On the essential dimension of cyclic p-groups

Mathieu Florence[1]

December 2006

Abstract. Let p be a prime number and $r \geq 1$ an integer. We compute the essential dimension of $\mathbb{Z}/p^r\mathbb{Z}$ over fields of characteristic not p, containing the p-th roots of unity (theorem 3.1). In particular, we have $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/8\mathbb{Z}) = 4$, a result which was conjectured by Buhler and Reichstein in 1995 (unpublished).

Keywords and Phrases: Galois cohomology, essential dimension, Severi-Brauer varieties.

A la mémoire de mon père.

Acknowledgements

We thank Jean Fasel and Giordano Favi for fruitful discussions about essential dimension.

Contents

1. Introduction

The notion of essential dimension was 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. The essential dimension of G over k, denoted by* $\mathrm{ed}_k(G)$*, is the smallest nonnegative integer n with the following property.*
For each field extension K/k, and each G_K-torsor $T \longrightarrow Spec(K)$, there exists a subfield K' of K, containing k, and a $G_{K'}$-torsor $T' \longrightarrow Spec(K')$, such that

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

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

Thus, $\mathrm{ed}_k(G)$ is the smallest number of algebraically independent parameters required to define G-torsors. It turned out that this number, even in apparently simple cases, is extremely difficult to compute. Focusing of finite abelian groups, let us mention some known results. Over fields containing all roots of unity, the essential dimension of a finite abelian group equals its rank, at least if the characteristic does not divide the order of the group under consideration ([BR], theorem 6.1). 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, and that 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.

2. Some auxiliary results

In this section, we introduce the material required to prove the main theorem. Before going any further, we briefly recall the notion of *friendly open subset*.
Let G/k be an algebraic group, where k is any field, and X/k an irreducible G-variety, on which G acts generically freely, 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 (see [BF], 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).*

If V is a finite dimensional vector space over some field k, we denote by $\mathbb{A}(V)$ the k-variety representing the functor $A \mapsto V \otimes_k A$, where A runs through all k-algebras. The following proposition seems to be well-known; as we lack a suitable reference, we include a proof.

Proposition 2.2. *Let k be a field, G/k a linear algebraic group, and V a finite-dimensional representation of G over k, which is generically free. Let $U \subset \mathbb{A}(V)$ be a friendly open subset. Then $\mathrm{ed}_k(G) + dim(G) = min(dim(\phi(U)))$, 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. We first prove that $\mathrm{ed}_k(G) + \dim(G) \geq \min(\dim(\phi(U)))$. By [BF], proposition 4.11, we know that the G-torsor $U \longrightarrow U/G$ is versal. Let $X \longrightarrow Y$ be a versal G-torsor, with $\dim(Y) = \mathrm{ed}_k(G)$. By the very definition of a versal torsor, there exists two commutative squares

$$\begin{array}{ccc} U & \overset{f}{\dashrightarrow} & X \\ \downarrow & & \downarrow \\ U/G & \overset{g}{\dashrightarrow} & Y \end{array}$$

and

$$\begin{array}{ccc} X & \overset{f'}{\dashrightarrow} & U \\ \downarrow & & \downarrow \\ Y & \overset{g'}{\dashrightarrow} & U/G, \end{array}$$

where the horizontal arrows are rational maps, and where f and f' are G-equivariant. Note that g (and hence f) is necessarily dominant. Indeed, let Y' be the closure of the image of g, and $X' := X \times_Y Y'$. Then the G-torsor $X' \longrightarrow Y'$ is versal (as a compression of the versal torsor $U \longrightarrow U/G$), which implies that $\dim(Y') \geq \mathrm{ed}_k(G) = \dim(Y)$. In other words, $Y = Y'$. Thus, the composite $\phi := f' \circ f$ is well-defined, and $\dim(\phi(U)) \leq \dim(X) = \mathrm{ed}_k(G) + \dim(G)$. The desired inequality follows. For the other inequality, let $\phi : U \dashrightarrow U$ be a G-equivariant rational map. We have a commutative square

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

Let S be the closure of the image of $\bar{\phi}$, and $T = U \times_{U/G} S$. Then $T \longrightarrow S$ is a versal G-torsor. Therefore, $\dim(\phi(U)) = \dim(T) = \dim(S) + \dim(G) \geq \mathrm{ed}_k(G) + \dim(G)$. □

The next lemma will be applied in order to prove the main theorem. It allows us to restrict our attention to a particular type of G-equivariant rational maps; namely, homogeneous ones.

