SOME CONSEQUENCES OF THE KARPENKO-MERKURJEV THEOREM

AUREL MEYER[†] AND ZINOVY REICHSTEIN[††]

To Andrei Alexandrovich Suslin on the occasion of his 60th birthday

Abstract. We use a recent theorem of N. A. Karpenko and A. S. Merkurjev to settle several questions in the theory of essential dimension.

1. Introduction

Let k be a field, Fields_k be the category of field extensions K/k, Sets be the category of sets, and $F\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor. Given a tower of field extensions $k \subset K \subset L$, we will denote the image of $a \in F(K)$ under the natural map $F(K) \to F(L)$ by a_L. Conversely, if $b \in F(L)$ lies in the image of this map, we will say that b *descends* to K.

Given a field extension K/k and $b \in F(L)$, the *essential dimension* $\mathrm{ed}_k(b)$ of b is defined as the minimal transcendence degree $\mathrm{trdeg}_k(K)$, as K ranges over all intermediate subfields $k \subset K \subset L$ such that b descends to K. Informally speaking, this is the minimal number of parameters one needs to define b. The essential dimension $\mathrm{ed}_k(F)$ of the functor F is the maximal value of $\mathrm{ed}_k(b)$, as L ranges over all field extensions of k and b ranges over $F(L)$. Informally speaking, this is the minimal number of parameters required to define any object of F.

The *essential dimension* $\mathrm{ed}_k(b;p)$ at a prime p is defined as the minimum of $\mathrm{ed}_k(b_{L'})$, taken over all finite field extensions L'/L such that the degree $[L' : L]$ is prime to p. The essential dimension of $\mathrm{ed}_k(F;p)$ of F at a prime p is the supremum of $\mathrm{ed}_k(b;p)$ taken over all $b \in F(L)$ and over all field extensions L/k.

An important example where the above notions lead to a rich theory is the nonabelian cohomology functor $F_G = H^1(*, G)$, sending a field K/k to the set $H^1(K, G)$ of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$, in the fppf topology. Here G is an algebraic group defined over k. The essential

1991 *Mathematics Subject Classification.* 20D15, 20C15, 20G15.

Key words and phrases. Essential dimension, linear representation, p-group, algebraic torus.

[†] Partially supported by a University Graduate Fellowship at the University of British Columbia.

[††] Partially supported by NSERC Discovery and Accelerator Supplement grants.

dimension of this functor can be thought of as a numerical measure of complexity of G-torsors over fields or, alternatively, as the minimal number of parameters required to define a versal G-torsor. In the case where G is a finite (constant) group defined over k, which will be the main focus of this paper, $\mathrm{ed}_k(G)$ is the minimal number of parameters required to describe all G-Galois extensions.

For details on the notion of essential dimension of a finite group we refer the reader to [BuR], [Re] or [JLY, Chapter 8], on the notion of essential dimension of a functor to [BF] or [BRV$_2$] and on essential dimension at a prime p to [Me].

N. Karpenko and A. Merkurjev [KM] recently proved the following formula for the essential dimension of a (finite) p-group.

Theorem 1.1. *Let G be a p-group and k be a field of characteristic $\neq p$ containing a primitive pth root of unity. Then*

$$\mathrm{ed}_k(G;p) = \mathrm{ed}_k(G) = \min \dim(V)\,,$$

where the minimum is taken over all faithful k-representations $G \hookrightarrow \mathrm{GL}(V)$.

The purpose of this paper is to explore some of the consequences of this theorem. The following notation will be used throughout.

We will fix a prime p and a base field k such that

$$\mathrm{char}(k) \neq p \text{ and } k \text{ contains } \zeta, \tag{1}$$

where ζ is a primitive pth root of unity if $p \geq 3$ and a primitive 4th root of unity if $p = 2$.

For a finite group H, we will denote the intersection of the kernels of all multiplicative characters $\chi\colon H \to k^*$ by H'. In particular, if k contains an eth root of unity, where e is the exponent of H, then $H' = [H, H]$ is the commutator subgroup of H.

All p-groups in this paper will be assumed to be finite. Given a p-group G, we set $C(G)$ to be the center of G and

$$C(G)_p := \{g \in C(G) \mid g^p = 1\} \tag{2}$$

to be the p-torsion subgroup of $C(G)$. We will view $C(G)_p$ and its subgroups as $\mathbb{F}_p$-vector spaces, and write "$\dim_{\mathbb{F}_p}$" for their dimensions. We further set

$$K_i := \bigcap_{[G:H]=p^i} H' \quad \text{and} \quad C_i := K_i \cap C(G)_p\,. \tag{3}$$

for every $i \geq 0$, $K_{-1} := G$ and $C_{-1} := K_{-1} \cap C(G)_p = C(G)_p$.

Our first main result is following theorem. Part (b) may be viewed as a variant of Theorem 1.1.

Theorem 1.2. *Let G be a p-group, k be a base field satisfying* (1) *and $\rho\colon G \hookrightarrow \mathrm{GL}(V)$ be a faithful linear k-representation of G. Then*

(a) ρ has minimal dimension among the faithful linear representations of G defined over k if and only if for every $i \geq 0$ the irreducible decomposition of ρ has exactly

$$\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i$$

irreducible components of dimension p^i, each with multiplicity 1.

