Invent. math. 172, 491–508 (2008)
DOI: 10.1007/s00222-007-0106-6

Inventiones mathematicae

Essential dimension of finite p-groups

Nikita A. Karpenko[1,⋆], **Alexander S. Merkurjev**[2,⋆⋆]

[1] Institut de Mathématiques de Jussieu, Université Pierre et Marie Curie (Paris 6), 4 place Jussieu, 75252 Paris Cedex 05, France
(e-mail: karpenko@math.jussieu.fr)
[2] Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA (e-mail: merkurev@math.ucla.edu)

Oblatum 25-VI-2007 & 22-XI-2007
Published online: 10 January 2008 –

Abstract. We prove that the essential dimension and p-dimension of a p-group G over a field F containing a primitive p-th root of unity is equal to the least dimension of a faithful representation of G over F.

The notion of the essential dimension $\mathrm{ed}(G)$ of a finite group G over a field F was introduced in [5]. The integer $\mathrm{ed}(G)$ is equal to the smallest number of algebraically independent parameters required to define a Galois G-algebra over any field extension of F. If V is a faithful linear representation of G over F then $\mathrm{ed}(G) \leq \dim(V)$ (cf. [2, Prop. 4.15]). The essential dimension of G can be smaller than $\dim(V)$ for every faithful representation V of G over F. For example, we have $\mathrm{ed}(\mathbb{Z}/3\mathbb{Z}) = 1$ over $\mathbb{Q}$ or any field F of characteristic 3 (cf. [2, Cor. 7.5]) and $\mathrm{ed}(S_3) = 1$ over $\mathbb{C}$ (cf. [5, Th. 6.5]).

In this paper we prove that if G is a p-group and F is a field of characteristic different from p containing p-th roots of unity, then $\mathrm{ed}(G)$ coincides with the least dimension of a faithful representation of G over F (cf. Theorem 4.1).

We also compute the essential p-dimension of a p-group G introduced in [15]. We show that $\mathrm{ed}_p(G) = \mathrm{ed}(G)$ over a field F containing p-th roots of unity.

⋆ The work of the first author has been partially supported by the Collaborative Research Centre 701 "Spectral Structures and Topological Methods in Mathematics" of the Bielefeld University.

⋆⋆ The work of the second author has been supported by the NSF grant DMS #0652316.

Mathematics Subject Classification (2000): 20G15; 14C35

Acknowledgement: We are grateful to Zinovy Reichstein for useful conversations and comments.

1. Preliminaries

In the paper the word “scheme” means a separated scheme of finite type over a field and “variety” an integral scheme.

1.1. Severi–Brauer varieties. (cf. [1]) Let A be a central simple algebra of degree n over a field F. The *Severi–Brauer variety* $P = \mathrm{SB}(A)$ of A is the variety of right ideals in A of dimension n. For a field extension L/F, the algebra A is split over L if and only if $P(L) \neq \emptyset$ if and only if $P_L \simeq \mathbb{P}^{n-1}_L$.

The change of field map $\deg : \mathrm{Pic}(P) \to \mathrm{Pic}(P_L) = \mathbb{Z}$ for a splitting field extension L/F identifies $\mathrm{Pic}(P)$ with $e\mathbb{Z}$, where e is the exponent (period) of A. In particular, P has divisors of degree e. The algebra A is split over L if and only if P_L has a prime divisor of degree 1 (a hyperplane).

1.2. Groupoids and gerbes. (cf. [4]) Let $\mathcal{X}$ be a groupoid over F in the sense of [19]. We assume that for any field extension L/F, the isomorphism classes of objects in the category $\mathcal{X}(L)$ form a set which we denote by $\widehat{\mathcal{X}}(L)$. We can view $\widehat{\mathcal{X}}$ as a functor from the category Fields/F of field extensions of F to Sets.

Example 1.2.1. If G is an algebraic group over F, then the groupoid BG is defined as the category of G-torsors over a scheme over F. Hence the functor $\widehat{BG}$ takes a field extension L/F to the set of all isomorphism classes of G-torsors over L.

Special examples of groupoids are *gerbes banded by a commutative group scheme* C over F. There is a bijection between the set of isomorphism classes of gerbes banded by C and the Galois cohomology group $H^2(F, C)$ (cf. [7, Ch. 4] and [13, Ch. 4, § 2]). The split gerbe BC corresponds to the trivial element of $H^2(F, C)$.

Example 1.2.2 (Gerbes banded by μ_n). Let A be a central simple F-algebra and n an integer with $[A] \in \mathrm{Br}_n(F) = H^2(F, \mu_n)$. Let P be the Severi–Brauer variety of A and S a divisor on P of degree n. Denote by $\mathcal{X}_A$ the gerbe banded by μ_n corresponding to $[A]$. For a field extension L/F, the set $\widehat{\mathcal{X}}_A(L)$ has the following explicit description (cf. [4]): $\widehat{\mathcal{X}}_A(L)$ is nonempty if and only if P is split over L. In this case $\widehat{\mathcal{X}}_A(L)$ is the set of equivalence classes of the set

$$\left\{ f \in L(P)^\times : \mathrm{div}(f) = nH - S_L, \text{ where } H \text{ is a hyperplane in } P_L \right\},$$

and two functions f and f' are equivalent if $f' = fh^n$ for some $h \in L(P)^\times$.

1.3. Essential dimension. Let $T : \mathit{Fields}/F \to \mathit{Sets}$ be a functor. For a field extension L/F and an element $t \in T(L)$, the *essential dimension* *of* t, denoted $\mathrm{ed}(t)$, is the least $\mathrm{tr.deg}_F(L')$ over all subfields $L' \subset L$ over F such that t belongs to the image of the map $T(L') \to T(L)$. The *essential dimension* $\mathrm{ed}(T)$ *of the functor* T is the supremum of $\mathrm{ed}(t)$ over all $t \in T(L)$ and field extensions L/F.

Let p be a prime integer and $t \in T(L)$. The *essential p-dimension of* t, denoted $\mathrm{ed}_p(t)$, is the least $\mathrm{tr.deg}_F(L'')$ over all subfields $L'' \subset L'$ over F, where L' is a finite field extension of L of degree prime to p such that the image of t in $T(L')$ belongs to the image of the map $T(L'') \to T(L')$. The *essential p-dimension* $\mathrm{ed}_p(T)$ *of the functor* T is the supremum of $\mathrm{ed}_p(t)$ over all $t \in T(L)$ and field extensions L/F. Clearly, $\mathrm{ed}(T) \geq \mathrm{ed}_p(T)$.

Let G be an algebraic group over F. The *essential dimension* $\mathrm{ed}(G)$ *of* G (respectively the *essential p-dimension* $\mathrm{ed}(G)$) is the essential dimension (respectively the essential p-dimension) of the functor taking a field extension L/F to the set of isomorphism classes of G-torsors over $\mathrm{Spec}\, L$.

If G is a finite group, we view G as a constant group over a field F. Every G-torsor over $\mathrm{Spec}\, L$ has the form $\mathrm{Spec}\, K$ where K is a Galois G-algebra over L. Therefore, $\mathrm{ed}(G)$ is the essential dimension of the functor taking a field L to the set of isomorphism classes of Galois G-algebras over L.

Example 1.3.1. Let $\mathcal{X}$ be a groupoid over F. The *essential dimension of* $\mathcal{X}$, denoted by $\mathrm{ed}(\mathcal{X})$, is the essential dimension $\mathrm{ed}(\widehat{\mathcal{X}})$ of the functor $\widehat{\mathcal{X}}$ defined in Sect. 1.2. The *essential p-dimension of* $\mathrm{ed}_p(\mathcal{X})$ is defined similarly. In particular, $\mathrm{ed}(BG) = \mathrm{ed}(G)$ and $\mathrm{ed}_p(BG) = \mathrm{ed}_p(G)$ for an algebraic group G over F.

1.4. Canonical dimension. (cf. [3], [11]) Let F be a field and $\mathcal{C}$ a class of field extensions of F. A field $E \in \mathcal{C}$ is called *generic* if for any $L \in \mathcal{C}$ there is an F-place $E \rightsquigarrow L$.

