Essential Dimension in Mixed Characteristic

Patrick Brosnan, Zinovy Reichstein, Angelo Vistoli

Received: July 11, 2018
Revised: October 3, 2018

Communicated by Nikita Karpenko

Abstract. Let G be a finite group, and let R be a discrete valuation ring with residue field k and fraction field K. We say that G is weakly tame at a prime p if it has no non-trivial normal p-subgroups. By convention, every finite group is weakly tame at 0. Using this definition, we show that if G is weakly tame at $\operatorname{char}(k)$, then $\operatorname{ed}_K(G) \geqslant \operatorname{ed}_k(G)$. Here $\operatorname{ed}_F(G)$ denotes the essential dimension of G over the field F. We also prove a more general statement of this type, for a class of étale gerbes $\mathscr{X}$ over R.

As a corollary, we show that if G is weakly tame at p, then $\operatorname{ed}_L(G) \geqslant \operatorname{ed}_k(G)$ for any field L of characteristic 0 and any field k of characteristic p, provided that k contains $\overline{\mathbb{F}}_p$. We also show that a conjecture of A. Ledet, asserting that $\operatorname{ed}_k(\mathbb{Z}/p^n\mathbb{Z}) = n$ for a field k of characteristic $p > 0$ implies that $\operatorname{ed}_{\mathbb{C}}(G) \geqslant n$ for any finite group G which is weakly tame at p and contains an element of order p^n. We give a number of examples, where an unconditional proof of the last inequality is out of the reach of all presently known techniques.

2010 Mathematics Subject Classification: 14A20, 13A18, 13A50
Keywords and Phrases: Essential dimension, Ledet's conjecture, genericity theorem, gerbe, mixed characteristic

1. Introduction

Let R be a discrete valuation ring with residue field k and fraction field K, and let G be a finite group. In this paper we will compare $\operatorname{ed}_K(G)$ and $\operatorname{ed}_k(G)$. More generally, we will compare $\operatorname{ed}_K(\mathscr{X})$ to $\operatorname{ed}_k(\mathscr{X})$ for an étale gerbe $\mathscr{X}$ over R. For an overview of the theory of essential dimension, we refer the reader to [BRV11, Mer13, Rei10].

To state our main result, we will need some definitions. Suppose S is a scheme. By an *étale gerbe* $\mathscr{X} \to S$ we mean an algebraic stack that is a gerbe in the étale topology on S. Furthermore, we will always assume that there exists an étale covering $\{S_i \to S\}$, such that the pullback $\mathscr{X}_{S_i}$ is of the form $\mathscr{B}_{S_i}G_i$, where $G_i \to S_i$ is a finite étale group scheme.

We say that a finite group G is *tame* (resp. *weakly tame*) at a prime number p if $p \nmid |G|$ (resp. G contains no non-trivial normal p-subgroup). Equivalently, G is tame at p if the trivial group is the (unique) p-Sylow subgroup of G, and G is weakly tame at p if the intersection of all p-Sylow subgroups of G is trivial. By convention we say that every finite group is both tame and weakly tame at 0. [1]

By a geometric point of S, we mean a morphism $\operatorname{Spec}\Omega \to S$ with Ω an algebraically closed field. We say that a finite étale group scheme G over S is *tame* (resp. *weakly tame*) if, for every geometric point $\operatorname{Spec}\Omega \to S$, the group $G(\Omega)$ is tame (resp. weakly tame) at $\operatorname{char}\Omega$. Similarly, we say that an étale gerbe $\mathscr{X} \to S$ is *tame* (resp. *weakly tame*) if, for every object ξ over a geometric point $\operatorname{Spec}\Omega \to S$, the automorphism group $\operatorname{Aut}_\Omega \xi$ is tame (resp. weakly tame) at $\operatorname{char}\Omega$.

A key result of [BRV11] is the so called *Genericity Theorem* for tame Deligne–Mumford stacks, [BRV11, Theorem 6.1]. The proof of this result in [BRV11] was based on the following.

Theorem 1.1 ([BRV11, Theorem 5.11]). *Let R be a discrete valuation ring (DVR) with residue field k and fraction field K, and let*

$$\mathscr{X} \longrightarrow \operatorname{Spec} R$$

be a tame étale gerbe. Then $\operatorname{ed}_K(\mathscr{X}_K) \geqslant \operatorname{ed}_k(\mathscr{X}_k)$.

Here $\mathscr{X}_K$ and $\mathscr{X}_k$ are respectively the generic fiber and the special fiber of $\mathscr{X} \to \operatorname{Spec} R$.

Unfortunately, the proof of [BRV11, Theorem 5.11] contains an error in the case when $\operatorname{char} K = 0$ and $\operatorname{char} k > 0$. This was noticed by Amit Hogadi, to whom we are very grateful. (See Remark 6.2 for an explanation of the error.) For the applications in [BRV11] only the equicharacteristic case was needed, so this mistake in the proof of Theorem 1.1 does not affect any other results in [BRV11] (the genericity theorem, in particular). However, the assertion of Theorem 1.1 in the mixed characteristic case remained of interest to us as a way of relating essential dimension in positive characteristic to essential dimension in characteristic 0. In this paper, our main result is the following strengthened version of Theorem 1.1.

Theorem 1.2. *Let R be a DVR with residue field k and fraction field K, and let*

$$\mathscr{X} \longrightarrow \operatorname{Spec} R$$

be a weakly tame étale gerbe. Then $\operatorname{ed}_K(\mathscr{X}_K) \geqslant \operatorname{ed}_k(\mathscr{X}_k)$.

[1] By a theorem of T. Nakayama [Nak47], G is weakly tame at p if and only if G admits a faithful completely reducible representation over some (and thus every) field of characteristic p. The significance of this condition in the study of essential dimension of finite groups was first observed by R. Lötscher [Löt10]. Note that Lötscher used the term “semifaithful” in place of “weakly tame”.

In particular, [BRV11, Theorem 5.11] is valid as stated. Moreover, our new proof is considerably shorter than the one in [BRV11]. And in Sections 3-5 we will deduce some rather surprising consequences.
We will give two proofs of our main result, one for gerbes of the form where $\mathscr{X} = \mathscr{B}_R G$, where G is a (constant) finite group (Theorem 2.4) and the other for the general case. The ideas in these two proofs are closely related; the proof of Theorem 2.4 allows us to introduce these ideas in the elementary setting of classical valuation theory. A separate proof of Theorem 2.4 also makes the applications in Sections 3-5 accessible to those readers who are not familiar with, or don't care for, the language of gerbes.

