ESSENTIAL DIMENSION OF FINITE p-GROUPS, MINI COURSE, LENS 2008

ALEXANDER S. MERKURJEV

We give a detailed proof of Theorem 5.1 below.

1. A lower bound for $\operatorname{ed}_p(G)$

Theorem 1.1. (cf. [1]) *Let $f : G \to H$ be a homomorphism of algebraic groups. Then for any H-torsor E over F, we have* $\operatorname{ed}_p(G) \geq \operatorname{ed}_p(E/G) - \dim(H)$.

Proof. Let L/F be a field extension and $x = (E', \alpha)$ an object of $(E/G)(L)$. Choose 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 scheme of isomorphisms $\operatorname{Iso}_{L''}\big(f_*(E''), E_{L''}\big)$ of H-torsors over L''. Clearly, Z is an H-torsor, so $\dim(Z) = \dim(H)$. 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, hence

$$\operatorname{tr.deg}\big(L''(z)\big) \leq \operatorname{tr.deg}(L'') + \dim(Z) = \operatorname{tr.deg}(L'') + \dim(H).$$

The isomorphism $\alpha_{L'}$ descends to an isomorphism of the H-torsors $f_*(E'')$ and E over $L''(z)$. Hence the isomorphism class of $x_{L'}$ belongs to the image of the map of sets of isomorphism classes induced by the functor $(E/G)\big(L''(z)\big) \to (E/G)(L')$. Therefore,

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

It follows that $\operatorname{ed}_p(G) \geq \operatorname{ed}_p(E/G) - \dim(H)$. $\square$

2. Algebras and representations

2.1. **Twisting.** Let G be an algebraic group, $E \to \operatorname{Spec} F$ a (right) G-torsor and X_0 be an "algebraic object" over F (variety, vector space, algebra etc). Assume that the automorphism group $\operatorname{Aut}(X_0)$ has a structure of an algebraic group over F and we are given a homomorphism of algebraic groups $G \to \operatorname{Aut}(X_0)$, i.e., G acts algebraically on X_0. We shall write $E \times_G X_0$ for the *twist of X_0 by E* that can be thought of either as the "factor object" of the "product" $E \times_G X_0$ by G (i.e., we identify "points" (eg, x) and (e, gx)), or the twisted form of X_0 given by the image of the class of E under the map

$$H^1(F, G) \to H^1\big(F, \operatorname{Aut}(X_0)\big).$$

Date: June, 2008.

Assume in addition that $G = \mathrm{Aut}(X_0)$. Then the map above is a bijection, so a twisted form X of X determines the G-torsor E via the formula $E := \mathrm{Iso}(X_0, X)$.

Example 2.1. Let $X_0 = \mathrm{End}(V)$ be the endomorphism algebra of a vector space V of dimension n over F. Then $\mathbf{PGL}(V)$. A twisted form of X_0 is a central simple algebra A of degree n over F. The corresponding G-torsor is $E = \mathrm{Iso}\big(\mathrm{End}(V), A\big)$. Conversely, if E is a $\mathbf{PGL}(V)$-torsor, then A is reconstructed from E as follows: $A = E \times_{\mathbf{PGL}(V)} \mathrm{End}(V)$.

2.2. **The map β^E.** Let

$$1 \to C \to G \to H \to 1 \tag{1}$$

be a central extension of algebraic groups over F and E an H-torsor over F. Consider the homomorphism

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

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

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

where ∂ is the connecting map for the exact sequence (1).

Consider the exact sequence (1). Let $V \in \mathrm{Rep}^{(\chi)}(G)$ for a character $\chi \in C^*$. As C is central in G, it acts trivially on $\mathrm{End}(V)$, so the G-action on $\mathrm{End}(V)$ boils down to an H-action.

We'd like to compute β^E.

Lemma 2.2. *Let $\chi \in C^*$ be a character and $V \in \mathrm{Rep}^{(\chi)}(G)$. Then the class $\beta^E(\chi)$ in $\mathrm{Br}(F)$ is represented by the central simple F-algebra $E \times_H \mathrm{End}(V)$.*

Proof. Consider the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\
 & & \chi\big\downarrow & & \big\downarrow & & \rho\big\downarrow & & \\
1 & \longrightarrow & \mathbf{G}_\mathrm{m} & \longrightarrow & \mathbf{GL}(V) & \longrightarrow & \mathbf{PGL}(V) & \longrightarrow & 1
\end{array}$$

The class $\beta^E(\chi)$ is equal to the image of $\rho^*(E)$ under the connecting map

$$\delta : H^1(F, \mathbf{PGL}(V)) \to H^2(F, \mathbf{G}_\mathrm{m}) = \mathrm{Br}(F).$$

Note that $H^1(F, \mathbf{PGL}(V))$ classifies both $\mathbf{PGL}(V)$-torsors and central simple F-algebras of degree $\dim(V)$, so that δ takes a central simple algebra to its class in $\mathrm{Br}(F)$.

The $\mathbf{PGL}(V)$-torsor $\rho^*(E)$ is equal to $E \times_H \mathbf{PGL}(V)$ and the corresponding algebra is

$$A = \big(E \times_H \mathbf{PGL}(V)\big) \times_{\mathbf{PGL}(V)} \mathrm{End}(V) = E \times_H \mathrm{End}(V). \qquad \square$$

2.3. **Generic H-torsor.** Let

$$1 \to C \to G \to H \to 1$$

be an exact sequence of finite groups. Let W be a faithful representation of H and W' an open subset of the affine space of W where H acts freely. Set $Y := W'/H$. Let E be the generic fiber of the H-torsor $\pi : W' \to Y$. 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 $c \in C$.