Definition 2.3. *Let V be a finite dimensional vector space over some field k, and d an integer. A non-zero rational map $\phi : \mathbb{A}(V) \longrightarrow \mathbb{A}(V)$ is said to be d-homogeneous if the following diagram commutes:*

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

We shall also say that ϕ is homogeneous if it is d-homogeneous for some (unique) $d \in \mathbb{Z}$.

Lemma 2.4. *Let k be a field, G/k a linear algebraic group, and V a finite-dimensional irreducible representation of G over k. Assume there exists a G-equivariant rational map $\mathbb{A}(V) \overset{\phi}{\dashrightarrow} \mathbb{A}(V)$ which is not dominant and non-zero. Then there exists $\mathbb{A}(V) \overset{\psi}{\dashrightarrow} \mathbb{A}(V)$ with the same properties, and which is moreover homogeneous.*

Proof. Identify $\mathbb{A}(V)$ with $\mathbb{A}^N$ using a basis of V/k. The map ϕ is now given by

$$(x_1, ..., x_N) \in \mathbb{A}^N \mapsto (\frac{P_1}{Q}, ..., \frac{P_N}{Q}),$$

where Q and the P_i's are non-zero polynomials in the x_j's. From the G-equivariance of ϕ and the irreducibility of V, it follows that the P_i's have the same degree d. Let d' be the degree of Q. Let H_i be the homogeneous component of degree d of P_i and S the homogeneous component of degree d' of Q. The hypothesis made on ϕ implies that there exists a non zero polynomial R in N variables such that $R(\frac{P_1}{Q}, ..., \frac{P_N}{Q})$=0. Write $R = R_n + R_{n-1} + ... + R_m$, where R_i is homogeneous of degree i and R_n,R_m are both non-zero. We have $\sum_{i=m}^{n} R_i(P_1, ..., P_N)Q^{n-i} = 0$. If $d' > d$, an easy degree consideration yields that $R_m(H_1, ..., H_N) = 0$. Similarly, if $d' < d$, we have $R_n(H_1, ..., H_N) = 0$. Finally, if $d = d'$, one gets $\sum_{i=m}^{n} R_i(H_1, ..., H_N)S^{n-i} = 0$. In all cases, we see that the map

$$\psi : (x_1, ..., x_N) \in \mathbb{A}^N \mapsto (\frac{H_1}{S}, ..., \frac{H_N}{S})$$

is not dominant. As it is obviously G-equivariant and homogeneous, we are done. □

The following theorem, due to Karpenko, is a key argument 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 a proof.

THEOREM 2.5 (see [Ka], theorem 2.1). *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 rational map $SB(A) \dashrightarrow SB(A)$ is dominant.*

Proof. Let $SB(A) \dashrightarrow SB(A)$ 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. *loc. cit.* for the definition of these numbers). The first one is easily seen to be p^n, as A is a division algebra. By *loc. cit.*, 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 $p^{n-1} = \deg(f)p^{n-1} \bmod p^n$. In particular, $\deg(f)$ is non-zero; that is to say, f is dominant. □

From now on, p will be a fixed prime number, K will be 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 $K_n = K(\mu_{p^n}(\bar{K}))$. Choose primitive p^n-th roots of unity $\zeta_n \in K_n$ such that $\zeta_{n+1}^p = \zeta_n$. We will sometimes identify G_n with $\mathbb{Z}/p^n\mathbb{Z}$ by sending ζ_n to 1. Let

$$s = \max\{n \in \mathbb{N}, \text{ such that } K = K_n\}$$

(we assume that s is finite; if not, the question we are dealing with has a trivial answer). We make the following assumptions on s:

i) We have $s \geq 1$,
ii) If $p = 2$ and $s = 1$, then $K_2 \neq K_3$.