Acknowledgements. Patrick Brosnan was partially supported by NSF grant DMS 1361159, Zinovy Reichstein by NSERC Discovery grant 253424-2017 and the Collaborative Research Group in Geometric and Cohomological Methods in Algebra at the Pacific Institute for the Mathematical Sciences, and Angelo Vistoli by research funds from the Scuola Normale Superiore.
The authors are grateful to the referee for a thorough reading and constructive suggestions and to Alexander Duncan and Najmuddin Fakhruddin for helpful comments.

2. Proof of Theorem 1.2 in the constant case

In this section we will prove the special case of Theorem 1.2, where $\mathscr{X} = \mathscr{B}_R G$ for G a finite group (viewed as a constant group scheme over $\operatorname{Spec} R$); see Theorem 2.4.
Throughout this section we will assume that L is a field equipped with a (surjective) discrete valuation $\nu \colon L^* \to \mathbb{Z}$ and K is a subfield of L such that $\nu(K^*) = \mathbb{Z}$. We will denote the residue fields of L and K by l and k, respectively. Similarly, we will denote the valuation rings by $\mathscr{O}_L$ and $\mathscr{O}_K$.
The following lemma is a special case of the Corollary to Theorem 1.20 in [Vaq06]. For the convenience of the reader, we supply a short proof.

Lemma 2.1. *$\operatorname{trdeg}_k(l) \leqslant \operatorname{trdeg}_K(L)$.*

Proof. Let $u_1, \dots, u_m \in l$ be algebraically independent over k. Lift each u_i to $v_i \in \mathscr{O}_L \subseteq L$. It now suffices to show that $v_1, \dots, v_m$ are algebraically independent over K. Assume the contrary: $f(v_1, \dots, v_m) = 0$ for some polynomial $0 \neq f(x_1, \dots, x_m) \in K[x_1, \dots, x_m]$. After clearing denominators we may assume that every coefficient of f lies in $\mathscr{O}_K$, and at least one of the coefficients has valuation 0. If f_0 is the image of f in $k[x_1, \dots, x_m]$ then $f_0 \neq 0$ and $f_0(u_1, \dots, u_m) = 0$. This contradicts our assumption that $u_1, \dots, u_m$ are algebraically independent over k. ♠

Let $L_m = \nu^{-1}(m) \cup \{0\}$ and $L_{\geqslant m} = \bigcup_{j \geqslant m} L_j$. Note that, by definition, $L_{\geqslant 0} = \mathscr{O}_L$ is the valuation ring of ν, $L_{\geqslant 1}$ is the maximal ideal, and $L_{\geqslant 0}/L_{\geqslant 1} = l$ is the residue field.

LEMMA 2.2. *Assume that g is an automorphism of L of finite order $d \geqslant 1$ preserving the valuation ν. Let $p = \operatorname{char}(l) \geqslant 0$. If g induces a trivial automorphism on both $L_{\geqslant 0}/L_{\geqslant 1}$ and $L_{\geqslant 1}/L_{\geqslant 2}$, then*

(a) $d = 1$ (i.e., $g = \mathrm{id}$ is the identity automorphism) if $p = 0$, and

(b) d is a power of p, if $p > 0$.

Part (a) is proved in [BR97, Lemma 5.1]; a minor variant of the same argument also proves (b). Alternatively, with some additional work, Lemma 2.2 can be deduced from [ZS58, Theorem 25, p. 295]. For the reader's convenience we will give a short self-contained proof below.

Proof. In case (b), write $d = mp^r$, where m is not divisible by p. After replacing g by g^{p^r}, we may assume that d is prime to p. In both parts we need to conclude that g is the identity.
Let G be the cyclic group generated by g; then G is linearly reductive. Since the action of G on l is trivial, the induced action on $L_{\geqslant i}/L_{\geqslant i+1}$ is l-linear. Furthermore, let $t \in L_1$ be a uniformizing parameter. By our assumption $g(t) = t \pmod{L_{\geqslant 2}}$. Thus multiplication by t^{i-1} induces the l-linear G-equivariant isomorphism $(L_{\geqslant 1}/L_{\geqslant 2})^{\otimes i} \simeq L_{\geqslant i}/L_{\geqslant i+1}$. Consequently, G acts trivially on $L_{\geqslant i}/L_{\geqslant i+1}$ for all $i \geqslant 0$. Since G is linearly reductive, from the exact sequence

$$0 \longrightarrow L_{\geqslant i}/L_{\geqslant i+1} \longrightarrow L_{\geqslant 0}/L_{\geqslant i+1} \longrightarrow L_{\geqslant 0}/L_{\geqslant i} \longrightarrow 0$$

we deduce, by induction on i, that G acts trivially on $L_{\geqslant 0}/L_{\geqslant i}$ for every $i \geqslant 1$. Since $\bigcap_{i \geqslant 0} L_{\geqslant i} = 0$, this implies that the action of G on $L_{\geqslant 0}$ is trivial. But $L_{\geqslant 0}$ is a domain with quotient field L, so G also acts trivially on L. Since G acts faithfully on L, we conclude that $G = \{1\}$, and the lemma follows. ♠

PROPOSITION 2.3. *Consider a faithful action of a finite group G on L, such that G preserves ν and acts trivially on K. Let Δ be the kernel of the induced G-action on l. Then $\Delta = \{1\}$ if $\operatorname{char}(k) = 0$ and Δ is a p-subgroup if $\operatorname{char}(k) = p$.*

Proof. Assume the contrary. Then we can choose an element $g \in \Delta$ of prime order q, such that $q \neq \operatorname{char}(k)$. Let M be the maximal ideal of the valuation ring $\mathscr{O}_L$. Since we are assuming that $\nu(K^*) = \nu(L^*) = \mathbb{Z}$, we can choose a uniformizing parameter $t \in K$ for ν. Since $g \in \Delta$, g acts trivially on both $l = \mathscr{O}_L/M$ and $M/M^2 = l \cdot t$. By Lemma 2.2, g acts trivially on L. This contradicts our assumption that G acts faithfully on L. ♠

We are now ready to prove the main result of this section.

THEOREM 2.4. *Let (R, ν) be a discrete valuation ring with residue field k and fraction field K, and G be a finite group. If $p = \operatorname{char}(k) > 0$, assume that G is weakly tame at p. Then $\operatorname{ed}_K(G) \geqslant \operatorname{ed}_k(G)$.*

Proof. Set $d \overset{\text{def}}{=} \operatorname{ed}_K(G)$. Let $R[G]$ be the group algebra of G and let $V_R = (\mathbb{A}_R)^{|G|}$ denote the corresponding R-scheme equipped with the (left) regular action of G. By definition d is the minimal transcendence degree $\operatorname{trdeg}_K(L)$, where L ranges over G-invariant intermediate subfields $K \subset L \subset K(V_K)$ such that the G-action on L is faithful; see [BR97]. Choose a G-invariant intermediate subfield L such that $\operatorname{trdeg}_K(L) = d$.