Theorem 2.3. *Let E be a generic H-torsor. Then for any character $\chi \in C^*$, we have* $\operatorname{ind} \beta^E(\chi) = \gcd \dim(V)$ *over all representations V in* $\mathrm{Rep}^{(\chi)}(G)$.

2.4. **Galois G-algebras.** Let S be a commutative ring and H a finite group acting on S by ring automorphisms $s \mapsto s^h$. Set

$$R := S^H := \{s \in S \quad \text{such that} \quad s^h = s \quad \text{for all} \quad h \in H\}$$

and denote by $S*H$ the crossed product with trivial factors. Namely, $S*H$ consists of formal sums $\sum_{h\in H} hs_h$ with $s_h \in S$. The product is given by the rule $(hs)(h's') = (hh')(s^{h'}s')$.

Let M be a right S-module. Suppose that H acts on M on the right such that $(ms)^h = m^h s^h$. Then M is a right $S{*}H$-module by $m(hs) = m^h s$. Conversely, a right $S{*}H$-module is a right S-module together with a right H-action as above. If M is a right $S{*}H$-module then the subset M^H of H-invariant elements in M is an R-module. We have a natural S-module homomorphism $M^H \otimes_R S \to M$, $m \otimes s \mapsto ms$.

We say that S is an *H-Galois algebra over R* is the morphism $\operatorname{Spec} S \to \operatorname{Spec} R$ is an H-torsor.

Proposition 2.4. [2] *The following are equivalent:*

1. *S is an H-Galois algebra over R.*
2. *The morphism* $\operatorname{Spec} S \to \operatorname{Spec} R$ *is a H-torsor.*
3. *For any $h \in H$, $h \neq 1$, the elements $s^h - s$ with $s \in S$ generate the unit ideal in S.*
4. *For every right $S*H$-module M, the natural map $M^H \otimes_R S \to M$ is an isomorphism.*

Corollary 2.5. *Let S be an H-Galois algebra over R. Then the functors between the categories of finitely generated right modules*

$$\mathsf{M}(R) \to \mathsf{M}(S*H) \qquad N \mapsto N \otimes_R S$$

$$\mathsf{M}(S*H) \to \mathsf{M}(R), \qquad M \mapsto M^H$$

are equivalences inverse to each other.

Remark 2.6. If H is a finite group then $E = \operatorname{Spec}(K)$ for a Galois H-algebra K and $E \times_H \operatorname{End}(V) = \big(K \otimes_F \operatorname{End}(V)\big)^H$ for a space $V \in \mathrm{Rep}^{(\chi)}(G)$.

2.5. **Proof of Theorem 2.3.** Let

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

be an exact sequence of finite groups with C in the center of G. Choose a finite dimensional H-space W such that there is a vector $w \in W$ satisfying $w^h \neq w$ for all $h \in H$, $h \neq 1$. (For example, one can take for W the space of the group algebra FH and $w = 1$.) Let S denote the symmetric algebra of W. The group H acts on S and set $R = S^H$. We have $Y = \operatorname{Spec}(R)$ and $L = F(R)$ the quotient field of R.

Set

$$r = \prod_{h \neq h'} (w^h - w^{h'}).$$

We have $r \in R$ and $r \neq 0$. By Proposition 2.4(3), the localization S_r is an H-Galois algebra over R_r.

Let $\chi : C \to F^\times$ be a character of C. Note that G acts upon S via the group homomorphism $G \to H$, so we have the ring $S{*}G$ is defined. We write $\mathsf{M}^{(\chi)}(S{*}G)$ for the full subcategory of $\mathsf{M}(S{*}G)$ consisting of all modules M satisfying $m^g = \chi(g)m$ for all $m \in M$ and $g \in C$. We also write $K^{(\chi)}(S{*}G)$ for the Grothendieck group of $\mathsf{M}^{(\chi)}(S{*}G)$.

Set $\operatorname{Rep}^{(\chi)}(G) = \mathsf{M}^{(\chi)}(FG)$. Let $V \in \operatorname{Rep}^{(\chi)}(G)$. The natural G-action of G on $\operatorname{End}_F(V)$ factors through an H-action. Set $V_{S_r} = V \otimes_F S_r$. We have

$$\operatorname{End}(V) \otimes_F S_r \simeq \operatorname{End}_{S_r}\big(V_{S_r}\big).$$

Consider the following algebra over R_r:

$$\mathcal{A} = \operatorname{End}_{S_r}\big(V_{S_r}\big)^H.$$

By Proposition 2.4(4),

$$\mathcal{A} \otimes_{R_r} S_r \simeq \operatorname{End}_{S_r}\big(V_{S_r}\big),$$

hence $\mathcal{A}$ is an Azumaya R_r-algebra (by descent as S_r is a faithfully flat R_r-algebra).

Recall that $L = F(R)$ is the quotient field of R. Set

$$A = \mathcal{A} \otimes_{R_r} F(R). \tag{3}$$

Clearly, A is a central simple algebra over $F(R)$ of degree $\dim V$. We also have

$$A = \big(\operatorname{End}(V) \otimes_F F(S)\big)^H,$$

where $F(S)$ is the quotient field of S. By Lemma 2.2, $[A] = \beta^E(\chi)$ in $\operatorname{Br}(L)$.

