is dominant. By Lemma 2.11, we may assume that ϕ is d-homogeneous for some integer d. Note that d is nonzero, since $\phi(tx) = t\phi(x)$ for x in a nonempty open subset of $\mathbb{A}_K(K_r) - \{0\}$ and $t \in G_s \subset \mathbb{G}_m$. Modding out by $\mathbb{G}_m$, which we can do by Lemma 2.2, we obtain a G_{r-s}-equivariant rational map ψ fitting into a commutative diagram

$$\begin{array}{ccc} \mathbb{A}_K(K_r) - \{0\} & \xrightarrow{\phi} & \mathbb{A}_K(K_r) - \{0\} \\ \downarrow & & \downarrow \\ \mathbb{P}_K(K_r) & \xrightarrow{\psi} & \mathbb{P}_K(K_r). \end{array}$$

Let $M = K(x_g, g \in G_{r-s})$ be the purely transcendental extension of K generated by variables $x_g, g \in G_{r-s}$. The group G_{r-s} acts on M in the obvious way; let $L = M^{G_{r-s}}$. Now we extend scalars from K to L. We get a G_{r-s}-equivariant rational map $\psi_L : \mathbb{P}_L(L_r) \dashrightarrow \mathbb{P}_L(L_r)$, where $L_r = K_r \otimes_K L$. Thanks to Lemma 2.14, we can twist both sides by the G_{r-s}-torsor P corresponding to the cyclic extension M/L. Using Lemma 3.5, we obtain a rational map ${}^P\psi_L : SB(A) \dashrightarrow SB(A)$, where A/L is the cyclic algebra $(M/L, \sigma, \zeta_s)$, with $\sigma = \zeta_{r-s}^{-1} \in G_{r-s}$. Combining Theorem 3.6 (with $t = r - s$) and Theorem 3.2, we get that ${}^P\psi_L$ is dominant. Hence also ψ is dominant, as it easily follows from the functorial properties of the twist (Lemma 2.14). This implies the existence of an open subset $U \subset \mathbb{A}_K(K_r) - \{0\}$ such that $\overline{\phi(\mathbb{A}_K(K_r) - \{0\})}$ intersects the $\mathbb{G}_m$-orbit of every element in U. But $\overline{\phi(\mathbb{A}_K(K_r) - \{0\})}$ is $\mathbb{G}_m$-invariant (remember that ϕ is d-homogeneous and that d is nonzero). Thus, ϕ itself is dominant. □

Corollary 4.2. *For any $n \geq 1$, we have* $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/2^n\mathbb{Z}) = 2^{n-1}$ *and* $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/3^n\mathbb{Z}) = 3^{n-1}$.

Proof. The first equality is a special case of the theorem. Note that, by a result of Ledet ([Le]), we have $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/p^n\mathbb{Z}) \leq \phi(p-1)p^{n-1}$. Hence, $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/3^n\mathbb{Z}) \leq 3^{n-1}$. But, as essential dimension decreases after a field extension, we also have $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/3^n\mathbb{Z}) \geq \mathrm{ed}_{\mathbb{Q}(\mu_3)}(\mathbb{Z}/3^n\mathbb{Z}) = 3^{n-1}$. □

References

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

[Bra] Brauer, R.: Über den Index und den Exponenten von Divisionsalgebren. Tohoku Math. J. **37**, 77–87 (1933)

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

[FF] Favi, G., Florence, M.: Tori and Essential Dimension. To appear in J. Algebra, available at http://www.math.uni-bielefeld.de/LAG/man/208.pdf

[JLY] Jensen, C.U., Ledet, A., Yui, N.: Generic Polynomials: Constructive Aspects of the Inverse Galois Problem. Math. Sci. Res. Inst. Publ. Ser., vol. 45. Cambridge University Press (2002)
[Ka] Karpenko, N.: On anisotropy of orthogonal involutions. J. Ramanujan Math. Soc. **15**(1), 1–22 (2002)
[Le] Ledet, A.: On the essential dimension of some semi-direct products. Can. Math. Bull. **45**, 422–427 (2002)
[Me] Merkurjev, A.: Degree formula. Available at http://www.mathematik.uni-bielefeld.de/rost/degree-formula.html
[Re] Reichstein, Z.: On the notion of essential dimension for algebraic groups. Transform. Groups **5**(3), 265–304 (2000)
[Ros] Rost, M.: Essential dimension of twisted C_4. Available at http://www.mathematik.uni-bielefeld.de/rost/ed.html#C4
[Row] Rowen, L.: Ring Theory, vol. 2. Pure Appl. Math., vol. 128. Academic Press, Boston (1988)
[Se] Serre, J.-P.: Groupes algébriques et corps de classes. Publ. Math. Inst. Math. Univ. Nancago VII. Hermann (1959)