We will now construct a G-invariant intermediate subfield $k \subset l \subset k(V_k)$, where V_k is the regular representation of G over k, as follows. Lift the given valuation $\nu\colon K^* \to \mathbb{Z}$ to the purely transcendental extension $K(V_K)$ of K in the obvious way. That is, $\nu : K(V_K)^* \to \mathbb{Z}$ is the divisorial valuation corresponding to the fiber of V_R over the closed point in $\operatorname{Spec} R$. The residue field of $K(V_K)$ is then $k(V_k)$. By restriction, ν is a valuation on L with $\nu(L^*) = \mathbb{Z}$. Let l be the residue field of L. Clearly $k \subset l \subset k(V_k)$ and ν is invariant under G. By Proposition 2.3, G acts faithfully on l. Moreover, by Lemma 2.1, $\operatorname{trdeg}_k(l) \leqslant d$. Thus $\operatorname{ed}_k(G) \leqslant d = \operatorname{ed}_K(G)$, as desired. ♠

3. Examples illustrating Theorem 2.4 and a simple application

Example 3.1. The following example shows that Theorem 2.4 fails if we do not assume that G is weakly tame. Choose R so that $\operatorname{char} K = 0$, $\operatorname{char} k = p > 0$, and K contains a p^2-th root of 1. Let $G = C_{p^2}$ be the cyclic group of order p^2. Since K contains a primitive p^2-th root of 1, $\operatorname{ed}_K(G) = \operatorname{ed}_K(\mathrm{C}_{p^2}) = 1$. On the other hand, $\operatorname{ed}_k(G) = \operatorname{ed}_k(\mathrm{C}_{p^2}) = 2$; this is a special (known) case of Ledet's conjecture, see Remark 4.2.

Example 3.2. Here is an example showing that Theorem 2.4 fails if we do not assume that R is a DVR. Let $R \subseteq \mathbb{C}[\![t]\!]$ be the subring consisting of power series in t whose constant term is real. Then R is a one-dimensional complete Noetherian local ring with quotient field $K = \mathbb{C}(\!(t)\!)$ and residue field $k = \mathbb{R}$, but not a DVR. Letting $G = C_4$ be the cyclic group of order 4, we see that in this situation $\operatorname{ed}_K(G) = \operatorname{ed}_{\mathbb{C}(\!(t)\!)}(\mathrm{C}_4) = 1$, while $\operatorname{ed}_k(G) = \operatorname{ed}_{\mathbb{R}}(\mathrm{C}_4) = 2$; see [BF03, Theorem 7.6].

Example 3.3. (cf. [Tos17, Remark 4.5(ii)]) This example shows that essential dimension is not semicontinuous in any reasonable sense, even in characteristic 0. Consider the scheme

$$S \stackrel{\text{def}}{=} \operatorname{Spec} \mathbb{Q}[u,x]/(x^2-u)\,.$$

The embedding $\mathbb{Q}[u] \subseteq \mathbb{Q}[u,x]/(x^2-u)$ gives a finite map $S \to \mathbb{A}^1_{\mathbb{Q}}$. If p is an odd prime, the inverse image of the prime $(u-p) \subseteq \mathbb{Q}[u]$ in S consists of a point s_p with residue field $k(s_p) = \mathbb{Q}(\sqrt{p}) = \mathbb{Q}[x]/(x^2-p)$. Then $\operatorname{ed}_{\mathbb{Q}(\sqrt{p})}(\mathrm{C}_4) = 1$ if -1 is a square modulo p, and $\operatorname{ed}_{\mathbb{Q}(\sqrt{p})}(\mathrm{C}_4) = 2$ if -1 is not a square modulo p; once again, see [BF03, Theorem 7.6]. Equivalently, $\operatorname{ed}_{\mathbb{Q}(\sqrt{p})}(\mathrm{C}_4) = 1$ if $p \equiv 1 \pmod 4$, and $\operatorname{ed}_{\mathbb{Q}(\sqrt{p})}(\mathrm{C}_4) = 2$ is $p \equiv 3 \pmod 4$. We conclude that the set of points $s \in S$ with $\operatorname{ed}_{k(s)}(\mathrm{C}_4) = 1$ is dense in S, and likewise for the set of points $s \in S$ with $\operatorname{ed}_{k(s)}(\mathrm{C}_4) = 2$ is also dense in S.

We conclude this section with an easy corollary of Theorem 2.4.

Corollary 3.4. *Let p be a prime, G a finite group weakly tame at p. Then*

(a) (cf. [Tos17, Corollary 4.2]*)* $\operatorname{ed}_{\mathbb{Q}}(G) \geqslant \operatorname{ed}_{\mathbb{F}_p}(G)$.

(b) If K is a field of characteristic 0 *and k a field of characteristic p containing $\overline{\mathbb{F}}_p$, then* $\mathrm{ed}_K(G) \geqslant \mathrm{ed}_k(G)$.

Proof. (a) follows directly from Theorem 2.4 by taking R to be the localization of the ring of integers $\mathbb{Z}$ at a prime ideal $p\mathbb{Z}$.
(b) Let $\overline{K}$ be the algebraic closure of K. Since $\mathrm{ed}_K(G) \geqslant \mathrm{ed}_{\overline{K}}(G)$, we may replace that K by $\overline{K}$ and thus assume that K is algebraically closed. Note that $\mathrm{ed}_K(G) = \mathrm{ed}_{\overline{\mathbb{Q}}}(G)$ and $\mathrm{ed}_k(G) = \mathrm{ed}_{\overline{\mathbb{F}}_p}(G)$; see [BRV07, Proposition 2.14] or [Tos17, Example 4.10].
Choose a number field $E \subseteq \overline{\mathbb{Q}}$ such that $\mathrm{ed}_E(G) = \mathrm{ed}_{\overline{\mathbb{Q}}}(G)$ and let $\mathfrak{p} \subseteq \mathscr{O}_E$ a prime in the ring $\mathscr{O}_E$ of algebraic integers in E lying over p. Set $E_0 \overset{\mathrm{def}}{=} \mathscr{O}_E/\mathfrak{p}$. Since k contains $\overline{\mathbb{F}}_p$, there is an embedding $E_0 \subseteq k$. By Theorem 2.4, $\mathrm{ed}_E(G) \geqslant \mathrm{ed}_{E_0}(G)$ and since $E_0 \subseteq k$, $\mathrm{ed}_{E_0}(G) \geqslant \mathrm{ed}_k(G)$. ♠