It is easy to check that i) and ii) imply 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). Let $r \geq 1$ be any integer. Our goal is to compute the number $\mathrm{ed}_K(\mathbb{Z}/p^r\mathbb{Z})$. It is 1 if $r \leq s$, so we assume $r \geq s$.

Consider $\mathbb{P}(K_r)$, the projective space of K_r viewed as a K-vector space. It is naturally endowed with an action of G_r. For this action, $G_s \subset G_r$ acts trivially. Thus, we have an induced action of $G_{r-s} = G_r/G_s$, which is easily seen to be faithful. The following easy lemma will be useful in the sequel.

LEMMA 2.6. *Let L/K be any field extension, and M/L a cyclic field extension, of group G_{r-s}. Then the twist of $\mathbb{P}(K_r)_L$ 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 $\sigma = \zeta_{r-s} \in G_{r-s}$. 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. Let $L_r = L \otimes_K K_r$. 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. First of all, this algebra clearly 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 $E = L^{p^{r-s}}$ of $\mathrm{End}_L(L_r)$ consisting of linear maps admitting $1, \zeta_r, ..., \zeta_r^{p^{r-s}-1}$ 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. It follows that A is presented as stated in the lemma, with $X = \zeta_r \in L_r$. □

In the proof of theorem 3.1, we shall apply theorem 2.5 to some particular division algebra, arising as a generalized version of the 'generic' division algebra of Brauer-Rowen ([Row]). *Mutatis mutandis*, the proof of the next theorem is the same as that of *loc. cit.*, theorem 7.3.8. We tried to harmonize our notations with those of Rowen, with one minor change: the letters q, n, t, k used in *loc. cit.* correspond here to p^q, p^n, p^t and p^k, respectively.

THEOREM 2.7. *Let n, t and $q \geq s$ be three integers, with $n \leq t \leq q+n$. Let $E_{q,t} = K_q(x_1, ..., x_{p^t})$ be purely transcendental over K_q. Let σ be the K_q-automorphism of order p^t of $E_{q,t}$, permuting the x_i's cyclically. Let $K_{q,n,t}$ be the subfield of $E_{q,t}$ fixed by σ^{p^n}. Then the cyclic algebra $R_{q,n,t} := (K_{q,n,t}, \sigma, \zeta_q)$ is a division algebra.*

Proof. We adopt the notations of *loc. cit.*, page 246. More precisely, let $F_0 = K_q$, $H = F_0[x_1, ..., x_{p^t}]$, $H_1 = \sum_{i=1}^{p^t} F_0 x_i$. Write $R_{q,n,t} = \sum_{i=0}^{p^n-1} K_{q,n,t} z^i$ where $zaz^{-1} = \sigma(a)$ for each $a \in K_{q,n,t}$ and $z^{p^n} = \zeta_q$. Choose a decomposition $F_0[X]/ < X^{p^t} - 1 >= L_1 \times ... \times L_u$ (direct product of fields). Let $V_i = L_i H_1$; these are simple σ-modules. Given $j = (j_1, ..., j_u) \in \mathbb{N}^u$, put $H_j = V_1^{j_1} ... V_u^{j_u}$. First of all, note that lemma 7.3.4 of *loc. cit.* remains valid in our setting (for 7.3.4 ii), note that, in fact, all p^{t-k}-th roots of unity occur as eigenvalues of σ^{p^k} acting on H). It is also clear that lemma 7.3.6 i) still holds, since the polynomial $X^{p^m} - \zeta_q$ is irreducible in $k_q[X]$, for any $m \geq 0$. With these lemmas at our disposal, the rest of the proof is exactly the same as that of *loc. cit.*, theorem 7.3.8. □

3. The main theorem

We are now ready to prove the theorem announced in the abstract. We keep the notations of the previous section.