(b) $\mathrm{ed}_k(G;p) = \mathrm{ed}_k(G) = \sum_{i=0}^{\infty}(\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i)p^i$.

Note that $K_i = C_i = \{1\}$ for large i (say, if $p^i \geq |G|$), so only finitely many terms in the above infinite sum are non-zero. We also remark that the minimal number of irreducible components in a faithful representations of a finite group (but not necessarily a p-group) was studied in [Ta, Na], see also [Lo, Section 4].

We will prove Theorem 1.2 in section 2; the rest of the paper will be devoted to its applications. The main results we will obtain are summarized below.

Classification of p-groups of essential dimension $\leq p$.

Theorem 1.3. *Let p be a prime, k be as in (1) and G be a p-group such that $G' \neq \{1\}$. Then the following conditions are equivalent.*

(a) $\mathrm{ed}_k(G) \leq p$,

(b) $\mathrm{ed}_k(G) = p$,

(c) The center $C(G)$ is cyclic and G has a subgroup H of index p such that $H' = \{1\}$.

Note that the assumption that $G' \neq \{1\}$ is harmless. Indeed, if $G' = \{1\}$ then by Theorem 1.2(b) $\mathrm{ed}_k(G) = \mathrm{rank}\,(G)$; cf. also [BuR, Theorem 6.1] or [BF, section 3].

Essential dimension of p-groups of nilpotency class 2.

Theorem 1.4. *Let G be a p-group of exponent e and k be a field of characteristic $\neq p$ containing a primitive e-th root of unity. Suppose the commutator subgroup $[G,G]$ is central in G. Then*

(a) $\mathrm{ed}_k(G;p) = \mathrm{ed}_k(G) \leq \mathrm{rank}\ C(G) + \mathrm{rank}\,[G,G](p^{\lfloor m/2 \rfloor} - 1)$, *where p^m is the order of $G/C(G)$.*

(b) Moreover, if $[G,G]$ is cyclic then $|G/C(G)|$ is a complete square and equality holds in (a). That is, in this case

$$\mathrm{ed}_k(G;p) = \mathrm{ed}_k(G) = \sqrt{|G/C(G)|} + \mathrm{rank}\ C(G) - 1\,.$$

Essential dimension of a quotient group. C. U. Jensen, A. Ledet and N. Yui asked if $\mathrm{ed}_k(G) \geq \mathrm{ed}_k(G/N)$ for every finite group G and normal subgroup $N \lhd G$; see [JLY, p. 204]. The following theorem shows that this inequality is false in general.

Theorem 1.5. *Let p be a prime and k be a field of characteristic $\neq p$ containing a primitive pth root of unity. For every real number $\lambda > 0$ there exists a p-group G and a central subgroup H of G such that* $\operatorname{ed}_k(G/H) > \lambda \operatorname{ed}_k(G)$.

Essential dimension of $\mathrm{SL}_n(\mathbb{Z})$. G. Favi and M. Florence [FF] showed that $\operatorname{ed}_k(\mathrm{GL}_n(\mathbb{Z})) = n$ for every $n \geq 1$ and $\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z})) = n-1$ for every odd n. For details, including the definitions of $\operatorname{ed}_k(\mathrm{GL}_n(\mathbb{Z}))$ and $\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z}))$, see Section 5. For even n Favi and Florence showed that $\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z})) = n-1$ or n and left the exact value of $\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z}))$ as an open question. In this paper we will answer this question as follows.

Theorem 1.6. *Suppose k is a field of characteristic $\neq 2$. Then*

$$\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z}); 2) = \operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z})) = \begin{cases} n-1, \text{ if } n \text{ is odd,} \\ n, \text{ if } n \text{ is even} \end{cases}$$

for any $n \geq 3$.

Acknowledgement. Theorems 1.4(b) and 1.5 first appeared in the unpublished preprint [BRV_1] by P. Brosnan, the second author and A. Vistoli. We thank P. Brosnan and A. Vistoli for allowing us to include them in this paper. Theorem 1.4(b) was, in fact, a precursor to Theorem 1.1; the techniques used in [BRV_1] were subsequently strengthened and refined by Karpenko and Merkurjev [KM] to prove Theorem 1.1. The proof of Theorem 1.4(b) in Section 4 may thus be viewed as a result of reverse engineering. We include it here because it naturally fits into the framework of this paper, because Theorem 1.4(b) is used in a crucial way in [BRV_2], and because a proof of this result has not previously appeared in print.

We are also grateful to R. Lötscher for pointing out and helping us correct an inaccuracy in the proof of Lemma 2.1.

2. Proof of Theorem 1.2

Throughout this section we assume k to be as in (1). An important role in the proof will be played by the p-torsion subgroup $C(G)_p$ of the center of G and by the descending sequences

$$K_{-1} = G \supset K_0 \supset K_1 \supset K_2 \supset \dots \quad \text{and}$$
$$C_{-1} = C(G)_p \supset C_0 \supset C_1 \supset C_2 \supset \dots$$

of characteristic subgroups of G defined in (3). To simplify the notation, we will write C for $C_{-1} = C(G)_p$ for the rest of this section. We will repeatedly use the well-known fact that

(4) A normal subgroup N of G is trivial if and only if $N \cap C$ is trivial.

We begin with three elementary lemmas.