Example 3.5. A. Duncan pointed out to us that equality in Corollary 3.4(b) does not always hold. For example, let $G = A_5$ be the alternating group of order 60 and $p = 2$. Note that since A_5 is simple, it is weakly tame at every prime. By [BR97, Theorem 6.7], $\mathrm{ed}_{\mathbb{C}}(A_5) = 2$. On the other hand, $A_5 \simeq \mathrm{SL}_2(\mathbb{F}_4)$ admits a 2-dimensional faithful linear representation over any field k containing $\mathbb{F}_4$, that is, the representation coming from the obvious inclusion of $\mathrm{SL}_2(\mathbb{F}_4)$ into $\mathrm{SL}_2(k)$. The natural (A_5-equivariant) projection $\mathbb{A}^2 \dashrightarrow \mathbb{P}^1$ now tells us that $\mathrm{ed}_k(A_5) = 1$. In summary,

$$2 = \mathrm{ed}_{\mathbb{C}}(A_5) > \mathrm{ed}_k(A_5) = 1.$$

Remark 3.6. The group $G = A_5$ in Example 3.5 is weakly tame but not tame at 2. We do not know of any such examples with G tame. We conjecture that they do not exist. That is, if $|G|$ is prime to p, then under the hypotheses of Corollary 3.4(b), $\mathrm{ed}_K(G) = \mathrm{ed}_k(G)$, provided that K is algebraically closed.

4. Ledet's conjecture and its consequences

The following conjecture is due to A. Ledet [Led04].

Conjecture 4.1. If k is a field of characteristic $p > 0$, n is a natural number, and C_{p^n} is a cyclic group of order p^n, then $\mathrm{ed}_k(\mathrm{C}_{p^n}) = n$.

Remark 4.2. It is known that $\mathrm{ed}_k(\mathrm{C}_{p^n}) \leqslant n$ for any field k of characteristic p and any $n \geqslant 1$ (see [Led04]); it is also known that $\mathrm{ed}_k(\mathrm{C}_{p^n}) \geqslant 2$ if $n \geqslant 2$ ([Led07, Theorems 5 and 7]). Thus Conjecture 4.1 holds for $n = 1$ and $n = 2$; it remains open for every $n \geqslant 3$.

Combining Conjecture 4.1 with Theorem 2.4, we obtain the following surprising result.

Proposition 4.3. *Assume that a finite group G is weakly tame at a prime p and contains an element of order p^n. Let K be a field of characteristic* 0. *If Conjecture 4.1 holds for C_{p^n}, then* $\mathrm{ed}_K(G) \geqslant n$.

Proof. By Corollary 3.4(b), with $k = \overline{\mathbb{F}}_p$, we have $\mathrm{ed}_K(G) \geqslant \mathrm{ed}_k(G)$. Since G contains C_{p^n}, $\mathrm{ed}_k(G) \geqslant \mathrm{ed}_k(\mathrm{C}_{p^n})$, and by Conjecture 4.1, $\mathrm{ed}_k(\mathrm{C}_{p^n}) = n$. ♠

Corollary 4.4. *Let p be a prime and n a positive integer. Choose a positive integer m such that $q \overset{\text{def}}{=} mp^n + 1$ is a prime. (By Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many such m.) Let C_q be a cyclic group of order q. Then $\operatorname{Aut} \mathrm{C}_q = (\mathbb{Z}/q\mathbb{Z})^*$ is cyclic of order mp^n; let $\mathrm{C}_{p^n} \subseteq (\mathbb{Z}/q\mathbb{Z})^*$ denote the subgroup of order p^n. Set $G \overset{\text{def}}{=} \mathrm{C}_{p^n} \ltimes \mathrm{C}_q$. Then*

(a) G is weakly tame at p, and

(b) if Conjecture 4.1 holds, then $\mathrm{ed}_K(G) \geqslant n$ for any field K of characteristic 0.

Proof. (a) Suppose $S \subseteq G$ is a normal p-subgroup. Then S lies in every Sylow p-subgroup of G, in particular, in C_{p^n}. Our goal is to show that $S = \{1\}$. The cyclic group C_q of prime order q acts on S by conjugation. Since $q > p^n \geqslant |S|$, this action is trivial. In other words, S is a central subgroup of G. In particular, S acts trivially on C_q by conjugation. On the other hand, by the definition of G, C_{p^n} acts faithfully on C_q by conjugation. We conclude that $S = \{1\}$, as desired.
(b) follows from Proposition 4.3. ♠

Remark 4.5. The inequality of Corollary 4.4(b) is equivalent to

$$\mathrm{ed}_{\mathbb{C}}(\mathrm{C}_{p^n} \ltimes \mathrm{C}_q) \geqslant n\,, \tag{4.1}$$

where $\mathbb{C}$ is the field of complex numbers (once again, see [BRV07, Proposition 2.14] or [Tos17, Example 4.10]). For $n = 2$ and 3, this inequality can be proved unconditionally (i.e., without assuming Conjecture 4.1) by appealing to the classifications of finite groups of essential dimension 1 and 2 over $\mathbb{C}$ in [BR97, Theorem 6.2] and [Dun13, Theorem 1.1] respectively.

Remark 4.6. Let G be a finite group. Set

$$\mathrm{ed}_k^{\mathrm{loc}}(G) := \max\{\mathrm{ed}_k(G;p) \,|\, p \text{ is a prime}\},$$

where $\mathrm{ed}_k(G;p)$ denotes essential dimension of G at a prime p and the superscript "loc" stands for "local".
Clearly $\mathrm{ed}_k(G) \geqslant \mathrm{ed}_k^{\mathrm{loc}}(G)$. In the language of [Rei10, Section 5], computing $\mathrm{ed}_k^{\mathrm{loc}}(G)$ is a Type I problem. When $\mathrm{char}(k) = 0$, this problem is solved, at least in principle, by the Karpenko-Merkurjev theorem [KM08]. Computing $\mathrm{ed}_k(G)$ in those cases, where $\mathrm{ed}_k(G) > \mathrm{ed}_k^{\mathrm{loc}}(G)$ is a Type II problem. Such problems tend to be very hard. For more on this, see [Rei10, Section 5] or the discussion after the statement of Theorem 2 in [Rei18].
Let us now return to the setting of Corollary 4.4, where $G = \mathrm{C}_{p^n} \ltimes \mathrm{C}_q$. Since all Sylow subgroups of $G = \mathrm{C}_{p^n} \ltimes \mathrm{C}_q$ are cyclic, one readily sees that $\mathrm{ed}_{\mathbb{C}}^{\mathrm{loc}}(G) = 1$. Thus the inequality (4.1) is a "Type II problem" whenever $n \geqslant 2$. An unconditional proof of this inequality is out of the reach of all currently available techniques for any $n \geqslant 3$. However, it is shown in [Rei18] (unconditionally) that

$$\lim_{n\to\infty} \mathrm{ed}_{\mathbb{C}}(\mathrm{C}_{p^n} \ltimes \mathrm{C}_q) \longrightarrow \infty$$

for any choice of q.