THEOREM 3.1. *We have* $\mathrm{ed}_K(\mathbb{Z}/p^r\mathbb{Z}) = p^{r-s}$.

Proof. By proposition 2.2, it is enough to show that every G_r-equivariant non-zero rational map $\mathbb{A}(K_r) - \stackrel{\phi}{-} \succ \mathbb{A}(K_r)$ is dominant. Assume the contrary: let $\mathbb{A}(K_r) - \stackrel{\phi}{-} \succ \mathbb{A}(K_r)$ be a non-zero, non-dominant G_r-equivariant rational map. Then by lemma 2.4, we can assume that ϕ is homogeneous: there exists an integer d such that $\phi(\lambda v) = \lambda^d \phi(v)$ for all $v \in \mathbb{A}(K_r)$ and all $\lambda \in K$. Thus, we have an induced G_{r-s}-equivariant rational map $\mathbb{P}(K_r) - \stackrel{\bar{\phi}}{-} \succ \mathbb{P}(K_r)$ (remember that here G_{r-s} is viewed as the quotient G_r/G_s). From the relation $\phi(\zeta_s v) = \zeta_s \phi(v)$, it follows that d is non-zero. Hence, $\bar{\phi}$ cannot be dominant. Let $M = K(x_g, g \in G_{r-s})$ be purely transcendental over K. The group G_{r-s} acts on M the obvious way; let $L = M^{G_{r-s}}$. Now extend scalars to L. We get a non-dominant G_{r-s}-equivariant rational map $\bar{\phi}_L : \mathbb{P}(L_r) - - \succ \mathbb{P}(L_r)$, where $L_r = K_r \otimes_K L$. We can twist both sides by the G_{r-s}-torsor corresponding to the cyclic extension M/L. Thanks to lemma 2.6, we obtain a non-dominant rational selfmap of $SB(A)$, where A/L is the cyclic algebra $(M/L, \sigma, \zeta_s)$, with $\sigma = \zeta_{r-s} \in G_{r-s}$. By theorem 2.7, A is a division algebra. This contradicts theorem 2.5. □

Corollary 3.2. *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 directly follows from the theorem. For the second one, 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 $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/3^n\mathbb{Z}) \geq \mathrm{ed}_{\mathbb{Q}(\mu_3)}(\mathbb{Z}/3^n\mathbb{Z}) = 3^{n-1}$.

□

Remark 3.3. At first sight, it seems that our strategy cannot be applied to compute the value of $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/11\mathbb{Z})$.

References

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

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

[FF] G. Favi, M. Florence. — *Tori and Essential Dimension*, preprint, available at http://www.math.uni-bielefeld.de/LAG/man/208.pdf

[JLY] C. U. Jensen, A. Ledet, N. Yui. — *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, MSRI Pub. Series 45 (2002), Cambridge University Press.

[Ka] N. Karpenko. — *On anisotropy of orthogonal involutions*, J. Ramanujan Math. Soc. 15, no. 1 (2002), 1-22.

[Le] A. Ledet. — *On the essential dimension of some semi-direct products*, Canad. Math. Bull. 45(2002), 422-427.

[Me] A. Merkurjev. — *Degree Formula*, available at http://www.mathematik.uni-bielefeld.de/ rost/degree-formula.html

[Re] Z. Reichstein. — *On the Notion of Essential Dimension for Algebraic Groups*, Transform. Groups 5, no. 3 (2000), 265-304.

[Ros] M. Rost. — *Essential dimension of twisted C_4*, available at http://www.mathematik.uni-bielefeld.de/ rost/ed.html#C4

[Row] L. Rowen. — *Ring Theory*, vol. 2, Pure and Applied Mathematics 128 (Boston, Academic Press, 1988).

Mathieu Florence, Ecole Polytechnique Fédérale de Lausanne, FSB-MA, CH-1015 Lausanne, Switzerland.
E-mail address: mathieu.florence@gmail.com