Lemma 2.1. $K_i = \bigcap_{\dim(\rho) \leq p^i} \ker(\rho)$, *where the intersection is taken over all irreducible representations ρ of G of dimension $\leq p^i$.*

Proof. Let $j \leq i$. Recall that every irreducible representation ρ of G of dimension p^j is induced from a 1-dimensional representation χ of a subgroup $H \subset G$ of index p^j; see [LG-P, (II.4)] for $p \geq 3$ (cf. also [Vo]) and [LG-P, (IV.2)] for $p = 2$. (Note that our assumption (1) on the base field k is crucial here. In the case where $k = \mathbb{C}$ a more direct proof can be found in [Se, Section 8.5]).

Thus $\ker(\rho) = \ker(\mathrm{ind}_H^G \chi) = \bigcap_{g \in G} g \ker(\chi) g^{-1}$, and since each $g \ker(\chi) g^{-1}$ contains $(gHg^{-1})'$, we see that $\ker(\rho) \supset K_j \supset K_i$. The opposite inclusion is proved in a similar manner. □

Lemma 2.2. *Let $\rho\colon G \to \mathrm{GL}(V)$ an irreducible representation of a p-group G. Then*

(a) $\rho(C)$ consists of scalar matrices. In other words, the restriction of ρ to C decomposes as $\chi \oplus \ldots \oplus \chi$ ($\dim(V)$ times), for some multiplicative character $\chi\colon C \to \mathbb{G}_m$. We will refer to χ as the character associated to ρ.

(b) $C_i = \bigcap_{\dim(\psi) \leq p^i} \ker(\chi_\psi)$, where the intersection is taken over all irreducible G-representations ψ of dimension $\leq p^i$ and $\chi_\psi\colon C \to \mathbb{G}_m$ denotes the character associated to ψ. In particular, if $\dim(\rho) \leq p^i$ then χ_ρ vanishes on C_i.

Proof. (a) follows from Schur's lemma. (b) By Lemma 2.1

$$C_i = C \cap \bigcap_{\dim(\psi) \leq p^i} \ker(\psi) = \bigcap_{\dim(\psi) \leq p^i} (C \cap \ker(\psi)) = \bigcap_{\dim(\psi) \leq p^i} \ker(\chi_\psi)\,.$$

□

Lemma 2.3. *Let G be a p-group and $\rho = \rho_1 \oplus \ldots \oplus \rho_m$ be the direct sum of the irreducible representations $\rho_i\colon G \to \mathrm{GL}(V_i)$. Let $\chi_i := \chi_{\rho_i}\colon C \to \mathbb{G}_m$ be the character associated to ρ_i.*

(a) ρ is faithful if and only if $\chi_1, \ldots, \chi_m$ span C^* as an $\mathbb{F}_p$-vector space.

(b) Moreover, if ρ is of minimal dimension among the faithful representations of G then $\chi_1, \ldots, \chi_m$ form an $\mathbb{F}_p$-basis of C^*.

Proof. (a) By (4), $\mathrm{Ker}(\rho)$ is trivial if and only if $\mathrm{Ker}(\rho) \cap C = \cap_{i=1}^m \mathrm{Ker}(\chi_i)$ is trivial. On the other hand, $\cap_{i=1}^m \mathrm{Ker}(\chi_i)$ is trivial if and only if $\chi_1, \ldots, \chi_m$ span C^*.

(b) Assume the contrary, say χ_m is a linear combination of $\chi_1, \ldots, \chi_{m-1}$. Then part (a) tells us that $\rho_1 \oplus \ldots \oplus \rho_{m-1}$ is a faithful representation of G, contradicting the minimality of $\dim(\rho)$. □

We are now ready to proceed with the proof of Theorem 1.2. Part (b) is an immediate consequence of part (a) and Theorem 1.1. We will thus focus on proving part (a). In the sequel for each $i \geq 0$ we will set

$$\delta_i := \dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i$$

and

$$\Delta_i := \delta_0 + \delta_1 + \cdots + \delta_i = \dim_{\mathbb{F}_p} C - \dim_{\mathbb{F}_p} C_i\,,$$

where the last equality follows from $C_{-1} = C$.

Our proof will proceed in two steps. In Step 1 we will construct a faithful representation μ of G such that for every $i \geq 0$ exactly δ_i irreducible components of μ have dimension p^i. In Step 2 we will show that $\dim(\rho) \geq \dim(\mu)$ for any other faithful representation ρ of G, and moreover equality holds if and only if ρ has exactly δ_i irreducible components of dimension p^i, for every $i \geq 0$.