The localization provides a surjective homomorphism

$$K(\mathcal{A}) \to K(A). \tag{4}$$

By Corollary 2.5, the category of right $\mathcal{A}$-modules and right $\operatorname{End}_{S_r}\big(V_{S_r}\big){*}H$-modules are equivalent. Thus the functor $M \mapsto M^H$ induces an isomorphism

$$K\big(\operatorname{End}_{S_r}(V_{S_r}){*}H\big) \xrightarrow{\sim} K(\mathcal{A}). \tag{5}$$

The category of right $\mathrm{End}_{S_r}\big(V_{S_r}\big)*H$-modules is equivalent to the subcategory of right $\mathrm{End}_{S_r}\big(V_{S_r}\big)*G$-modules with C acting trivially. Hence we have an isomorphism

$$K^{(1)}\big(\mathrm{End}_{S_r}(V_{S_r})*G\big) \xrightarrow{\sim} K\big(\mathrm{End}_{S_r}(V_{S_r})*H\big). \tag{6}$$

By Morita equivalence, the functors

$$\mathsf{M}(S_r*G) \to \mathsf{M}\big(\mathrm{End}_{S_r}(V_{S_r})*G\big), \qquad N \mapsto N \otimes_F V^*$$

$$\mathsf{M}\big(\mathrm{End}_{S_r}(V_{S_r})*G\big) \to \mathsf{M}(S_r*G), \qquad M \mapsto M \otimes_{\mathrm{End}(F)} V$$

are equivalences inverse to each other. Moreover, under these equivalences, the subcategory $\mathsf{M}^{(\chi)}(S_r*G)$ corresponds to $\mathsf{M}^{(1)}\big(\mathrm{End}_{S_r}(V_{S_r})*G\big)$. Hence we get an isomorphism

$$K^{(\chi)}\big(S_r*G\big) \xrightarrow{\sim} K^{(1)}\big(\mathrm{End}_{S_r}(V_{S_r})*G\big). \tag{7}$$

By localization, we have a surjection

$$K^{(\chi)}\big(S*G\big) \to K^{(\chi)}\big(S_r*G\big). \tag{8}$$

We will be using

Theorem 2.7. [5, Th. 7] *Let $B = B_0 \oplus B_1 \oplus \dots$ be a graded Noetherian ring. Suppose*

1. *B is flat as a left B_0-module,*
2. *B_0 is of finite Tor-dimension as a left B-module.*

Then the exact functor $\mathsf{M}(B_0) \to \mathsf{M}(B)$ taking an S to $S \otimes_{B_0} B$ yields an isomorphism

$$K(B_0) \xrightarrow{\sim} K(B).$$

Example 2.8. Let H be finite group and $W \in \mathrm{Rep}(H)$ over a field F. The (polynomial) ring $S := \mathsf{S}(W)$ is graded with the zero component F. Let

$$B := \mathsf{S}(W)*H.$$

We view B as a graded ring with $B_0 = F*H = FH$ (the group algebra). We claim that B satisfies the conditions of Theorem 2.7. Note that B_i is a free left B_0-module for every i. It is known that the global dimension of the ring S is finite. Choose a finite projective resolution $P^\bullet \to F$ of S-modules. As B is a free right S-module, $B \otimes_S P^\bullet \to B \otimes_S F$ is a finite projective resolution of $B \otimes_S F = FH = B_0$. Hence B_0 is of finite Tor-dimension as a left B-module.

Finally, by Theorem 2.7 and Example 2.8, we have an isomorphism

$$K\big(\mathrm{Rep}^{(\chi)}(G)\big) = K^{(\chi)}(FG) \xrightarrow{\sim} K^{(\chi)}\big(S*G\big). \tag{9}$$

The surjective composition $K\big(\mathrm{Rep}^{(\chi)}(G)\big) \to K(A)$ of the maps (11)-(9) takes the class of a $U \in \mathrm{Rep}^{(\chi)}(G)$ to the class of the right A-module

$$\big(U \otimes_F V^* \otimes_F F(S)\big)^H$$

of dimension $\dim U \cdot \dim V$ over the field $F(R)$. On the other hand, the group $K(A)$ is infinite cyclic group generated by the class of a simple module of dimension $\operatorname{ind}(A) \cdot \dim V$ over $F(R)$. The result follows.

Remark 2.9. The surjective map $K\big(\operatorname{Rep}^{(\chi)}(G)\big) \to K(A)$ constructed in the proof depends on the choice of V and takes $[V]$ to $[A]$.

3. Canonical p-dimension of a product of Severi-Brauer variety

Let F be an arbitrary field and p a prime integer, $D \subset \operatorname{Br}_p(F)$ be a subgroup. We write $\operatorname{ed}_p(D)$ for the essential p-dimension of the class of splitting field extensions for D.

Theorem 3.1. *Let $D \subset \operatorname{Br}_p(F)$ be a finite subgroup of rank r. Then*

$$\operatorname{ed}_p(D) = \min \sum_{i=1}^{r} \big(\operatorname{ind}(a_i) - 1\big)$$

where the minimum is taken over all bases $a_1, \dots, a_r$ of D over $\mathbb{Z}/p\mathbb{Z}$.

Let $a = \{a_1, \dots, a_r\}$ be a basis of D. For any i let A_i be a central division F-algebra (of degree $\operatorname{ind}(a_i)$) representing a_i and $P_i = SB(A_i)$. Set $P_a := P_1 \times P_2 \times \cdots \times P_r$. Note that P_a depends on the choice of the basis a.

The classes of splitting fields of P and D coincide, hence

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

We shall produce a basis $a_1, \dots, a_r$ of D such that $\operatorname{cdim}_p(P_a) = \dim(P_a)$, i.e., P_a is not p-compressible.