REMARK 4.7. It is shown in [RV18] that if G is a finite group and k is a field of characteristic p, then

$$\mathrm{ed}_k(G;p) = \begin{cases} 1, \text{ if } p \text{ divides } |G|, \text{ and} \\ 0, \text{ otherwise.} \end{cases} \tag{4.2}$$

In particular, $\mathrm{ed}_k^{\mathrm{loc}}(C_{p^n}) = 1$ for every $n \geqslant 1$. So, for $n \geqslant 2$, Conjecture 4.1 is also a Type II problem. Thus the situation in Corollary 4.4(b) can be described as follows: we deduce one Type II assertion from another, without being able to prove either one from first principles. Another results of this type is [DR15, Proposition 10.8]; further examples can be found in the next section.

REMARK 4.8. In view of (4.2), Corollary 3.4(b) continues to hold if we replace essential dimension by essential dimension at p, for trivial reasons. Moreover, under the assumptions of Corollary 3.4, (a′) $\mathrm{ed}_{\mathbb{Q}}(G;p) \geqslant \mathrm{ed}_{\mathbb{F}_p}(G;p)$ and (b′) $\mathrm{ed}_K(G;p) \geqslant \mathrm{ed}_k(G;p)$, for any finite group G, not necessarily weakly tame. In (b′) we can also drop the requirement that k should contain $\overline{\mathbb{F}}_p$. Note however that our proof of Theorem 2.4 breaks down if we replace essential dimension by essential dimension at p.

5. ESSENTIAL DIMENSION OF $\mathrm{PSL}_2(q)$

Let p be a prime, $q = p^r$ be a prime power and $\mathbb{F}_q$ be a field of q elements. Let $G = \mathrm{PSL}_2(q) = \mathrm{PSL}(2, \mathbb{F}_q)$. (To avoid confusion, we remind the reader that G is the quotient of $\mathrm{SL}(2, \mathbb{F}_q)$ by its subgroup $\{\pm 1\}$. In general, it is not the same thing as the group $\mathrm{PSL}_2(\mathbb{F}_q)$ of $\mathbb{F}_q$ points of the algebraic group $\mathrm{PSL}_2 = \mathrm{PGL}_2$.) For $q > 3$, it is well known that G is simple; see, e.g., [Die71, p. 39] or [Gor80, p. 419]. Hence, G is weakly tame at every prime. In this section we will work over the field $k = \mathbb{C}$ of complex numbers and deduce lower bounds on $\mathrm{ed}_{\mathbb{C}}(G)$ from Ledet's conjecture.
For some q, these lower bounds are Type II bounds, in the sense of Remark 4.6, and are genuinely new. To establish this we will compute $\mathrm{ed}_{\mathbb{C}}^{\mathrm{loc}}(G)$ in every case. We begin with the following well-known description of the Sylow subgroups of $\mathrm{PSL}_2(q)$.

LEMMA 5.1. *Let p and ℓ be prime numbers and set $q = p^r$ for some positive integer r. Let G_ℓ denote an ℓ-Sylow subgroup of $G = \mathrm{PSL}_2(q)$. Then*

(a) *For $\ell = p$, we have $G_\ell \cong (C_p)^r$.*
(b) *For $\ell \notin \{2, p\}$, G_ℓ is cyclic.*
(c) *For p odd and $\ell = 2$, G_ℓ is dihedral.*

Proof. See [Gor80, Lemma 1.1 on page 418]. ♠

PROPOSITION 5.2. *Let p be a prime and $q = p^r$ be a prime power.*

(a) $\mathrm{ed}_{\mathbb{C}}^{\mathrm{loc}}(\mathrm{PSL}_2(q)) = \begin{cases} r, & q \text{ even;} \\ \max(2, r), & q \text{ odd.} \end{cases}$

(b) Let ℓ be a prime and s be a nonnegative integer such that $2\ell^s$ divides q^2-1. If Ledet's Conjecture 4.1 *holds for cyclic groups of order ℓ^s in characteristic ℓ, then* $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(q)) \geqslant s$.

Note that part (b) is conditional on Ledet's conjecture but part (a) is not.

Proof. Set $G = \mathrm{PSL}_2(q)$. We begin by pointing out that

$$|G| = \begin{cases} (q-1)q(q+1)/2, & 2 \nmid q; \\ (q-1)q(q+1), & 2|q. \end{cases} \tag{5.1}$$

(a) Recall that $\mathrm{ed}_{\mathbb{C}}(G;\ell) = \mathrm{ed}_{\mathbb{C}}(G_\ell;\ell)$, where G_ℓ is a Sylow ℓ-subgroup of G. So we only need to consider the primes ℓ dividing $|G|$; otherwise $G_\ell = \{1\}$ and $\mathrm{ed}_{\mathbb{C}}(G_\ell;\ell) = 0$.
If $\ell \neq 2$ or p, then by Lemma 5.1(b), G_ℓ is cyclic; hence, $\mathrm{ed}_{\mathbb{C}}(G_\ell) = 1$.
If $\ell = p$, then by Lemma 5.1(a), $G_\ell = G_p = (C_p)^r$, and $\mathrm{ed}_{\mathbb{C}}(G_p;p) = r$.
If $\ell = 2$ and p is odd, then by Lemma 5.1(c), G_ℓ is a dihedral group; hence, G_ℓ has a 2-dimensional faithful linear representation over $\mathbb{C}$. We conclude that $\mathrm{ed}_{\mathbb{C}}(G_2;2) \leqslant 2$. On the other hand, since G_2 is not cyclic and $|G_2| \equiv 0 \pmod 4$, $\mathrm{ed}_{\mathbb{C}}(G_\ell) \geqslant 2$ by [BR97, Theorem 6.2]. So $\mathrm{ed}_{\mathbb{C}}(G_\ell) = 2$.
This proves part (a) for the case that p is odd. The case that p is even follows directly from Lemma 5.1 by the same method.
(b) Note that the assertion of part (b) is vacuous if $\ell = p$ or $p = 2$. So we may assume that p is odd and $\ell \neq p$. Then it follows from Lemma 5.1 that the Sylow ℓ-subgroup of $\mathrm{PSL}_2(q)$ is cyclic if ℓ is odd and dihedral if $\ell = 2$. Thus, by (5.1), $\mathrm{PSL}_2(q)$ contains an element of order ℓ^s, and the desired inequality follows from Proposition 4.3. ♠

Remark 5.3. Note that, for odd ℓ, Proposition 5.2(a) gives the Type I lower bound: $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(q)) \geqslant \max\{2, r\}$; cf. Remark 4.6. We also know which finite simple groups have essential dimension 1, 2 or 3 from [BR97, Theorem 6.2], [Dun13] and [Bea14], respectively. Thus the lower bound of Proposition 5.2(b) is only of interest in those cases, where

$$s \geqslant \max\{r+1, 5\}.$$

In such cases an unconditional proof of the lower bound

$$\mathrm{ed}_{\mathbb{C}}(\mathrm{PGL}_2(q)) \geqslant s$$

(i.e., a proof that does not rely on Ledet's conjecture) is not known.