Step 1: We begin by constructing μ. By definition,

$$C = C_{-1} \supset C_0 \supset C_1 \supset \dots ,$$

where the inclusions are not necessarily strict. Dualizing this flag of $\mathbb{F}_p$-vector spaces, we obtain a flag

$$(0) = (C^*)_{-1} \subset (C^*)_0 \subset (C^*)_1 \subset \dots$$

of $\mathbb{F}_p$-subspaces of C^*, where

$$(C^*)_i := \{\chi \in C^* \mid \chi \text{ is trivial on } C_i\} \simeq (C/C_i)^*.$$

Let $\mathrm{Ass}(C) \subset C^*$ be the set of characters of C associated to irreducible representations of G, and let $\mathrm{Ass}_i(C)$ be the set of characters associated to irreducible representations of dimension p^i. Lemma 2.2(b) tells us that

$$\mathrm{Ass}_0(C) \cup \mathrm{Ass}_1(C) \cup \dots \cup \mathrm{Ass}_i(C) \text{ spans } (C^*)_i$$

for every $i \geq 0$. Hence, we can choose a basis $\chi_1, \dots, \chi_{\Delta_0}$ of $(C^*)_0$ from $\mathrm{Ass}_0(C)$, then complete it to a basis $\chi_1, \dots, \chi_{\Delta_1}$ of $(C^*)_1$ by choosing the last $\Delta_1 - \Delta_0$ characters from $\mathrm{Ass}_1(C)$, then complete this basis of $(C^*)_1$ to a basis of $(C^*)_2$ by choosing $\Delta_2 - \Delta_1$ additional characters from $\mathrm{Ass}_2(C)$, etc. We stop when $C_i = (0)$, i.e., $\Delta_i = \dim_{\mathbb{F}_p} C$.

By the definition of $\mathrm{Ass}_i(C)$, each χ_j is the associated character of some irreducible representation μ_j of G. By our construction

$$\mu = \mu_1 \oplus \dots \oplus \mu_{\dim_{\mathbb{F}_p}(C)}$$

has the desired properties. Indeed, since $\chi_1, \dots, \chi_{\dim_{\mathbb{F}_p}(C)}$ form a basis of C^*, Lemma 2.3 tells us that μ is faithful. On the other hand, by our construction exactly

$$\delta_i - \delta_{i-1} = \dim_{\mathbb{F}_p} C_i^* - \dim_{\mathbb{F}_p} C_{i-1}^* = \dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i$$

of the characters $\chi_1, \dots, \chi_c$ come from $\mathrm{Ass}_i(C)$. Equivalently, exactly

$$\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C$$

of the irreducible representations $\mu_1, \dots, \mu_c$ are of dimension p^i.

Step 2: Let $\rho\colon G \to \mathrm{GL}(V)$ be a faithful linear representation of G of the smallest possible dimension,

$$\rho = \rho_1 \oplus \dots \oplus \rho_c$$

be its irreducible decomposition, and $\chi_i\colon C \to \mathbb{G}_m$ be the character associated to ρ_i. By Lemma 2.3(b), $\chi_1, \dots, \chi_c$ form a basis of C^*. In particular,

$c = \dim_{\mathbb{F}_p} C$ and at most $\dim_{\mathbb{F}_p} C - \dim_{\mathbb{F}_p} C_i$ of the characters $\chi_1, \ldots, \chi_c$ can vanish on C_i. On the other hand, by Lemma 2.2(b) every representation of dimension $\leq p^i$ vanishes on C_i. Thus if exactly d_i of the irreducible representations $\rho_1, \ldots, \rho_c$ have dimension p^i then

$$d_0 + d_1 + d_2 + \ldots + d_i \leq \dim_{\mathbb{F}_p} C - \dim_{\mathbb{F}_p} C_i$$

for every $i \geq 0$. For $i \geq 0$, set $D_i := d_0 + \cdots + d_i =$ number of representations of dimension $\leq p^i$ among $\rho_1, \ldots, \rho_c$. We can now write the above inequality as

$$D_i \leq \Delta_i \text{ for every } i \geq 0. \tag{5}$$

Our goal is to show that $\dim(\rho) \geq \dim(\mu)$ and that equality holds if and only if exactly δ_i of the irreducible representations $\rho_1, \ldots, \rho_{\dim_{\mathbb{F}_p}(C)}$ have dimension p^i. The last condition translates into $d_i = \delta_i$ for every $i \geq 0$, which is, in turn equivalent to $D_i = \Delta_i$ for every $i \geq 0$.

Indeed, setting $D_{-1} := 0$ and $\Delta_{-1} := 0$, we have,

$$\begin{aligned}\dim(\rho) - \dim(\mu) = \sum_{i=0}^{\infty}(d_i - \delta_i)p^i = \sum_{i=0}^{\infty}(D_i - \Delta_i)p^i - \sum_{i=0}^{\infty}(D_{i-1} - \Delta_{i-1})p^i \\ = \sum_{i=0}^{\infty}(D_i - \Delta_i)(p^i - p^{i+1}) \geq 0\,,\end{aligned}$$

where the last inequality follows from (5). Moreover, equality holds if and only if $D_i = \Delta_i$ for every $i \geq 0$, as claimed. This completes the proof of Step 2 and thus of Theorem 1.2. □

3. Proof of Theorem 1.3

Since $K_0 = G'$ is a non-trivial normal subgroup of G, we see that $K_0 \cap C(G)$ and thus $C_0 = K_0 \cap C(G)_p$ is non-trivial. This means that in the summation formula of Theorem 1.2(b) at least one of the terms

$$(\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i)p^i$$

with $i \geq 1$ will be non-zero. Hence, $\mathrm{ed}_k(G) \geq p$; this shows that (a) and (b) are equivalent. Moreover, equality holds if and only if (i) $\dim_{\mathbb{F}_p} C_{-1} = 1$, (ii) $\dim_{\mathbb{F}_p} C_0 = 1$ and (iii) C_1 is trivial. Since we are assuming $K_0 = G' \neq \{1\}$ and hence, $C_0 = K_0 \cap C(G)_p \neq \{1\}$ by (4), (ii) follows from (i) and thus can be dropped.