The *canonical dimension* $\mathrm{cdim}(\mathcal{C})$ of the class $\mathcal{C}$ is the minimum of the $\mathrm{tr.deg}_F E$ over all generic fields $E \in \mathcal{C}$.

Let p be a prime integer. A field E in a class $\mathcal{C}$ is called *p-generic* if for any $L \in \mathcal{C}$ there is a finite field extension L' of L of degree prime to p and an F-place $E \rightsquigarrow L'$. The *canonical p-dimension* $\mathrm{cdim}_p(\mathcal{C})$ of the class $\mathcal{C}$ is the least $\mathrm{tr.deg}_F E$ over all p-generic fields $E \in \mathcal{C}$. Obviously, $\mathrm{cdim}(\mathcal{C}) \geq \mathrm{cdim}_p(\mathcal{C})$.

Let $T : \mathit{Fields}/F \to \mathit{Sets}$ be a functor. Denote by $\mathcal{C}_T$ the class of *splitting fields of* T, i.e., the class of field extensions L/F such that $T(L) \neq \emptyset$. The *canonical dimension (p-dimension) of* T, denoted $\mathrm{cdim}(T)$ (respectively $\mathrm{cdim}_p(T)$), is the canonical dimension (p-dimension) of the class $\mathcal{C}_T$.

If X is a scheme over F, we write $\mathrm{cdim}(X)$ and $\mathrm{cdim}_p(X)$ for the canonical dimension and p-dimension of X viewed as a functor $L \mapsto X(L) = \mathrm{Mor}_F(\mathrm{Spec}\, L, X)$.

Example 1.4.1. Let $\mathcal{X}$ be a groupoid over F. We define the *canonical dimension* $\mathrm{cdim}(\mathcal{X})$ *and p-dimension* $\mathrm{cdim}_p(\mathcal{X})$ *of* $\mathcal{X}$ as the canonical dimension and p-dimension of the functor $\widehat{\mathcal{X}}$.

Example 1.4.2. If X is a regular and complete variety over F viewed as a functor then $\operatorname{cdim}(X)$ is equal to the smallest dimension of a closed subvariety $Z \subset X$ such that there is a rational morphism $X \dashrightarrow Z$ (cf. [11, Cor. 4.6]). If p is a prime integer then $\operatorname{cdim}_p(X)$ is equal to the smallest dimension of a closed subvariety $Z \subset X$ such that there are dominant rational morphisms $X' \dashrightarrow X$ of degree prime to p and $X' \dashrightarrow Z$ for some variety X' (cf. [11, Prop. 4.10]).

*Remark 1.4.2 (*A relation between essential and canonical dimension*).* Let $T : \mathit{Fields}/F \to \mathit{Sets}$ be a functor. We define the "contraction" functor $T^c : \mathit{Fields}/F \to \mathit{Sets}$ as follows. For a field extension L/F, we have $T^c(L) = \emptyset$ if $T(L)$ is empty and $T^c(L)$ is a one element set otherwise. If X is a regular and complete variety over F viewed as a functor then one can show that $\operatorname{ed}(X^c) = \operatorname{cdim}(X)$ and $\operatorname{ed}_p(X^c) = \operatorname{cdim}_p(X)$.

1.5. Valuations. Let K/F be a regular field extension, i.e., for any field extension L/F, the ring $K \otimes_F L$ is a domain. We write KL for the quotient field of $K \otimes_F L$.

Let v be a valuation on L over F with residue field R. Let O be the associated valuation ring and M its maximal ideal. As $K \otimes_F R$ is a domain, the ideal $\widetilde{M} := K \otimes_F M$ in the ring $\widetilde{O} := K \otimes_F O$ is prime. The localization ring $\widetilde{O}_{\widetilde{M}}$ is a valuation ring in KL with residue field KR. The corresponding valuation $\tilde{v}$ of KL is called the *canonical extension of* v *on* KL. Note that the groups of values of v and $\tilde{v}$ coincide.

We shall need the following lemma.

Lemma 1.1 (cf. [11, Lemma 3.2]). *Let v be a discrete valuation (of rank 1) of a field L with residue field R and L'/L a finite field extension of degree prime to p. Then v extends to a discrete valuation of L' with residue field R' such that the ramification index and the degree $[R' : R]$ are prime to p.*

Proof. If L'/L is separable and $v_1, \ldots, v_k$ are all the extensions of v on L' then $[L' : L] = \sum e_i[R_i : R]$ where e_i is the ramification index and R_i is the residue field of v_i (cf. [20, Ch. VI, Th. 20 and p. 63]). It follows that the integer $e_i[R_i : R]$ is prime to p for some i.

If L'/L is purely inseparable of degree q then the valuation v' of L' defined by $v'(x) = v(x^q)$ satisfies the desired properties. The general case follows. □

2. Canonical dimension of a subgroup of $\operatorname{Br}(F)$

Let F be an arbitrary field, p a prime integer and D a finite subgroup of $\operatorname{Br}_p(F)$ of dimension r over $\mathbb{Z}/p\mathbb{Z}$. In this section we determine the canonical dimension $\operatorname{cdim} D$ and the canonical p-dimension $\operatorname{cdim}_p D$ of the class of common splitting fields of all elements of D. We say that a basis $\{a_1, a_2, \ldots, a_r\}$ of D is *minimal* if for any $i = 1, \ldots, r$ and any element $d \in D$ outside of the subgroup generated by $a_1, \dots, a_{i-1}$, we have $\operatorname{ind} d \geq \operatorname{ind} a_i$.

One can construct a minimal basis of D by induction as follows. Let a_1 be a nonzero element of D of minimal index. If the elements $a_1, \dots, a_{i-1}$ are already chosen for some $i \leq r$, we take for the a_i an element of D of the minimal index among the elements outside of the subgroup generated by $a_1, \dots, a_{i-1}$.

In this section we prove the following

Theorem 2.1. *Let F be an arbitrary field, p a prime integer, $D \subset \operatorname{Br}_p(F)$ a subgroup of dimension r and $\{a_1, a_2, \dots, a_r\}$ a minimal basis of D. Then*

$$\operatorname{cdim}_p(D) = \operatorname{cdim}(D) = \Big(\sum_{i=1}^{r} \operatorname{ind} a_i\Big) - r\ .$$

We prove Theorem 2.1 in several steps.

Let $\{a_1, a_2, \dots, a_r\}$ be a minimal basis of D. For every $i = 1, 2, \dots, r$, let P_i be the Severi–Brauer variety of a central division F-algebra A_i representing the element $a_i \in \operatorname{Br}_p F$. We write P for the product $P_1 \times P_2 \times \cdots \times P_r$. We have

$$\dim P = \sum_{i=1}^{r} \dim P_i = \Big(\sum_{i=1}^{r} \operatorname{ind} a_i\Big) - r.$$

Moreover, the classes of splitting fields of P and D coincide, hence $\operatorname{cdim}(D) = \operatorname{cdim}(P)$ and $\operatorname{cdim}_p(D) = \operatorname{cdim}_p(P)$. Thus, the statement of Theorem 2.1 is equivalent to the equality $\operatorname{cdim}_p(P) = \operatorname{cdim}(P) = \dim(P)$.

Let $r \geq 1$ and $0 \leq n_1 \leq n_2 \leq \cdots \leq n_r$ be integers and $K = K(n_1, \dots, n_r)$ the subgroup of the polynomial ring $\mathbb{Z}[x]$ in r variables $x = (x_1, \dots, x_r)$ generated by the monomials $p^{e(j_1,\dots,j_r)} x_1^{j_1} \dots x_r^{j_r}$ for all $j_1, \dots, j_r \geq 0$, where the exponent $e(j_1, \dots, j_r)$ is 0 if all the $j_1, \dots, j_r$ are divisible by p, otherwise $e(j_1, \dots, j_r) = n_k$ with the maximum k such that j_k is not divisible by p. In fact, K is a subring of $\mathbb{Z}[x]$.

Remark 2.2. Let $A_1, \dots, A_r$ be central division algebras over some field such that for any non-negative integers $j_1, \dots, j_r$, the index of the tensor product $A_1^{\otimes j_1} \otimes \cdots \otimes A_r^{\otimes j_r}$ is equal to $p^{e(j_1,\dots,j_r)}$. The group K can be interpreted as the colimit of the Grothendieck groups of the product over $i = 1, \dots, r$ of the Severi–Brauer varieties of the matrix algebras $M_{l_i}(A_i)$ over all positive integers $l_1, \dots, l_r$.