Remark 5.4. It follows from Proposition 5.2(a) that $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(q)) \geqslant \mathrm{ed}^{\mathrm{loc}}_{\mathbb{C}}(\mathrm{PSL}_2(q)) \geqslant r$ for any $q = p^r$. Hence, if we want to deduce an interesting (Type II) lower bound on $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(q))$ from Proposition 4.3, we need ℓ^s to divide $q \pm 1 = p^r \pm 1$ for some prime ℓ and some integer $s \geqslant r+1$. This can only happen if $\ell < p$. In particular, this method gives no new information about $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(q))$ in the case, where q is a power of 2.

Example 5.5. Let $p = 31$ and $q = p^2 = 961$. Then $(q-1)/2 = 960$ is divisible by 2^6. Thus Proposition 5.2 yields

(a) $\mathrm{ed}^{\mathrm{loc}}_{\mathbb{C}}(\mathrm{PSL}_2(961)) = 2$ but (b) $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(961)) \geqslant 5$.

Now let $q = p = 65537$. Note that p is a Fermat prime, $p = 2^{16} + 1$. Here Proposition 5.2 yields

(a) $\mathrm{ed}^{\mathrm{loc}}_{\mathbb{C}}(\mathrm{PSL}_2(65537)) = 2$ but (b) $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(65537)) \geqslant 15$.

In both cases the inequality (b) is conditional on Ledet's conjecture.

Remark 5.6. It follows from [Rei18, Theorem 2] that for any $d \geqslant 1$ there are only finitely many non-abelian simple finite groups G such that $\mathrm{ed}_{\mathbb{C}}(G) \leqslant d$. In some ways this assertion is more satisfying than the inequality of Proposition 5.2(b): it is unconditional (does not rely on Ledet's conjecture), and it covers all finite simple groups, not just those of the form $\mathrm{PSL}_2(q)$. On the other hand, it does not give an explicit lower bound on $\mathrm{ed}_{\mathbb{C}}(G)$ for any particular finite simple group G.

6. Proof of Theorem 1.2

We begin by remarking that an étale gerbe $\mathscr{X} \to S$ is weakly tame if and only if there exists an étale cover $\{S_i \to S\}$ such that each $\mathscr{X}_{S_i} \to S_i$ is equivalent to $\mathscr{B}_{S_i} G_i \to S_i$ with G_i weakly tame étale group schemes over S_i.

Our proof of Theorem 1.2 will rely on the following Lemma 6.1. To state it, we need the notion of *versal object* of an algebraic stack. This is standard for classifying stacks of algebraic groups, but does not seem to be in the literature in the general case, so a short discussion is in order.

Let $\mathscr{X} \to \operatorname{Spec} F$ be an algebraic stack of finite type over a field. Then $\mathscr{X}$ preserves inductive limits, in the following sense: if $\{A_i\}$ is an inductive system of F-algebras over a filtered poset, the induced functor $\varinjlim \mathscr{X}(A_i) \to \mathscr{X}(\varinjlim A_i)$ is an equivalence of categories. If L is an extension of F then we can view L as the inductive limit of its subalgebras $R \subseteq K$ of finite type over F; hence, given an object $\xi \in \mathscr{X}(L)$, there exists a finitely generated subalgebra $R \subseteq K$ and an object $\xi_R \in \mathscr{X}(R)$ whose image in $\mathscr{X}(L)$ is isomorphic to ξ.

We say that an object $\xi \in \mathscr{X}(L)$ is *versal* if it satisfies the following condition, which expresses the fact that every object of $\mathscr{X}$ over an extension of F can be obtained by specialization of ξ.

For any R and ξ_R as above, and any object $\eta \in \mathscr{X}(K)$ over an extension K of F that is an infinite field, there exists a homomorphism of F-algebras $R \to K$ such that the image of ξ_R in $\mathscr{X}(K)$ under the induced functor $\mathscr{X}(R) \to \mathscr{X}(K)$ is isomorphic to η.

Versal object don't exist in general; for example, they don't exist when $\mathscr{X}$ has positive-dimensional moduli space. When they do exist, however, they control the essential dimension, that is, $\xi \in \mathscr{X}(L)$ is versal, then the essential dimension of ξ is easily seen to be the essential dimension of $\mathscr{X}$ (in other words, no object of $\mathscr{X}$ defined over a field can have essential dimension larger than that of ξ).

Lemma 6.1. *Let $\mathscr{X}_F \to \operatorname{Spec} F$ be a finite étale gerbe over a field F. Suppose that A is a non-zero finite F-algebra, and that the morphism $\operatorname{Spec} A \to \operatorname{Spec} F$ has a lifting $\phi\colon \operatorname{Spec} A \to \mathscr{X}_F$. Consider the locally free sheaf $\phi_*\mathscr{O}_{\operatorname{Spec} A}$ on $\mathscr{X}_F$; call $\mathscr{V} \to \mathscr{X}_F$ the corresponding vector bundle on $\mathscr{X}_F$. Then $\mathscr{V}$ has a non-empty open subscheme $U \subseteq \mathscr{V}$. Furthermore, if $k(U)$ is the field of rational functions on U, the composite $\operatorname{Spec} k(U) \to U \subseteq \mathscr{V} \to \mathscr{X}_F$ gives a versal object of $\mathscr{X}_F\bigl(k(U)\bigr)$.*

Proof. Let us show that $\mathscr{V}$ is generically a scheme. We can extend the base field F, so that it is algebraically closed; in this case $\mathscr{X}_F$ is the classifying space $\mathscr{B}_F G$ of a finite group G, and there exists a homomorphism of F-algebras $A \to F$. The vector bundle $\mathscr{V} \to \mathscr{X}_F$ corresponds to a representation V of G; by the semicontinuity of the degree of the stabilizer for finite group actions, it is enough to show that V has a point with trivial stabilizer. The homomorphism $A \to F$ gives a morphism $\operatorname{Spec} F \to \operatorname{Spec} A$, and the composite $\operatorname{Spec} F \to \operatorname{Spec} A \to \mathscr{B}_F G$ corresponds to the trivial G-torsor on $\operatorname{Spec} F$. If we call $\mathscr{W}$ the pushforward of $\mathscr{O}_{\operatorname{Spec} F}$ to $\mathscr{B}_F G$, then $\mathscr{W} \subseteq \mathscr{V}$. On the other hand $\mathscr{W}$ corresponds to the regular representation of G, and so the generic stabilizer is trivial, which proves what we want.