It now suffices to prove that (i) and (iii) are equivalent to condition (c) of the theorem. Since $C_{-1} = C(G)_p$, (i) is equivalent to $C(G)$ being cyclic. On the other hand, (iii) means that

$$K_1 = \bigcap_{[G:H]=p} H' \tag{6}$$

intersects $C(G)_p$ trivially. Since K_1 is a normal subgroup of G, (4) tells us that (iii) holds if and only if $K_1 = \{1\}$.

It remains to show that $K_1 = \{1\}$ if and only if $H' = \{1\}$ for some subgroup H of G of index p. One direction is obvious: if $H' = \{1\}$ for some H of index p then the intersection (6) is trivial. To prove the converse, assume the contrary: the intersection (6) is trivial but $H' \neq \{1\}$ for every subgroup H of index p. Since every such H is normal in G (and so is H'), (4) tells us that that $H' \neq \{1\}$ if and only if $H' \cap C(G) \neq \{1\}$. Since $C(G)$ is cyclic, the latter condition is equivalent to $C(G)_p \subset H'$. Thus

$$C(G)_p \subset K_1 = \bigcap_{[G:H]=p} H' ,$$

contradicting our assumption that $K_1 = \{1\}$.

To sum up, we have shown that (c) is equivalent to conditions (i) and (iii) above, and that these conditions are in turn, equivalent to (a) (or to (b)). This completes the proof of Theorem 1.3.

Remark 3.1. p-groups that have a faithful representation of degree p over a field k, satisfying (1) are described in [LG-P, II.4, III.4, IV.2]; see also [Vo]. Combining this description with Theorem 1.1 yields the following variant of Theorem 1.3.

Let k be a field satisfying (1) *and G be a p-group such that $G' \neq \{1\}$. Then the following conditions are equivalent:*

(a) $\mathrm{ed}_k(G) \leq p$,

(b) $\mathrm{ed}_k(G) = p$,

(c) G is isomorphic to a subgroup of $\mathbb{Z}/p^\alpha \wr \mathbb{Z}/p = (\mathbb{Z}/p^\alpha)^p \rtimes \mathbb{Z}/p$, for some $\alpha \geq 1$ such that k contains a primitive root of unity of degree p^α. □

4. Proof of Theorems 1.4 and 1.5

Proof of Theorem 1.4. Since the commutator $K_0 = [G, G]$ is central, $C_0 = K_0 \cap C(G)_p$ is of dimension $\mathrm{rank}\,[G, G]$ and the p^0 term in the formula of Theorem 1.2 is $(\mathrm{rank}\, C(G) - \mathrm{rank}\,[G, G])$.

Let $Q = G/C(G)$ which is abelian by assumption. Let $h_1, ..., h_s$ be generators of $[G, G]$, where $s = \mathrm{rank}\,[G, G]$, so that

$$[G, G] = \mathbb{Z}/p^{e_1} h_1 \oplus \cdots \oplus \mathbb{Z}/p^{e_1} h_1 ,$$

written additively. For $g_1, g_2 \in G$ the commutator can then be expressed as

$$[g_1, g_2] = \beta_1(g_1, g_2)h_1 + \ldots + \beta_s(g_1, g_2)h_s .$$

Note that each $\beta_i(g_1, g_2)$ depends on g_1, g_2 only modulo the center $C(G)$. Thus each β_i descends to a skew-symmetric bilinear form

$$Q \times Q \to \mathbb{Z}/p^{e_i}$$

which, by a slight abuse of notation, we will continue to denote by β_i. Let p^m be the order of Q. For each form β_i there is an isotropic subgroup Q_i of Q of order at least $p^{\lfloor (m+1)/2 \rfloor}$ (or equivalently, of index at most $p^{\lfloor m/2 \rfloor}$ in Q); see [AT, Corollary 3]. Pulling these isotropic subgroups back to G, we obtain

subgroups $G_1, \ldots, G_s$ of G of index $\leq p^{\lfloor m/2 \rfloor}$ with the property that $G_i' = [G_i, G_i]$ lies in the subgroup of $C(G)$ generated by $h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_s$. In particular, $G_1' \cap \cdots \cap G_s' = \{1\}$. Thus, all K_i (and hence, all C_i) in (3) are trivial for $i \geq \lfloor m/2 \rfloor$, and Theorem 1.2 tells us that

$$\mathrm{ed}_k(G) = \dim_{\mathbb{F}_p} C_{-1} - \dim_{\mathbb{F}_p} C_0 + \sum_{j=1}^{\lfloor m/2 \rfloor} (\dim_{\mathbb{F}_p} C_{j-1} - \dim_{\mathbb{F}_p} C_j) p^j \leq$$

$$\dim_{\mathbb{F}_p} C_{-1} - \dim_{\mathbb{F}_p} C_0 + \sum_{j=1}^{\lfloor m/2 \rfloor} (\dim_{\mathbb{F}_p} C_{j-1} - \dim_{\mathbb{F}_p} C_j) \cdot p^{\lfloor m/2 \rfloor} =$$

$$\mathrm{rank}\ C(G) + \mathrm{rank}\ [G,G](p^{\lfloor m/2 \rfloor} - 1)\,.$$

(b) In general, the skew-symmetric bilinear forms β_i may be degenerate. However, if $[G, G]$ is cyclic, i.e., $s = 1$, then we have only one form, β_1, which is easily seen to be non-degenerate. For notational simplicity, we will write β instead of β_1. To see that β is non-degenerate, suppose $\overline{g} := g$ (modulo $C(G)$) lies in the kernel of β for some $g \in G$. Then by definition

$$\beta(g, g_1) = g g_1 g^{-1} g_1^{-1} = 1$$

for every $g_1 \in G$. Hence, g is central in G, i.e., $\overline{g} = 1$ in $Q = G/C(G)$, as claimed.