We say that a basis $\{a_1, a_2, \dots, a_r\}$ of D is *minimal* if for any $i = 1, \dots, r$ 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 $a_1, \dots, a_{i-1}$.

Thus, it is suffices to prove the following

Proposition 3.2. *Let $D \subset \operatorname{Br}_p(F)$ a subgroup of dimension r and $a = \{a_1, a_2, \dots, a_r\}$ a minimal basis of D. Then the variety P_a constructed above is not p-compressible.*

Remark 3.3. It is not obvious that the sum $\sum_{i=1}^{r} \operatorname{ind} a_i$ is the smallest for a minimal basis $\{a_1, a_2, \dots, a_r\}$. However, this fact is a consequence of Proposition 3.2.

Fix a minimal basis a of D and set $P := P_a$. Let $d = \dim P$ and $\alpha \in \operatorname{CH}^d(P \times P)$. The *first multiplicity* $\operatorname{mult}_1(\alpha)$ *of* α is the image of α under the push-forward map $\operatorname{CH}^d(P \times P) \to \operatorname{CH}^0(P) = \mathbb{Z}$ given by the first projection $P \times P \to P$. Similarly, we define the *second multiplicity* $\operatorname{mult}_2(\alpha)$.

Proposition 3.4. *Let $D \subset \mathrm{Br}_p(F)$ a subgroup of dimension r, $a = \{a_1, a_2, \dots, a_r\}$ a minimal basis of D and $P = P_a$. Then for any element $\alpha \in \mathrm{CH}^d(P \times P)$, we have*

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

Now we show that Proposition 3.4 implies Proposition 3.2.

As $\mathrm{cdim}_p P \le \mathrm{cdim}\, P \le \dim P$, 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 Proposition 3.4, we have $\mathrm{mult}_2(\alpha) \neq 0$, i.e., $Z = P$. It follows that P is not p-compressible.

Thus, it suffices to prove Proposition 3.4.

Let A be a central simple algebra in $\mathrm{Br}_p(F)$ and $P = SB(A)$. We shall need to study the Grothendieck group $K_0(P)$. In the split case, P is a projective space of dimension $\deg(A) - 1$, hence

$$K_0(P) = \coprod_{0 \le j < \deg(A)} \mathbb{Z}\, x^j,$$

where x_i is the class of $\mathcal{O}(-1)$. Then $h := 1 - x$ is the class of a hyperplane and $h^{\deg A} = 0$. Consider the polynomial ring $\mathbb{Z}[x]$. We have a ring isomorphism

$$K_0(P) = \mathbb{Z}[x]/\big(h^{\deg A}\big).$$

On the other hand, we can embed $K_0(P)$ into $\mathbb{Z}[x]$ as the subgroup generated by the monomials x^j with $j < \deg A$.

In the general case, by the theorem [5, §9] of Quillen,

$$K_0(P) \simeq \coprod_{0 \le j < \deg(A)} K_0(A^{\otimes j}).$$

The image of the natural map $K_0(A^{\otimes j}) \to K_0(\overline{A}^{\otimes j}) = \mathbb{Z}$, (where the "bar" denote objects over a splitting field) is equal to $\mathrm{ind}(A^{\otimes j})\mathbb{Z}$. The image of the injective homomorphism $K_0(P) \to K_0(\overline{P})$ identifies $K_0(P)$ with the subgroup generated by $\mathrm{ind}(A^{\otimes j})\, \mathbb{Z}\, x^j$ for all $j \ge 0$, more precisely,

$$K_0(P) = \coprod_{0 \le j < \deg(A)} \mathrm{ind}(A^{\otimes j})\, \mathbb{Z}\, x^j,$$

of $K_0(\overline{P})$. Let $\mathrm{ind}(A) = p^n$. Write for any $j \ge 0$:

$$e(j) = \begin{cases} n, & \text{if } p \text{ does not divide } j; \\ 1, & \text{otherwise.} \end{cases}$$

Thus, $\mathrm{ind}(A^{\otimes j}) = p^{e(j)}$ and the ring $K_0(P)$ depends only on n.

Denote by $K(n)$ the subgroup of $\mathbb{Z}[x]$ generated by the monomials $p^n x^j$ if j is not divisible by p and x^j if j is divisible by p. Clearly, $K(n)$ is a subring of $\mathbb{Z}[x]$.

We have a natural surjective ring homomorphism $K(n) \to K_0(P)$. Write $h := 1 - x$. As $p^n | \deg(A)$ we have $h^{\deg A} \in K(n)$. As the image of h in $K_0(\overline{P})$ is the class of a hyperplane, the image of $h^{\deg A}$ in $K_0(P)$ is zero.

Proposition 3.5. *The induced homomorphism $K(m)/(h^{\deg A}) \to K_0(P)$ is an isomorphism.*

Proof. Set $d = \deg A$. By induction on k we show that the quotient ring $K(m)/(h^d)$ is additively generated by $p^{e(j)}x^j$ with $j < d$. Indeed, the polynomial $x^d - (-h)^d = x^d - (x-1)^d$ is a linear combination with integer coefficients of $p^{e(j)}x^j$ with $j < d$. Consequently, for any $k \geq d$, multiplying the equality by $p^{e(k-d)}x^{k-d} = p^{e(k)}x^{k-d}$, we see that the polynomial $p^{e(k)}x^k = p^{e(k)}x^{i+k}$ modulo the ideal (h^d) is a linear combination with integer coefficients of the $p^{e(j)}x^j$ with $j < k$. □

Corollary 3.6. *Let g be a polynomial in h lying in $K(n)$ for some $m \geq 0$. Let bh^{i-1} be a monomial of g such that i is divisible by p^n. Then b is divisible by p^n.*

Proof. By Proposition 3.5, the factor ring $K(n)/(h^i)$ is isomorphism to $K_0(P)$ where P is the Severi-Brauer variety of an algebra of index p^n and degree i. Thus, $K(n)/(h^i)$ is additively generated by $p^{e(j)}(1-h)^j$ with $j < i$. Only the generator $p^{e(i-1)}(1-h)^{i-1} = p^n(1-h)^{i-1}$ has a nonzero h^{i-1}-coefficient and that coefficient is divisible by p^n. □

Note that we have a canonical embedding of groups $K_0(P) \subset K(n)$.

Now consider a more general situation. Let $A_1, A_2, \dots A_r$ be central simple algebras in $\mathrm{Br}_p(F)$, $P_i = SB(A_i)$ and $P = P_1 \times \cdots \times P_r$. We shall need to study the Grothendieck group $K_0(P)$. In the split case (when all the algebras A_i split), P is the product of r projective spaces of dimensions $\deg(A_1) - 1, \dots, \deg(A_r) - 1$ respectively. Write $x_i \in K_(\overline{P})$ for the pullback of the class of $\mathcal{O}(-1)$ on the i-th component of the product and set

$$x^j = x_1^{j_1} \cdots x_r^{j_r}$$

for a multi-index $j = (j_1, \dots, j_r)$. We also write $0 \leq j < \deg A$ for a multi-index j such that $0 \leq j_i < \deg A_i$ for all $i = 1, \dots, r$.

We have

$$K_0(P) = \coprod_{0 \leq j < \deg A} \mathbb{Z}\, x^j,$$

Then $h_i := 1 - x_i$ is the class of a hyperplane on the i-th component and $h_i^{\deg A_i} = 0$. Consider $x = (x_1, \dots, x_r)$ as a tuple of variables and the polynomial ring $\mathbb{Z}[x]$. We have

$$K_0(P) = \mathbb{Z}[x]/\big(h_1^{\deg A_1}, \dots, h_r^{\deg A_r}\big).$$

In the general case, by Quillen's theorem,

$$K_0(P) \simeq \coprod_{0 \leq j < \deg A} K_0(A^{\otimes j}),$$

where $A^{\otimes j} = A_1^{\otimes j_1} \otimes \cdots \otimes A_r^{\otimes j_r}$. The image of the injective homomorphism $K_0(P) \to K_0(\overline{P})$ identifies $K_0(P)$ with the subgroup

$$K_0(P) = \coprod_{0 \le j < \deg A} \operatorname{ind}(A^{\otimes j})\ \mathbb{Z}\ x^j,$$

of $K_0(\overline{P})$.

Suppose now that the algebras A_i represent a minimal basis $a = \{a_1, \dots, a_r\}$ of the subgroup D. Set $\operatorname{ind}(a_i) = p^{n_i}$ and $a^j = a_1^{j_1} \cdots a_r^{j_r} \in \operatorname{Br}_p(F)$ for a multi-index $j = (j_1, \dots, j_r) \ge 0$. Recall that by the definition of a minimal basis, $0 \le n_1 \le n_2 \le \cdots \le n_r$ and $\log_p \operatorname{ind}(a^j) \ge n_k$ with the largest k such that j_k is not divisible by p.

Let us introduce the following notation. Let $r \ge 1$ and $0 \le n_1 \le n_2 \le \cdots \le n_r$ be integers. For all $j = (j_1, \dots, j_r) \ge 0$, we define the number $e(j)$ as follows:

$$e(j) = \begin{cases} 0, & \text{if all the } j_1, \dots, j_r \text{ are divisible by } p; \\ n_k, & \text{with the largest } k \text{ such that } j_k \text{ is not divisible by } p. \end{cases}$$

Thus, we have

$$\log_p \operatorname{ind}(a^j) \ge e(j).$$

Let $K = K(n_1, \dots, n_r)$ be the subgroup of the polynomial ring $\mathbb{Z}[x]$ in r variables $x = (x_1, \dots, x_r)$ generated by the monomials $p^{e(j)} x^j$ for all $j \ge 0$. In fact, K is a subring of $\mathbb{Z}[x]$. By construction, we have canonical embeddings of groups

$$K_0(P) \subset K \subset \mathbb{Z}[x].$$

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

Proposition 3.7. *Let $f = f(h) \in K$ be a nonzero polynomial and bh^i for a multi-index $i \ge 0$ be a monomial of the least degree of f. Assume that the integer b is not divisible by p. Then $p^{n_1} \mid i_1, \dots, p^{n_r} \mid i_r$.*

Proof. We proceed by induction on $m = r + n_1 + \cdots + n_r \ge 1$. The case $m = 1$ is trivial. If $m > 1$ and $n_1 = 0$, then

$$e(j) = e(j'),$$

where $j' = (j_2, \dots, j_r)$. It follows that

$$K = K(n_2, \dots, n_r)[x_1] = K(n_2, \dots, n_r)[h_1].$$

Write f in the form

$$f = \sum_{i \ge 0} h_1^i \cdot g_i$$

with $g_i = g_i(h_2, \dots, h_r) \in K(n_2, \dots, n_r)$. Then $bh_2^{i_2} \dots h_r^{i_r}$ is the monomial of the least degree of g_{i_1}. We can apply the induction to $g_{i_1} \in K(n_2, \dots, n_r)$.

In what follows we assume that $n_1 \ge 1$.

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

Consider the additive operation $\varphi\colon \mathbb{Z}[x] \to \mathbb{Q}[x]$ defined by

$$\varphi(g) = \frac{1}{p}\ x_1 \cdot \frac{\partial g}{\partial x_1}.$$

We have

$$\varphi(x^j) = \frac{j_1}{p}\ x^j.$$

It follows that

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

and

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

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 $-\frac{bi_1}{p}\ h_1^{i_1-1}h_2^{i_2}\cdots h_r^{i_r}$ is a monomial of $\varphi(f)$ considered as a polynomial in h. As

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

we see that $-\frac{bi_1}{p}\ h_1^{i_1-1}$ is a monomial of a polynomial from $K(n_1 - 1)$. It follows that $\frac{i_1}{p}$ is an integer and by Corollary 3.6, this integer is divisible by p^{n_1-1}. Therefore $p^{n_1} \mid i_1$. $\square$

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 3.8. *Let $P = P_a$ for a minimal basis a. Then 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

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

where the bottom map is an isomorphism as $\overline{P}$ is split. 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 $h_1^{\operatorname{ind} a_1}, \dots, h_r^{\operatorname{ind} a_r}$. 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 $G^j K_0(\overline{P})$ is identified with the group of all homogeneous polynomials of degree j.

Recall that
$$K_0(P) \subset K(n_1, \dots, n_r) \subset \mathbb{Z}[x],$$
where $n_i = \log_p\big(ind(a_i)\big)$.

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 $G^j K_0(\overline{P})$ is the j-th homogeneous part f_j of f. As the degree of f with respect to h_i is less than $\operatorname{ind} a_i$, it follows from Proposition 3.7 that all the coefficients of f_j are divisible by p. □

Now we prove Proposition 3.4. The homomorphism
$$f\colon \mathrm{CH}^d(P \times P) \to (\mathbb{Z}/p\mathbb{Z})^2,$$
taking an $\alpha \in \mathrm{CH}^d(P \times P)$ to $\big(\mathrm{mult}_1(\alpha), \mathrm{mult}_2(\alpha)\big)$ 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, by the Projective Bundle Theorem, 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 3.8, 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 $(1, 1)$.

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

If $\mathcal{X}$ is a gerbe banded by C then we have pairings
$$\mathrm{B}C \times \mathcal{X} \to \mathcal{X}, \quad (t, x) \mapsto t + x,$$
$$\mathcal{X} \times \mathcal{X} \to \mathrm{B}C, \quad (x, x') \mapsto x - x'.$$
We have the associativity property: $(t + x) - x' = t + (x - x')$.

In this section we relate the essential and canonical p-dimensions of gerbes banded by $(\boldsymbol{\mu}_p)^s$ where $s \geq 0$.

Proposition 4.1. *Let $\mathcal{X}$ be a gerbe banded by C. Then*
$$\mathrm{ed}_p(\mathcal{X}) \leq \mathrm{cdim}_p(\mathcal{X}) + \mathrm{ed}_p(\mathrm{B}C).$$

Proof. Let L/F be a field extension, $x \in \mathcal{X}(L)$, L'/L a finite field extension of degree prime to p and a subfield $K \subset L'$ such that $\mathcal{X}(K) \neq \emptyset$ and $\mathrm{cdim}_p(\mathcal{X}) = \operatorname{tr.deg}_F(K)$. Take any $y \in \mathcal{X}(K)$ and set $t := x_{L'} - y_{L'} \in \mathrm{B}C(L')$. Choose a field extension L''/L' of degree prime to p, a subfield $K' \subset L''$ over F and

$t' \in \mathrm{B}C(K')$ with $t'_{L''} = t_{L''}$ and $\mathrm{tr.deg}_F(K') = \mathrm{ed}_p(t)$. Then $x_{L''} = t'_{L''} + y_{L''}$ is defined over KK', hence

$$\mathrm{ed}_p(x) \le \mathrm{tr.deg}_F(KK') \le \mathrm{tr.deg}_F(K) + \mathrm{tr.deg}_F(K') = \\ \mathrm{cdim}_p(\mathcal{X}) + \mathrm{ed}_p(t) \le \mathrm{cdim}_p(\mathcal{X}) + \mathrm{ed}_p(\mathrm{B}C). \quad \square$$

Question 4.2. *Let $\mathcal{X}$ be a gerbe banded by C. Is it true that*

$$\mathrm{ed}_p(\mathcal{X}) = \mathrm{cdim}_p(\mathcal{X}) + \mathrm{ed}_p(\mathrm{B}C)?$$

In the following theorem we show that the answer is "yes" is $C = (\boldsymbol{\mu}_p)^s$ when p is a prime integer.

Let $\mathcal{X}$ a gerbe banded by $C = (\boldsymbol{\mu}_p)^s$ over F. The gerbe $\mathcal{X}$ is given by an element in $H^2(F, C) = \mathrm{Br}_p(F)^s$, i.e., by an s-tuple of central simple algebras $A_1, A_2, \dots, A_s$ with $[A_i] \in \mathrm{Br}_p(F)$. Let P be the product of the Severi-Brauer varieties $P_i := \mathrm{SB}(A_i)$ and D the subgroup of $\mathrm{Br}_p(F)$ generated by the $[A_i]$, $i = 1, \dots, s$. Note that the classes of splitting fields for $\mathcal{X}$, D and P coincide. Moreover, if R is a local commutative F-algebra then the following are equivalent:

1. $\mathcal{X}(R) \ne \emptyset$.
2. $P(R) \ne \emptyset$.
3. The algebras A_i are split by R.

Notation: an object $z \in \mathrm{B}C(R)$ defines the isomorphism class in $H^1_{\acute{e}t}(R, C) = (R^\times / R^{\times p})^s$. We write $z_i \in R^\times$ for the components of z.

Theorem 4.3. *Let p be a prime integer and $\mathcal{X}$ a gerbe banded by $C = (\boldsymbol{\mu}_p)^s$ over F. Then*

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

Proof. In view of Proposition 4.1, it suffices to prove the inequality $\mathrm{ed}_p(\mathcal{X}) \ge \mathrm{cdim}_p(P) + s$.

Let $\mathcal{C}$ be the class of splitting fields for $\mathcal{X}$ (and for P). Choose a *minimal* field in $\mathcal{C}$, i.e., a field $K \in \mathcal{C}$ satisfying $\mathrm{tr.deg}_F(K) = \mathrm{ed}_p^{\mathcal{C}}(K) = \mathrm{cdim}_p(\mathcal{X})$. Choose also an object $x \in \mathcal{X}(K)$. Set $L := K(t_1, \dots, t_s)$ and $x' := t + x_L \in \mathcal{X}(L)$, where $t := (t_1, \dots, t_s) \in \mathrm{B}C(L)$. It is sufficient to prove the inequality $\mathrm{ed}_p(x') \ge \mathrm{cdim}_p(\mathcal{X}) + s$.

Let L'/L be a finite field extension of degree prime to p, $L'' \subset L'$ a subfield over F and $y \in \mathcal{X}(L'')$ such that $y_{L'} = x'_{L'}$. It suffices to show that $\mathrm{tr.deg}_F(L'') \ge \mathrm{cdim}_p(\mathcal{X}) + s$.

Let $L_i := K(t_i, \dots, t_s)$ 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 7.1, 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 K' of degree over K 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 $a_{ij} \in \mathbb{Z}$. It follows that the columns $v'(t_i)$ are linearly independent modulo p.

Write v'' for the restriction of v' on L''.

Claim: $\operatorname{rank}(v'') = s$.

To prove the claim let $R'' \subset L''$ be the valuation ring of v''. As $P(L'') \neq \emptyset$ and P is complete then $P(R'') \neq \emptyset$. It follows that $\mathcal{X}(R'') \neq \emptyset$. Choose any $x'' \in \mathcal{X}(R'')$ and set $z := y - x''_{L''} \in \mathrm{B}C(L'')$. Hence

$$z_{L'} = y_{L'} - x''_{L'} = \big(t_{L'} + x_{L'}\big) - x''_{L'} = t_{L'} + \big(x_{L'} - x''_{L'}\big).$$

Note that the element $x_{L'} - x''_{L'}$ is in the image of $\mathrm{B}C(R') \to \mathrm{B}C(L')$, where $R' \subset L'$ is the valuation ring of v'. Thus, there exist $r_i \in R'^{\times}$ and $v_i \in L'^{\times}$ such that

$$z_i = t_i \cdot r_i \cdot v_i^p$$

and hence $v''(z_i) \equiv v'(t_i)$ modulo p for all $i = 1, \dots, s$. It follows that the columns $v''(z_i)$ are linearly independent modulo p and hence generate a submodule of rank s in $\mathbb{Z}^s$. This means that $\operatorname{rank}(v'') = s$, proving the claim.

Let K'' be the residue field of v''. As $K \in \mathcal{C}$, $K'' \subset K'$, $[K' : K]$ is prime to p and K is minimal, we have $\operatorname{tr.deg}_F(K'') = \operatorname{tr.deg}_F(K)$. It follows that

$$\operatorname{tr.deg}_F(L'') \geq \operatorname{tr.deg}_F(K'') + \operatorname{rank}(v'') = \operatorname{tr.deg}_F(K) + s = \operatorname{cdim}_p(\mathcal{X}) + s. \quad \square$$

5. Main theorem

Theorem 5.1. (cf. [4]) *Let G be a finite group, p be prime integer and F a field of characteristic different from p. Then $\operatorname{ed}_p(G)$ is equal to the least dimension of a faithful H-space of a Sylow p-subgroup H of G over the field $F(\xi_p)$.*

We have $\operatorname{ed}_p(G) = \operatorname{ed}_p(H) = \operatorname{ed}_p(H_{F(\xi_p)})$. Hence $\operatorname{ed}_p(G)$ is at most the dimension of a faithful H-space of a Sylow p-subgroup H of G over the field $F(\xi_p)$. Thus we may suppose that G is a p-group, F contains p-th roots of unity, and we need to show that there is a faithful representation V of G 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

$$1 \to C \to G \to H \to 1. \tag{10}$$

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

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

as in Section 2.2. Note that as $\mu_p \subset F^\times$, so we can identify C with $(\boldsymbol{\mu}_p)^s$.

Consider the gerbe $\mathcal{X}^E := E/G$ banded by C. The classes of splitting fields of the gerbe $\mathcal{X}^E$ and the subgroup $\mathrm{Im}(\beta^E)$ coincide.

By Theorem 6.3, applied to the subgroup $\mathrm{Im}(\beta^E) \subset \mathrm{Br}(F)$, we can complete any basis of $\mathrm{Ker}(\beta^E)$ to a basis $\chi_1, \chi_2, \dots, \chi_s$ of C^* over $\mathbb{Z}/p\mathbb{Z}$ such that

$$\mathrm{cdim}_p(\mathcal{X}^E) = \mathrm{cdim}_p\big(\mathrm{Im}(\beta^E)\big) = \sum_{i=1}^{s}\big(\mathrm{ind}\,\beta^E(\chi_i) - 1\big).$$

It follows from Theorem 4.3 that

$$\mathrm{ed}_p(\mathcal{X}^E) = \mathrm{cdim}_p(\mathcal{X}^E) + s = \sum_{i=1}^{s} \mathrm{ind}\,\beta^E(\chi_i). \tag{11}$$

Now we choose specific E, namely a generic H-torsor over a field extension L of F.

Note that dimension of every irreducible representation of G is a power of p. Indeed, let q be the order of G. It is known that every irreducible representation of G is defined over the field $K := F(\mu_q)$. Since F contains p-th roots of unity, the degree $[K : F]$ is a power of p. Let V be an irreducible G-space. Write V as a direct sum of V_i over K. As each V_i is absolutely irreducible, $\dim(V_i)$ divides $|G|$ and hence is a power of p. The group $\Gamma := \mathrm{Gal}(K/F)$ permutes transitively the V_i. As $|\Gamma|$ is a power of p, the number of the V_i's is also a power of p.

Hence gcd in Theorem 2.3 can be replaced by min. By Theorem 2.3, for any character $\chi \in C^*$, there is representation $V_\chi \in \mathrm{Rep}^{(\chi)}(G)$ such that $\mathrm{ind}\,\beta^E(\chi) = \dim(V_\chi)$. Let V be the direct sum of V_{χ_i}, $i = 1, \dots, s$. It follows from (11) that

$$\mathrm{ed}_p(\mathcal{X}^E) = \dim(V).$$

Applying Theorem 1.1 for the gerbe $\mathcal{X}$ over the field L, we get the inequality

$$\mathrm{ed}_p(G) \geq \mathrm{ed}_p(G_L) \geq \mathrm{ed}_p(\mathcal{X}^E) = \dim(V).$$

It suffices to show that V is a faithful G-space. Since the χ_i's form a basis of C^*, the C-space V is faithful. Let N be the kernel of V. As every nontrivial normal subgroup of G intersects C nontrivially, we have $N = \{1\}$, i.e., the G-space V is faithful.

Remark 5.2. The proof of Theorem 5.1 shows how to construct a faithful G-space for a p-group G over a field F containing p-th roots of unity. For every character $\chi \in C^*$ choose a representation $V_\chi \in \mathrm{Rep}^{(\chi)}(G)$ of the least dimension. It appears as an irreducible component of the least 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 least $\dim(V_{\chi_1})$. 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 $V = \coprod V_{\chi_i}$ is a faithful G-space of the least dimension and $\mathrm{ed}_p(G) = \dim(V)$.

6. Applications

Theorem 6.1. *Let G be a p-group and F a field containing p-th roots of unity. Then* $\mathrm{ed}(G) = \mathrm{ed}_p(G)$ *is equal to the least dimension of a faithful G-space over F.*

Proof. Let V be a faithful G-space of the least dimension. Then by Theorem 5.1,

$$\dim(V) = \mathrm{ed}_p(G) \leq \mathrm{ed}(G) \leq \dim(V). \qquad \square$$

Corollary 6.2. [3] *Let G be a cyclic group of primary order p^n and F a field containing p-th roots of unity. Then* $\mathrm{ed}(G) = \mathrm{ed}_p(G) = \big[F(\xi_{p^n}) : F\big]$.

Proof. The G-space $F(\xi_{p^n})$ is faithful irreducible of the smallest dimension. $\square$

Theorem 6.3. *Let G_1 and G_2 be two p-groups and F a field of characteristic different from p containing p-th roots 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 $\mathrm{ed}(G_1 \times G_2) \leq \mathrm{ed}(G_1) + \mathrm{ed}(G_2)$.

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 5.2. 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 $\mathrm{ed}(G_j) \leq \dim(W_j)$. As $W_1 \oplus W_2 = V$, we have

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

The following corollary is a generalization of Corollary 6.2.

Corollary 6.4. *Let F be a field containing p-th roots of unity. Then*

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

7. Appendix

Lemma 7.1. *Let $L \in \mathsf{Fields}/F$, v a discrete valuation of L over F and L'/L a finite field extension of degree prime to p. Then there exists a geometric valuation v' of L' extending v such that the ramification index and the degree of the residue field extension $F(v')/F(v)$ are prime to p.*

Proof. If L'/L is separable and $v_1, \dots, v_k$ are all the extensions of v on L' then $[L' : L] = \sum e_i[F(v_i) : F(v)]$ where e_i is the ramification index (cf. [6, Ch. VI, Th. 20 and p. 63]). It follows that the integer $[F(v_i) : F(v)]$ 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. $\square$

References

[1] P. Brosnan, Z. Reichstein, and A. Vistoli, *Essential dimension and algebraic stacks I*, LAGRS preprint server, `http://www.math.uni-bielefeld.de/LAG/` (n. 275, 2007).

[2] S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. **52** (1965), 15–33.

[3] M. Florence, *On the essential dimension of cyclic p-groups*, Invent. Math. ***** (2008), no. *, *–*.

[4] N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. ***** (2008), no. *, *–*.

[5] D. Quillen, *Higher algebraic K-theory. I*, (1973), 85–147. Lecture Notes in Math., Vol. 341.

[6] O. Zariski and P. Samuel, *Commutative algebra. Vol. II*, Springer-Verlag, New York, 1975, Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA

E-mail address: `merkurev@math.ucla.edu`