Let us show that the composite $\operatorname{Spec} k(U) \to U \subseteq \mathscr{V} \to \mathscr{X}_F$ is versal; the argument is standard. Suppose that K is an extension of F that is an infinite field, and consider a morphism $\operatorname{Spec} K \to \mathscr{X}_F$. It is enough to prove that for any open subscheme $U \subseteq \mathscr{V}$, the morphism $\operatorname{Spec} K \to \mathscr{X}_F$ factors through $U \subseteq \mathscr{V} \to \mathscr{X}_F$. The pullback $V_K \to \operatorname{Spec} K$ of $\mathscr{V} \to \mathscr{X}_F$ is a vector space on K, and the inverse image $U_K \subseteq V_K$ of $U \subseteq \mathscr{V}$ is a non-empty open subscheme; hence $U_K(K) \neq \emptyset$, which ends the proof. ♠

Proof of Theorem 1.2. Let $\widehat{R}$ be the completion of R and $\widehat{K}$ be the fraction field of $\widehat{R}$. Then clearly $K \subset \widehat{K}$ and thus $\operatorname{ed}_K(\mathscr{X}_K) \geqslant \operatorname{ed}_{\widehat{K}}(\mathscr{X}_{\widehat{K}})$. Thus for the purpose of proving Theorem 1.2, we may replace R by $\widehat{R}$. In other words, we may (and will) assume that R is complete.

Let $R \to A$ be an étale faithfully flat algebra such that $\mathscr{X}(A) \neq \emptyset$; since R is henselian, by passing to a component of $\operatorname{Spec} A$ we can assume that $R \to A$ is finite. An object of $\mathscr{X}(A)$ gives a lifting $\phi\colon \operatorname{Spec} A \to \mathscr{X}$; this is flat and finite. Let $\mathscr{V} \to \mathscr{X}$ be the vector bundle corresponding to $\phi_*\mathscr{O}_{\operatorname{Spec} A}$. If $U \to \mathscr{V}$ is the largest open subscheme of $\mathscr{V}$, the Lemma above implies that $U \to \operatorname{Spec} R$ is surjective. Denote by U_K and U_k respectively the generic and special fiber of $U \to \operatorname{Spec} R$; call E and E_0 the fields of rational functions on U_K and U_k respectively. Again because of the Lemma, the objects $\xi\colon \operatorname{Spec} E \to \mathscr{X}_K$ and $\xi_0\colon \operatorname{Spec} E_0 \to \mathscr{X}_k$ are versal.

Consider the local ring $\mathscr{O}_E$ of U at the generic point of U_k, which is a DVR. The residue field of $\mathscr{O}_E$ is E_0, and we have a morphism $\Xi\colon \operatorname{Spec} \mathscr{O}_E \to \mathscr{X}$ whose restrictions to $\operatorname{Spec} K$ and $\operatorname{Spec} k$ are isomorphic to ξ and ξ_0 respectively.

Set $m \overset{\text{def}}{=} \operatorname{ed}_K(\mathscr{X}_K)$; we need to show that ξ_0 has a compression of transcendence degree at most m.

There exists a field of definition $K \subseteq L \subseteq E$ for ξ such that $\operatorname{trdeg}_K L = m$; call $\theta\colon \operatorname{Spec} L \to \mathscr{X}$ the corresponding morphism, so that we have a factorization $\operatorname{Spec} E \to \operatorname{Spec} L \xrightarrow{\theta} \mathscr{X}$ for ξ. Consider the intersection $\mathscr{O}_L \overset{\text{def}}{=} \mathscr{O}_E \cap L \subseteq E$; then $\mathscr{O}_L$ is a DVR with quotient field L. Call L_0 it residue field; we have $L_0 \subseteq E_0$. By Lemma 2.1, $\operatorname{trdeg}_k L_0 \leqslant \operatorname{trdeg}_K L$.

Now it suffices to show that $\xi_0\colon \operatorname{Spec} E_0 \to \mathscr{X}$ factors through $\operatorname{Spec} L_0$. Assume that we have proved that the morphism $\theta\colon \operatorname{Spec} L \to \mathscr{X}$ extends to a morphism $\Theta\colon \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$. The composite $\operatorname{Spec} E \subseteq \operatorname{Spec} \mathscr{O}_E \xrightarrow{\Xi} \mathscr{X}$ is isomorphic to the composite $\operatorname{Spec} E \to \operatorname{Spec} L \subseteq \operatorname{Spec} \mathscr{O}_L \xrightarrow{\Theta} \mathscr{X}$; since $\mathscr{X}$ is separated, it follows from the valuative criterion of separation that the composite $\operatorname{Spec} \mathscr{O}_E \to \operatorname{Spec} \mathscr{O}_L \xrightarrow{\Theta} \mathscr{X}$ is isomorphic to $\Xi\colon \operatorname{Spec} \mathscr{O}_E \to \mathscr{X}$. By restricting to the central fibers we deduce that $\xi_0\colon \operatorname{Spec} E_0 \to \mathscr{X}$ is isomorphic to the composite $\operatorname{Spec} E_0 \to \operatorname{Spec} L_0 \to \mathscr{X}$, and we are done.

To prove the existence of the extension $\Theta\colon \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$, notice that the uniqueness of such extension implies that to prove its existence we can pass to a finite étale extension $R \subseteq R'$, where R' is a DVR; it is straightforward to check that formation of $\mathscr{O}_L$ and $\mathscr{O}_E$ commutes with such a base change. Hence we can assume that $\mathscr{X}$ has a section, so that $\mathscr{X} = \mathscr{B}_R G$, where $G \to \operatorname{Spec} R$ is a finite étale weakly tame group scheme. By passing to a further covering we can assume that $G \to \operatorname{Spec} R$ is constant, that is, the product of $\operatorname{Spec} R$ with a finite group Γ. If A is an R-algebra, an action of G on $\operatorname{Spec} A$ corresponds to an action of Γ.