We conclude that the order of $Q = G/C(G)$ is a perfect square, say p^{2i}, and Q contains a maximal isotropic subgroup $I \subset Q$ of order $p^i = \sqrt{|G/C(G)|}$; see [AT, Corollary 4]. The preimage of I in G is a maximal abelian subgroup of index p^i. Consequently, $K_0 = [G, G], K_1, \ldots, K_{i-1}$ are all of rank 1 and K_i is trivial, where $p^i = \sqrt{|G/C(G)|}$. Moreover, since all of these groups lie in $[G, G]$ and hence, are central, we have $C_i = (K_i)_p$ and thus

$$\dim_{\mathbb{F}_p}(C_0) = \dim_{\mathbb{F}_p}(C_1) = \ldots = \dim_{\mathbb{F}_p}(C_{i-1}) = 1 \text{ and } \dim_{\mathbb{F}_p}(C_i) = 0\,.$$

Specializing the formula of Theorem 1.4 to this situation, we obtain part (b). □

Proof of Theorem 1.5. Let Γ be the non-abelian group of order p^3 given by generators x, y, z and relations $x^p = y^p = z^p = [x, z] = [y, z] = 1$, $[x, y] = z$. Choose a multiplicative character $\chi\colon H \to k^*$ of the subgroup $A = \langle x, z \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^2$ which is non-trivial on the center $\langle z \rangle$ of Γ and consider the p-dimensional induced representation $\mathrm{Ind}_A^\Gamma(\chi)$. Since the center $\langle z \rangle$ of Γ does not lie in the kernel of $\mathrm{Ind}_A^\Gamma(\chi)$, we conclude that $\mathrm{Ind}_A^\Gamma(\chi)$ is faithful. Thus we have constructed a faithful p-dimensional representation of Γ defined over k. Consequently

$$\mathrm{ed}_k(\Gamma) \leq p\,. \tag{7}$$

Taking the direct sum of n copies of this representation, we obtain a faithful representation of Γ^n of dimension np. Thus for any $n \geq 1$ we have

$$\operatorname{ed}_k \Gamma^n \leq np\,. \tag{8}$$

(We remark that both (7) and (8) are in fact equalities. Indeed, if ζ_{p^2} is a primitive root of unity of degree p^2 then

$$\operatorname{ed}_k(\Gamma) \geq \operatorname{ed}_{k(\zeta_{p^2})}(\Gamma) = \sqrt{p^2} + 1 - 1 = p\,,$$

where the middle equality follows from Theorem 1.4(b). Hence, we have $\operatorname{ed}_k(\Gamma) = p$. Moreover, by [KM, Theorem 5.1], $\operatorname{ed}_k \Gamma^n = n \cdot \operatorname{ed}_k(\Gamma) = np$. However, we will only need the upper bound (8) in the sequel.)

The center of Γ is $\langle z \rangle$; denote it by C. The center of Γ^n is then isomorphic to C^n. Let H_n be the subgroup of C^n consisting of n-tuples $(c_1, \dots, c_n)$ such that $c_1 \cdots c_n = 1$. The center $C(\Gamma^n/H_n)$ of Γ^n/H_n is clearly cyclic of order p (it is generated by the class of the element $(z, 1, \dots, 1)$ modulo H_n), and the commutator $[\Gamma^n/H_n, \Gamma^n/H_n]$ is central. Hence,

$$\operatorname{ed}_k(\Gamma^n/H_n) \geq \operatorname{ed}_{k(\zeta^2)}(\Gamma^n/H_n) = \sqrt{p^{2n}} + 1 - 1 = p^n\ , \tag{9}$$

where the middle equality follows from Theorem 1.4(b). Setting $G = \Gamma^n$ and $H = H_n$, and comparing (8) with (9), we see that the desired inequality $\operatorname{ed}_k(G/H) > \lambda \operatorname{ed}_k(G)$ holds for suitably large n. □

5. Proof of Theorem 1.6

Recall that the essential dimension of the group $\mathrm{GL}_n(\mathbb{Z})$ over a field k, or $\operatorname{ed}_k(\mathrm{GL}_n(\mathbb{Z}))$ for short, is defined as the essential dimension of this functor

$$H^1(*, \mathrm{GL}_n(\mathbb{Z}))\colon K \to \{K\text{-isomorphism classes of } n\text{-dimensional } K\text{-tori}\}\,,$$

where K/k is a field extension. Similarly $\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z}))$ is defined as the essential dimension of the functor

$$H^1(*, \mathrm{SL}_n(\mathbb{Z}))\colon K \to \{K\text{-isomorphism classes of } n\text{-dimensional } K\text{-tori with } \phi_T \subset \mathrm{SL}_n(\mathbb{Z})\ \}\,,$$

where $\phi_T\colon \mathrm{Gal}(K) \to \mathrm{GL}_n(\mathbb{Z})$ is the natural representation of the Galois group of K on the character lattice of T. The essential dimensions $\operatorname{ed}_k(\mathrm{GL}_n(\mathbb{Z}); p)$ and $\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z}); p)$ are respectively the essential dimensions of the above functors at a prime p.