We set $h = (h_1, \dots, h_r)$ with $h_i = 1 - x_i \in \mathbb{Z}[x]$.

Proposition 2.3. *Let $bh_1^{i_1} \dots h_r^{i_r}$ be a monomial of the lowest total degree of a polynomial f in the variables h lying in K. Assume that the integer b is not divisible by p. Then $p^{n_1} | i_1, \dots, p^{n_r} | i_r$.*

Proof. We recast the proof for $r = 1$ given in [8, Lemma 2.1.2] to the case of arbitrary r.

We proceed by induction on $m = r + n_1 + \cdots + n_r$. The case $m = 1$ is trivial. If $m > 1$ and $n_1 = 0$, then $K = K(n_2, \ldots, n_r)[x_1]$ and we are done by induction applied to $K(n_2, \ldots, n_r)$. In what follows we assume that $n_1 \geq 1$.

Since $K(n_1, n_2, \ldots, n_r) \subset K(n_1 - 1, n_2, \ldots, n_r)$, by the induction hypothesis $p^{n_1-1}|i_1, p^{n_2}|i_2, \ldots, p^{n_r}|i_r$. It remains to show that i_1 is divisible by p^{n_1}.

Consider the additive operation $\varphi : \mathbb{Z}[x] \to \mathbb{Q}[x]$ which takes a polynomial $g \in \mathbb{Z}[x]$ to the polynomial $p^{-1}x_1 \cdot g'$, where g' is the partial derivative of g with respect to x_1. We have

$$\varphi(K) \subset K(n_1 - 1, n_2 - 1, \ldots, n_r - 1) \subset K(n_1 - 1)[x_2, \ldots, x_r]$$

and

$$\varphi\big(h_1^{j_1}h_2^{j_2}\cdots h_r^{j_r}\big) = -p^{-1}j_1h_1^{j_1-1}h_2^{j_2}\cdots h_r^{j_r} + p^{-1}j_1h_1^{j_1}h_2^{j_2}\cdots h_r^{j_r}.$$

Since $bh_1^{i_1}\cdots h_r^{i_r}$ is a monomial of the lowest total degree of the polynomial f, it follows that $-bp^{-1}i_1h_1^{i_1-1}h_2^{i_2}\cdots h_r^{i_r}$ is a monomial of $\varphi(f)$ considered as a polynomial in h. As

$$\varphi(f) \in K(n_1 - 1)[x_2, \ldots, x_r]\ ,$$

we see that $-bp^{-1}i_1h_1^{i_1-1}$ is a monomial of a polynomial from $K(n_1 - 1)$. It follows that $p^{-1}i_1$ is an integer and by Lemma 2.4 below, this integer is divisible by p^{n_1-1}. Therefore $p^{n_1}|i_1$. □

Lemma 2.4. *Let g be a polynomial in h_1 lying in $K(m)$ for some $m \geq 0$. Let bh_1^{i-1} be a monomial of g such that i is divisible by p^m. Then b is divisible by p^m.*

Proof. We write h for h_1 and x for x_1. Note that $h^i \in K(m)$ since i is divisible by p^m. Moreover, the quotient ring $K(m)/(h^i)$ is additively generated by $p^{e(j)}x^j$ with $j < i$. Indeed, the polynomial $x^i - (-h)^i = x^i - (x-1)^i$ is a linear combination with integer coefficients of $p^{e(j)}x^j$ with $j < i$. Consequently, for any $k \geq 0$, multiplying by $p^{e(k)}x^k$, we see that the polynomial $p^{e(i+k)}x^{i+k} = p^{e(k)}x^{i+k}$ modulo the ideal (h^i) is a linear combination with integer coefficients of the $p^{e(j)}x^j$ with $j < i + k$.

Thus, $K(m)/(h^i)$ is additively generated by $p^{e(j)}(1-h)^j$ with $j < i$. Only the generator $p^{e(i-1)}(1-h)^{i-1} = p^m(1-h)^{i-1}$ has a nonzero h^{i-1}-coefficient and that coefficient is divisible by p^m. □

Let Y be a scheme over the field F. We write $\mathrm{CH}(Y)$ for the Chow group of Y and set $\mathrm{Ch}(Y) = \mathrm{CH}(Y)/p\,\mathrm{CH}(Y)$. We define $\mathrm{Ch}(\overline{Y})$ as the colimit of $\mathrm{Ch}(Y_L)$ where L runs over all field extensions of F. Thus for any field extension L/F, we have a canonical homomorphism $\mathrm{Ch}(Y_L) \to \mathrm{Ch}(\overline{Y})$. This homomorphism is an isomorphism if $Y = P$, the variety defined above, and L is a splitting field of P.

We define $\overline{\mathrm{Ch}}(Y)$ to be the image of the homomorphism $\mathrm{Ch}(Y) \to \mathrm{Ch}(\overline{Y})$.

Proposition 2.5. *We have* $\overline{\mathrm{Ch}}^j(P) = 0$ *for any* $j > 0$.

Proof. Let $K_0(P)$ be the Grothendieck group of P. We write $K_0(\overline{P})$ for the colimit of $K_0(P_L)$ taken over all field extensions L/F. The group $K_0(\overline{P})$ is canonically isomorphic to $K_0(P_L)$ for any splitting field L of P. Each of the groups $K_0(P)$ and $K_0(\overline{P})$ is endowed with the topological filtration. The subsequent factor groups $G^jK_0(P)$ and $G^jK_0(\overline{P})$ of these filtrations fit into the commutative square

$$\begin{array}{ccc} \mathrm{CH}^j(\overline{P}) & \longrightarrow & G^jK_0(\overline{P}) \\ \uparrow & & \uparrow \\ \mathrm{CH}^j(P) & \longrightarrow & G^jK_0(P) \end{array}$$

where the top map is an isomorphism. Therefore it suffices to show that the image of the homomorphism $G^jK_0(P) \to G^jK_0(\overline{P})$ is divisible by p for any $j > 0$.

The ring $K_0(\overline{P})$ is identified with the quotient of the polynomial ring $\mathbb{Z}[h]$ by the ideal generated by $h_1^{\mathrm{ind}\, a_1}, \dots, h_r^{\mathrm{ind}\, a_r}$. Under this identification, the element h_i is the pull-back to P of the class of a hyperplane in P_i over a splitting field and the j-th term $K_0(\overline{P})^{(j)}$ of the filtration is generated by the classes of monomials of degree at least j. The group $G^jK_0(\overline{P})$ is identified with the group of all homogeneous polynomials of degree j.

The group $K_0(P)$ is isomorphic to the direct sum of $K_0(B)$, where $B = A_1^{\otimes j_1} \otimes \cdots \otimes A_r^{\otimes j_r}$, over all j_i with $0 \le j_i < \mathrm{ind}\, a_i$ (cf. [14, § 9]). The image of the natural map $K_0(B) \to K_0(B_L) = \mathbb{Z}$, where L is a splitting field of B, is equal to $\mathrm{ind}(a_1^{j_1} \cdots a_r^{j_r})\mathbb{Z}$. The image of the homomorphism $K_0(P) \to K_0(\overline{P})$ (which is in fact an injection) is generated by

$$\mathrm{ind}\left(a_1^{j_1} \cdots a_r^{j_r}\right)(1 - h_1)^{j_1} \cdots (1 - h_r)^{j_r}$$

over all $j_1, \dots, j_r \ge 0$.