The vector bundle $\mathscr{V} \to \mathscr{X}$ corresponds to a vector bundle $V_R \to \operatorname{Spec} R$ with an R-linear action of Γ, such that the induced representations of Γ on V_K and V_k are faithful. Call $\widetilde{E}$ the function field of V_K and $\widetilde{E}_0$ the function field of V_k; then $\widetilde{E}^\Gamma = E$, and therefore $\mathscr{O}_{\widetilde{E}}^\Gamma = \mathscr{O}_E$. The factorization $\operatorname{Spec} E \to \operatorname{Spec} L \to \mathscr{X}$ gives a Γ-torsor $\operatorname{Spec} \widetilde{L} \to \operatorname{Spec} L$ whose lift to $\operatorname{Spec} E$ is isomorphic to $\operatorname{Spec} \widetilde{E} \to \operatorname{Spec} E$; then $\widetilde{L}$ is a Γ-invariant subfield of $\widetilde{E}$. Then $\mathscr{O}_{\widetilde{L}} \overset{\text{def}}{=} \widetilde{L} \cap \mathscr{O}_{\widetilde{E}}$ is a Γ-invariant DVR, and $\mathscr{O}_{\widetilde{L}}^\Gamma = \widetilde{L}^\Gamma \cap \mathscr{O}_{\widetilde{E}}^\Gamma = \mathscr{O}_L$.

Call $\mathfrak{m}_{\widetilde{L}} \subseteq \mathscr{O}_{\widetilde{L}}$ the maximal ideal, and set $\widetilde{L}_0 \overset{\text{def}}{=} \mathscr{O}_{\widetilde{L}}/\mathfrak{m}_{\widetilde{L}}$. If $t \in R$ is the uniformizing parameter, the image of t in $\mathscr{O}_{\widetilde{L}}$, which we denote again by t, is a uniformizing parameter; this is Γ-invariant. The action of Γ on $\mathscr{O}_{\widetilde{L}}$ descends to an action of Γ on $\widetilde{L}_0$. By Proposition 2.3, this action is faithful.

So the action of Γ on $\operatorname{Spec} L_0$ is free over k; this implies that the action of Γ on $\operatorname{Spec} \mathscr{O}_{\widetilde{L}} \to \operatorname{Spec} R$ is free, so $\operatorname{Spec} \mathscr{O}_{\widetilde{L}} \to (\operatorname{Spec} \mathscr{O}_{\widetilde{L}})/G = \operatorname{Spec} \mathscr{O}_L$ is a Γ-torsor. This gives the desired morphism $\Theta\colon \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$, and ends the proof of the Theorem. ♠

REMARK 6.2. The problem with the proof of [BRV11, Theorem 5.11] was in the last sentence of the second paragraph on page 1094. We claimed there that the discrete valuation ring R in the proof can be replaced with the ring called $W(k(s))$. Since the essential dimension of the generic point can go up when we

make this replacement, this is, in fact, not allowable. (In effect, our mistake boils down to using an inequality in the wrong direction.)
Note also that the proof of the characteristic 0 genericity theorem in [BRV07] does not rely on Theorem 1.1. For that argument, which was different from the proof of [BRV11, Theorem 6.1], see [BRV07, Theorem 4.1].

References

[Bea14] Arnaud Beauville, *Finite simple groups of small essential dimension*, Trends in contemporary mathematics, Springer INdAM Ser., vol. 8, Springer, Cham, 2014, pp. 221–228. MR 3586401

[BF03] Grégory Berhuy and Giordano Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. 8 (2003), 279–330.

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. 106 (1997), no. 2, 159–179.

[BRV07] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli, *Essential dimension and algebraic stacks*, 2007, `arXiv:math/0701903v1 [math.AG]`.

[BRV11] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli, *Essential dimension of moduli of curves and other algebraic stacks*, J. Eur. Math. Soc. (JEMS) 13 (2011), no. 4, 1079–1112, With an appendix by Najmuddin Fakhruddin. MR 2800485

[Die71] Jean A. Dieudonné, *La géométrie des groupes classiques*, Springer-Verlag, Berlin-New York, 1971, Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5. MR 0310083

[DR15] Alexander Duncan and Zinovy Reichstein, *Versality of algebraic group actions and rational points on twisted varieties*, J. Algebraic Geom. 24 (2015), no. 3, 499–530, With an appendix containing a letter from J.-P. Serre. MR 3344763

[Dun13] Alexander Duncan, *Finite groups of essential dimension 2*, Comment. Math. Helv. 88 (2013), no. 3, 555–585.

[Gor80] Daniel Gorenstein, *Finite groups*, second ed., Chelsea Publishing Co., New York, 1980. MR 569209

[KM08] Nikita A. Karpenko and Alexander S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. 172 (2008), no. 3, 491–508. MR MR2393078

[Led04] Arne Ledet, *On the essential dimension of p-groups*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 159–172. MR 2059762

[Led07] Arne Ledet, *Finite groups of essential dimension one*, J. Algebra 311 (2007), no. 1, 31–37. MR 2309876

[Löt10] Roland Lötscher, *Application of multihomogeneous covariants to the essential dimension of finite groups*, Transform. Groups 15 (2010), no. 3, 611–623. MR 2718939

[Mer13] Alexander S. Merkurjev, *Essential dimension: a survey*, Transform. Groups 18 (2013), no. 2, 415–481. MR 3055773

[Nak47] Tadasi Nakayama, *Finite groups with faithful irreducible and directly indecomposable modular representations*, Proc. Japan Acad. 23 (1947), no. 3, 22–25. MR 0042418

[Rei10] Zinovy Reichstein, *Essential dimension*, Proceedings of the International Congress of Mathematicians. Volume II, Hindustan Book Agency, New Delhi, 2010, pp. 162–188. MR 2827790

[Rei18] Zinovy Reichstein, *The Jordan property of Cremona groups and essential dimension*, 2018, to appear in Arch. Math.

[RV18] Zinovy Reichstein and Angelo Vistoli, *Essential dimension of finite groups in prime characteristic*, C. R. Math. Acad. Sci. Paris 356 (2018), no. 5, 463–467. MR 3790415

[Tos17] Dajano Tossici, *Essential dimension of group schemes over a local scheme*, J. Algebra 492 (2017), 1–27. MR 3709138

[Vaq06] Michel Vaquié, *Valuations and local uniformization*, Singularity theory and its applications, Adv. Stud. Pure Math., vol. 43, Math. Soc. Japan, Tokyo, 2006, pp. 477–527. MR 2325152

[ZS58] Oscar Zariski and Pierre Samuel, *Commutative algebra, Volume I*, The University Series in Higher Mathematics, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958, With the cooperation of I. S. Cohen. MR 0090581

Patrick Brosnan
Department of Mathematics
1301 Mathematics Building
University of Maryland
College Park
MD 20742-4015
USA
pbrosnan@gmail.com

Zinovy Reichstein
Department of Mathematics
1984 Mathematics Road
University of British Columbia
Vancouver, BC V6T 1Z2
Canada
reichst@math.ubc.ca

Angelo Vistoli
Scuola Normale Superiore
Piazza dei Cavalieri 7
56126 Pisa
Italy
angelo.vistoli@sns.it