G. Favi and M. Florence [FF] showed that for $\Gamma = \mathrm{GL}_n(\mathbb{Z})$ or $\mathrm{SL}_n(\mathbb{Z})$,

$$\operatorname{ed}_k(\Gamma) = \max\{\operatorname{ed}_k(F) | F \text{ finite subgroup of } \Gamma\}. \tag{10}$$

From this they deduced that

$$\operatorname{ed}_k(\mathrm{GL}_n(\mathbb{Z})) = n, \quad \text{and} \quad \operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z})) = \begin{cases} n-1, \text{ if } n \text{ is odd,} \\ n-1 \text{ or } n, \text{ if } n \text{ is even.} \end{cases}$$

For details, see [FF, Theorem 5.4].

Favi and Florence also proved that $\operatorname{ed}_k(\mathrm{SL}_2(\mathbb{Z})) = 1$ if k contains a primitive 12th root of unity and asked whether $\operatorname{ed}_k(\mathrm{SL}_n(\mathbb{Z})) = n-1$ or n in the

case where $n \geq 4$ is even; see [FF, Remark 5.5]. In this section we will prove Theorem 1.6 which shows that the answer is always n.

A minor modification of the arguments in [FF] shows that (10) holds also for essential dimension at a prime p:

$$\mathrm{ed}_k(\Gamma; p) = \max\{\mathrm{ed}_k(F; p) | F \text{ a finite subgroup of } \Gamma\}, \tag{11}$$

where $\Gamma = \mathrm{GL}_n(\mathbb{Z})$ or $\mathrm{SL}_n(\mathbb{Z})$. The finite groups F that Florence and Favi used to find the essential dimension of $\mathrm{GL}_n(\mathbb{Z})$ and $\mathrm{SL}_n(\mathbb{Z})$ (n odd) are $(\mathbb{Z}/2\mathbb{Z})^n$ and $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ respectively. Thus $\mathrm{ed}_k(\mathrm{GL}_n(\mathbb{Z}); 2) = \mathrm{ed}_k(\mathrm{GL}_n(\mathbb{Z})) = n$ for every $n \geq 1$ and $\mathrm{ed}_k(\mathrm{SL}_n(\mathbb{Z}); 2) = \mathrm{ed}_k(\mathrm{SL}_n(\mathbb{Z})) = n - 1$ if n is odd.

Our proof of Theorem 1.6 will rely on part (b) of the following easy corollary of Theorem 1.2.

Corollary 5.1. *Let G be a p-group, and k be as in* (1).

(a) If $C(G)_p \subset K_i$ then $\mathrm{ed}_k(G)$ is divisible by p^{i+1}.

(b) If $C(G)_p \subset G'$ then $\mathrm{ed}_k(G)$ is divisible by p.

(c) If $C(G)_p \subset G^{(i)}$, where $G^{(i)}$ denotes the ith derived subgroup of G, then $\mathrm{ed}_k(G)$ is divisible by p^i.

Proof. (a) $C(G)_p \subset K_i$ implies $C_{-1} = C_0 = \cdots = C_i$. Hence, in the formula of Theorem 1.2(b) the $p^0, p^1, \ldots, p^i$ terms appear with coefficient 0. All other terms are divisible by p^{i+1}, and part (a) follows.

(b) is an immediate consequence of (a), since $K_0 = G'$.

(c) By [H, Theorem V.18.6] $G^{(i)}$ is contained in the kernel of every p^{i-1}-dimensional representation of G. Lemma 2.1 now tells us that $G^{(i)} \subset K_{i-1}$ and part (c) follows from part (a). □

Proof of Theorem 1.6. We assume that $n = 2d \geq 4$ is even. To prove Theorem 1.6 it suffices to find a 2-subgroup F of $\mathrm{SL}_n(\mathbb{Z})$ of essential dimension n.

Diagonal matrices and permutation matrices generate a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ isomorphic to $\mu_2^n \rtimes \mathrm{S}_n$. The determinant function restricts to a homomorphism

$$\det\colon \mu_2^n \rtimes \mathrm{S}_n \to \mu_2$$

sending $((\epsilon_1, \ldots, \epsilon_n), \tau)) \in \mu_2^n \rtimes \mathrm{S}_n$ to the product $\epsilon_1\epsilon_2 \cdots \epsilon_n \cdot \mathrm{sign}(\tau)$. Let P_n be a Sylow 2-subgroup of S_n and F_n be the kernel of $\det\colon \mu_2^n \rtimes P_n \to \mu_2$. By construction F_n is a finite 2-group contained in $\mathrm{SL}_n(\mathbb{Z})$. Theorem 1.6 is now a consequence of the following proposition.