We embed $K_0(\overline{P})$ into the polynomial ring $\mathbb{Z}[x] = \mathbb{Z}[x_1, \dots, x_r]$ as a subgroup by identifying a monomial $h_1^{j_1} \cdots h_r^{j_r}$ where $0 \le j_i < \mathrm{ind}\, a_i$ with the polynomial $(1 - x_1)^{j_1} \cdots (1 - x_r)^{j_r}$. As the elements $a_1, \dots, a_r$ form a minimal basis of D, the index $\mathrm{ind}(a_1^{j_1} \cdots a_r^{j_r})$ is a power of p with the exponent at least $e(\log_p \mathrm{ind}\, a_1, \dots, \log_p \mathrm{ind}\, a_r)$. Therefore,

$$K_0(P) \subset K(\log_p \mathrm{ind}\, a_1, \dots, \log_p \mathrm{ind}\, a_r) \subset \mathbb{Z}[x].$$

An element of $K_0(P)^{(j)}$ with $j > 0$ is a polynomial f in h of degree at least j. The image of f in $G^jK_0(\overline{P})$ is the j-th homogeneous part f_j of f. As the degree of f with respect to h_i is less than $\mathrm{ind}\, a_i$, it follows from Proposition 2.3 that all the coefficients of f_j are divisible by p. $\square$

Let $d = \dim P$ and $\alpha \in \mathrm{CH}^d(P \times P)$. The *first multiplicity* $\mathrm{mult}_1(\alpha)$ *of* α is the image of α under the push-forward map $\mathrm{CH}^d(P \times P) \to \mathrm{CH}^0(P) = \mathbb{Z}$ given by the first projection $P \times P \to P$ (cf. [10]). Similarly, we define the *second multiplicity* $\mathrm{mult}_2(\alpha)$.

Corollary 2.6. *For any element* $\alpha \in \mathrm{CH}^d(P \times P)$, *we have*

$$\mathrm{mult}_1(\alpha) \equiv \mathrm{mult}_2(\alpha) \quad \textit{modulo } p.$$

Proof. We follow the proof of [9, Th. 2.1]. The homomorphism

$$f : \mathrm{CH}^d(P \times P) \to (\mathbb{Z}/p\mathbb{Z})^2,$$

taking an $\alpha \in \mathrm{CH}^d(P \times P)$ to $(\mathrm{mult}_1(\alpha), \mathrm{mult}_2(\alpha))$ modulo p, factors through the group $\overline{\mathrm{Ch}}^d(P \times P)$. Since for any i, any projection $P_i \times P_i \to P_i$ is a projective bundle, the Chow group $\overline{\mathrm{Ch}}^d(P \times P)$ is a direct some of several copies of $\overline{\mathrm{Ch}}^i(P)$ for some i's and the value $i = 0$ appears once. By Proposition 2.5, the dimension over $\mathbb{Z}/p\mathbb{Z}$ of the vector space $\overline{\mathrm{Ch}}^d(P \times P)$ is equal to 1 and consequently the dimension of the image of f is at most 1. Since the image of the diagonal class under f is $(1, 1)$, the image of f is generated by $(1, 1)$. □

Corollary 2.7. *Any rational map* $P \dashrightarrow P$ *is dominant.*

Proof. Let $\alpha \in \mathrm{CH}^d(P \times P)$ be the class of the closure of the graph of a rational map $P \dashrightarrow P$. We have $\mathrm{mult}_1(\alpha) = 1$. Therefore, by Corollary 2.6, $\mathrm{mult}_2(\alpha) \neq 0$, and it follows that the rational map is dominant. □

Corollary 2.8. $\mathrm{cdim}_p P = \mathrm{cdim}\, P = \dim P$.

Proof. As $\mathrm{cdim}_p P \leq \mathrm{cdim}\, P \leq \dim P$, it suffices to show that $\mathrm{cdim}_p P = \dim P$. Let $Z \subset P$ be a closed subvariety and $f : P' \dashrightarrow P$ and $g : P' \dashrightarrow Z$ dominant rational morphisms such that $\deg f$ is prime to p. Let α be the class in $\mathrm{CH}^d(P \times P)$ of the closure in $P \times P$ of the image of $f \times g : P' \dashrightarrow P \times Z$. As $\mathrm{mult}_1(\alpha) = \deg f$ is prime to p, by Corollary 2.6, we have $\mathrm{mult}_2(\alpha) \neq 0$, i.e., $Z = P$. By Example 1.4.2, $\mathrm{cdim}_p P = \dim P$. □

The corollary completes the proof of Theorem 2.1.

Remark 2.9. Theorem 2.1 can be generalized to the case of any finite subgroup $D \subset \mathrm{Br}(F)$ consisting of elements of p-primary orders. Let $\{a_1, a_2, \ldots, a_r\}$ be elements of D such that their images $\{a_1', a_2', \ldots, a_r'\}$ in D/D^p form a minimal basis, i.e., for any $i = 1, \ldots r$ and any element $d \in D$ with the class in D/D^p outside of the subgroup generated by $a_1', \ldots, a_{i-1}'$, the inequality $\mathrm{ind}\, d \geq \mathrm{ind}\, a_i$ holds. In particular, $\{a_1, a_2, \ldots, a_r\}$ generate D. Then, as in Theorem 2.1, we have

$$\mathrm{cdim}_p(D) = \mathrm{cdim}(D) = \Big(\sum_{i=1}^{r} \mathrm{ind}\, a_i\Big) - r.$$

Indeed, the group D and the variety $P = P_1 \times \cdots \times P_r$, where P_i for every $i = 1, \dots, r$ is the Severi–Brauer variety of a central division algebra representing the element a_i, have the same splitting fields. Therefore, $\operatorname{cdim}(D) = \operatorname{cdim}(P)$ and $\operatorname{cdim}_p(D) = \operatorname{cdim}_p(P)$. Corollaries 2.6, 2.7 and 2.8 hold for P since $K_0(P) \subset K(\log_p \operatorname{ind} a_1, \dots, \log_p \operatorname{ind} a_r)$.

Remark 2.10. One can compute the canonical p-dimension of an arbitrary finite subgroup of $D \subset \operatorname{Br}(F)$ as follows. Let D' be the Sylow p-subgroup of D. Write $D = D' \oplus D''$ for a subgroup $D'' \subset D$ and let L/F be a finite field extension of degree prime to p such that D'' is split over L. Then $D_L = D'_L$ and $\operatorname{cdim}_p(D) = \operatorname{cdim}_p(D_L) = \operatorname{cdim}_p(D'_L) = \operatorname{cdim}_p(D') = \operatorname{cdim}(D')$.

3. Essential and canonical dimension of gerbes banded by $(\boldsymbol{\mu}_p)^s$

In this section we relate the essential and canonical (p-)dimensions of gerbes banded by $(\boldsymbol{\mu}_p)^s$ where $s \geq 0$. The following statement is a generalization of [4, Th. 7.1].

Theorem 3.1. *Let p be a prime integer and $\mathcal{X}$ a gerbe banded by $(\boldsymbol{\mu}_p)^s$ over an arbitrary field F. Then*

$$\operatorname{ed}(\mathcal{X}) = \operatorname{ed}_p(\mathcal{X}) = \operatorname{cdim}_p(\mathcal{X}) + s = \operatorname{cdim}(\mathcal{X}) + s.$$

Proof. The gerbe $\mathcal{X}$ is given by an element in $H^2(F, (\boldsymbol{\mu}_p)^s) = \operatorname{Br}_p(F)^s$, i.e., by an s-tuple of central simple algebras $A_1, A_2, \dots, A_s$ with $[A_i] \in \operatorname{Br}_p(F)$. Let P be the product of the Severi–Brauer varieties $P_i := \operatorname{SB}(A_i)$ and D the subgroup of $\operatorname{Br}_p(F)$ generated by the $[A_i]$, $i = 1, \dots, s$. As the classes of splitting fields for $\mathcal{X}$, D and P coincide, we have

$$\begin{aligned}\operatorname{cdim}(\mathcal{X}) &= \operatorname{cdim}(P) = \operatorname{cdim}(D) = \operatorname{cdim}_p(D)\\ &= \operatorname{cdim}_p(P) = \operatorname{cdim}_p(\mathcal{X})\end{aligned} \tag{1}$$

by Theorem 2.1. We shall prove the inequalities $\operatorname{ed}_p(\mathcal{X}) \geq \operatorname{cdim}(P) + s \geq \operatorname{ed}(\mathcal{X})$.

Let S_i be a divisor on P_i of degree p. Let L/F be a field extension and $f_i \in L(P_i)^\times$ with $\operatorname{div}(f_i) = pH_i - (S_i)_L$, where H_i is a hyperplane in $(P_i)_L$ for $i = 1, \dots, s$. We write $\langle f_i \rangle_{i=1}^s$ for the corresponding element in $\widehat{\mathcal{X}}(L)$ (cf. Sect. 1.2).

By Example 1.4.2, there is a closed subvariety $Z \subset P$ and a rational dominant morphism $P \dashrightarrow Z$ with $\dim(Z) = \operatorname{cdim}(P) = \operatorname{cdim}_p(P)$. We view $F(Z)$ as a subfield of $F(P)$. As $P(L) \neq \emptyset$ and P is regular, there is an F-place $\gamma : F(P) \rightsquigarrow L$ (cf. [11, § 4.1]). Since Z is complete, the valuation ring of the restriction $\gamma|_{F(Z)} : F(Z) \rightsquigarrow L$ dominates a point in Z. It follows that $Z(L) \neq \emptyset$. Choose a point $y \in Z$ such that $F' := F(y) \subset L$.

Since $P(F') \neq \emptyset$, the P_i are split over F', hence $\operatorname{Pic}(P_i)_{F'} = \mathbb{Z}$ and there are functions $g_i \in F'(P_i)^\times$ with $\operatorname{div}(g_i) = pH'_i - (S_i)_{F'}$, where H'_i is a hyperplane in P_i for $i = 1, \dots, s$. As $\mathrm{Pic}(P_i)_L = \mathbb{Z}$, there are functions $h_i \in L(P_i)^\times$ with $\mathrm{div}(h_i) = (H_i')_L - H_i$. We have

$$\mathrm{div}(g_i)_L = \mathrm{div}(f_i) + \mathrm{div}\left(h_i^p\right),$$

hence

$$a_i g_i = f_i h_i^p$$

for some $a_i \in L^\times$. It follows that $\langle f_i \rangle_{i=1}^s = \langle a_i g_i \rangle_{i=1}^s$ in $\mathcal{X}(L)$, therefore $\langle f_i \rangle_{i=1}^s$ is defined over the field $F'(a_1, a_2, \dots, a_s)$. Hence

$$\mathrm{ed}\langle f_i \rangle_{i=1}^s \leq \mathrm{tr.deg}_F(F') + s \leq \dim(Z) + s = \mathrm{cdim}(P) + s,$$

and therefore $\mathrm{ed}(\mathcal{X}) \leq \mathrm{cdim}(P) + s$.

We shall prove the inequality $\mathrm{ed}_p(\mathcal{X}) \geq \mathrm{cdim}(P) + s$. As $P(F(Z)) \neq \emptyset$, there are functions $f_i \in F(Z)(P_i)^\times$ with $\mathrm{div}(f_i) = pH_i - (S_i)_{F(Z)}$, where H_i is a hyperplane in $(P_i)_{F(Z)}$. Let $L := F(Z)(t_1, t_2, \dots, t_s)$, where the t_i are variables, and consider the point $\langle t_i f_i \rangle_{i=1}^s \in \widehat{\mathcal{X}}(L)$.

We claim that $\mathrm{ed}_p\langle t_i f_i \rangle_{i=1}^s \geq \mathrm{cdim}(P) + s$. Let L' be a finite extension of L of degree prime to p and $L'' \subset L'$ a subfield such that the image of $\langle t_i f_i \rangle_{i=1}^s$ in $\widehat{\mathcal{X}}(L')$ is defined over L'', i.e., there are functions $g_i \in L''(P_i)^\times$ and $h_i \in L'(P_i)^\times$ with $t_i f_i = g_i h_i^p$. We shall show that $\mathrm{tr.deg}_F(L'') \geq \mathrm{cdim}(P) + s$.

Let $L_i := F(Z)(t_i, \dots, t_s)$ and v_i be the discrete valuation of L_i corresponding to the variable t_i for $i = 1, \dots, s$. We construct a sequence of field extensions L_i'/L_i of degree prime to p and discrete valuations v_i' of L_i' for $i = 1, \dots, s$ by induction on i as follows. Set $L_1' = L'$. Suppose the fields $L_1', \dots, L_i'$ and the valuations $v_1', \dots, v_{i-1}'$ are constructed. By Lemma 1.1, there is a valuation v_i' of L_i' with residue field L_{i+1}' extending the discrete valuation v_i of L_i' with the ramification index e_i and the degree $[L_{i+1}' : L_{i+1}]$ prime to p.

The composition v' of the discrete valuations v_i' is a valuation of L' with residue field of degree over $F(Z)$ prime to p. A choice of prime elements in all the L_i' identifies the group of values of v' with $\mathbb{Z}^s$. Moreover, for every $i = 1, \dots, s$, we have

$$v'(t_i) = e_i \varepsilon_i + \sum_{j>i} a_{ij} \varepsilon_j$$

where the ε_i's denote the standard basis elements of $\mathbb{Z}^s$ and $a_{ij} \in \mathbb{Z}$.

Write v'' for the restriction of v' on L''. Let $K = F(P)$. We extend canonically the valuations v' and v'' to valuations $\tilde{v}'$ and $\tilde{v}''$ of KL' and KL'' respectively (cf. Sect. 1.5). Note that $f_i \in K(Z)^\times$, $g_i \in (KL'')^\times$ and $h_i \in (KL')^\times$. We have

$$e_i \varepsilon_i + \sum_{j>i} a_{ij} \varepsilon_j = v'(t_i) = \tilde{v}'(t_i f_i) \equiv \tilde{v}''(g_i) \quad (mod\ p).$$

Since e_i are prime to p, the elements $\tilde{v}''(g_i)$ generate a subgroup of $\mathbb{Z}^s$ of finite index. It follows that the value group of $\tilde{v}''$ is of rank s, hence $\operatorname{rank}(v'') = \operatorname{rank}(\tilde{v}'') = s$.

Let R'' and R' be residue fields of v'' and v' respectively. We have the inclusions $R'' \subset R' \supset F(Z)$ and $[R' : F(Z)]$ is prime to p. By [20, Ch. VI, Th. 3, Cor. 1],

$$\text{(2)} \qquad \operatorname{tr.deg}_F(L'') \geq \operatorname{tr.deg}_F(R'') + \operatorname{rank}(v'') = \operatorname{tr.deg}_F(R'') + s.$$

As $P(L'') \neq \emptyset$, there is an F-place $F(P) \rightsquigarrow L''$. Composing it with the place $L'' \rightsquigarrow R''$ given by v'', we get an F-place $F(P) \rightsquigarrow R''$. As P is complete, we have $P(R'') \neq \emptyset$, i.e., R'' is a splitting field of P.

We prove that R'' is a p-generic splitting field of P. Let M be a splitting field of P. A regular system of parameters at the image of a morphism $\alpha : \operatorname{Spec} M \to P$ yields an F-place $F(P) \rightsquigarrow M$ that is a composition of places associated with discrete valuations (cf. [11, § 1.4]). By [11, Lemma 3.2] applied to the restriction of α to $F(Z)$, there is a finite field extension M' of M and an F-place $R' \rightsquigarrow M'$. Restricting to R'' we get an F-place $R'' \rightsquigarrow M'$, i.e., R'' is a p-generic splitting field of P.

By the definition of the canonical p-dimension,

$$\operatorname{cdim}(P) = \operatorname{tr.deg}_F F(Z) = \operatorname{tr.deg}_F R' \geq \operatorname{tr.deg}_F(R'') \geq \operatorname{cdim}_p(P).$$

It follows that $\operatorname{tr.deg}_F(R'') = \operatorname{cdim}(P)$ by (1) and therefore, $\operatorname{tr.deg}_F(L'') \geq \operatorname{cdim}(P) + s$ by (2). The claim is proved.

It follows from the claim that $\operatorname{ed}_p(\mathcal{X}) \geq \operatorname{cdim}(P) + s$. □

4. Main theorem

The main result of the paper is the following

Theorem 4.1. *Let G be a p-group and F a field of characteristic different from p containing a primitive p-th root of unity. Then* $\operatorname{ed}_p(G)$ *over F is equal to* $\operatorname{ed}(G)$ *over F and coincides with the least dimension of a faithful representation of G over F.*

The rest of the section is devoted to the proof of the theorem. As was mentioned in the introduction, we have $\operatorname{ed}_p(G) \leq \operatorname{ed}(G) \leq \dim(V)$ for any faithful representation V of G over F. We shall construct a faithful representation V of G over F with $\operatorname{ed}_p(G) \geq \dim(V)$.

Denote by C the subgroup of all central elements of G of exponent p and set $H = G/C$, so we have an exact sequence

$$\text{(3)} \qquad 1 \to C \to G \to H \to 1.$$

Let $E \to \operatorname{Spec} F$ be an H-torsor and $\operatorname{Spec} F \to BH$ be the corresponding morphism. Set $\mathcal{X}^E := BG \times_{BH} \operatorname{Spec} F$. Then $\mathcal{X}^E$ is a gerbe over F banded by C and its class in $H^2(F, C)$ coincides with the image of the class of E under the connecting map $H^1(F,H) \to H^2(F,C)$ (cf. [13, Ch. 4, § 2]). An object of $\mathcal{X}^E$ over a field extension L/F is a pair (E',α), where E' is a G-torsor over L and $\alpha : E'/C \xrightarrow{\sim} E_L$ is an isomorphism of H-torsors over L.

Alternatively, $\mathcal{X}^E = [E/G]$ with objects (over L) G-equivariant morphisms $E' \to E_L$, where E' is a G-torsor over L (cf. [19]).

A lower bound for $\operatorname{ed}(G)$ was established in [4, Prop. 2.20]. We give a similar bound for $\operatorname{ed}_p(G)$.

Theorem 4.2. *For any H-torsor E over F, we have* $\operatorname{ed}_p(G) \geq \operatorname{ed}_p(\mathcal{X}^E)$.

Proof. Let L/F be a field extension and $x = (E',\alpha)$ an object of $\mathcal{X}^E(L)$. Choose a field a field extension L'/L of degree prime to p and a subfield $L'' \subset L'$ over F such that $\operatorname{tr.deg}(L'') = \operatorname{ed}_p(E')$ and there is a G-torsor E'' over L'' with $E''_{L'} \simeq E'_{L'}$.

We shall write Z for the (zero-dimensional) scheme of isomorphisms $\operatorname{Iso}_{L''}(E''/C, E_{L''})$ of H-torsors over L''. The image of the morphism $\operatorname{Spec} L' \to Z$ over L'' representing the isomorphism $\alpha_{L'}$ is a one point set $\{z\}$ of Z. The field extension $L''(z)/L''$ is algebraic since $\dim Z = 0$.

The isomorphism $\alpha_{L'}$ descends to an isomorphism of the H-torsors E''/C and E over $L''(z)$. Hence the isomorphism class of $x_{L'}$ belongs to the image of the map $\widehat{\mathcal{X}}^E(L''(z)) \to \widehat{\mathcal{X}}^E(L')$. Therefore,

$$\operatorname{ed}_p(G) \geq \operatorname{ed}_p(E') = \operatorname{tr.deg}(L'') = \operatorname{tr.deg}(L''(z)) \geq \operatorname{ed}_p(x).$$

It follows that $\operatorname{ed}_p(G) \geq \operatorname{ed}_p(\mathcal{X}^E)$. $\square$

Let $C^* := \operatorname{Hom}(C, \mathbf{G}_{\mathrm{m}})$ denote the character group of C. An H-torsor E over F yields a homomorphism

$$\beta^E : C^* \to \operatorname{Br}(F)$$

taking a character $\chi : C \to \mathbf{G}_{\mathrm{m}}$ to the image of the class of E under the composition

$$H^1(F,H) \xrightarrow{\partial} H^2(F,C) \xrightarrow{\chi_*} H^2(F,\mathbf{G}_{\mathrm{m}}) = \operatorname{Br}(F),$$

where ∂ is the connecting map for the exact sequence (3). Note that as $\mu_p \subset F^\times$, the intersection of $\operatorname{Ker}(\chi_*)$ over all characters $\chi \in C^*$ is trivial. It follows that the classes of splitting fields of the gerbe $\mathcal{X}^E$ and the subgroup $\operatorname{Im}(\beta^E)$ coincide. It follows that

$$\operatorname{cdim}_p(\mathcal{X}^E) = \operatorname{cdim}_p(\operatorname{Im}(\beta^E)). \tag{4}$$

Let $\chi_1, \chi_2, \dots, \chi_s$ be a basis of C^* over $\mathbb{Z}/p\mathbb{Z}$ such that $\{\beta^E(\chi_1), \dots, \beta^E(\chi_r)\}$ is a minimal basis of $\operatorname{Im}(\beta^E)$ for some r and $\beta^E(\chi_i) = 1$ for $i > r$. By Theorem 2.1, we have

$$\operatorname{cdim}_p(\operatorname{Im}(\beta^E)) = \Big(\sum_{i=1}^{r} \operatorname{ind} \beta^E(\chi_i)\Big) - r = \Big(\sum_{i=1}^{s} \operatorname{ind} \beta^E(\chi_i)\Big) - s. \tag{5}$$

In view of (4) and Theorems 3.1 and 4.2, we shall find an H-torsor E (over a field extension of F) so that the integer in (5) is as large as possible. Let U be a faithful representation of H and X an open subset of the affine space $\mathbb{A}(U)$ of U where H acts freely. Set $Y := X/H$. Let E be the generic fiber of the H-torsor $\pi : X \to Y$. It is a "generic" H-torsor over the function field $L := F(Y)$.

Let $\chi : C \to \mathbf{G}_{\mathrm{m}}$ be a character and $\mathrm{Rep}^{(\chi)}(G)$ the category of all finite dimensional representations ρ of G such that $\rho(c)$ is multiplication by $\chi(c)$ for any $c \in C$. Fix a representations $\rho : G \to \mathbf{GL}(W)$ in $\mathrm{Rep}^{(\chi)}(G)$. The conjugation action of G on $B := \mathrm{End}(W)$ factors through an H-action. By descent (cf. [13, Ch. 1, § 2]), there is (a unique up to canonical isomorphism) Azumaya algebra $\mathcal{A}$ over Y and an H-equivariant algebra isomorphism $\pi^*(\mathcal{A}) \simeq B_X := B \times X$. Let A be the generic fiber of $\mathcal{A}$; it is a central simple algebra over $L = F(Y)$.

Consider the homomorphism $\beta^E : C^* \to \mathrm{Br}(L)$.

Lemma 4.3. *The class of A in* $\mathrm{Br}(L)$ *coincides with* $\beta^E(\chi)$.

Proof. Consider the commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & C \arrow[r] \arrow[d, "\chi"'] & G \arrow[r] \arrow[d, "\rho"'] & H \arrow[r] \arrow[d, "\alpha"'] & 1 \\ 1 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] & \mathbf{GL}(W) \arrow[r] & \mathbf{PGL}(W) \arrow[r] & 1 \end{tikzcd}$$

The image of the H-torsor $\pi : X \to Y$ under α is the $\mathbf{PGL}(W)$-torsor

$$E' := \mathbf{PGL}(W)_X/H \to Y$$

where $\mathbf{PGL}(W)_X := \mathbf{PGL}(W) \times X$ and H acts on $\mathbf{PGL}(W)_X$ by $h(a, x) = (ah^{-1}, hx)$. The conjugation action of $\mathbf{PGL}(W)$ on B gives rise to an isomorphism between $\mathbf{PGL}(W)_X$ and the H-torsor $\mathrm{Iso}_X(B_X, \mathrm{End}(W)_X)$ of isomorphisms between the (split) Azumaya $\mathcal{O}_X$-algebras B_X and $\mathrm{End}(W)_X$. Note that this isomorphism is H-equivariant if H acts by conjugation on B_X and trivially on $\mathrm{End}(W)_X$. By descent,

$$E' \simeq \mathrm{Iso}_Y(\mathcal{A}, \mathrm{End}(W)_Y).$$

Therefore, the image of the class of the torsor $E' \to Y$ under the connecting map for the bottom row of the diagram coincides with the class of the Azumaya algebra $\mathcal{A}$. Restricting to the generic fiber yields $[A] = \beta^E(\chi)$. $\square$

Theorem 4.4. *For any character $\chi \in C^*$, we have* $\mathrm{ind}\, \beta^E(\chi) = \min \dim(V)$ *over all representations V in* $\mathrm{Rep}^{(\chi)}(G)$.

Proof. We follow the approach given in [12]. Let H act on a scheme Z over F. We also view Z as a G-scheme. Denote by $\mathcal{M}(G, Z)$ the (abelian) category of left G-modules on Z that are coherent $\mathcal{O}_Z$-modules (cf. [18, § 1.2]). In particular, $\mathcal{M}(G, \operatorname{Spec} F) = \operatorname{Rep}(G)$, the category off all finite dimensional representations of G.

Note that C acts trivially on Z. For a character $\chi : C \to \mathbf{G}_{\mathrm{m}}$, let $\mathcal{M}^{(\chi)}(G, Z)$ be the full subcategory of $\mathcal{M}(G, Z)$ consisting of G-modules on which C acts via χ. For example, $\mathcal{M}^{(\chi)}(G, \operatorname{Spec} F) = \operatorname{Rep}^{(\chi)}(G)$.

We write $K_0(G, Z)$ and $K_0^{(\chi)}(G, Z)$ for the Grothendieck groups of $\mathcal{M}(G, Z)$ and $\mathcal{M}^{(\chi)}(G, Z)$ respectively.

Every M in $\mathcal{M}(G, Z)$ is a direct sum of unique submodules $M^{(\chi)}$ of M in $\mathcal{M}^{(\chi)}(G, Z)$ over all characters χ of C. It follows that

$$K_0(G, Z) = \coprod K_0^{(\chi)}(G, Z).$$

Let q be the order of G. By [17, Th. 24], every irreducible representation of G is defined over the field $F(\mu_q)$. Since F contains p-th roots of unity, the degree $[F(\mu_q) : F]$ is a power of p. Hence the dimension of any irreducible representation of G over F is a power of p. It follows by Lemma 4.3 that it suffices to show $\operatorname{ind}(A) = \gcd \dim(V)$ over all representations V in $\operatorname{Rep}^{(\chi)}(G)$.

The image of the map $\dim : K_0(A) \to \mathbb{Z}$ given by the dimension over L is equal to $\operatorname{ind}(A) \cdot \dim(W) \cdot \mathbb{Z}$. To finish the proof of the theorem it suffices to construct a surjective homomorphism

$$K_0(\operatorname{Rep}^{(\chi)}(G)) \to K_0(A) \tag{6}$$

such that the composition $K_0(\operatorname{Rep}^{(\chi)}(G)) \to K_0(A) \xrightarrow{\dim} \mathbb{Z}$ is given by the dimension times $\dim(W)$.

First of all we have

$$K_0(\operatorname{Rep}^{(\chi)}(G)) \simeq K_0^{(\chi)}(G, \operatorname{Spec} F). \tag{7}$$

Recall that X an open subset of $\mathbb{A}(U)$ where H acts freely. By homotopy invariance in the equivariant K-theory [18, Cor. 4.2],

$$K_0(G, \operatorname{Spec} F) \simeq K_0(G, \mathbb{A}(U)).$$

It follows that

$$K_0^{(\chi)}(G, \operatorname{Spec} F) \simeq K_0^{(\chi)}(G, \mathbb{A}(U)). \tag{8}$$

By localization [18, Th. 2.7], the restriction homomorphism

$$K_0^{(\chi)}(G, \mathbb{A}(U)) \to K_0^{(\chi)}(G, X). \tag{9}$$

is surjective.

Denote by $\mathcal{M}^{(1)}(G, X, B_X)$ the category of left G-modules M on X that are coherent $\mathcal{O}_X$-modules and right B_X-modules such that C acts trivially on M and the G-action on M and the conjugation G-action on B_X agree.

The corresponding Grothendieck group is denoted by $K_0^{(1)}(G, X, B_X)$. For any object L in $\mathcal{M}^{(\chi)}(G, X)$, the group C acts trivially on $L \otimes_F W^*$ and B acts on the right on $L \otimes_F W^*$. We have Morita equivalence

$$\mathcal{M}^{(\chi)}(G, X) \xrightarrow{\sim} \mathcal{M}^{(1)}(G, X, B_X)$$

given by $L \mapsto L \otimes_F W^*$ (with the inverse functor $M \mapsto M \otimes_B W$). Hence

$$K_0^{(\chi)}(G, X) \simeq K_0^{(1)}(G, X, B_X). \tag{10}$$

Now, as C acts trivially on X and B_X, the category $\mathcal{M}^{(1)}(G, X, B_X)$ is equivalent to the category $\mathcal{M}(H, X, B_X)$ of left H-modules M on X that are coherent $\mathcal{O}_X$-modules and right B_X-modules such that the G-action on M and the conjugation G-action on B_X agree. Hence

$$K_0^{(1)}(G, X, B_X) \simeq K_0(H, X, B_X). \tag{11}$$

Recall that $Y = X/H$. By descent, the category $\mathcal{M}(H, X, B_X)$ is equivalent to the category $\mathcal{M}(Y, \mathcal{A})$ of coherent $\mathcal{O}_Y$-modules that are right $\mathcal{A}$-modules. Hence

$$K_0(H, X, B_X) \simeq K_0(Y, \mathcal{A}). \tag{12}$$

The restriction to the generic point of Y gives a surjective homomorphism

$$K_0(Y, \mathcal{A}) \to K_0(A). \tag{13}$$

The homomorphism (6) is the composition of (7), (8), (9), (10), (11), (12) and (13). It takes the class of a representation V to the class in $K_0(A)$ of the generic fiber of the vector bundle $((V \otimes W^*) \times X)/H$ over Y of rank $\dim(V) \cdot \dim(W)$. □

Remark 4.5. The theorem holds with min replaced by the gcd (with the same proof) in a more general context when the sequence (3) is an arbitrary exact sequence of algebraic groups with C a central diagonalizable subgroup of G.

Example 4.6 (cf. [6], [4, § 14], [16, Th. 7.3.8]). Let p be a prime integer, F be a field of characteristic different from p and C_m the cyclic group $\mathbb{Z}/p^m\mathbb{Z}$. Let $K = F(t_1, \dots, t_{p^m})$ and C_m act on the variables $t_1, \dots, t_{p^m}$ by cyclic permutations. Then K is a Galois C_m-algebra over K^{C_m}. Assume that F contains a primitive root of unity ξ_{p^k} for some k. The image of the class of K under the connecting map $H^1(F, C_m) \to H^2(F, C_k) \simeq \mathrm{Br}_{p^k}(F)$ for the exact sequence

$$1 \to C_k \to C_n \to C_m \to 1,$$

where $n = k + m$, is the class of the cyclic algebra $A = (K/K^{C_m}, \xi_{p^k})$. The group C_n acts F-linearly on $F(\xi_{p^n})$ by multiplication by roots of unity making the F-space $F(\xi_{p^n})$ a faithful representation of C_n of the smallest dimension. By Theorem 4.4 and Remark 4.5, we have

$$\mathrm{ind}(A) = [F(\xi_{p^n}) : F].$$

We can now complete the proof of Theorem 4.1. By Theorem 4.4, there are representations V_i in $\mathrm{Rep}^{(\chi_i)}(G)$ such that $\operatorname{ind}\beta^E(\chi_i) = \dim(V_i)$, $i = 1, \dots, s$. Let V be the direct sum of all the V_i. By Theorem 4.2 (applied to the group G over L and the generic torsor E), Theorem 3.1, (4) and (5), we have

$$\mathrm{ed}_p(G) \geq \mathrm{ed}_p(G_L) \geq \mathrm{ed}_p(\mathcal{X}^E) = \mathrm{cdim}_p(\mathcal{X}^E) + s = \mathrm{cdim}_p(\mathrm{Im}(\beta^E)) + s$$
$$= \sum_{i=1}^{s} \operatorname{ind}\beta^E(\chi_i) = \sum_{i=1}^{s} \dim(V_i) = \dim(V).$$

Since $\chi_1, \chi_2, \dots, \chi_s$ generate C^*, the restriction of V on C is faithful. As every nontrivial normal subgroup of G intersects C nontrivially, the G-representation V is faithful. We have constructed a faithful representation V of G over F with $\mathrm{ed}_p(G) \geq \dim(V)$. The theorem is proved.

Remark 4.7. The proof of Theorem 4.1 shows how to compute the essential dimension of G over F. For every character $\chi \in C^*$ choose a representation $V_\chi \in \mathrm{Rep}^{(\chi)}(G)$ of the smallest dimension. It appears as an irreducible component of the smallest dimension of the induced representation $\mathrm{Ind}_C^G(\chi)$. We construct a basis $\chi_1, \dots, \chi_s$ of C^* by induction as follows. Let χ_1 be a nonzero character with the smallest $\dim(V_{\chi_1})$. If the characters $\chi_1, \dots, \chi_{i-1}$ are already constructed for some $i \leq s$, then we take for χ_i a character with minimal $\dim(V_{\chi_i})$ among all the characters outside of the subgroup generated by $\chi_1, \dots, \chi_{i-1}$. Then V is a faithful representation of the least dimension and $\mathrm{ed}(G) = \sum_{i=1}^{s} \dim(V_{\chi_i})$.

Remark 4.8. We can compute the essential p-dimension of an arbitrary finite group G over a field F of characteristic different from p. (We don't assume that F contains p-th roots of unity.) Let G' be a Sylow p-subgroup of G. One can prove that $\mathrm{ed}_p(G) = \mathrm{ed}_p(G')$ and $\mathrm{ed}_p(G')$ does not change under field extensions of degree prime to p. In particular $\mathrm{ed}_p(G') = \mathrm{ed}_p(G'_{F'})$ where $F' = F(\mu_p)$. It follows from Theorem 4.1 that $\mathrm{ed}_p(G)$ coincides with the least dimension of a faithful representation of G' over F'.

5. An application

Theorem 5.1. *Let G_1 and G_2 be two p-groups and F a field of characteristic different from p containing a primitive p-th root of unity. Then*

$$\mathrm{ed}(G_1 \times G_2) = \mathrm{ed}(G_1) + \mathrm{ed}(G_2).$$

Proof. The index j in the proof takes the values 1 and 2. If V_j is a faithful representation of G_j then $V_1 \oplus V_2$ is a faithful representation of $G_1 \times G_2$. Hence $\mathrm{ed}(G_1 \times G_2) \leq \mathrm{ed}(G_1) + \mathrm{ed}(G_2)$ (cf. [5, Lemma 4.1(b)]).

Denote by C_j the subgroup of all central elements of G_j of exponent p. Set $C = C_1 \times C_2$. We identify C^* with $C_1^* \oplus C_2^*$.

For every character $\chi \in C^*$ choose a representation $\rho_\chi : G_1 \times G_2 \to \mathbf{GL}(V_\chi)$ in $\mathrm{Rep}^{(\chi)}(G_1 \times G_2)$ of the smallest dimension. We construct a basis $\{\chi_1, \chi_2, \dots, \chi_s\}$ of C^* following Remark 4.7. We claim that all the χ_i can be chosen in one of the C_j^*. Indeed, suppose the characters $\chi_1, \dots, \chi_{i-1}$ are already constructed, and let χ_i be a character with minimal $\dim(V_{\chi_i})$ among the characters outside of the subgroup generated by $\chi_1, \dots, \chi_{i-1}$. Let $\chi_i = \chi_i^{(1)} + \chi_i^{(2)}$ with $\chi_i^{(j)} \in C_j^*$. Denote by ε_1 and ε_2 the endomorphisms of $G_1 \times G_2$ taking (g_1, g_2) to $(g_1, 1)$ and $(1, g_2)$ respectively. The restriction of the representation $\rho_{\chi_i} \circ \varepsilon_j$ on C is given by the character $\chi_i^{(j)}$. We replace χ_i by $\chi_i^{(j)}$ with j such that $\chi_i^{(j)}$ does not belong to the subgroup generated by $\chi_1, \dots, \chi_{i-1}$. The claim is proved.

Let W_j be the direct sum of all the V_{χ_i} with $\chi_i \in C_j^*$. Then the restriction of W_j on C_j is faithful, hence so is the restriction of W_j on G_j. It follows that $\mathrm{ed}(G_j) \le \dim(W_j)$. As $W_1 \oplus W_2 = V$, we have

$$\mathrm{ed}(G_1) + \mathrm{ed}(G_2) \le \dim(W_1) + \dim(W_2) = \dim(V) = \mathrm{ed}(G_1 \times G_2). \qquad \square$$

Corollary 5.2. *Let F be a field as in Theorem 5.1. Then*

$$\mathrm{ed}(\mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_s}\mathbb{Z}) = \sum_{i=1}^{s} [F(\xi_{p^{n_i}}) : F].$$

Proof. By Theorem 5.1, it suffices to consider the case $s = 1$. This case has been done in [6]. It is also covered by Theorem 4.1 as the natural representation of the group $\mathbb{Z}/p^n\mathbb{Z}$ in the F-space $F(\xi_{p^n})$ is faithful irreducible of the smallest dimension (cf. Remark 4.6). $\square$

References

1. Artin, M.: Brauer–Severi varieties (Notes by A. Verschoren). In: van Oystaeyen, F.M.J., Verschoren, A.H.M.J. (eds.) Brauer Groups in Ring Theory and Algebraic Geometry (Wilrijk, 1981). Lect. Notes Math., vol. 917, pp. 194–210. Springer, Berlin (1982)
2. Berhuy, G., Favi, G.: Essential dimension: a functorial point of view (after A. Merkurjev). Doc. Math. **8**, 279–330 (2003) (electronic)
3. Berhuy, G., Reichstein, Z.: On the notion of canonical dimension for algebraic groups. Adv. Math. **198**(1), 128–171 (2005)
4. Brosnan, P., Reichstein, Z., Vistoli, A.: Essential dimension and algebraic stacks. LAGRS preprint server, http://www.math.uni-bielefeld.de/lag/ (2007)
5. Buhler, J., Reichstein, Z.: On the essential dimension of a finite group. Compos. Math. **106**(2), 159–179 (1997)
6. Florence, M.: On the essential dimension of cyclic p-groups. Invent. Math. **171**, 175–189 (2008)
7. Giraud, J.: Cohomologie non abélienne. Grundlehren Math. Wiss., vol. 179. Springer, Berlin (1971)

8. Karpenko, N.A.: Grothendieck Chow motives of Severi–Brauer varieties (Russian). Algebra Anal. **7**(4), 196–213 (1995) (transl. in St. Petersbg. Math. J. **7**(4), 649–661 (1996))
9. Karpenko, N.A.: On anisotropy of orthogonal involutions. J. Ramanujan Math. Soc. **15**(1), 1–22 (2000)
10. Karpenko, N.A., Merkurjev, A.S.: Essential dimension of quadrics. Invent. Math. **153**(2), 361–372 (2003)
11. Karpenko, N.A., Merkurjev, A.S.: Canonical p-dimension of algebraic groups. Adv. Math. **205**(2), 410–433 (2006)
12. Merkurjev, A.S.: Maximal indices of Tits algebras. Doc. Math. **1**(12), 229–243 (1996) (electronic)
13. Milne, J.S.: Étale Cohomology. Princeton University Press, Princeton, N.J. (1980)
14. Quillen, D.: Higher Algebraic K-Theory, I. Lect. Notes Math., vol. 341, pp. 85–147. Springer, Berlin (1973)
15. Reichstein, Z., Youssin, B.: Essential dimensions of algebraic groups and a resolution theorem for G-varieties. Canad. J. Math. **52**(5), 1018–1056 (2000) (With an appendix by J. Kollár and E. Szabó)
16. Rowen, L.H.: Ring Theory, vol. II. Pure Appl. Math., vol. 128. Academic Press, Boston, MA (1988)
17. Serre, J.-P.: Linear Representations of Finite Groups. Grad. Texts Math., vol. 42. Springer, New York (1977) (Transl. from the 2nd French edn. by L.L. Scott)
18. Thomason, R.W.: Algebraic K-theory of group scheme actions. In: Algebraic Topology and Algebraic K-theory (Princeton, N.J., 1983). Ann. Math. Stud., vol. 113, pp. 539–563. Princeton Univ. Press, Princeton, NJ (1987)
19. Vistoli, A.: Intersection theory on algebraic stacks and on their moduli spaces. Invent. Math. **97**(3), 613–670 (1989)
20. Zariski, O., Samuel, P.: Commutative Algebra, vol. II. Grad. Texts Math. vol. 29. Springer, New York (1975) (Reprint of the 1960 edn.)