Proposition 5.2. *If $\mathrm{char}(k) \neq 2$ then $\mathrm{ed}_k(F_{2d}) = 2d$ for any $d \geq 2$.*

To prove the proposition, let

$$D_{2d} = \{\mathrm{diag}(\epsilon_1, \ldots, \epsilon_{2d}) \,|\, \text{each } \epsilon_i = \pm 1 \text{ and } \epsilon_1\epsilon_2 \cdots \epsilon_{2d} = 1\}$$

be the subgroup of "diagonal" matrices contained in F_{2d}.

Since $D_{2d} \simeq \mu_2^{2d-1}$ has essential dimension $2d-1$, we see that $\mathrm{ed}_k(F_{2d}) \geq \mathrm{ed}_k(D_{2d}) = 2d - 1$. On the other hand the inclusion $F_{2d} \subset \mathrm{SL}_{2d}(\mathbb{Z})$ gives

rise to a $2d$-dimensional representation of F_{2d}, which remains faithful over any field k of characteristic $\neq 2$. Hence, $\mathrm{ed}_k(F_{2d}) \leq 2d$. We thus conclude that

$$\mathrm{ed}_k(F_{2d}) = 2d - 1 \text{ or } 2d. \tag{12}$$

Using elementary group theory, one easily checks that

$$C(F_{2d}) \subset [F_{2d}, F_{2d}] \subset F'_{2d}\,. \tag{13}$$

Thus, if $k' \supset k$ is a field as in (1), $\mathrm{ed}_{k'}(F_{2d})$ is even by Corollary 5.1; since $\mathrm{ed}_k(F_{2d}) \geq \mathrm{ed}_{k'}(F_{2d})$, (12) now tells us that $\mathrm{ed}_k(F_{2d}) = 2d$. This completes the proof of Proposition 5.2 and thus of Theorem 1.6. □

Remark 5.3. The assumption that $d \geq 2$ is essential in the proof of the inclusion (13). In fact, $F_2 \simeq \mathbb{Z}/4\mathbb{Z}$, so (13) fails for $d = 1$.

Remark 5.4. Note that for any integers $m, n \geq 2$, F_{m+n} contains the direct product $F_m \times F_n$. Thus

$$\mathrm{ed}_k(F_{m+n}) \geq \mathrm{ed}_k(F_m \times F_n) = \mathrm{ed}_k(F_m) + \mathrm{ed}_k(F_n)\,,$$

where the last equality follows from [KM, Theorem 5.1]. Thus Proposition 5.2 only needs to be proved for $d = 2$ and 3 (or equivalently, $n = 4$ and 6); all other cases are easily deduced from these by applying the above inequality recursively, with $m = 4$. In particular, the group-theoretic inclusion (13) only needs to be checked for $d = 2$ and 3. Somewhat to our surprise, this reduction does not appear to simplify the proof of Proposition 5.2 presented above to any significant degree.

Remark 5.5. It is interesting to note that while the value of $\mathrm{ed}_k(\mathrm{SL}_2(\mathbb{Z}))$ depends on the base field k (see [FF, Remark 5.5]), for $n \geq 3$, the value of $\mathrm{ed}_k(\mathrm{SL}_n(\mathbb{Z}))$ does not (as long as $\mathrm{char}(k) \neq 2$).

References

[AT] A. Amitsur, J.-P. Tignol, *Symplectic modules*, Israel J. Math. **54** (1986), 267-290.

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

[BRV$_1$] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension and algebraic stacks*, 2007, `arXiv:math/0701903v1 [math.AG]`.

[BRV$_2$] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension, spinor groups and quadratic forms*, 10 pages, Annals of Math. **171** (2010), no. 1, 533–544.

[BuR] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159-179.

[FF] G. Favi, M. Florence, *Tori and essential dimension*, J. Algebra, **319** (2008), no. 9, 3885-3900.

[H] B. Huppert, Endliche Gruppen. I, Die Grundlehren der Mathematischen Wissenschaften, **134** Springer-Verlag, 1967.

[JLY] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002, Constructive aspects of the inverse Galois problem.

[KM] N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite p-groups*, Inventiones Math., **172**, no. 3 (2008), pp. 491-508.

[LG-P] C. R. Leedham-Green, W. Plesken, *Some remarks on Sylow subgroups of general linear groups*, Math. Z. **191** (1986), no. 4, 529–535.

[Lo] R. Lötscher, *Application of multihomogeneous covariants to the essential dimension of finite groups*, `http://arxiv.org/PS_cache/arxiv/pdf/0811/0811.3852v1.pdf`

[Na] T. Nakayama, *Finite groups with faithful irreducible and directly indecomposable modular representations*, Proc. Japan Acad. **23** (1947), no. 3, 22–25.

[Me] A. Merkurjev, *Essential dimension*, in Quadratic forms – algebra, arithmetic, and geometry (R. Baeza, W.K. Chan, D.W. Hoffmann, and R. Schulze-Pillot, eds.), Contemporary Mathematics **493** (2009), 299–326.

[Re] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.

[Se] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, **42**. Springer-Verlag, New York–Heidelberg, 1977.

[Ta] M. Tazawa, *Über die isomorphe Darstellung der endliehen Gruppe*, Tôhoku Math. J. **47** (1940), 87–93.

[Vo] R. T. Vol'vacev, *Sylow p-subgroups of the full linear group* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963), 1031–1054.

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada