ESSENTIAL DIMENSION: A SURVEY

ALEXANDER S. MERKURJEV

Abstract. In the paper we survey research on the essential dimension. The highlights of the survey are the computations of the essential dimensions of finite groups, groups of multiplicative type and the spinor groups. We present self-contained proofs of these cases and give applications in the theory of simple algebras and quadratic forms.

1. Introduction

Informally speaking, the essential dimension of an algebraic object is the minimal number of algebraically independent parameters one needs to define the object. To motivate this notion, let us consider an example where the object is a quadratic extension of a field. Let F be a base field, K/F a field extension and L/K a quadratic extension. Then L is generated over K by an element α with the minimal polynomial $t^2 + at + b$ with $a, b \in K$, so L can be given by the two parameters a and b. But we can do better: if both a and b are nonzero, by scaling α, we can achieve $a = b$, i.e., just one parameter a is needed. Equivalently, we can say that the quadratic extension L/K is defined over the smaller field $K_0 = F(a)$, namely, if $L_0 = K_0[t]/(t^2 + at + a)$, then $L \simeq L_0 \otimes_{K_0} K$, i.e., L/K is defined over the field K_0 of transcendence degree at most 1 over F. We say that the essential dimension of L/K is at most 1.

The notion of the essential dimension was defined by J. Buhler and Z. Reichstein in [12] for the class of finite Galois field extensions with a given Galois group and later in [82] was extended to the class of G-torsors for an arbitrary algebraic group G. Many classical objects such as simple algebras, quadratic and hermitian forms, algebras with involutions, etc. can be viewed as torsors under classical algebraic groups. The only property of a class of algebraic objects needed to define the essential dimension is that for every field extension K/F we must have a set $\mathcal{F}(K)$ of isomorphism classes of objects, and for every field homomorphism $K \to L$ over F - a change of field map $\mathcal{F}(K) \to \mathcal{F}(L)$. In other words, $\mathcal{F}$ is a functor from the category *Fields*$_F$ of field extensions of F to the category of sets. The essential dimension for an arbitrary functor *Fields*$_F \to$ *Sets* was defined in [7].

The essential dimension of a functor $\mathcal{F}$ (of a class of algebraic objects) is an integer that measures the complexity of the functor $\mathcal{F}$. One of the applications of the essential dimension is as follows: Suppose we would like to check whether a classification conjecture for the class of objects given by $\mathcal{F}$ holds. Usually, a classification conjecture assumes another functor $\mathcal{L}$ (a classification list) together with a morphism of functors $\mathcal{L} \to \mathcal{F}$, and the conjecture asserts that this morphism is surjective. Suppose we can compute the essential dimensions of $\mathcal{L}$ and $\mathcal{F}$, and it turns out that $\operatorname{ed}(\mathcal{L}) < \operatorname{ed}(\mathcal{F})$, i.e., the functor $\mathcal{F}$ is "more complex" than $\mathcal{L}$. This

---

The work has been supported by the NSF grant DMS #1160206.

means that no morphism between $\mathcal{L}$ and $\mathcal{F}$ can be surjective and the classification conjecture fails. Thus, knowing the essential dimension allows us to predict the complexity of the structure. We have examples in quadratic form theory (Theorem 9.5 and Section 9c) and in the theory of simple algebras (Corollaries 10.7 and 10.8).

Typically, the problem of computing the essential dimension of a functor splits into two problems of finding upper and lower bounds. To obtain an upper bound, one usually finds a classifying scheme of the smallest possible dimension. Finding lower bounds is more complicated.

Let p be a prime integer. The essential p-dimension is the version of the essential dimension that ignores "prime to p effects". Usually, the essential p-dimension is easier to compute than the ordinary essential dimension.

If the algebraic structures given by a functor $\mathcal{F}$ are classified (parameterized), then the essential dimension of $\mathcal{F}$ can be computed by counting the number of algebraically independent parameters. But the essential dimension can be computed in some cases where the classification theorem is not available. The most impressive example is the structure given by the $\mathbf{Spin}_n$-torsors (equivalently, nondegenerate quadratic forms of dimension n with trivial discriminant and Clifford invariant). The classification theorem is available for $n \leq 14$ only, but the exact value of the essential dimension was computed for every n and this value is exponential in n.

The canonical dimension is a special case of the essential dimension. The canonical dimension of varieties measures their incompressibility. This can be studied by means of the theory of Chow motives.

The notion of the essential dimension of a functor can be naturally extended to the categories fibered in groupoids. This allows us to unite the essential dimension of schemes and algebraic groups. We study the essential dimension of special types of the categories fibered in groupoids such as stacks and gerbes.

Essential dimension, which is defined in elementary terms, has surprising connections to many problems in algebra and algebraic geometry. Below is the list of some areas of algebra related to the essential dimension:

- Birational algebraic geometry
- Intersection algebraic cycles
- Equivariant compressions of varieties
- Incompressible varieties
- Chow motives
- Chern classes
- Equivariant algebraic K-theory
- Galois cohomology
- Representation theory of algebraic groups
- Fibered categories, algebraic stacks
- Valuation theory

The goal of this paper is to survey some of the research on the essential dimension. The highlights of the survey are the computations of the essential dimensions of finite groups, groups of multiplicative type and the spinor groups. We present self-contained proofs of these cases.

We use the following notation. The base field is always denoted by F. Write F_{sep} for a separable closure of F. A *variety* over F is an integral separated scheme

X of finite type over F. If K/F is a field extension, we write X_K for the scheme $X \times_{\operatorname{Spec} F} \operatorname{Spec} K$.

ACKNOWLEDGEMENTS. The author thanks Alex Duncan, Nikita Karpenko, Mark MacDonald and the referee for useful comments and suggestions.

CONTENTS

2. DEFINITION AND SIMPLE PROPERTIES OF THE ESSENTIAL DIMENSION

2a. **Definition of the essential dimension.** The essential dimension of a functor was defined in [7]. Let F be a field and write Fields_F for the category of field extensions of F. The objects of Fields_F are arbitrary field extensions of F and morphisms are field homomorphisms over F.

Let $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ be a functor, K/F a field extension, $x \in \mathcal{F}(K)$ and $\alpha : K_0 \to K$ a morphism in Fields_F (i.e., K is a field extension of K_0 over F). We say that x is *defined over* K_0 (or K_0 *is a field of definition of* x) if there is an element $x_0 \in \mathcal{F}(K_0)$ such that $\mathcal{F}(\alpha)(x_0) = x$, i.e., x belongs to the image of the map $\mathcal{F}(\alpha) : \mathcal{F}(K_0) \to \mathcal{F}(K)$. Abusing notation, we write $x = (x_0)_K$.

We define the *essential dimension of* x:

$$\operatorname{ed}(x) := \min \operatorname{tr.deg}_F(K_0),$$

where the minimum is taken over all fields of definition K_0 of x and the *essential dimension of the functor* $\mathcal{F}$:

$$\operatorname{ed}(\mathcal{F}) := \max \operatorname{ed}(x),$$

where the maximum runs over all field extensions K/F and all $x \in \mathcal{F}(K)$.

2b. **Definition of the essential p-dimension.** Let p be a prime integer. The idea of the essential p-dimension is to "ignore field extensions of degree prime to p". We say that a field extension K'/K is a *prime to* p *extension* if K'/K is finite and the degree $[K' : K]$ is prime to p.

Let $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ be a functor, K/F a field extension, $x \in \mathcal{F}(K)$ and K_0 a field extension of F. We say that x is *p-defined over* K_0 (or that K_0 *is a field of p-definition of* x) if there are morphisms $K_0 \to K'$ and $K \to K'$ in Fields_F for some field K'/F and an element $x_0 \in \mathcal{F}(K_0)$ such that K'/K is a prime to p extension and $(x_0)_{K'} = x_{K'}$ in $\mathcal{F}(K')$.

We define the *essential p-dimension of* x:

$$\operatorname{ed}_p(x) := \min \operatorname{tr.deg}_F(K_0),$$

where the minimum is taken over all fields of p-definition K_0 of x and the *essential p-dimension of the functor* $\mathcal{F}$:

$$\operatorname{ed}_p(\mathcal{F}) := \max \operatorname{ed}_p(x),$$

where the maximum runs over all field extensions K/F and all $x \in \mathcal{F}(K)$.

It follows from the definition that

$$\mathrm{ed}_p(x) := \min \mathrm{ed}(x_L),$$

where L runs over all prime to p extensions of K.

We have the inequality $\mathrm{ed}_p(\mathcal{F}) \leq \mathrm{ed}(\mathcal{F})$ for every p.

The definition of the essential p-dimension formally works for $p = 0$ if a prime to $p = 0$ field extension K'/K is defined as trivial, i.e., $K' = K$. The essential 0-dimension coincides then with the essential dimension, i.e., $\mathrm{ed}_0(\mathcal{F}) = \mathrm{ed}(\mathcal{F})$. This allows us to study simultaneously both the essential dimension and the essential p-dimension. We will write "$p \geq 0$", meaning p is either a prime integer or $p = 0$.

2c. **Simple properties and examples.** Let X be a scheme over F. We can view X as a functor from Fields_F to Sets taking a field extension K/F to the set of K-points $X(K) := \mathrm{Mor}_F(\mathrm{Spec}\, K, X)$.

Proposition 2.1. [70, Corollary 1.4] *For any scheme X of finite type over F, we have $\mathrm{ed}_p(X) = \dim(X)$ for all $p \geq 0$.*

Proof. Let $\alpha : \mathrm{Spec}\, K \to X$ be a point of X over a field $K \in \mathsf{Fields}/F$ with image $\{x\}$. Every field of p-definition of α contains a subfield isomorphic to the residue field $F(x)$. Moreover, α is defined over $F(x)$ hence $\mathrm{ed}_p(\alpha) = \mathrm{tr.deg}_F\, F(x) = \dim(x)$. It follows that $\mathrm{ed}_p(X) = \dim(X)$. □

The following proposition of a straightforward consequence of the definition.

Proposition 2.2. [7, Lemma 1.11] *Let $\mathcal{F}$ and $\mathcal{F}'$ be two functors from $\mathsf{Fields_F}$ to Sets. Then*

$$\mathrm{ed}_p(\mathcal{F} \times \mathcal{F}') \leq \mathrm{ed}_p(\mathcal{F}) + \mathrm{ed}_p(\mathcal{F}')$$

for every $p \geq 0$.

Let $p \geq 0$. A morphism of functors $\alpha : \mathcal{F} \to \mathcal{F}'$ from $\mathsf{Fields_F}$ to Sets is called *p-surjective* if for every field K/F and every element $x \in \mathcal{F}'(K)$, there is a prime to p extension K'/K such that $x_{K'}$ belongs to the image of the map $\alpha_{K'} : \mathcal{F}(K') \to \mathcal{F}'(K')$. If $p = 0$, the 0-surjectivity is the usual surjectivity of $\mathcal{F}(K) \to \mathcal{F}'(K)$ for all K.

Similarly, the morphism α is *p-injective* if for every field K/F and every two elements $x, y \in \mathcal{F}(K)$ such that $\alpha_K(x) = \alpha_K(y)$, there is a prime to p extension K'/K such that $x_{K'} = y_{K'}$ in $\mathcal{F}(K')$. The morphism α is *p-bijective* if it is p-injective and p-surjective.

Proposition 2.3. [70, Proposition 1.3] *Let $p \geq 0$ and $\alpha : \mathcal{F} \to \mathcal{F}'$ a morphism of functors from $\mathsf{Fields_F}$ to Sets.*

1. *If α is p-surjective, then $\mathrm{ed}_p(\mathcal{F}) \geq \mathrm{ed}_p(\mathcal{F}')$.*
2. *If α is p-bijective, then $\mathrm{ed}_p(\mathcal{F}) = \mathrm{ed}_p(\mathcal{F}')$.*

Example 2.4. For an integer $n > 0$ and a field extension K/F, let $\mathcal{F}(K)$ be the set of similarity classes of all $n \times n$ matrices over K, or, equivalently, the set of isomorphism classes of linear operators in an n-dimensional vector space over K. The rational canonical form shows that it suffices to give n parameters to define an operator, so $\mathrm{ed}(\mathcal{F}) \leq n$. On the other hand, the coefficients of the characteristic polynomial of an operator yield a surjective morphism of functors $\mathcal{F} \to \mathbb{A}^n_F$, hence by Propositions 2.1 and 2.3, $\mathrm{ed}(\mathcal{F}) \geq \mathrm{ed}(\mathbb{A}^n_F) = \dim(\mathbb{A}^n_F) = n$, therefore, $\mathrm{ed}(\mathcal{F}) = n$.

The problem of computing the essential p-dimension of a functor $\mathcal{F}$ very often splits into the two problem of finding a lower and an upper bound for $\operatorname{ed}_p(\mathcal{F})$, and in some cases the bounds match.

For a field extension L/F, there is an obvious functor $r_{L/F} : \mathit{Fields}_L \to \mathit{Fields}_F$. We will write $\mathcal{F}_L$ for the composition of a functor $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ with $r_{L/F}$ and call it the *restriction of $\mathcal{F}$ to L*.

Proposition 2.5. [70, Proposition 1.5] *For any functor $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ and a field extension L/F, we have:*

1. $\operatorname{ed}_p(\mathcal{F}) \geq \operatorname{ed}_p(\mathcal{F}_L)$ *for every $p \geq 0$.*
2. *If L/F is a prime to p extension, then* $\operatorname{ed}_p(\mathcal{F}) = \operatorname{ed}_p(\mathcal{F}_L)$.

Let $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ be a functor. A scheme X of finite type over F is called *p-classifying for $\mathcal{F}$* if there is p-surjective morphism of functors $X \to \mathcal{F}$. A *classifying scheme* is a 0-classifying scheme.

Classifying schemes are used to obtain upper bounds for the essential dimension. Propositions 2.1 and 2.3 yield:

Corollary 2.6. *Let $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ be a functor and X a p-classifying scheme for $\mathcal{F}$. Then* $\dim(X) \geq \operatorname{ed}_p(\mathcal{F})$.

3. ESSENTIAL DIMENSION OF ALGEBRAIC GROUPS

3a. **Torsors.** We will write "algebraic group over F" for a group scheme of finite type over F.

Let G be an algebraic group over F. A *G-scheme* is a scheme X of finite type over F together with a (left) G-action on X. We write $m_X : G \times X \to X$ for the action morphism.

Let E be a G-scheme and Y a G-scheme with the trivial G-action. A G-equivariant morphism $f : E \to Y$ is called a *G-torsor* (or we say that *E is a G-torsor over Y*) if f is faithfully flat and the morphism

$$(m_E, p_E) : G \times E \to E \times_Y E$$

is an isomorphism (here $p_E : G \times E \to E$ is the projection). The latter condition is equivalent to the following: For any commutative F-algebra R and for any R-point $y \in Y(R)$, either the fiber of the map $E(R) \to Y(R)$ over y is empty or the group $G(R)$ acts simply transitively on the fiber.

For every scheme Y over F, the projection $G \times Y \to Y$ has a natural structure of a G-torsor, called the *trivial G-torsor over Y*.

Isomorphism classes of G-torsor over X are in a bijective correspondence with the first flat cohomology pointed set $H^1_{fppf}(X, G)$ (see [77, Ch. III, §4]). If G is smooth, this set coincides with the first étale cohomology pointed set $H^1_{\acute{e}t}(X, G)$. If F is a field, we write $H^1(F, G)$ for $H^1_{\acute{e}t}\big(\operatorname{Spec}(F), G\big) = H^1_{\acute{e}t}\big(\operatorname{Gal}(F_{\mathrm{sep}}/F), G(F_{\mathrm{sep}})\big)$.

Example 3.1. Let G be a finite (constant) group over F. A G-torsor over F is of the form $\operatorname{Spec}(L) \to \operatorname{Spec}(F)$, where L is a Galois G-algebra.

Example 3.2. Let A be an "algebraic object" over F such as algebra, quadratic form, etc. Suppose that the automorphism group $G = \mathbf{Aut}(A)$ has the structure of an algebraic group, in particular, $G(K) = \operatorname{Aut}_K(A_K)$ for every field extension K/F. We say that an object B is a *twisted form of A* if B is isomorphic to A over

F_{sep}. If E is a G-torsor over F, then the "diagonal" action of G on $E\times A$ descends to a twisted form B of A. The G-torsor E can be reconstructed from B via the isomorphism $E\simeq \mathbf{Iso}(B,A)$.

Thus, for any G-object A over F, we have a bijection

$$G\text{-torsors over } F \quad\longleftrightarrow\quad \boxed{\text{Twisted forms of } A}$$

In the list of examples below we have twisted forms of the

- Matrix algebra $M_n(F)$ with $\mathbf{Aut}\big(M_n(F)\big)=\mathbf{PGL}_n$, the projective linear group,
- Algebra $F^n=F\times F\times\cdots\times F$ with $\mathbf{Aut}(F^n)=S_n$, the symmetric group,
- Split nondegenerate quadratic form q_n of dimension n with $\mathbf{Aut}(q_n)=\mathbf{O}_n$, the orthogonal group,
- Split Cayley algebra C with $\mathbf{Aut}(C)=G_2$:

$$\begin{array}{rcl}
\mathbf{PGL}_n\text{-torsors} & \longleftrightarrow & \boxed{\text{Central simple algebras of degree } n}\\
S_n\text{-torsors} & \longleftrightarrow & \boxed{\text{Étale algebras of degree } n}\\
\mathbf{O}_n\text{-torsors} & \longleftrightarrow & \boxed{\text{Nonsingular quadratic forms of dimension } n}\\
G_2\text{-torsors} & \longleftrightarrow & \boxed{\text{Cayley-Dickson algebras}}
\end{array}$$

3b. **Definition of the essential dimension of algebraic groups.** Let G be an algebraic group over F. Consider the functor

$$G\textsf{-}\mathit{torsors} : \mathit{Fields}_F \to \mathit{Sets},$$

taking a field K/F to the set G-*torsors*(K) of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$. The *essential p-dimension* $\mathrm{ed}_p(G)$ *of* G is defined in [83] as the essential dimension of the functor G-*torsors*:

$$\mathrm{ed}_p(G) := \mathrm{ed}_p(G\text{-}\mathit{torsors}).$$

Thus, the essential p-dimension of G measures the complexity of the class of G-torsors over field extensions of F.

Proposition 2.2 yields:

Proposition 3.3. *For algebraic groups G_1 and G_2, we have*

$$(G_1\times G_2)\text{-}\mathit{torsors} \simeq \big(G_1\text{-}\mathit{torsors}\big)\times\big(G_2\text{-}\mathit{torsors}\big) \quad \text{and}$$
$$\mathrm{ed}_p(G_1\times G_2)\le \mathrm{ed}_p(G_1)+\mathrm{ed}_p(G_2)$$

for every $p\ge 0$.

We consider only linear algebraic group except in the last Section 11.

3c. **Cohomological invariants.** Cohomological invariants provide lower bounds for the essential dimension (see [83]). Let M be a Galois module over F, i.e., M is a (discrete) abelian group equipped with a continuous action of the absolute Galois group $\mathrm{Gal}(F_{\mathrm{sep}}/F)$ of F. For a field extension K/F, M can be viewed as a Galois module over K and therefore, for every $d\ge 0$, we have a *degree d cohomological functor*

$$H : \mathit{Fields}_F \to \mathit{AbelianGroups}$$
$$K \mapsto H^d(K,M).$$

A *degree d cohomological invariant u with values in M of a functor $\mathcal{F} : \textsf{Fields}_F \to \textsf{Sets}$* is a morphism of functors $u : \mathcal{F} \to H$, where we view H as a functor to $\textsf{Sets}$. An invariant u is called *nontrivial* if there is a field extension K/F containing an algebraic closure of F and an element $x \in \mathcal{F}(K)$ such that $u_K(x) \neq 0$ in $H(K)$.

The following statement provides a lower bound for the essential p-dimension of a functor.

Theorem 3.4. *Let $\mathcal{F} : \textsf{Fields}_F \to \textsf{Sets}$ be a functor, M a torsion Galois module over F and $p \geq 0$. If $p > 0$ we assume that the order of every element of M is a power of p. If $\mathcal{F}$ admits a nontrivial degree d cohomological invariant with values in M, then* $\operatorname{ed}_p(\mathcal{F}) \geq d$.

Proof. By Proposition 2.5, we may assume that F is algebraically closed. Choose a field extension K/F and an element $x \in \mathcal{F}(K)$ such that $u_K(x) \neq 0$ in $H(K)$. It suffices to show that $\operatorname{ed}_p(x) \geq d$. Suppose the opposite. Then there are field homomorphisms $K \to K'$ and $K_0 \to K'$ over F with K'/K a prime to p extension and $\operatorname{tr.deg}_F(K_0) < d$, and an element $x_0 \in \mathcal{F}(K_0)$ such that $(x_0)_{K'} = x_{K'}$. The composition $H^d(K, M) \to H^d(K', M) \to H^d(K, M)$ of the restriction and corestriction homomorphisms is multiplication by $[K' : K]$ and hence is an isomorphism due to the assumption on M. It follows that $u_K(x)_{K'} \neq 0$ in $H(K')$. As $u_{K_0}(x_0)_{K'} = u_K(x)_{K'}$, we have $u_{K_0}(x_0) \neq 0$ in $H^d(K_0)$. Since K_0 is an extension of the algebraically closed field F of transcendence degree less than d, by a theorem of Serre [93, Ch. II, §4, Proposition 11], $H(K_0) = H^d(K_0, M) = 0$, a contradiction. □

Example 3.5. Write $\boldsymbol{\mu}_n$ for the group of n-th roots of unity over a field F such that n is not divisible by $\operatorname{char}(F)$. For a field extension K/F, we have the Kummer isomorphism

$$K^\times/K^{\times n} \xrightarrow{\sim} H^1(K, \boldsymbol{\mu}_n), \quad aK^n \mapsto (a).$$

It follows that $\big(\mathbf{G}_{\mathrm{m}}\big)^s$ is a classifying variety for $(\boldsymbol{\mu}_n)^s$, where $\mathbf{G}_{\mathrm{m}} := \operatorname{Spec} F[t, t^{-1}]$ is the *multiplicative group*, hence $\operatorname{ed}(\boldsymbol{\mu}_n)^s \leq s$. On the other hand, if p is a prime divisor of n, then the cohomological degree s invariant

$$(a_1, a_2, \dots, a_s) \mapsto (a_1) \cup (a_2) \cup \cdots \cup (a_s) \in H^s\big(K, \boldsymbol{\mu}_p^{\otimes s}\big)$$

is not trivial [7, Corollary 4.9], hence $\operatorname{ed}_p(\boldsymbol{\mu}_n)^s = \operatorname{ed}(\boldsymbol{\mu}_n)^s = s$.

Example 3.6. Let $\mathbf{O}_n$ be the orthogonal group of a nondegenerate quadratic form of dimension n over a field F with $\operatorname{char}(F) \neq 2$. For a field extension K/F, the set $H^1(K, \mathbf{O}_n)$ is bijective to the set of isomorphism classes of nondegenerate quadratic forms of dimension n. Every such form q is diagonalizable, i.e, $q \simeq \langle a_1, a_2, \dots, a_n\rangle$ with $a_i \in K^\times$. It follows that $\big(\mathbf{G}_{\mathrm{m}}\big)^n$ is a classifying variety for $\mathbf{O}_n$, hence $\operatorname{ed}(\mathbf{O}_n) \leq n$. On the other hand, the cohomological degree n invariant

$$\langle a_1, a_2, \dots, a_n\rangle \mapsto (a_1) \cup (a_2) \cup \cdots \cup (a_n) \in H^n(K, \mathbb{Z}/2\mathbb{Z})$$

is well defined and nontrivial [26, §17], hence $\operatorname{ed}_2(\mathbf{O}_n) = \operatorname{ed}(\mathbf{O}_n) = n$.

Example 3.7. Let p be a prime integer and F a field containing a primitive p-th root of unity. If $p = 2$ we assume that F contains a primitive 4-th root of unity. Write $\textsf{CSA}_{p^n,p}(K)$ for the set of isomorphism classes of central simple algebras of degree p^n and exponent dividing p over a field extension K/F. By [73], every algebra A in $\mathsf{CSA}_{p^n,p}(K)$ is Brauer equivalent to the tensor product of cyclic algebras $C_1 \otimes C_2 \otimes \ldots \otimes C_m$, each of degree p. The *k-th divided power of A* is

$$s_k(A) := \sum [C_{i_1}] \cup [C_{i_2}] \cup \cdots \cup [C_{i_k}] \in H^{2k}(K, \mathbb{Z}/p\mathbb{Z}),$$

where the sum is taken over all k-tuples $i_1 < i_2 < \cdots < i_k$ and $[C_j] \in H^2(K, \mathbb{Z}/p\mathbb{Z})$. The class $s_k(A)$ is well defined by [32]. For example, if A is the tensor product of n cyclic algebras (a_i, b_i) of degree p, $i = 1, \ldots, n$, over the field $K = F(a_1, \ldots, a_n, b_1, \ldots, b_n)$ of rational functions, then $s_n(A)$ is nonzero in $H^{2n}(K, \mathbb{Z}/p\mathbb{Z})$, i.e., s_n is a nontrivial cohomological invariant of $\mathsf{CSA}_{p^n,p}$. It follows that $\operatorname{ed}_p(\mathsf{CSA}_{p^n,p}) \geq 2n$ (cf., [84, Example 2.8]). For better lower bounds on $\operatorname{ed}_p(\mathsf{CSA}_{p^n,p})$ see Theorem 10.6.

3d. **Generically free and versal G-schemes.** Let G be an algebraic group over a field F. A G-scheme X is called *generically free* if there is a nonempty dense subscheme $U \subset X$ and a G-torsor $U \to Y$ with Y a variety over F. A G-invariant open subscheme of a generically free G-scheme is also a generically free G-scheme.

The generic fiber $E \to \operatorname{Spec} F(Y)$ of $U \to Y$ is the G-torsor that is independent of the choice of the open set U. We call this torsor the *G-torsor associated to the G-scheme* X and write $F(X)^G$ for the field $F(Y)$.

Conversely, every G-torsor $E \to \operatorname{Spec} K$ for a finitely generated field extension K/F extends to a G-torsor $X \to Y$ for a variety Y over F with $F(Y) \simeq K$.

By [19, Exposé V, Théorème 8.1], a G-scheme X is generically free if and only if there is a dense open subset $U \subset X$ such that the scheme-theoretic stabilizer of every point in U is trivial.

Remark 3.8. An action of a finite group on a variety is generically free if and only if it is faithful.

Let X be a generically free G-scheme. A *G-compression of X* is a G-equivariant dominant rational morphism $X \dashrightarrow X'$ to a generically free G-scheme X'. Following [83], we write $\operatorname{ed}(X, G)$ for the smallest integer

$$\operatorname{tr.deg}_F\bigl(F(X')^G\bigr) = \dim(X') - \dim(G)$$

over all generically free G-varieties X' such that there is G-compression $X \dashrightarrow X'$.

A G-compression $X \dashrightarrow X'$ yields an embedding of fields $F(X')^G \hookrightarrow F(X)^G$, moreover, the G-torsor $E \to \operatorname{Spec} F(X)^G$ associated to X is defined over $F(X')^G$.

The following lemma compares the number $\operatorname{ed}(X, G)$ with the essential dimension of the associated torsor E as defined in Section 3b.

Lemma 3.9. [7, §4] *Let X be a generically free G-scheme and $E \to \operatorname{Spec}\bigl(F(X)^G\bigr)$ the associated G-torsor. Then* $\operatorname{ed}(X, G) = \operatorname{ed}(E)$ *and*

$$\operatorname{ed}(G) = \max \operatorname{ed}(X, G),$$

where the maximum is taken over all generically free G-schemes X.

We say that a generically free G-scheme is *G-incompressible* if for any G-compression $X \dashrightarrow X'$ we have $\dim(X) = \dim(X')$, or equivalently, $\operatorname{ed}(X, G) = \dim(X) - \dim(G)$. Every generically free G-scheme admits a G-compression to a G-incompressible scheme.

A (linear) representation V of G is called *generically free* if V is generically free as a variety. Generically free G-representations exist: embed G into $U := \mathbf{GL}_{n,F}$ for some n as a closed subgroup. Then U is an open subset in the affine space $M_n(F)$ on which G acts linearly with trivial stabilizers.

Following [20], we call a G-scheme X *versal* if for every generically free G-scheme X' with the field $F(X')^G$ infinite and every dense open G-invariant set $U \subset X$, there is a G-equivariant rational morphism $X' \dashrightarrow U$.

By definition, a dense open G-invariant subset of a versal G-scheme is also versal.

Proposition 3.10. [26, §5] *Every G-representation V, viewed as a G-scheme, is versal.*

Proof. Let X be a generically free G-scheme with the field $F(X)^G$ infinite and $U \subset V$ a nonempty open G-invariant subscheme. We need to prove that there is a G-equivariant rational morphism $X \dashrightarrow U$.

Replacing X be a G-invariant dense subset, we may assume that X is a G-torsor over a variety Y. The diagonal G-action on $V \times X$ yields a G-torsor $V \times X \to Z$ for a variety Z. The projection $f : V \times X \to X$ descents to a morphism $g : Z \to Y$. The image Z' of $U \times X$ in Z is a dense open subscheme.

As f is a vector bundle, so is g. The generic fiber W of g is a vector space over the infinite field $F(Y) = F(X)^G$. As the $F(Y)$-points are dense in W, there is a vector in W that belongs to the open subset Z'. This vector yields a rational splitting $h : Y \dashrightarrow Z'$ of g. Then the pull-back of the G-torsor $U \times X \to Z'$ under h is isomorphic to $X \to Y$, hence h yields a G-equivariant rational morphism $X \dashrightarrow U \times X$. The composition of this morphism with the projection $U \times X \to U$ is the desired rational morphism. □

Proposition 3.11. *Let X be a versal generically free G-scheme (for example, a generically free representation of G). Then* $\operatorname{ed}(X, G) = \operatorname{ed}(G)$.

Proof. By Lemma 3.9, it suffices to show that $\operatorname{ed}(X, G) \geq \operatorname{ed}(Z, G)$ for every generically free G-scheme Z. We may assume that $\operatorname{ed}(Z, G) > 0$, i.e. the field $F(Z)^G$ is infinite.

Let $f : X \dashrightarrow X'$ be a G-compression with X' a generically free G-scheme and $\operatorname{tr.deg}_F\big(F(X')^G\big) = \operatorname{ed}(X, G)$. Shrinking X and X', we may assume that f is regular and X' is a G-torsor over some variety. As X is versal, there is a G-equivariant morphism $Z \dashrightarrow X$. Composing with f, we get a G-compression of Z onto a subvariety of X', hence

$$\operatorname{ed}(Z, G) \leq \dim(X') - \dim(G) = \operatorname{tr.deg}_F\big(F(X')^G\big) = \operatorname{ed}(X, G). \qquad \square$$

Let X be a versal generically free G-scheme. The G-torsor $E \to \operatorname{Spec} F(X)^G$ associated to X is called a *generic G-torsor.* Lemma 3.9 and Proposition 3.11 yield:

Corollary 3.12. *Let E be a generic G-torsor. Then* $\operatorname{ed}(E) = \operatorname{ed}(G)$.

Proposition 3.11 also gives:

Proposition 3.13. (Upper bound) *For an algebraic group G, we have*

$$\operatorname{ed}(G) = \min \dim(X) - \dim(G),$$

where the minimum is taken over all versal generically free G-varieties X. In particular, if V is a generically free representation of G, then

$$\operatorname{ed}(G) \leq \dim(V) - \dim(G).$$

If a G-scheme X is versal and generically free, and $X \dashrightarrow X'$ is a G-compression, then the G-scheme X' is also versal and generically free. Every versal G-scheme X admits a G-equivariant rational morphism $V \dashrightarrow X$ for every generically free G-representation V, and this morphism is dominant (and therefore, is a G-compression) if X is G-incompressible, hence $F(X)$ is a subfield of the purely transcendental extension $F(V)/F$.

We have proved:

Proposition 3.14. *Every versal G-incompressible G-scheme X is a unirational variety with* $\dim(X) = \operatorname{ed}(G) + \dim(G)$.

Let H be a subgroup of an algebraic group G. Then every generically free G-representation is also a generically free H-representation. This yields:

Proposition 3.15. [9, Lemma 2.2] *Let H be a subgroup of an algebraic group G. Then*

$$\operatorname{ed}_p(G) + \dim(G) \geq \operatorname{ed}_p(H) + \dim(H)$$

for every $p \geq 0$.

3e. **Special groups.** For a scheme X over F we let n_X denote the $\gcd \deg(x)$ over all closed points $x \in X$.

Let G be an algebraic group over F. The *torsion index t_G of G* is the least common multiple of the numbers n_X over all G-torsors $X \to \operatorname{Spec}(K)$, as K ranges over the field extensions of F. Prime divisors of t_G are called *torsion primes for G* [90, Sec. 2.3].

An algebraic group G over F is called *special* if for any field extension K/F, every G-torsor over $\operatorname{Spec} K$ is trivial. Clearly, special group schemes have no torsion primes. Examples of special groups are $\mathbf{GL}_n$, $\mathbf{SL}_n$, $\mathbf{Sp}_{2n}$.

The last statement of the following proposition was proven in [83, Proposition 5.3] in the case when F is algebraically closed.

Proposition 3.16. [70, Proposition 4.4], [98, Proposition 4.3] Let G be an algebraic group over F. Then

1. A prime integer p is a torsion prime for G if and only if $\operatorname{ed}_p(G) > 0$.
2. An algebraic group scheme G is special if and only if $\operatorname{ed}(G) = 0$.

3f. **The valuation method.** Valuation theory provides lower bounds for the essential dimension. Let K/F be a field extension and v a valuation on K over F, i.e., v is trivial on F. Let $F(v)$ be the residue field of v, it is an extension of F. The method is based on the inequality [104, Ch. VI, Th. 3, Cor. 1]

$$\operatorname{tr.deg}_F(K) \geq \operatorname{tr.deg}_F\big(F(v)\big) + \operatorname{rank}(v), \tag{3.1}$$

where $\operatorname{rank}(v)$ is the *rank* of the valuation v.

Proposition 3.17. [12], [33, Theorem 1.2] *Let G be a finite group, F a field such that* $\operatorname{char}(F)$ *does not divide $|G|$, and $m > 1$ an integer. If G has no nontrivial central cyclic subgroup of order prime to m, then* $\operatorname{ed}(G \times \boldsymbol{\mu}_m) = \operatorname{ed}(G) + 1$.

Proof. Recall that $H^1(K, \boldsymbol{\mu}_m) = K^\times / K^{\times m}$. Therefore, we have a surjection of functors

$$\big(G\text{-}\mathit{torsors}\big) \times \mathbf{G}_{\mathrm{m}} \to (G \times \boldsymbol{\mu}_m)\text{-}\mathit{torsors}.$$

By Proposition 3.3 and Example 3.5, $\operatorname{ed}(G \times \boldsymbol{\mu}_m) \leq \operatorname{ed}(G) + 1$.

Let V be a faithful G-representation and $\operatorname{Spec}(L) \to \operatorname{Spec}(K)$ the associated generic G-torsor, where $L = F(V)$ and $K = F(V)^G$. Note that as L/F is purely transcendental, the fields F and L have the same roots of unity: $\mu(L) = \mu(F)$.

The pair $\alpha := \big(L((t))/K((t)), t\big)$, where t is a variable, represents a $(G \times \boldsymbol{\mu}_m)$-torsor over the Laurent power series field $K((t))$. Let L_0/K_0 be a G-Galois subextension of $L((t))/K((t))$ over F and $t_0 \in K_0^\times$ an element such that $\operatorname{tr.deg}_F(K_0) = \operatorname{ed}(\alpha)$ and the image of t_0 in $K((t))^\times$ is equal to the class of t modulo $K((t))^{\times m}$, i.e., $t = t_0 \cdot s^m$ for some $s \in K((t))^\times$.

Consider the valuation v on $L((t))$ over L with t a prime element. We have $v(t_0) = 1 - mv(s)$. It follows that $v(t_0) \neq 0$ and hence the restriction v_0 of v on L_0 is a nontrivial discrete valuation (of rank 1). We can view the completions $\widehat{L}_0$ and $\widehat{K}_0$ with respect to v_0 as subfields of $L((t))$ and $K((t))$ respectively, and the extension $\widehat{L}_0/\widehat{K}_0$ is G-Galois.

Moreover, the ramification index of the extension $K((t))/\widehat{K}_0$ is relatively prime to m as it divides $v(t_0)$. Since the extension $L((t))/K((t))$ is unramified, the ramification index of $\widehat{L}_0/\widehat{K}_0$ is relatively prime to m. It follows that the order of the inertia subgroup $H \subset G$ for the extension $\widehat{L}_0/\widehat{K}_0$ is prime to m. By [92, Ch. IV, §2], H is normal in G and there is a G-equivariant embedding $H \hookrightarrow \mu(\widehat{L}_0)$. As $\mu(\widehat{L}_0) \subset \mu(L((t))) = \mu(F)$, the G-action (by conjugation) on H is trivial, hence H is a central cyclic subgroup of G. By assumption, H is trivial, i.e., the extension L_0/K_0 is unramified. Therefore, the extension $\overline{L}_0/\overline{K}_0$ of residue fields is G-Galois and it is a subextension of L/K, i.e., L/K is defined over $\overline{K}_0$. By definition of the essential dimension, Corollary 3.12 and (3.1),

$$\begin{aligned}\operatorname{ed}(G) + 1 = \operatorname{ed}(L/K) + 1 \leq \operatorname{tr.deg}_F(\overline{K}_0) + 1 \leq \\ \operatorname{tr.deg}_F(K_0) = \operatorname{ed}(\alpha) \leq \operatorname{ed}(G \times \boldsymbol{\mu}_m).\end{aligned}$$ □

Corollary 3.18. [12, Corollary 5.5] *Let p be a prime integer and F a field containing a primitive p-th root of unity such that* $\operatorname{char}(F)$ *does not divide* $|G|$. *Assume that the center of G is a p-group* (*possibly trivial*). Then $\operatorname{ed}\big(G \times \mathbb{Z}/p\mathbb{Z}\big) = \operatorname{ed}(G) + 1$.

Other examples of the valuation method are given in Theorem 5.11 and in Section 10b.

3g. **The fixed point method.**

Theorem 3.19. [28, Theorem 1.2] *If G is connected algebraic group, A is a finite abelian subgroup of G and* $\operatorname{char}(F)$ *does not divide* $|A|$, *then*

$$\operatorname{ed}(G) \geq \operatorname{rank}(A) - \operatorname{rank} C_G^0(A),$$

where $C_G^0(A)$ is the connected component of the centralizer of A in G. Moreover, if A is a p-groups, then

$$\operatorname{ed}_p(G) \geq \operatorname{rank}(A) - \operatorname{rank} C_G^0(A),$$

This inequality, conjectured by J.-P. Serre, generalizes previous results in [86] (where $\operatorname{char}(F)$ is assumed to be 0 and $C_G(A)$ to be finite) and [16] (where A is assumed to be a 2-group).

The proof is based on the following theorem.

Theorem 3.20. [86, Appendix] *Let A be an abelian group and let F have primitive root of unity of order the exponent of A. Let $f : Y \dashrightarrow X$ be an A-equivariant rational morphism of A-schemes. If Y has a smooth A-fixed F-point and X is complete then X has an A-fixed F-point.*

Proof. Induction on $n = \dim(Y)$. The case $n = 0$ is obvious. In general, let $y \in Y$ be a smooth A-fixed F-point and $g : \widetilde{Y} \to Y$ the blowing-up of Y at y. The exceptional divisor E is isomorphic to $\mathbb{P}(V) \simeq \mathbb{P}^{n-1}$, where V is the tangent space of Y at y. As A is abelian, by the assumption on the roots of unity, A has an eigenvector in V and hence $\mathbb{P}(V)$ has an A-fixed F-point. Since X is complete, the composition $f \circ g$ restricts to an A-equivariant rational morphism $\mathbb{P}(V) \dashrightarrow X$. By induction, X has an A-fixed F-point. □

The following corollary gives a necessary condition for a G-scheme to be versal.

Corollary 3.21. *Let X be a complete versal G-scheme and $A \subset G$ a finite abelian subgroup such that F has a primitive root of unity of order the exponent of A. Then X has an A-fixed F-point.*

Proof. Let V be a generically free G-scheme. As X is versal, there is G-equivariant rational morphism $V \dashrightarrow X$. The zero vector in V is an A-fixed point. By the theorem, X has an A-fixed point. □

3h. **Exceptional groups.** In the table one finds the bounds for the essential p-dimension of split semisimple algebraic groups of exceptional types. Regarding bounds for $\mathrm{ed}_p(G)$, p prime, we assume that the characteristic of the base field is different from p. It is sufficient to consider the torsion primes for each group (see Proposition 3.16).

p	G_2	F_4	E_6^{ad}	E_6^{sc}	E_7^{ad}	E_7^{sc}	E_8
0	3	$5 \le 7$	$4 \le 65$	$4 \le 8$	$8 \le 118$	$7 \le 29$	$9 \le 231$
2	3	5	3	3	$8 \le 57$	$7 \le 27$	$9 \le 120$
3	–	3	$4 \le 21$	4	3	3	$5 \le 73$
5	–	–	–	–	–	–	3

We have the following lower bounds for $\mathrm{ed}_p(G)$:

The lower bounds for $\mathrm{ed}_p(G)$ with $p > 0$ in the table are valid over an arbitrary field of characteristic different from p. The lower bound for $\mathrm{ed}(G)$ is the maximum of the lower bounds for $\mathrm{ed}_p(G)$ over all $p > 0$.

Case $p = 2$: All lower bounds are listed in [16] or given by the Rost invariant (see [26]).

Case $p > 2$: All lower bounds follow from [28] over an arbitrary field of characteristic different from p. They all come from finite abelian elementary p-subgroups with finite centralizer (see Theorem 3.19), except for E_7, $p = 3$. In the case E_7^{sc}, $p = 3$, the lower bound is given by the Rost invariant and $\mathrm{ed}_3(E_7^{ad}) = \mathrm{ed}_3(E_7^{sc})$.

Now consider the upper bounds for $\mathrm{ed}_p(G)$:

Case G_2: Every Cayley-Dickson algebra can be given by 3 parameters (see [48, Chapter VIII]), hence $\mathrm{ed}(G_2) = \mathrm{ed}_3(G_2) = 3$.

Case E_6^{ad}, E_7^{ad}, E_8 and $p = 0$: see [56, Corollary 1.4] (over an algebraically closed field of characteristic 0).

Case F_4 and E_6^{sc} and $p = 0$: due to MacDonald, unpublished; $\mathrm{char}(F) \neq 2$ or 3. It was shown in [83, Proposition 11.7] that $\mathrm{ed}(E_6^{sc}) \leq \mathrm{ed}(F_4)+1$ (see also [27, 9.12]).

Case E_7^{sc} and $p = 0$: In [62], $\mathrm{char}(F) \neq 2$ or 3.

Case $p \neq 0$:

$(F_4, 2)$, $(F_4, 3)$, $(E_6, 2)$, $(E_6^{sc}, 3)$, $(E_8, 5)$: follow from [26, 22.10]. A finite elementary abelian subgroup $H \subset G$ was found such that the morphism H-*torsors* $\to$ G-*torsors* is surjective.
$(E_7, 3)$: see [28, 9.6].
$(E_7^{sc}, 2)$: see [62].
$(E_6^{ad}, 3)$, $(E_7^{ad}, 2)$, $(E_8, 2)$, $(E_8, 3)$: see [61].
It was claimed in [49] that $ed(F_4) = 5$ but there were gaps in the proof.

3i. **Symmetric and alternating groups.** Let F be a field of characteristic zero.

The study of the essential dimension of the symmetric group S_n and the alternating group A_n was initiated in [12, Theorem 6.5]. An S_n-torsor over a field extension K/F is given by a S_n-Galois K-algebra or, equivalently, a degree n étale K-algebra. The group A_n is a subgroup of S_n, hence $\mathrm{ed}(A_n) \leq \mathrm{ed}(S_n)$ by Proposition 3.15.

The group $S_n \times \mathbb{Z}/2\mathbb{Z}$ (respectively, $A_n \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) is isomorphic to a subgroup of S_{n+2} (respectively, A_{n+4}). By Corollary 3.18,

$$\mathrm{ed}(S_{n+2}) \geq \mathrm{ed}(S_n) + 1, \quad \mathrm{ed}(A_{n+4}) \geq \mathrm{ed}(A_n) + 2 \quad \text{if} \quad n \geq 4.$$

The standard S_n-action on the product X of n copies of the projective line $\mathbb{P}^1_F$ commutes element-wise with the diagonal action of the automorphism group $H := \mathbf{PGL}_2$ of $\mathbb{P}^1_F$. The variety X is birationally S_n-isomorphic to the affine space $\mathbb{A}^n_F$ with the standard linear action of S_n. By Proposition 3.10, the S_n-variety X is versal. If $n \geq 5$, the induced action of S_n on X/H is faithful and therefore, is versal as X/H is an S_n-compression of X. Hence

$$\mathrm{ed}(S_n) \leq \dim(X/H) = \dim(X) - \dim(H) = n - 3.$$

As A_4 contains a subgroup $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, hence $\mathrm{ed}(A_4) \geq \mathrm{ed}(H) = 2$ by Example 3.5 and Proposition 3.15.

The lower bound $\mathrm{ed}(A_6) \geq 3$ was obtained in [94, Theorem 3.6]. By Proposition 2.5, we may assume that F is algebraically closed. Suppose that $\mathrm{ed}(A_6) = 2$. By Proposition 3.14, there is a unirational surface X with a faithful versal A_6-action. In view of the equivariant resolution of singularities (see [94, Theorem 2.1]) we may assume that X is smooth projective. By a theorem of Castelnuovo, X is a rational surface. In view of Enriques-Manin-Iskovskikh classification of minimal rational G-surfaces (see [63] and [31]), X is either a conic bundle over $\mathbb{P}^1$ or a del Pezzo surface. The classification of minimal rational G-surfaces reduces the problem to an A_6-action on the projective plane $\mathbb{P}^2$. It is then shown that the (abelian) 3-Sylow subgroup of A_6 acts on $\mathbb{P}^2$ without fixed points contradicting Corollary 3.21.

The lower bound $\mathrm{ed}(A_7) \geq 4$ was proved in [22] along similar lines. Suppose $\mathrm{ed}(A_7) = 3$. By Proposition 3.14, there exists a unirational smooth projective 3-fold X with a faithful versal A_7-action. As X is unirational, it is rationally connected. Rationally connected 3-folds with a faithful A_7-action were classified in [80, Theorem

1.5]. For each such an X one finds an abelian subgroup of A_7 without fixed points contradicting Corollary 3.21.

We collect all the facts in the following theorem.

Theorem 3.22. *All known values of the essential dimension of* A_n *and* S_n *are collected in the following table:*

n	1	2	3	4	5	6	7
$\mathrm{ed}(A_n)$	0	0	1	2	2	3	4
$\mathrm{ed}(S_n)$	0	1	1	2	2	3	4

Moreover, we have the following inequalities:

$$n-3 \geq \mathrm{ed}(S_n) \geq \left[\frac{n+1}{2}\right]$$

$$n-3 \geq \mathrm{ed}(A_n) \geq \begin{cases} \frac{n}{2}, & \textit{if } n \textit{ is even;} \\ \frac{n-1}{2}, & \textit{if } n \equiv 1 \textit{ mod } 4; \\ \frac{n+1}{2}, & \textit{if } n \equiv 3 \textit{ mod } 4. \end{cases}$$

The values of the essential p-dimension for $p > 0$ were computed in [74, Corollary 4.2]:

$$\mathrm{ed}_p(S_n) = \left[\frac{n}{p}\right].$$

3j. **Finite groups of low essential dimension.** Let G be a nontrivial finite group. Since there is a field extension with Galois group G, the group G has nontrivial G-torsors and hence G is not special, hence $\mathrm{ed}(G) \geq 1$ by Proposition 3.16. If $\mathrm{ed}(G) = 1$, every faithful G-representation compresses to a curve C with a faithful G-action. As C is unirational, by Lüroth Theorem, we may assume that $C = \mathbb{P}^1_F$, hence $G \subset \mathrm{Aut}(\mathbb{P}^1_F) = \mathbf{PGL}_2$. It turns out that the G-action on $\mathbb{P}^1_F$ is versal if and only if G can be lifted to $\mathbf{GL}_2$ (see [21, Corollary 3.4]).

Theorem 3.23. [55, Theorem 1] *A nontrivial finite group* G *has essential dimension* 1 *over a field* F *if and only if there exists an embedding* $G \hookrightarrow \mathbf{GL}_2$ *over* F *such that the image of* G *contains no scalar matrices other than the identity.*

In [17] the authors give a complete classification of finite groups of essential dimension 1 over an arbitrary field. Over an algebraically closed field of characteristic zero, $\mathrm{ed}(G) = 1$ if and only if G is nontrivial cyclic or odd dihedral [12, Theorem 6.2].

Finite groups of essential dimension 2 were classified in [21]. Suppose that $\mathrm{ed}(G) = 2$ for a finite group G. By Proposition 3.14, there is a unirational (and hence rational) smooth projective surface X with a faithful versal G-action. Using the Enriques-Manin-Iskovskikh classification of minimal rational G-surfaces, for each G-action on X it was decided in [21] whether X is versal.

Theorem 3.24. [21, Theorem 1.1] *Let* F *be an algebraically closed field of characteristic* 0 *and* $T = (\mathbf{G}_{\mathrm{m}})^2$ *a* 2*-dimensional torus. If* G *is a finite group of essential dimension* 2 *then* G *is isomorphic to a subgroup of one of the following groups:*

(1) $\mathbf{GL}_2$,
(2) $\mathrm{PSL}_2(\mathbb{F}_7)$*, the simple group of order 168,*
(3) S_5*, the symmetric group,*

(4) $T \rtimes G_1$, *where* $|G \cap T|$ *is coprime to* 2 *and* 3 *and*

$$G_1 = \left\langle \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq D_{12},$$

(5) $T \rtimes G_2$, *where* $|G \cap T|$ *is coprime to* 2 *and*

$$G_2 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq D_{8},$$

(6) $T \rtimes G_3$, *where* $|G \cap T|$ *is coprime to* 3 *and*

$$G_3 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\rangle \simeq S_{3},$$

(7) $T \rtimes G_4$, *where* $|G \cap T|$ *is coprime to* 3 *and*

$$G_4 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq S_{3},$$

Furthermore, any finite subgroup of these groups has essential dimension ≤ 2.

Finite simple groups of essential dimension 3 were classified in [5]. Let G be a finite simple group with $\mathrm{ed}(G) = 3$. By Proposition 3.14, there exists a unirational (and hence rationally connected) smooth projective 3-fold X with a faithful versal G-action. Rationally connected 3-folds with a faithful action of a finite simple group were classified in [80, Theorem 1.5]. One can rule out most of the groups thanks to Corollary 3.21. Unfortunately this criterion does not apply to $\mathrm{PSL}_2(\mathbb{F}_{11})$.

Theorem 3.25. [5] *The simple groups of essential dimension* 3 *are* A_6 *and possibly* $\mathrm{PSL}_2(\mathbb{F}_{11})$. *The essential dimension of* $\mathrm{PSL}_2(\mathbb{F}_{11})$ *is either* 3 *or* 4.

3k. **Essential p-dimension over fields of characteristic p.** (See [53] and [54].)

Let F be a field of characteristic $p > 0$ and $G = \mathbb{Z}/p^n\mathbb{Z}$. By [92, Ch. II, §5], for a field extension K/F, the group $H^1(K, G)$ is isomorphic to a factor group of the group of *Witt vectors* $W_n(K)$. Thus, the affine space $\mathbb{A}^n_F$ is a classifying variety for G and hence $\mathrm{ed}(G) \leq n$.

Conjecture 3.26. *Over a field of characteristic* $p > 0$,

$$\mathrm{ed}_p(\mathbb{Z}/p^n\mathbb{Z}) = \mathrm{ed}(\mathbb{Z}/p^n\mathbb{Z}) = n.$$

The conjecture holds for $n = 1$ and 2 by Theorem 3.23.

Theorem 3.27. *Let* F *be a field of characteristic* $p > 0$ *and* $|F| \geq p^n$ *for some* $n > 0$. *Then* $\mathrm{ed}\big(\mathbb{Z}/p\mathbb{Z}\big)^n = 1$.

Proof. By assumption, the group $(\mathbb{Z}/p\mathbb{Z})^n$ can be embedded into $\mathbf{GL}_2$ as a unipotent subgroup of upper triangular matrices. The induced action on the projective line $\mathbb{P}^1$ is faithful and versal, hence $\mathrm{ed}\big(\mathbb{Z}/p\mathbb{Z}\big)^n \leq 1$. □

4. Canonical dimension

4a. **Definition of the canonical dimension.** The notion of canonical dimension of G-schemes was introduced in [6]. In this section we define the canonical p-dimension of a functor (see [47, §2] and [70, §1.6]).

Let $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ be a functor and $x \in \mathcal{F}(K)$ for a field extension K/F. A subfield $K_0 \subset K$ over F is called a *detection field of* x (or K_0 *is a detection field of* x) if $\mathcal{F}(K_0) \neq \emptyset$. Define the *canonical dimension of* x:

$$\operatorname{cdim}(x) := \min \operatorname{tr.deg}_F(K_0),$$

where the minimum is taken over all detection fields K_0 of x. Note that $\operatorname{cdim}(x)$ depends only on $\mathcal{F}$ and K but not on x.

For $p \geq 0$ we define

$$\operatorname{cdim}_p(x) := \min \operatorname{cdim}(x_L),$$

where L runs over all prime to p extensions of K. We set

$$\operatorname{cdim}_p(\mathcal{F}) := \max \operatorname{cdim}_p(x),$$

where the maximum runs over all field extensions K/F and all $x \in \mathcal{F}(K)$.

Define the functor $\widehat{\mathcal{F}}$ by

$$\widehat{\mathcal{F}}(K) = \begin{cases} \{K\}, & \text{if } \mathcal{F}(K) \neq \emptyset; \\ \emptyset, & \text{otherwise.} \end{cases}$$

It follows from the definitions of the canonical and the essential dimension that

$$\operatorname{cdim}_p(\mathcal{F}) = \operatorname{ed}_p(\widehat{\mathcal{F}}),$$

i.e., the canonical dimension is a special case of the essential dimension. Since there is a natural surjection $\mathcal{F} \to \widehat{\mathcal{F}}$, we have

$$\operatorname{cdim}_p(\mathcal{F}) \leq \operatorname{ed}_p(\mathcal{F})$$

by Proposition 2.3.

A functor $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ is called a *detection functor* if $|\mathcal{F}(K)| \leq 1$ for every field extension K/F. For example, $\widehat{\mathcal{F}}$ is a detection functor for every functor $\mathcal{F}$.

A class $\mathcal{C}$ of fields in Fields_F closed under extensions determines the detection functor $\mathcal{F}_{\mathcal{C}} : \mathit{Fields}_F \to \mathit{Sets}$ defined by

$$\mathcal{F}_{\mathcal{C}}(K) = \begin{cases} \{K\}, & \text{if } K \in \mathcal{C}; \\ \emptyset, & \text{otherwise.} \end{cases}$$

We define the *essential* p*-dimension* of the class $\mathcal{C}$ by

$$\operatorname{ed}_p(\mathcal{C}) := \operatorname{ed}_p(\mathcal{F}_{\mathcal{C}}) = \operatorname{cdim}_p(\mathcal{F}_{\mathcal{C}}).$$

Every functor $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$ determines the class $\mathcal{C}_{\mathcal{F}}$ of field extensions K/F such that $\mathcal{F}(K) \neq \emptyset$. The class $\mathcal{C}_{\mathcal{F}}$ is closed under extensions. In particular, we get mutually inverse bijections $\mathcal{C} \mapsto \mathcal{F}_{\mathcal{C}}$ and $\mathcal{F} \mapsto \mathcal{C}_{\mathcal{F}}$ between the classes of field extensions in Fields_F closed under extensions and the (isomorphism classes of) detection functors, moreover,

$$\operatorname{cdim}_p(\mathcal{F}) = \operatorname{ed}_p(\mathcal{C}_{\mathcal{F}}).$$

4b. **Canonical p-dimension of a variety.** Let X be a scheme of finite type over F. Viewing X as a functor from Fields_F to Sets, we have the *canonical* p*-dimension* $\operatorname{cdim}_p(X)$ of X defined. In other words, $\operatorname{cdim}_p(X)$ is the essential p-dimension of the class

$$\mathcal{C}_X = \{K \in \mathit{Fields}_F \quad \text{such that} \quad X(K) \neq \emptyset\}.$$

By Proposition 2.1, $\operatorname{cdim}_p(X) \leq \operatorname{ed}_p(X) = \dim(X)$.

Recall that n_X denotes the $\gcd \deg(x)$ over all closed points $x \in X$.

Lemma 4.1. *Let X be a variety over F and $p \geq 0$. Then*

(1) *If $(n_X, p) = 1$ (this means $n_X = 1$ if $p = 0$), then $\operatorname{cdim}_p(X) = 0$.*
(2) *If $\operatorname{cdim}_p(X) = 0$ and X is geometrically irreducible, then $(n_X, p) = 1$.*

Proof. (1) By assumption, there is prime to p extension L/F such that $X(L) \neq \emptyset$. Let $x \in X(K)$ for a field extension K/F. By [70, Lemma 6.1], there is a prime to p extension K'/K that admits an F-homomorphism $L \to K'$. It follows that L is a detection field of $x_{K'}$, hence $\operatorname{cdim}_p(x) \leq \operatorname{tr.deg}_F(L) = 0$.

(2) Let $x_{gen} \in X\big(F(X)\big)$ be the generic point. By assumption, $\operatorname{cdim}_p(x_{gen}) = 0$, hence there is a prime to p extension $K'/F(X)$ and a subfield $K_0 \subset K'$ such that $X(K_0) \neq \emptyset$ and $\operatorname{tr.deg}_F(K_0) = 0$, i.e., $[K_0 : F] < \infty$. As X is geometrically irreducible, X_{K_0} is a variety and $[K_0(X) : F(X)] = [K_0 : F]$. Since $K_0(X)$ is a subfield of K', the finite extensions $K_0(X)/F(X)$ and K_0/F have degree prime to p. The variety X has a point over K_0, hence $(n_X, p) = 1$. □

Write x_{gen} for the generic point of a variety X in $X\big(F(X)\big)$.

Lemma 4.2. *Let X be a variety over F and $p \geq 0$. Then $\operatorname{cdim}_p(x_{gen})$ is the least dimension of the image of a morphism $X' \to X$, where X' is a variety over F admitting a dominant morphism $X' \to X$ of degree prime to p (of degree 1 if $p = 0$). In particular, $\operatorname{cdim}(x_{gen})$ is the least dimension of the image of a rational morphism $X \dashrightarrow X$.*

Proof. Choose a prime to p extension $K'/F(X)$ and a subfield $K_0 \subset K'$ such that $X(K_0) \neq \emptyset$ and $\operatorname{tr.deg}_F(K_0) = \operatorname{cdim}_p(x_{gen})$. Let Z be the closure of the image of a point $x_0 : \operatorname{Spec} K_0 \to X$. We have $\dim(Z) \leq \operatorname{tr.deg}_F(K_0)$. The compositions

$$\operatorname{Spec} K' \to \operatorname{Spec} F(X) \xrightarrow{x_{gen}} X \quad \text{and} \quad \operatorname{Spec} K' \to \operatorname{Spec} K_0 \xrightarrow{x_0} Z$$

yield a model X' of K' and two dominant morphisms $X' \to X$ of degree prime to p and $X' \to Z$ (cf. [70, §6]). We have

$$\operatorname{cdim}_p(x_{gen}) = \operatorname{tr.deg}_F(K_0) \geq \dim(Z).$$

Let $X' \to X$ be a dominant morphism of degree prime to p and let $X' \to X$ be another morphism with the image $Z \subset X$. Then $F(X')$ is a field extension of $F(Z)$ and $F(X')/F(X)$ is a field extension of degree prime to p. It follows that $(x_{gen})_{F(X')}$ is detected by $F(Z)$. By the definition of canonical p-dimension, we have

$$\operatorname{cdim}_p(x_{gen}) \leq \operatorname{tr.deg}_F\big(F(Z)\big) = \dim(Z). \qquad \square$$

We say that a scheme X over F is *p-incompressible* if $\operatorname{cdim}_p(X) = \dim(X)$. A scheme X is *incompressible* if it is 0-incompressible. Every p-incompressible scheme is incompressible.

Proposition 4.3. *Let X be a variety over F. Then X is p-incompressible if and only if for any variety X' over F admitting a dominant morphism $X' \to X$ of degree prime to p, every morphism $X' \to X$ is dominant. In particular, X is incompressible if and only if every rational morphism $X \dashrightarrow X$ is dominant.*

Proof. Suppose that for any variety X' over F admitting a dominant morphism $X' \to X$ of degree prime to p, every morphism $X' \to X$ is dominant. By Lemma 4.2, $\dim(X) \geq \operatorname{cdim}_p(X) \geq \operatorname{cdim}_p(x_{gen}) = \dim(X)$. It follows that $\operatorname{cdim}_p(X) = \dim(X)$.

Conversely, suppose that $\operatorname{cdim}_p(X) = \dim(X)$. There is a field extension K/F and a point $x \in X(K)$ with $\operatorname{cdim}_p(x) = \dim(X)$. Let $f : X' \to X$ be a dominant morphism of degree prime to p and let $g : X' \to X$ be another morphism. We need to show that g is dominant. By construction, the morphism $x : \operatorname{Spec}(K) \to X$ is dominant. In view of [70, Lemma 6.1], there is field extension K'/K of degree prime to p and a point $x' \in X'(K')$ such that $f(x') = x$. Let Z be the image of the composition $g \circ x' : \operatorname{Spec}(K') \to X$. Then $F(Z)$ is a subfield of K', hence $x_{K'}$ is detected by $F(Z)$. As $\dim(Z) = \operatorname{tr.deg}_F\big(F(Z)\big) \geq \operatorname{cdim}_p(x) = \dim(X)$, we must have $Z = X$, i.e., $g \circ x'$ is dominant. It follows that g is dominant. □

Proposition 4.4. [46, Corollary 4.11] *Let X be a regular complete variety over F. Then $\operatorname{cdim}_p(X)$ is the least dimension of the image of a morphism $X' \to X$, where X' is a variety over F admitting a dominant morphism $X' \to X$ of degree prime to p (of degree 1 if $p = 0$). In particular, $\operatorname{cdim}(X)$ is the least dimension of the image of a rational morphism $X \dashrightarrow X$.*

Proof. Write d for the least dimension of the image of a morphism $X' \to X$, where X' is a variety over F admitting a dominant morphism $X' \to X$ of degree prime to p. Let $Z \subset X$ be a closed subvariety of dimension d and $X' \to X$, $X' \to Z$ dominant morphisms with the first one of degree prime to p. Replacing X' by the closure of the graph of the diagonal morphism $X' \to X \times Z$ we may assume that X' is complete.

Let $x \in X(K)$ for a field extension K/F, i.e., $x : \operatorname{Spec} K \to X$ is a morphism over F. Write $\{\bar{x}\} \subset X$ for the image of x. As $\bar{x}$ is a non-singular point of X, there is a geometric valuation v of $F(X)$ over F with center $\bar{x}$ and $F(v) = F(\bar{x}) \subset K$ by [70, Lemma 6.6]. We view $F(X)$ as a subfield of $F(X')$. As $F(X')/F(X)$ is a finite extension of degree prime to p, by [70, Lemma 6.4], there is an extension v' of v on $F(X')$ such that $F(v')/F(v)$ is a finite extension of degree prime to p. Since X' is complete, v' has center $x' \in X'$. Let z be the image of x' in Z. As $F(x') \subset F(v')$, the extension $F(x')/F(\bar{x})$ is finite of degree prime to p.

By [70, Lemma 6.1], there is a prime to p extension K'/K that admits an F-homomorphism $F(x') \to K'$. Thus, $F(z)$ is a subfield of K', hence $F(z)$ is a detection field of $x_{K'}$, therefore,

$$\operatorname{cdim}_p(x) \leq \operatorname{tr.deg}_F F(z) \leq \dim(Z),$$

and $\operatorname{cdim}_p(X) \leq \dim(Z) = d$.

By Lemma 4.2, we have the opposite inequality $\operatorname{cdim}_p(X) \geq \operatorname{cdim}_p(x_{gen}) = d$. □

Let X and Y be varieties over F and $d = \dim(X)$. A *correspondence from X to Y*, denoted $\alpha\colon X \rightsquigarrow Y$, is an element $\alpha \in \operatorname{CH}_d(X \times Y)$ of the Chow group of classes of algebraic cycles of dimension d on $X \times Y$. If $\dim(Y) = d$, we write $\alpha^t\colon Y \rightsquigarrow X$ for the image of α under the exchange isomorphism $\operatorname{CH}_d(X \times Y) \simeq \operatorname{CH}_d(Y \times X)$.

Let $\alpha\colon X \rightsquigarrow Y$ be a correspondence. Assume that Y is complete. The projection morphism $p\colon X \times Y \to X$ is proper and hence the push-forward homomorphism

$$p_*\colon \operatorname{CH}_d(X \times Y) \to \operatorname{CH}_d(X) = \mathbb{Z} \cdot [X]$$

is defined [25, § 1.4]. The integer $\operatorname{mult}(\alpha) \in \mathbb{Z}$ such that $p_*(\alpha) = \operatorname{mult}(\alpha) \cdot [X]$ is called the *multiplicity* of α. For example, if α is the the class of the closure of the graph of a rational morphism $X \dashrightarrow Y$ of varieties of the same dimension, then $\operatorname{mult}(\alpha) = 1$ and $\operatorname{mult}(\alpha^t) := \deg(f)$ the *degree* of f.

Proposition 4.5. [39, Lemma 2.7] *Let p be a prime integer and X a complete variety. Suppose that for every correspondence $\alpha : X \rightsquigarrow X$ such that* $\operatorname{mult}(\alpha)$ *is not divisible by p, the integer* $\operatorname{mult}(\alpha^t)$ *is also not divisible by p. Then X is p-incompressible.*

Proof. Let $f, g : X' \to X$ be two morphisms such that f is dominant of degree prime to p. Let $\alpha \in \operatorname{CH}_d(X \times X)$, where $d = \dim(X)$, be the class of the closure of the graph of the morphism $(f, g) : X' \to X \times X$. Then $\operatorname{mult}(\alpha) = \deg(f)$ is prime to p. By assumption, $\deg(g) = \operatorname{mult}(\alpha^t)$ is also prime to p. In particular, $\deg(g) \neq 0$ and g is dominant. By Proposition 4.4, X is p-incompressible. □

4c. **Chow motives.** Let Λ be a commutative ring. Write $\mathit{CM}(F, \Lambda)$ for the additive category of *Chow motives with coefficients in* Λ over F (see [23, §64]). If X is a smooth complete scheme, we let $M(X)$ denote its motive in $\mathit{CM}(F, \Lambda)$. We write $\Lambda(i)$, $i \geq 0$, for the *Tate motives.* For example, the motive of the projective space $\mathbb{P}^n$ is isomorphic to $\Lambda \oplus \Lambda(1) \oplus \cdots \oplus \Lambda(n)$ in $\mathit{CM}(F, \Lambda)$.

Let X be a smooth complete variety over F and M a motive in $\mathit{CM}(F, \mathbb{Z})$. We call M *split*, if it is a (finite) direct sum of Tate motives. We call X *split*, if its motive $M(X)$ is split. For example, $\mathbb{P}^n$ is split. We call M or X *geometrically split*, if it splits over a field extension of F.

By [69, Proposition 1.5], X is split if and only the integral bilinear form $(u, v) \mapsto \deg(uv)$ on $\operatorname{CH}(X)$ is unimodular and the natural homomorphism $\operatorname{CH}(X) \to \operatorname{CH}(X_L)$ is an isomorphism for any field extension L/F. An isomorphism between $M(X)$ and a sum of Tate motives is given by a $\mathbb{Z}$-basis $u_1, \dots, u_n$ and the dual basis $v_1, \dots, v_n$ of $\operatorname{CH}(X)$. In particular, the Chow group $\operatorname{CH}(X)$ is free abelian of finite rank.

Let M be a geometrically split motive. Over an extension L/F, the motive M is isomorphic to a finite sum of Tate motives. The *rank* $\operatorname{rank}(M)$ of M is defined as the number of the summands in this decomposition. For example, $\operatorname{rank}\bigl(M(X)\bigr)$ coincides with the rank of the free abelian group $\operatorname{CH}(X_L)$ for a splitting field L/F.

For any integer n, we write $v_p(n)$ for the value on n of the p-adic valuation. Recall that n_X is the greatest common divisor of the degrees of closed points of a variety X.

Proposition 4.6. [42, Lemma 2.21] *Let M be a direct summand of the motive of a geometrically split variety X* (with coefficients $\Lambda = \mathbb{Z}/p\mathbb{Z}$). Then $v_p(n_X) \leq v_p\bigl(\operatorname{rank}(M)\bigr)$.

Proof. Let $M = (X, \pi)$ for a projector π. Write $\Lambda' = \mathbb{Z}/p^n\mathbb{Z}$ for some n and $M' := (X, \pi')$ a lift of M in $\mathit{CM}(X, \Lambda')$ with respect to the ring homomorphism $\Lambda' \to \Lambda$. The rank of the motive M' coincides with $m := \operatorname{rank}(M)$. Let L/F be a splitting field of the motive M'. Mutually inverse isomorphisms between M'_L and a direct sum of m Tate motives are given by two sequences of homogeneous elements $a_1, \dots, a_m$ and $b_1, \dots, b_m$ in $\operatorname{CH}(X_L) \otimes \Lambda'$, satisfying $\pi'_L = a_1 \times b_1 + \cdots + a_m \times b_m$ and such that for any $i, j = 1, \dots, m$ the degree $\deg(a_i b_j)$ in Λ' is 0 for $i \neq j$ and 1 for $i = j$. The pull-back of π' via the diagonal morphism $X \to X \times X$ is therefore a 0-cycle class on X of degree $m + p^n\mathbb{Z} \in \Lambda'$. It follows that $m \in n_X\mathbb{Z} + p^n\mathbb{Z}$ for every n, hence $v_p(n_X) \leq v_p(m)$. □

Corollary 4.7. *Assume that for a splitting field L the rank of the group* $\operatorname{CH}(X_L)$ *is equal to n_X. If n_X is a power of a prime p, then the motive $M(X)$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$ is indecomposable.*

We say that X *satisfies the nilpotence principle*, if for any field extension L/F, the kernel of the change of field homomorphism $\operatorname{End}(M(X)) \to \operatorname{End}(M(X_L))$ consists of nilpotents. Every projective homogeneous variety under an action of a semisimple algebraic group is geometrically split and satisfies the nilpotence principle (see [13]).

A motive M is called *indecomposable* if M is not isomorphic to the direct sum of two nonzero objects in $\mathit{CM}(F, \Lambda)$. A relation between indecomposability of the motive of a variety X and p-incompressibility of X is given in the following proposition.

Proposition 4.8. [42, Lemma 2.23] *If the motive $M(X)$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$ of a smooth complete geometrically split variety X satisfying the nilpotence principle is indecomposable, then the variety X is p-incompressible.*

Proof. Suppose X is not p-incompressible. By Proposition 4.4, there are morphisms $f, g : X' \to X$ such that f is dominant of degree prime to p and g is not dominant. Let $\alpha \in \mathrm{CH}_d(X \times X)/p$, where $d = \dim(X)$, be the class of the closure of the graph of the morphism $(f, g) : X' \to X \times X$. Then $\operatorname{mult}(\alpha) \neq 0$ and $\operatorname{mult}(\alpha^t) = 0$. As X is geometrically split and satisfies the nilpotence principle, by [42, Corollary 2.2], a power of the correspondence α is a projector that determines a nontrivial direct summand of $M(X)$, a contradiction. $\square$

Example 4.9. (see [34] or [35]) Let A be a central division F-algebra of degree $d + 1 = p^n$, where p is a prime integer. Let $X = \mathrm{SB}(A)$ be the *Severi-Brauer variety* of right ideals in A of dimension $d + 1$. The variety X has a point over a field extension L/F if and only if the algebra A_L is split. Over such an L we have $X_L \simeq \big(\mathbb{P}^d\big)_L$. It follows that $n_X = d + 1$ and $\operatorname{rank}\big(\mathrm{CH}(X_L)\big) = d + 1$. In view of Corollary 4.7, X is indecomposable in $\mathit{CM}(F, \mathbb{Z}/p\mathbb{Z})$ and hence is p-incompressible by Proposition 4.8. In particular, $\operatorname{cdim}(X) = \operatorname{cdim}_p(X) = d = p^n - 1$.

Example 4.10. Let q be a nondegenerate quadratic form over F. We will consider the following cases:

(i) $\dim(q) = 2m + 1$,

(ii) $\dim(q) = 2m$ and the discriminant of q is not trivial,

(iii) $\dim(q) = 2m$ and the discriminant of q is trivial.

Let A be the even Clifford algebra of q in the case (i), the Clifford algebra in the case (ii) and a simple component of the even Clifford algebra in the case (iii). Write X for the variety of maximal totally isotropic subspaces X_{max} in (i) and (ii) and a connected component of X_{max} in the case (iii). Assume that the value n_X is the largest possible, i.e., $n_X = 2^m$ in (i) and (ii), and $n_X = 2^{m-1}$ in the case (iii). This condition holds if A is a division algebra. By [23, Theorem 86.12], we have $\operatorname{rank}\big(\mathrm{CH}(X_{\mathrm{sep}})\big) = n_X$. In view of Corollary 4.7, X is indecomposable in $\mathit{CM}(F, \mathbb{Z}/2\mathbb{Z})$ and hence is 2-incompressible by Proposition 4.8. In particular, $\operatorname{cdim}(X) = \operatorname{cdim}_2(X) = \dim(X)$.

Remark 4.11. We give some other examples of p-incompressible projective homogeneous varieties.

A generalization of Example 4.9 (see [42]): Let D be a central division algebra of degree p^n, m an integer with $0 \leq m \leq n - 1$. Then the *generalized Severi-Brauer variety* $\mathrm{SB}_{p^m}(D)$ of right ideals in D of reduced dimension p^m is p-incompressible. The case $p = 2$ and $m = n - 1$ was proved earlier in [64] and [66].

Let F be a field, L/F a quadratic separable field extension and D a central division L-algebra of degree 2^n such that the norm algebra $N_{L/F}(D)$ is split. For any integer $i = 0, \dots, n$, the Weil corestriction $R_{L/F}\operatorname{SB}_{2^i}(D)$ is 2-incompressible [41, Theorem 1.1].

Let q be a non-degenerate quadratic form over F. Let i be an integer satisfying $1 \le i \le (\dim q)/2$, Q_i the Grassmannian of i-dimensional totally isotropic subspaces. If the degree of every closed point on Q_i is divisible by 2^i and the Witt index of the quadratic form $q_{F(Q_i)}$ equals i, then the variety Q_i is 2-incompressible [40, Theorem 7]. The case of $i = 1$ was known before by [45] (the proof is essentially contained in [101]; the characteristic 2 case has been treated later on in [23]). For $i = 2$ and odd-dimensional q, it has been proved in [65]. The case of maximal i, i.e., of $i = [n/2]$, was also known before (see [36, Theorem 1.1] and [100]).

Let K/F be a separable quadratic field extension. Let h be a *generic* K/F-hermitian form of an arbitrary dimension $n \ge 0$. For $r = 0, 1, \dots, [n/2]$, the unitary grassmannian of r-dimensional totally isotropic subspaces is 2-incompressible [43, Theorem 8.1].

4d. **Strongly p-incompressible varieties.** Let p be a prime integer and $R = (r_1, r_2, \dots)$ a sequence of non-negative integers, almost all zero. Consider the "smallest" symmetric polynomial Q_R in the variables $X_1, X_2, \dots$ containing the monomial

$$(X_1 \dots X_{r_1})^{p-1}(X_{r_1+1} \dots X_{r_1+r_2})^{p^2-1}(X_{r_1+r_2+1} \dots X_{r_1+r_2+r_3})^{p^3-1} \dots$$

and write Q_R as a polynomial on the standard symmetric functions:

$$Q_R = P_R(\sigma_1, \sigma_2, \dots).$$

For any smooth projective variety X of dimension $|R|$, we define the *characteristic number*

$$R(X) := \deg c_R(-T_X) \in \mathbb{Z},$$

where c_R is the characteristic class $c_R := P_R(c_1, c_2, \dots)$ and T_X is the tangent bundle of X.

By definition, n_X divides $R(X)$, hence $v_p\big(R(X)\big) \ge v_p(n_X)$ for any R. A smooth projective variety X is caller *p-rigid*, if $v_p\big(R(X)\big) = v_p(n_X)$ for some R.

A smooth projective variety X is called *strongly p-incompressible*, if for any projective variety Y with $v_p(n_Y) \ge v_p(n_X)$, $\dim Y \le \dim X$, and a multiplicity 1 correspondence $X \rightsquigarrow Y$, one has $\dim Y = \dim X$ and there also exists a multiplicity 1 correspondence $Y \rightsquigarrow X$. In particular, any strongly p-incompressible variety is p-incompressible.

Proposition 4.12. [68, Theorem 7.2] *Assume that* $\operatorname{char}(F) \ne p$. *Then any p-rigid variety over F is strongly p-incompressible.*

Example 4.13. Let p be a prime integer and $\alpha = \{a_1, a_2, \dots, a_n\} \in K_n(F)/pK_n(F)$ a symbol in the Milnor K-group of F modulo p (see [78]). We write α_L for the image of α in $K_n(L)/pK_n(L)$ for a field extension L/F. A smooth projective variety X is called a *p-generic splitting variety of* α if $\alpha_{F(X)} = 0$ and X has a closed point of degree prime to p over every field extension K/F such that $\alpha_K = 0$. In view of [95], p-generic splitting varieties exist for every symbol over a field of characteristic 0 and by [95, Proposition 2.6], every p-generic splitting variety X of a nontrivial symbol with $\dim(X) = p^{n-1} - 1$ is p-rigid (for the sequence R with $r_{n-1} = 1$ and $r_i = 0$ for all $i \ne n - 1$). It follows from Proposition 4.12 that X is strongly p-incompressible.

Example 4.14. Let q be a nondegenerate quadratic form over a field F and X the projective quadric hypersurface over F given by q. The *first Witt index* $i_1(X)$ is the Witt index of q over the function field $F(X)$. It is shown in [45] (if $\operatorname{char}(F) \neq 2$) and in [99] (if $\operatorname{char}(F) = 2$) that X is strongly 2-incompressible if and only if $i_1(X) = 1$.

An example with hermitian quadric of dimension $2^r - 1$ is considered in [89, Theorem A].

4e. **Products of Severi-Brauer varieties.** Let F be an arbitrary field, p a prime integer and $D \subset \operatorname{Br}_p(F)$ a subgroup, where $\operatorname{Br}_p(F)$ is the subgroup of elements of exponent dividing p in the *Brauer group* $\operatorname{Br}(F)$ of F. We write $\operatorname{ed}_p(D)$ for the essential p-dimension of the class of splitting field extensions for D (i.e., field extensions that split all elements in D) and $\operatorname{ind}(d)$ for the *index* of d in $\operatorname{Br}(F)$.

The goal of this section is to prove the following theorem.

Theorem 4.15. *Let p be a prime integer, F a field of characteristic different from p and D a finite elementary p-subgroup of the Brauer group $\operatorname{Br}(F)$. Then*

$$\operatorname{ed}\bigl(D\bigr) = \operatorname{ed}_p\bigl(D\bigr) = \min \sum_{d\in\mathcal{A}} \bigl(\operatorname{ind}(d) - 1\bigr),$$

where the minimum is taken over all bases $\mathcal{A}$ of D over $\mathbb{Z}/p\mathbb{Z}$.

Let $\mathcal{A} = \{d_1, \dots, d_r\}$ be a basis of D. For every i, A_i a central division F-algebra (of degree $\operatorname{ind}(d_i)$) representing d_i and $P_i = \operatorname{SB}(A_i)$ the Severi-Brauer variety of A_i. Set $P_{\mathcal{A}} := P_1 \times P_2 \times \cdots \times P_r$. Note that $P_{\mathcal{A}}$ depends on the choice of the basis $\mathcal{A}$.

The classes of splitting fields of $P_{\mathcal{A}}$ and D coincide for every basis $\mathcal{A}$. Hence

$$\operatorname{ed}_p(D) \leq \operatorname{ed}(D) = \operatorname{cdim}(P_{\mathcal{A}}) \leq \dim(P_{\mathcal{A}}) = \sum_{i=1}^{r} \bigl(\operatorname{ind}(d_i) - 1\bigr). \tag{4.1}$$

We will produce a basis $\mathcal{A}$ of D such that $\operatorname{cdim}_p(P_{\mathcal{A}}) = \dim(P_{\mathcal{A}})$. The latter is equivalent to the fact that $P_{\mathcal{A}}$ is p-incompressible.

We say that a basis $\mathcal{A} = \{d_1, \dots, d_r\}$ of D is *minimal* if for every $i = 1, \dots, r$ and any element $d \in D \setminus \operatorname{span}(d_1, \dots, d_{i-1})$, we have $\operatorname{ind}(d) \geq \operatorname{ind}(d_i)$.

Remark 4.16. One can construct a minimal basis of D by induction as follows: Let d_1 be a nonzero element of D of the minimal index. If the elements $d_1, \dots, d_{i-1}$ are already chosen for some $i \leq r$, we take for the d_i an element of D of the minimal index among the elements in $D \setminus \operatorname{span}(d_1, \dots, d_{i-1})$.

Thus, it is suffices to prove the following proposition.

Proposition 4.17. *Let $D \subset \operatorname{Br}_p(F)$ be a subgroup of dimension r and $\mathcal{A} = \{d_1, d_2, \dots, d_r\}$ a minimal basis of D. Then the variety $P_{\mathcal{A}}$ constructed above is p-incompressible.*

Fix a minimal basis $\mathcal{A}$ of D. In view of Proposition 4.5 it suffices to prove the following proposition.

Proposition 4.18. *Let $D \subset \operatorname{Br}_p(F)$ be a finite subgroup and $\mathcal{A}$ a minimal basis of D. Then for every correspondence $\alpha : P_{\mathcal{A}} \rightsquigarrow P_{\mathcal{A}}$, we have*

$$\operatorname{mult}(\alpha) \equiv \operatorname{mult}(\alpha^t) \pmod{p}.$$

Let A be a central simple algebra in $\mathrm{Br}_p(F)$ and $P := \mathrm{SB}(A)$. We will study the Grothendieck group $K_0(P)$ (see [81]). In the split case, P is a projective space of dimension $\deg(A) - 1$, hence

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

where $\xi \in K_0(P)$ is the class of the invertible sheaf $O(-1)$. Then $1 - \xi$ is the class of a hyperplane and $(1 - \xi)^{\deg A} = 0$. Consider the polynomial ring $\mathbb{Z}[x]$. We have a ring isomorphism

$$K_0(P) \simeq \mathbb{Z}[x]/\big((1 - x)^{\deg A}\big),$$

taking ξ to the class of x. On the other hand, we can embed the group $K_0(P)$ into $\mathbb{Z}[x]$, $\xi^i \mapsto x^i$, as the subgroup generated by the monomials x^j with $j < \deg A$.

In the general case, by a theorem of Quillen (see [81, §9]),

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

The image of the natural map $K_0(A^{\otimes j}) \to K_0(\overline{A}^{\otimes j}) = \mathbb{Z}$, (where "bar" denotes 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 $\mathrm{ind}(A^{\otimes j})\,\mathbb{Z}\,\xi^j$ for all $j \ge 0$. More precisely,

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

Let $\mathrm{ind}(A) = p^n$. For any $j \ge 0$, write:

$$e(j) = \begin{cases} 0, & \text{if } j \text{ is divisible by } p; \\ n, & \text{otherwise.} \end{cases}$$

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 $p^{e(j)}x^j$ for $j \ge 0$. Clearly, $K(n)$ is a subring of $\mathbb{Z}[x]$.

There is a natural surjective ring homomorphism $K(n) \to K_0(P)$. Write $h := 1 - x$. We have $h^{\deg A} \in K(n)$. Since 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 4.19. *The induced homomorphism $K(n)/(h^{\deg A}) \to K_0(P)$ is an isomorphism.*

Proof. Set $m = \deg A$. It suffices to show that the quotient ring $K(n)/(h^m)$ is additively generated by $p^{e(j)}x^j$ with $j < m$. Note that the polynomial $x^m - (-h)^m = x^m - (x-1)^m$ is a linear combination with integer coefficients of $p^{e(j)}x^j$ with $j < m$:

$$x^m - (-h)^m = \sum_{j=0}^{m-1} a_j\, p^{e(j)} x^j.$$

For any $k \ge m$, multiplying both sides of this equality by $p^{e(k-m)}x^{k-m} = p^{e(k)}x^{k-m}$, we see that the polynomial $p^{e(k)}x^k$ modulo the ideal (h^m) is a linear combination with integer coefficients of the $p^{e(j)}x^j$ with $j < k$, and the proof concludes by induction on k. ☐

Corollary 4.20. *Let g be a polynomial in the variable $h = 1 - x$ lying in $K(n)$ for some $n \geq 0$. 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 4.19, the factor ring $K(n)/(h^i)$ is isomorphic 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 $p^{e(j)}x^j = p^{e(j)}(1-h)^j$ 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 also have a canonical embedding of groups $K_0(P) \subset K(n)$.

Now consider the following more general situation. Let $A_1, A_2, \dots, A_r$ be central simple algebras in $\mathrm{Br}_p(F)$, $P_i = \mathrm{SB}(A_i)$ and $P = P_1 \times \cdots \times P_r$. We will consider 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 $\xi_i \in K_0(\overline{P})$ for the pullback of the class of $O(-1)$ on the i-th component of the product and set

$$\xi^j := \xi_1^{j_1} \cdots \xi_r^{j_r}$$

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

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

Then $1 - \xi_i \in K_0(\overline{P})$ is the pull-back of the class of a hyperplane on the i-th component. We have $(1-\xi_i)^{\deg A_i} = 0$.

Consider an r-tuple of variables $x = (x_1, \dots, x_r)$ and the polynomial ring $\mathbb{Z}[x]$. We have

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

where $h_i := 1 - x_i$.

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

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

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

Suppose now that the algebras A_i are division algebras representing a minimal basis $\mathcal{A} = \{d_1, \dots, d_r\}$ of the subgroup D. Set $p^{n_i} := \mathrm{ind}(d_i) = \deg(d_i)$ and $d^j := d_1^{j_1} \cdots d_r^{j_r} \in \mathrm{Br}_p(F)$ for a multi-index $j = (j_1, \dots, j_r) \geq 0$. Recall that by the definition of a minimal basis, $0 \leq n_1 \leq n_2 \leq \cdots \leq n_r$ and $\log_p \mathrm{ind}(a^j) \geq n_k$ with the largest k such that j_k is not divisible by p.

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

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

Thus, we have

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

Let $K := K(n_1, \ldots, n_r)$ be the subgroup of the polynomial ring $\mathbb{Z}[x]$ in r variables $x = (x_1, \ldots, x_r)$ generated by the monomials $p^{e(j)}x^j$ for all $j \geq 0$. 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 $h = (h_1, \ldots, h_r)$ with $h_i = 1 - x_i \in \mathbb{Z}[x]$, thus, $\mathbb{Z}[x] = \mathbb{Z}[h]$.

Proposition 4.21. *Let $f = f(h) \in K$ be a nonzero polynomial and ch^i, for a multi-index $i \geq 0$ and $c \in \mathbb{Z}$, a nonzero monomial of the least degree of f. Assume that the integer c is not divisible by p. Then $p^{n_1} \mid i_1, \ldots, p^{n_r} \mid i_r$.*

Proof. We proceed by induction on $m = r + n_1 + \cdots + n_r \geq 1$. The case $m = 1$ is trivial. If $m > 1$ and $n_1 = 0$, then for any $j = (j_1, \ldots, j_r)$, we have

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

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

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

Write f in the form

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

with $g_i = g_i(h_2, \ldots, h_r) \in K(n_2, \ldots, n_r)$. Then $ch_2^{i_2} \ldots h_r^{i_r}$ is the monomial of the least degree of g_{i_1}. We can apply the induction hypothesis to $g_{i_1} \in K(n_2, \ldots, n_r)$.

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

Since $K(n_1, n_2, \ldots, n_r) \subset K(n_1 - 1, n_2, \ldots, n_r)$, by the induction hypothesis, $p^{n_1 - 1} \mid i_1,\ p^{n_2} \mid i_2, \ldots, p^{n_r} \mid i_r$. 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

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

for any j. It follows that

$$\varphi(K) \subset K(n_1 - 1)[x_2, \ldots, x_r] = K(n_1 - 1)[h_2, \ldots, h_r] \tag{4.2}$$

and

$$\varphi(h^j) = -\frac{1}{p}\, x_1 \cdot \frac{\partial(h^j)}{\partial h_1} = -\frac{j_1}{p}\, h_1^{j_1 - 1} h_2^{j_2} \cdots h_r^{j_r} + \frac{j_1}{p}\, h_1^{j_1} h_2^{j_2} \cdots h_r^{j_r}.$$

Since $ch_1^{i_1} \cdots h_r^{i_r}$ is a monomial of the lowest total degree of the polynomial f, it follows that $-\frac{ci_1}{p}\, h_1^{i_1 - 1} h_2^{i_2} \cdots h_r^{i_r}$ is a monomial of $\varphi(f)$ considered as a polynomial in h. By (4.2), $-\frac{ci_1}{p}\, h_1^{i_1 - 1}$ is a monomial of a polynomial from $K(n_1 - 1)$. Since c is not divisible by p, it follows that $\frac{i_1}{p}$ is an integer and by Corollary 4.20, this integer is divisible by p^{n_1-1}. Therefore p^{n_1} divides i_1. $\square$

Let $\mathcal{A}$ be a minimal basis of D and set $P := P_{\mathcal{A}}$. We write $\overline{P}$ for P over a splitting field.

Proposition 4.22. *For any $j > 0$, we have*

$$\operatorname{Im}\bigl(\mathrm{CH}^j(P) \to \mathrm{CH}^j(\overline{P})\bigr) \subset p\,\mathrm{CH}^j(\overline{P}).$$

Proof. Each of the groups $K_0(P)$ and $K_0(\overline{P})$ is endowed with the topological filtration (see [81]). The subsequent factor groups $K_0(P)^{(j/j+1)}$ and $K_0(\overline{P})^{(j/j+1)}$ of these filtrations fit into the commutative square

$$\begin{tikzcd}
\mathrm{CH}^j(P) \arrow[r] \arrow[d] & K_0(P)^{(j/j+1)} \arrow[d] \\
\mathrm{CH}^j(\overline{P}) \arrow[r] & K_0(\overline{P})^{(j/j+1)}
\end{tikzcd}$$

where the bottom map is an isomorphism as $\overline{P}$ is split. Therefore it suffices to show that the image of the homomorphism $K_0(P)^{(j/j+1)} \to K_0(\overline{P})^{(j/j+1)}$ 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 $h_1^{\operatorname{ind} d_1}, \dots, h_r^{\operatorname{ind} d_r}$. 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 in h of degree at least j. The group $K_0(\overline{P})^{(j/j+1)}$ is then 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 $n_i = \log_p\bigl(\operatorname{ind}(d_i)\bigr)$.

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 $K_0(\overline{P})^{(j/j+1)}$ is the j-th homogeneous part f_j of f. As the degree of f with respect to h_i is less than $\operatorname{ind} d_i$, it follows from Proposition 4.21 that all the coefficients of f_j are divisible by p. $\square$

Now we prove Proposition 4.18. Note that any projection $P_i \times P_i \to P_i$ is a projective bundle for every i. By the Projective Bundle Theorem [23, Theorem 57.14], the Chow group $\mathrm{CH}^n(P \times P)$ is naturally isomorphic to a direct some of several copies of $\mathrm{CH}^j(X)$ for some j's and the value $j = 0$ appears once. By Proposition 4.22, the image of the composition

$$f\colon \mathrm{CH}^n(P \times P) \to \mathrm{CH}^n(\overline{P} \times \overline{P}) \to (\mathbb{Z}/p\mathbb{Z})^2,$$

where $n = \dim(P)$, taking a correspondence $\alpha \in \mathrm{CH}^n(P \times P)$ to $\bigl(\operatorname{mult}(\alpha), \operatorname{mult}(\alpha^t)\bigr)$ modulo p is cyclic generated by the image of the direct summand of $\mathrm{CH}^n(P \times P)$ isomorphic to $\mathrm{CH}^0(P) \simeq \mathbb{Z}$. Since the image of the diagonal class under f is $(\bar{1}, \bar{1})$, the image of f is generated by $(\bar{1}, \bar{1})$.

4f. **A conjecture.** Let A be a central division F-algebra of degree n. Write $n = q_1 q_2 \cdots q_r$ where the q_i are powers of distinct primes. Then A is a tensor product $A_1 \otimes A_2 \otimes \ldots \otimes A_r$, where A_i is a central division F-algebra of degree q_i [29, Theorem 4.4.6]. A field extension K/F splits A if and only if K splits A_i for all i. In other words, the variety $\mathrm{SB}(A)$ has an K-point if and only if the variety $Y := \mathrm{SB}(A_1) \times \mathrm{SB}(A_2) \times \cdots \times \mathrm{SB}(A_r)$ has an K-point. Hence

$$\operatorname{cdim}\bigl(\mathrm{SB}(A)\bigr) = \operatorname{cdim}(Y) \leq \dim(Y) = \sum_{i=1}^{r} (q_i - 1).$$

It was conjectured in [18] that the inequality is actually an equality:

Conjecture 4.23. *Let $A = A_1 \otimes A_2 \otimes \ldots \otimes A_r$ be the tensor product of central division F-algebras of degree $q_1, q_2, \ldots, q_r$, where q_i are powers of distinct primes. Then*

$$\operatorname{cdim}\bigl(\mathrm{SB}(A)\bigr) = \sum_{i=1}^{r} (q_i - 1).$$

This conjecture was proved in the case when $r = 1$, i.e., when $\deg(A)$ is power of a prime integer (Example 4.9) and in the case $n = 6$ if $\operatorname{char}(F) = 0$ (see [18, Theorem 1.3]). The proof uses classification of rational surfaces, especially, del Pezzo surfaces of degree 6.

4g. **Canonical p-dimension of algebraic groups.** Let G be an algebraic group over F and $p \geq 0$. The *canonical p-dimension of G* is the maximum of the canonical p-dimension of all G-torsors over all field extensions of F.

The following statements follow from Lemma 4.1.

Lemma 4.24. *Let G be an algebraic group over F and p a prime integer. Then*

1. *If $\operatorname{cdim}_p(G) \neq 0$, then p is a torsion prime for G.*
2. *If p is a torsion prime for G and G is connected, then $\operatorname{cdim}_p(G) \neq 0$.*

Lemma 4.25. *A connected group G is special if and only if $\operatorname{cdim}(G) = 0$.*

Let p be a prime integer. The canonical p-dimension of split semisimple groups was computed in [46] (classical groups) and [103] (exceptional groups).

Type A_{n-1}: If d divides n,

$$\operatorname{cdim}_p\bigl(\mathbf{SL}_n / \boldsymbol{\mu}_d\bigr) = \begin{cases} p^m - 1, & \text{if } p \text{ divides } d; \\ 0, & \text{otherwise.} \end{cases}$$

where p^m is the largest power of p dividing n.

Type B_n:

$$\operatorname{cdim}_2 \mathbf{SO}_{2n+1} = \frac{n(n+1)}{2},$$

$$\operatorname{cdim}_2 \mathbf{Spin}_{2n+1} = \frac{n(n+1)}{2} - 2^k + 1,$$

where k is the smallest integer such that $2^k > n$.

Type C_n:

$$\operatorname{cdim}_2 \mathbf{Sp}_{2n} = 0,$$

$$\operatorname{cdim}_2 \mathbf{PGSp}_{2n} = 2^m - 1,$$

where 2^m is the largest power of 2 dividing $2n$.

Type D_n: Let 2^m be the largest power of 2 dividing n and k the smallest integer such that $2^k \geq n$.

$$\begin{aligned} \operatorname{cdim}_2 \mathbf{Spin}_{2n} &= \frac{n(n-1)}{2} - 2^k + 1, \\ \operatorname{cdim}_2 \mathbf{SO}_{2n} &= \frac{n(n-1)}{2}, \\ \operatorname{cdim}_2 \mathbf{PGO}^+_{2n} &= \frac{n(n-1)}{2} + 2^m - 1, \\ \operatorname{cdim}_2 \mathbf{Spin}^+_{2n} &= \frac{n(n-1)}{2} + 2^m - 2^k, \end{aligned}$$

if n is even for the last two group.

Type G_2: $\operatorname{cdim}_2(G) = 3$.

Type F_4: $\operatorname{cdim}_2(F_4) = 3$, $\operatorname{cdim}_3(F_4) = 8$.

Type E_6: $\operatorname{cdim}_2(E_6) = 3$, $\operatorname{cdim}_3(E_6^{sc}) = 8$, $\operatorname{cdim}_3(E_6^{ad}) = 16$.

Type E_7: $\operatorname{cdim}_2(E_7^{sc}) = 17$, $\operatorname{cdim}_2(E_7^{ad}) = 18$, $\operatorname{cdim}_3(E_7) = 8$.

Type E_8: $\operatorname{cdim}_2(E_8) = 60$, $\operatorname{cdim}_3(E_8) = 28$, $\operatorname{cdim}_5(E_8) = 24$.

Example 4.26. Let $G = \mathbf{GL}_n / \boldsymbol{\mu}_d$ (we don't assume that d divides n). The connecting map

$$H^1(K, G) \to H^2(K, \boldsymbol{\mu}_d) = \operatorname{Br}_d(K)$$

for the exact sequence $1 \to \boldsymbol{\mu}_d \to \mathbf{GL}_n \to G \to 1$ yields a bijection between G-$\mathit{torsors}(K)$ and the set $\mathit{CSA}_{n,d}(K)$ of isomorphism classes of central simple algebras of degree n and exponent dividing d. Note that if p a prime divisor of d, then there is a division algebra A over a field extension of F of degree the largest power p^m of p dividing n and exponent dividing d. The classes of splitting fields of A and the corresponding Severi-Brauer variety coincide. It follows from Example 4.9 that

$$\operatorname{cdim}_p(\mathbf{GL}_n / \boldsymbol{\mu}_d) = \operatorname{cdim}_p(\mathit{CSA}_{n,\,d}) = p^m - 1.$$

The computation of the canonical dimension of an algebraic groups (for p = 0) is a much harder problem. Conjecture 4.23 would imply that if $n = q_1 q_2 \cdots q_r$, where q_i are powers of distinct primes, then

$$\operatorname{cdim}(\mathbf{PGL}_n) = \sum_{i=1}^{r} (q_i - 1).$$

It is shown in [18] that $\operatorname{cdim}(\mathbf{PGL}_6) = 3$ over a field of characteristic 0. This is the only group having more than one torsion primes with the known value of the canonical dimension.

It is proved in [37] that $\operatorname{cdim}(\mathbf{Spin}_{2n+1}) = \operatorname{cdim}(\mathbf{Spin}_{2n+2}) \leq n(n-1)/2$ and this is equality if n is a power of 2. The value of $\operatorname{cdim}(\mathbf{Spin}_n)$ for all $n \leq 16$ was determined in [38].

5. Fiber Dimension Theorem

The essential dimension of fibered categories was defined in [10].

5a. **Categories fibered in groupoids.** In many examples of functors $\mathcal{F} : \mathsf{Fields}_F \to \mathsf{Sets}$, the sets $\mathcal{F}(K)$ are isomorphism classes of objects in certain categories. It turned out that it is convenient to consider these categories which usually form what is called the categories fibered in groupoids.

Let $\mathsf{Schemes}_F$ be the category of schemes over F, $\pi : \mathcal{X} \to \mathsf{Schemes}_F$ a functor, a an object of $\mathcal{X}$ and $X = \pi(a)$. We say that *a is an object over X*. For every scheme X over F, all objects over X form the *fiber category $\mathcal{X}(X)$* with the morphisms f satisfying $\pi(f) = 1_X$.

Let $f : a \to b$ be a morphism in $\mathcal{X}$ and $\alpha := \pi(f) : X \to Y$, so that a is an object over X and b is over Y. We say that the *morphism f is over α*.

The category $\mathcal{X}$ equipped with a functor π is called a *category fibered in groupoids* over F (CFG) if the following two conditions hold:

(1) For every morphism $\alpha : X \to Y$ in $\mathsf{Schemes}_F$ and every object b in $\mathcal{X}$ over Y, there is an object a in $\mathcal{X}$ over X and a morphism $a \to b$ over α.

(2) For every pair of morphisms $\alpha : X \to Y$ and $\beta : Y \to Z$ in $\mathsf{Schemes}_F$ and morphisms $g : b \to c$ and $h : a \to c$ in $\mathcal{X}$ over β and $\beta \circ \alpha$ respectively, there is a unique morphism $f : a \to b$ over α such that $h = g \circ f$.

It follows from the definition that the object a in (1) is uniquely determined by b and α up to canonical isomorphism. We will write b_X for a. The fiber categories $\mathcal{X}(X)$ are *groupoids* for every X, i.e., every morphism in $\mathcal{X}(X)$ is an isomorphism.

Suppose $\mathcal{X}(X)$ is a *small category* for every X, i.e., objects in $\mathcal{X}(X)$ form a set. We have a functor $\mathcal{F}_{\mathcal{X}} : \mathsf{Fields}_F \to \mathsf{Sets}$, taking a field K to the set of isomorphism classes in $\mathcal{F}(K) := \mathcal{F}(\operatorname{Spec} K)$ and a field extension $\alpha : K \to L$ to the map $[a] \mapsto [a_L]$, where $[a]$ denotes the isomorphism class of a.

Example 5.1. Every scheme X over F can be viewed as a CFG as follows: An object of X (as a CFG) is a scheme Y over X, i.e., a morphism $Y \to X$ over F. A morphism between two objects is a morphism of schemes over X. The functor $\pi : X \to \mathsf{Schemes}_F$ takes a scheme Y over X to Y and a morphism between two schemes over X to itself. Note that the fiber groupoids $X(Y) = \operatorname{Mor}(Y, X)$ are sets, i.e., every morphism in $X(Y)$ is the identity.

Example 5.2. Let an algebraic group G act on a scheme X over F. We define the CFG X/G as follows: An object of X/G is a diagram

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "\rho"'] & X , \\ Y & \end{tikzcd}$$

where ρ is a G-torsor and φ is a G-equivariant morphism. A morphism between two such diagrams is a morphism between the G-torsors satisfying obvious compatibility condition. The functor $\pi : X/G \to \mathsf{Schemes}_F$ takes the diagram to Y.

If $E \to Y$ is a G-torsor, then $E/G \simeq Y$.

If $X = \operatorname{Spec}(F)$, we write BG for X/G. This is the category of G-torsors $E \to Y$ over a scheme Y.

Example 5.3. Let K/F be a finite Galois field extension with Galois group H and $f : G \to H$ a surjective homomorphism of finite groups with kernel N. Then G acts on $\operatorname{Spec}(K)$ via f. An object of the fiber of the category $\mathcal{X} := \operatorname{Spec}(K)/G$ over

$\operatorname{Spec}(F)$ is a G-torsor $E \to \operatorname{Spec}(F)$ together with an isomorphism $E/N \xrightarrow{\sim} \operatorname{Spec}(K)$ of H-torsors. By Example 3.1, $E \simeq \operatorname{Spec}(L)$, where L/F is a Galois extension with Galois group G such that $L^N \simeq K$. In other words, L/F is a solution of the *embedding problem* in Galois theory given by K/F and f (see [30]).

All CFG's over F form a 2-category, in which morphisms $(\mathcal{X}, \pi) \to (\mathcal{X}', \pi')$ are functors $\varphi : \mathcal{X} \to \mathcal{X}'$ such that $\pi' \circ \varphi = \pi$, and 2-morphisms $\varphi_1 \to \varphi_2$ for morphisms $\varphi_1, \varphi_2 : (\mathcal{X}, \pi) \to (\mathcal{X}', \pi')$ are natural transformations $t : \varphi_1 \to \varphi_2$ such that $\pi'(t_a) = 1_{\pi(a)}$ for all objects a of $\mathcal{X}$. For a scheme X over F and a CFG $\mathcal{X}$ over F, the morphisms $\operatorname{Mor}_{CFG}(X, \mathcal{X})$ have a structure of a category. By a variant of the Yoneda Lemma, the functor

$$\operatorname{Mor}_{CFG}(X, \mathcal{X}) \to \mathcal{X}(X),$$

taking a morphism $f : X \to \mathcal{X}$ to $f(1_X)$, is an equivalence of categories.

We will use the notion of 2-fiber product in the 2-category of CFG's over F. If $\varphi : \mathcal{X} \to \mathcal{Z}$ and $\psi : \mathcal{Y} \to \mathcal{Z}$ are two morphisms of CFG's over F a 2-fiber product $\mathcal{X} \times_{\mathcal{Z}} \mathcal{Y}$ is a CFG over F whose objects are triples (x, y, f), where x and y are objects of $\mathcal{X}$ and $\mathcal{Y}$ over a scheme X and $f : \varphi(x) \to \psi(y)$ is an isomorphism in $\mathcal{Z}$ lying over the identity of X. The diagram

$$\begin{tikzcd}
\mathcal{X} \times_{\mathcal{Z}} \mathcal{Y} \arrow[r, "\beta"] \arrow[d, "\alpha"'] & \mathcal{Y} \arrow[d, "\psi"] \\
\mathcal{X} \arrow[r, "\varphi"] & \mathcal{Z}
\end{tikzcd}$$

with the obvious functors α and β is 2-*commutative* (i.e. the two compositions $\mathcal{X} \times_{\mathcal{Z}} \mathcal{Y} \to \mathcal{Z}$ are 2-isomorphic).

Let $f : \mathcal{X} \to \mathcal{Y}$ be a morphism of CFG's over F. An object of the fiber category $\mathcal{Y}(Y)$ for a scheme Y determines a morphism $y : Y \to \mathcal{Y}$ of CFG's over F. The *fiber of f over y* is defined as the 2-fiber product

$$\mathcal{X}_y := \mathcal{X} \times_{\mathcal{Y}} Y.$$

Example 5.4. Let G be an algebraic group and X a G-scheme over F. We have a natural morphism $f : X/G \to (\operatorname{Spec} F)/G = BG$. A G-torsor $E \to Y$ determines a morphism $y : Y \to BG$. Then the scheme $X_E := (X \times E)/G$, the twist of X by the torsor E, is the fiber $(X/G)_y$ of f over y.

Example 5.5. Let $G \to H$ be a homomorphism of algebraic groups over F. An H-torsor $E \to Y$ determines a morphism $y : Y \to BH$. Then E/G is the fiber $(BG)_y$ of the morphism $BG \to BH$ over y.

5b. **Essential and canonical dimension of categories fibered in groupoids.** Let $\mathcal{X}$ be a CFG over F, $x : \operatorname{Spec}(K) \to \mathcal{X}$ a morphism for a field extension K/F and $K_0 \subset K$ a subfield over F. We say that x is *defined over* K_0 (or that K_0 *is a field of definition of* x) if there exists a morphism $x_0 : \operatorname{Spec}(K_0) \to \mathcal{X}$ such that the diagram

$$\begin{tikzcd}
\operatorname{Spec}(K) \arrow[r, "x"] \arrow[d] & \mathcal{X} \\
\operatorname{Spec}(K_0) \arrow[ur, "x_0"'] &
\end{tikzcd}$$

2-commutes. We say that x is *detected by* K_0 (or that K_0 *is a detection field of* x) if there exists a morphism $x_0 : \mathrm{Spec}(K_0) \to \mathcal{X}$.

Define

$$\mathrm{ed}(x) := \min \mathrm{tr.deg}_F(K_0), \quad \mathrm{cdim}(x) := \min \mathrm{tr.deg}_F(K_0'),$$

where the minimum is taken over all fields of definition K_0 of x, respectively, over all detection fields K_0' of x. For $p \geq 0$, we define

$$\mathrm{ed}_p(x) := \min \mathrm{ed}(x_L), \quad \mathrm{cdim}_p(x) := \min \mathrm{cdim}(x_L),$$

where L runs over all prime to p extensions of K. We set

$$\mathrm{ed}_p(\mathcal{X}) := \max \mathrm{ed}_p(x), \quad \mathrm{cdim}_p(\mathcal{X}) := \max \mathrm{cdim}_p(x),$$

where the maximum runs over all field extensions K/F and morphisms $x : \mathrm{Spec}(K) \to \mathcal{X}$.

If the fiber category $\mathcal{X}(X)$ is small for every X, we have the functor $\mathcal{F}_{\mathcal{X}} : \mathit{Fields}_F \to \mathit{Sets}$ (see Section 5a). It follows from the definitions that

$$\mathrm{ed}_p(\mathcal{X}) = \mathrm{ed}_p(\mathcal{F}_{\mathcal{X}}), \quad \mathrm{cdim}_p(\mathcal{X}) = \mathrm{cdim}_p(\mathcal{F}_{\mathcal{X}}).$$

Note that for an algebraic group G, we have $\mathrm{ed}_p(BG) = \mathrm{ed}_p(G)$ for every $p \geq 0$.

The following theorem generalizes [10, Theorem 3.2].

Theorem 5.6. (Fiber Dimension Theorem, [60, Theorem 1.1]) Let $f : \mathcal{X} \to \mathcal{Y}$ be a morphism of CFG's over F. Then for every $p \geq 0$,

$$\begin{aligned} \mathrm{ed}_p(\mathcal{X}) &\leq \mathrm{ed}_p(\mathcal{Y}) + \max \mathrm{ed}_p(\mathcal{X}_y), \\ \mathrm{cdim}_p(\mathcal{X}) &\leq \mathrm{ed}_p(\mathcal{Y}) + \max \mathrm{cdim}_p(\mathcal{X}_y), \end{aligned}$$

where the maximum is taken over all field extensions K/F and all morphisms $y : \mathrm{Spec}(K) \to \mathcal{Y}$ of CFG's over F.

Proof. We will give a proof of the first inequality. Let K/F be a field extension, $x : \mathrm{Spec}\, K \to \mathcal{X}$ be a morphism, and set $y = f \circ x : \mathrm{Spec}\, K \to \mathcal{Y}$. By definition of $\mathrm{ed}_p(y)$, there exist a prime to p extension K'/K and a subfield $K_0 \subset K'$ over F such that $\mathrm{tr.deg}_F(K_0) = \mathrm{ed}_p(y)$ together with a 2-commutative diagram

$$\begin{tikzcd}
\mathrm{Spec}\, K' \arrow[rr] \arrow[d] & & \mathrm{Spec}\, K_0 \arrow[d, "y_0"] \\
\mathrm{Spec}\, K \arrow[r, "x"] & \mathcal{X} \arrow[r, "f"] & \mathcal{Y}.
\end{tikzcd}$$

By the universal property of 2-fiber product there exists a morphism $z : \mathrm{Spec}\, K' \to \mathcal{X}_{y_0}$ such that the diagram

$$\begin{tikzcd}
\mathrm{Spec}\, K' \arrow[r, "z"] \arrow[d] & \mathcal{X}_{y_0} \arrow[r] \arrow[d] & \mathrm{Spec}\, K_0 \arrow[d, "y_0"] \\
\mathrm{Spec}\, K \arrow[r, "x"] & \mathcal{X} \arrow[r, "f"] & \mathcal{Y}
\end{tikzcd}$$

2-commutes. By the definition of $\mathrm{ed}_p(z)$, there is a prime to p field extension K''/K' and a subfield $K_1 \subset K''$ over K_0 with $\mathrm{tr.deg}_{K_0}(K_1) = \mathrm{ed}_p(z)$ such that the above diagram can be completed to a 2-commutative diagram

$$\begin{tikzcd}
\operatorname{Spec} K'' \arrow[r] \arrow[d] & \operatorname{Spec} K_1 \arrow[d] & \\
\operatorname{Spec} K' \arrow[r, "z"] \arrow[d] & \mathcal{X}_{y_0} \arrow[r] \arrow[d] & \operatorname{Spec} K_0 \arrow[d, "y_0"] \\
\operatorname{Spec} K \arrow[r, "x"] & \mathcal{X} \arrow[r, "f"] & \mathcal{Y}.
\end{tikzcd}$$

Therefore, x is p-defined over K_1. It follows that

$$\operatorname{ed}_p(x) \leq \operatorname{tr.deg}_F(K_1) = \operatorname{tr.deg}_F(K_0) + \operatorname{tr.deg}_{K_0}(K_1) = \\ \operatorname{ed}_p(y) + \operatorname{ed}_p(z) \leq \operatorname{ed}_p(\mathcal{Y}) + \operatorname{ed}_p(\mathcal{X}_{y_0}). \quad \square$$

Theorem 5.6 and Examples 5.4 and 5.5 give:

Corollary 5.7. [10, Corollary 3.3] *Let G be an algebraic group and X a G-scheme. Then*

$$\operatorname{ed}_p(X/G) \leq \operatorname{ed}_p(G) + \dim(X)$$

for every $p \geq 0$.

Corollary 5.8. *Let $G \to H$ be a homomorphism of algebraic groups over F. Then*

$$\operatorname{ed}_p(G) \leq \operatorname{ed}_p(H) + \max \operatorname{ed}_p(E/G)$$

for every $p \geq 0$, where the maximum is taken over all field extensions K/F and all H-torsors $E \to \operatorname{Spec} K$.

5c. **Essential and canonical dimension of a gerbe.** Let G be an algebraic group and $C \subset G$ a smooth central subgroup. As C is commutative, the isomorphism classes of C-torsors over a scheme X form an abelian group. The group operation can be set up on the level of categories as a pairing

$$\mathrm{B}C \times \mathrm{B}C \to \mathrm{B}C, \quad (I, I') \mapsto (I \times_X I')/C,$$

where I and I' are C-torsors over X and an element c in C acts on $I \times_X I'$ by (c, c^{-1}), making $\mathrm{B}C$ a "group object" in the category of CFG's. We will write $(t, t') \mapsto t + t'$ for this operation and 0 for the trivial C-torsor.

We set $H = G/C$ and let E be an H-torsor over $\operatorname{Spec}(F)$. Consider the fibered category $\mathcal{X} := E/G$. An object of $\mathcal{X}(X)$ over a scheme X is a "lift" of the H-torsor $E \times X \to X$ to a G-torsor $J \to X$ together with an isomorphism $J/C \xrightarrow{\sim} E \times X$. The latter shows that J is a C-torsor over $E \times X$.

The exactness of the sequence

$$H^1_{\acute{e}t}(X, G) \to H^1_{\acute{e}t}(X, H) \to H^2_{\acute{e}t}(X, C)$$

for a scheme X implies that $\mathcal{X}$ has an object over X if and only if the image of $\theta(\mathcal{X})$ in $H^2_{\acute{e}t}(X, C)$ of the class of E is trivial. We say that $\mathcal{X}$ is *split* over a field extension K/F if $\mathcal{X}(K) \neq \emptyset$. Thus, the classes of splitting fields of $\mathcal{X}$ and $\theta(\mathcal{X})$ coincide.

By [48, §28], the group $H^1(K, C)$ acts transitively (but not simply transitively in general) on the fibers of the map $H^1(K, G) \to H^1(K, H)$ for every field extension

K/F. This can also be set up in the context of categories as follows: First, we have the "action" functor

$$\mathrm{B}C \times \mathcal{X} \to \mathcal{X}, \quad (t, x) \mapsto t + x, \tag{5.1}$$

taking a pair of objects (I, J), where $I \to X$ is a C-torsor and $q : J \to X$ is a G-torsor, to the G-torsor $(I \times_X J)/C$.

We also have the "subtraction" functor

$$\mathcal{X} \times \mathcal{X} \to \mathrm{B}C, \quad (x, x') \mapsto x - x', \tag{5.2}$$

taking a pair of objects (J, J') over X to $I := (J \times_{E \times X} J')/C$. We view I as a C-torsor via the C action on the first factor J. Thus, $\mathrm{B}C$ "acts simply transitively" on $\mathcal{X}$.

Note that $\mathcal{X}$ is split if and only if $X \simeq \mathrm{B}C$. As every H-torsor $E \to \operatorname{Spec}(F)$ is split over a field extension of F, the fibered category $\mathcal{X}$ can be viewed as a "twisted form" of $\mathrm{B}C$, or a "$\mathrm{B}C$-torsor".

The pairings satisfy the following properties:

$$\begin{aligned}(t + t') + x &\simeq t + (t' + x)\\ (t + x) - x' &\simeq t + (x - x')\\ (x - x') + x' &\simeq x\\ x - x &\simeq 0\\ 0 + x &\simeq x\end{aligned}$$

for $t, t' \in \mathrm{B}C(X)$ and $x, x' \in \mathcal{X}(X)$.

Remark 5.9. Let C be a commutative group. A fibered category $\mathcal{X}$ equipped with the two pairings as in (5.1) and (5.2) satisfying the conditions above is known as a *gerbe banded by C*. There is an element $\theta(\mathcal{X}) \in H^2(F, C)$ attached to $\mathcal{X}$ such that $\mathcal{X}$ has an object over a scheme X if and only if $\theta(\mathcal{X})$ is trivial over X. In particular, the classes of splitting fields for $\mathcal{X}$ and $\theta(\mathcal{X})$ coincide.

Now we connect the essential and canonical dimension of a gerbe.

Proposition 5.10. *Let $\mathcal{X}$ be gerbe banded by $C = (\boldsymbol{\mu}_p)^s$ (for example, $\mathcal{X} = E/G$ as above). Then*

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

for every $p \geq 0$.

Proof. Let K/F be a field extension, $x \in \mathcal{X}(K)$, K'/K a prime to p field extension and a subfield $K_0 \subset K'$ such that $\mathcal{X}(K_0) \neq \emptyset$ and $\mathrm{cdim}_p(\mathcal{X}) = \operatorname{tr.deg}_F(K_0)$. Take any $y \in \mathcal{X}(K_0)$ and set $t := x_{K'} - y_{K'} \in \mathrm{B}C(K')$. Choose a prime to p field extension K''/K', a subfield $K_1 \subset K''$ over F and a $t' \in \mathrm{B}C(K_1)$ with $t'_{K''} = t_{K''}$ and $\operatorname{tr.deg}_F(K_1) = \mathrm{ed}_p(t)$. Then $x_{K''} \simeq t'_{K''} + y_{K''}$ is defined over K_0K_1, hence

$$\begin{aligned}\mathrm{ed}_p(x) \leq \operatorname{tr.deg}_F(K_0K_1) &\leq \operatorname{tr.deg}_F(K_0) + \operatorname{tr.deg}_F(K_1)\\ &= \mathrm{cdim}_p(\mathcal{X}) + \mathrm{ed}_p(t) \leq \mathrm{cdim}_p(\mathcal{X}) + \mathrm{ed}_p(\mathrm{B}C). \quad \square\end{aligned}$$

In the following theorem we show that the inequality is in fact the equality if $C = (\boldsymbol{\mu}_p)^s$, where p is a prime integer, over a field F of characteristic different from p. Recall that $\mathrm{ed}_p(\mathrm{B}C) = s$ in this case by Example 3.5.

Let R be a commutative F-algebra and $r_i \in R^\times$, $i = 1, \dots, s$. Then the ring $R[x_1, \dots, x_s]/(x_1^p - r_1, \dots, x_s^p - r_s)$ is a Galois C-algebra over R. We simply write (r) or $(r_1, \dots, r_s)$ for the corresponding C-torsor over $\operatorname{Spec}(R)$, so we view (r) as an object of $\mathrm{B}C(R)$. The C-torsors (r) and (r') are isomorphic if and only if $r_i R^{\times p} = r'_i R^{\times p}$ for all i. Moreover, if $\operatorname{Pic}(R) = 1$ (for example, when R is a local ring), then every C-torsor over $\operatorname{Spec}(R)$ is isomorphic to a torsor of the form (r) with $r_i \in R^\times$.

Let $\mathcal{X}$ be a gerbe banded by $C = (\boldsymbol{\mu}_p)^s$ over F. A choice of a basis of the character group $\widehat{C}$ identifies the group $H^2(F, C)$ with $\operatorname{Br}_p(F)^s$. The corresponding element $\theta \in H^2(F, C) \simeq \operatorname{Br}_p(F)^s$ can be represented by an s-tuple of central simple algebras $A_1, A_2, \dots, A_s$ with $[A_i] \in \operatorname{Br}_p(F)$. Let P be the product of the Severi-Brauer varieties $P_i = \operatorname{SB}(A_i)$. Note that $\mathcal{X}$ has an object over a field extension L/F (i.e., $\mathcal{X}$ is split over L) if and only if $P(L) \neq \emptyset$.

The following theorem was proved in [10, Theorem 4.1] in the case $s = 1$.

Theorem 5.11. *Let p be a prime integer and $\mathcal{X}$ a gerbe banded by $C = (\boldsymbol{\mu}_p)^s$ over a field F of characteristic different from p. Then*

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

Proof. In view of Proposition 5.10 and Example 3.5, it suffices to prove the inequality $\operatorname{ed}_p(\mathcal{X}) \geq \operatorname{cdim}_p(\mathcal{X}) + s$.

Let $x \in \mathcal{X}(K)$ for a field extension K/F. Set $L := K(t_1, \dots, t_s)$, where $t_1, \dots, t_s$ are variables and $x' := (t) + x_L \in \mathcal{X}(L)$, where $(t) = (t_1, \dots, t_s) \in \mathrm{B}C(L)$.

Set L'/L be a prime to p field extension, let $L_0 \subset L'$ be a subfield over F and $y \in \mathcal{X}(L_0)$ such that $y_{L'} = x'_{L'}$ and $\operatorname{tr.deg}_F(L_0) = \operatorname{ed}_p(x')$.

Let $L_i := K(t_i, \dots, t_s)$ and v_i the discrete valuation of L_i corresponding to the variable t_i for $i = 1, \dots, s$. We construct a sequence of prime to p field extensions L'_i/L_i 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. 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 on 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 elements $v'(t_i)$ are linearly independent in $\mathbb{Z}^s$ modulo p.

Write v_0 for the restriction of v' on L_0.

Claim: $\operatorname{rank}(v_0) = s$.

To prove the claim let $R_0 \subset L_0$ be the valuation ring of v_0. Since $\mathcal{X}(L_0) \neq \emptyset$, we have $P(L_0) \neq \emptyset$. As P is complete, the set $P(R_0)$ is not empty, hence the algebras A_i are split over R_0 and therefore, $\mathcal{X}(R_0) \neq \emptyset$. Choose any object $x_0 \in \mathcal{X}(R_0)$. The difference $y - (x_0)_{L_0}$ in $\mathrm{B}C(L_0)$ is isomorphic to (z) for some $z_i \in (L_0)^\times$. Hence

$$(z)_{L'} \simeq y_{L'} - (x_0)_{L'} \simeq x'_{L'} - (x_0)_{L'} \simeq \big((t)_{L'} + x_{L'}\big) - (x_0)_{L'} \simeq (t)_{L'} + \big(x_{L'} - (x_0)_{L'}\big).$$

Note that the element $x_{L'} - (x_0)_{L'}$ is in the image of $\mathrm{B}C(R') \to \mathrm{B}C(L')$, where $R' \subset L'$ is the valuation ring of v'. Hence, we have $x_{L'} - (x_0)_{L'} \simeq (r)$ for some $r_i \in (R')^{\times}$.

Thus, $(z)_{L'} \simeq (t)_{L'} + (r)_{L'} \simeq (tr)_{L'}$, hence there exist $w_i \in L'^{\times}$ such that

$$z_i = t_i r_i w_i^p$$

and therefore, $v_0(z_i) \equiv v'(t_i)$ modulo p for all $i = 1, \dots, s$. It follows that the elements $v_0(z_i)$ are linearly independent modulo p and hence generate a submodule of rank s in $\mathbb{Z}^s$. This means that $\mathrm{rank}(v_0) = s$, proving the claim.

Let K_0 be the residue field of v_0. As $P(R_0) \neq \emptyset$, one has $P(K_0) \neq \emptyset$ and hence $\mathcal{X}(K_0) \neq \emptyset$. Moreover, $K_0 \subset K'$ and $[K' : K]$ is prime to p, so K_0 is a detection field of $x_{K'}$ and therefore,

$$\mathrm{tr.deg}_F(K_0) \geq \mathrm{cdim}_p(x).$$

It follows from (3.1) that

$$\mathrm{ed}_p(\mathcal{X}) \geq \mathrm{ed}_p(x') = \mathrm{tr.deg}_F(L_0) \geq \mathrm{tr.deg}_F(K_0) + \mathrm{rank}(v_0) \geq \mathrm{cdim}_p(x) + s.$$

Since the above inequality holds for every K/F and $x \in \mathcal{X}(K)$, we have

$$\mathrm{ed}_p(\mathcal{X}) \geq \mathrm{cdim}_p(\mathcal{X}) + s. \qquad \square$$

Let $\mathcal{X}$ be gerbe banded by $C = (\boldsymbol{\mu}_p)^s$. Let $\widehat{C}$ denote the character group $\mathrm{Hom}(C, \mathbf{G}_{\mathrm{m}})$ of C. Taking the cup-product with $\theta(\mathcal{X})$ for the pairing

$$\widehat{C} \otimes H^2(F, C) \to H^2(F, \mathbf{G}_{\mathrm{m}}) = \mathrm{Br}(F)$$

we get a homomorphism $\beta^{\mathcal{X}} : \widehat{C}(F) \to \mathrm{Br}(F)$. Let $D(\mathcal{X})$ be its image. Clearly, $\theta(\mathcal{X})$ is split over a field extension K/F if and only if $D(\mathcal{X})$ is split over K. In particular,

$$\mathrm{cdim}_p(\mathcal{X}) = \mathrm{ed}_p\big(D(\mathcal{X})\big) = \mathrm{ed}_p\big(\mathrm{Im}(\beta^{\mathcal{X}})\big) \tag{5.3}$$

for all $p \geq 0$.

Corollary 5.12. *Let F be a field of characteristic different from p, $\mathcal{X}$ a gerbe banded by $C = (\boldsymbol{\mu}_p)^s$. Then*

$$\mathrm{ed}\big(\mathcal{X}\big) = \mathrm{ed}_p\big(\mathcal{X}\big) = \min \sum_{\chi \in \mathcal{B}} \mathrm{ind}\big(\beta^{\mathcal{X}}(\chi)\big),$$

where the minimum is taken over all bases $\mathcal{B}$ of $\widehat{C}$ over $\mathbb{Z}/p\mathbb{Z}$.

Proof. Any basis of $\widehat{C}$ contains a subset that maps bijectively by β onto a basis of D. Hence by Theorems 4.15, 5.11 and (5.3),

$$\begin{aligned}\mathrm{ed}_p(\mathcal{X}) = \mathrm{cdim}_p(\mathcal{X}) + s = \mathrm{ed}_p(D) + s &= \min \sum_{d \in \mathcal{A}} \big(\mathrm{ind}(d) - 1\big) + s \\ &= \min \sum_{\chi \in \mathcal{B}} \big(\mathrm{ind}\big(\beta^{\mathcal{X}}(\chi)\big) - 1\big) + s = \min \sum_{\chi \in \mathcal{B}} \mathrm{ind}\big(\beta^{\mathcal{X}}(\chi)\big),\end{aligned}$$

where the minima are taken over all bases $\mathcal{A}$ and $\mathcal{B}$ of D and $\widehat{C}$ respectively. By Proposition 5.10 and Theorems 4.15, 5.11,

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

6. Lower bounds for the essential dimension of algebraic groups

Let G be an algebraic group, C a central smooth subgroup of G and set $H = G/C$, so we have an exact sequence:

$$1 \to C \to G \to H \to 1. \tag{6.1}$$

Fix an H-torsor E over $\operatorname{Spec}(F)$ and consider the homomorphism

$$\beta^E : \widehat{C} \to \operatorname{Br}(F) \tag{6.2}$$

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

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

where ∂ is the connecting map for the exact sequence (6.1).

We write $\operatorname{Rep}(G)$ for the category of all finite dimensional representations of G over F. For a character $\chi \in \widehat{C}$ write $\operatorname{Rep}^{(\chi)}(G)$ for the full subcategory of all G-representations V such that $cv = \chi(c)v$ any c in C and $v \in V$.

If C is a diagonalizable group, then every C-space V is the direct sum of the eigenspaces $V^{(\chi)}$ over all $\chi \in \widehat{C}$ [48, §22]. Since the restriction homomorphism $F[G]^{(\chi)} \to F[C]^{(\chi)}$ is surjective, we have $F[G]^{(\chi)} \neq 0$ for every χ. A nonzero function in $F[G]^{(\chi)}$ generates a nonzero finite dimensional G-subspace of $F[G]$ in $\operatorname{Rep}^{(\chi)}(G)$. It follows that the category $\operatorname{Rep}^{(\chi)}(G)$ is nontrivial for all $\chi \in \widehat{C}$.

The following theorem was proved in [47, Theorem 4.4, Remark 4.5].

Theorem 6.1. (Index Theorem) *Let C be a diagonalizable central smooth subgroup of an algebraic group G, $H = G/C$, and $\chi : C \to \mathbf{G}_{\mathrm{m}}$ a character. Then*

1. *For every H-torsor E and every V in $\operatorname{Rep}^{(\chi)}(G)$, the integer $\operatorname{ind}\beta^E(\chi)$ divides $\dim(V)$.*
2. *Let E be a generic H-torsor (over a field extension of F). Then*

$$\operatorname{ind}\beta^E(\chi) = \gcd\dim(V),$$

where the gcd is taken over all G-representations V in $\operatorname{Rep}^{(\chi)}(G)$.

Proof. (1) The natural homomorphism $G \to \mathbf{GL}(V)$ for a G-representation V in $\operatorname{Rep}^{(\chi)}(G)$ factors through a map $H \to \mathbf{PGL}(V)$. By [47, Lemma 4.3], the composition

$$H^1(F, H) \to H^1\big(F, \mathbf{PGL}(V)\big) \to \operatorname{Br}(F)$$

takes the class of an H-torsor E to $\beta^E(\chi)$. It follows that $\operatorname{ind}\beta^E(\chi)$ divides $\dim(V)$.

(2) Let U be a generically free representation of H, X a nonempty open subset of U and $\pi : X \to Y$ an H-torsor. Let E be the generic fiber of π. It is a generic H-torsor over the function field $L := F(Y)$.

Let $\chi \in \widehat{C}$. Fix a nonzero G-representation W in $\operatorname{Rep}^{(\chi)}(G)$. The conjugation action of G on $B := \operatorname{End}(W)$ factors through an H-action. By descent (cf. [77, Ch. 1, §2]), there is (a unique up to canonical isomorphism) Azumaya algebra $\mathcal{A}$ over Y and an H-equivariant algebra isomorphism $\pi^*(\mathcal{A}) \simeq B_X := B \times X$. Let A be the generic fiber of $\mathcal{A}$; it is a central simple algebra over L with $\beta^E(\chi) = [A]$ for the map $\beta^E : \widehat{C} \to \operatorname{Br}(L)$.

Let Z be a G-scheme. Write $\mathcal{M}(G, Z)$ for the (abelian) category of left G-modules on Z that are coherent $\mathcal{O}_Z$-modules (see [96, §1.2]). In particular, $\mathcal{M}(G, \operatorname{Spec} F) = \operatorname{Rep}(G)$.

Now assume that C acts trivially on Z. Let $\mathcal{M}^{(\chi)}(G,Z)$ be the full subcategory of $\mathcal{M}(G,Z)$ consisting of G-modules on which C acts via χ. For example, $\mathcal{M}^{(\chi)}(G,\operatorname{Spec}F)=\operatorname{Rep}^{(\chi)}(G)$.

We make use of the equivariant K-theory. Write $K_0(G,Z)$ and $K_0^{(\chi)}(G,Z)$ for the Grothendieck groups of $\mathcal{M}(G,Z)$ and $\mathcal{M}^{(\chi)}(G,Z)$ respectively.

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

$$K_0(G,Z)=\coprod_{\chi\in\widehat{C}}K_0^{(\chi)}(G,Z).$$

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

$$K_0\big(\operatorname{Rep}^{(\chi)}(G)\big)\to K_0(A) \tag{6.3}$$

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

First, we have a canonical isomorphism

$$K_0\big(\operatorname{Rep}^{(\chi)}(G)\big)\simeq K_0^{(\chi)}(G,\operatorname{Spec}F). \tag{6.4}$$

Recall that X an open subscheme of U. By homotopy invariance in the equivariant K-theory [96, Cor. 4.2],

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

It follows that

$$K_0^{(\chi)}(G,\operatorname{Spec}F)\simeq K_0^{(\chi)}(G,U). \tag{6.5}$$

By localization [96, Th. 2.7], the restriction homomorphism

$$K_0^{(\chi)}(G,U)\to K_0^{(\chi)}(G,X). \tag{6.6}$$

is surjective.

Write $\mathcal{M}^{(1)}(G,X,B_X)$ for the category of left G-modules M on X that are coherent $\mathcal{O}_X$-modules and right B_X-modules such that C acts trivially on M and the G-action on M and the conjugation G-action on B_X agree. The corresponding Grothendieck group is denoted by $K_0^{(1)}(G,X,B_X)$. For any object N in $\mathcal{M}^{(\chi)}(G,X)$, the group C acts trivially on $N\otimes_F W^*$ and B acts on the right on $N\otimes_F W^*$. We have Morita equivalence

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

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

$$K_0^{(\chi)}(G,X)\simeq K_0^{(1)}(G,X,B_X). \tag{6.7}$$

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

$$K_0^{(1)}(G,X,B_X)\simeq K_0(H,X,B_X). \tag{6.8}$$

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

$$K_0(H, X, B_X) \simeq K_0(Y, \mathcal{A}). \tag{6.9}$$

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

$$K_0(Y, \mathcal{A}) \to K_0(A). \tag{6.10}$$

The homomorphism (6.3) is the composition of (6.4), (6.5), (6.6), (6.7), (6.8), (6.9) and (6.10). It takes the class of a representation V to the class in $K_0(A)$ of the generic fiber of the vector bundle $\big((V \otimes W^*) \times X\big)/H$ over Y of rank $\dim(V) \cdot \dim(W)$. $\square$

Suppose that the central subgroup C of a group G is isomorphic to the product of s copies of $\boldsymbol{\mu}_p$. The character group $\widehat{C}$ is a vector space of dimension s over $\mathbb{Z}/p\mathbb{Z}$. For every $\chi \in \widehat{C}$ write n_χ for the gcd of $\dim(V)$ over all $V \in \operatorname{Rep}^{(\chi)}(G)$. A basis $\mathcal{B}$ for $\widehat{C}$ is called *minimal*, if the sum $\sum_{\chi \in \mathcal{B}} n_\chi$ is the smallest possible.

Theorem 6.2. [84, Theorem 4.1] *Let p is a prime integer different from* $\operatorname{char}(F)$ *and G an algebraic group having a central subgroup C isomorphic to $(\boldsymbol{\mu}_p)^s$. Then*

$$\operatorname{ed}_p(G) \geq \sum_{\chi \in \mathcal{B}} n_\chi - \dim(G)$$

for a minimal basis $\mathcal{B}$ of $\widehat{C}$.

Proof. Set $H = G/C$, so we have an exact sequence (6.1). Let $E \to \operatorname{Spec}(L)$ be a generic H-torsor over a field extension L/F. Consider the gerbe $\mathcal{X} = E/G_L$ over L banded by C_L.

By Proposition 2.5 and Corollary 5.7,

$$\operatorname{ed}_p(G) \geq \operatorname{ed}_p(G_L) \geq \operatorname{ed}_p(\mathcal{X}) - \dim(E) = \operatorname{ed}_p(\mathcal{X}) - \dim(G).$$

The H-torsor E yields a homomorphism β^E in (6.2). By Corollary 5.12,

$$\operatorname{ed}_p(\mathcal{X}) = \min \sum_{\chi \in \mathcal{B}} \operatorname{ind}\big(\beta^E(\chi)\big),$$

where the minimum is taken over all bases $\mathcal{B}$ of $\widehat{C}$. By Theorem 6.1,

$$\operatorname{ind}\big(\beta^E(\chi)\big) = n_\chi.$$ $\square$

Corollary 6.3. *Assume in addition, that for every $\chi \in \widehat{C}$, there is V_χ in* $\operatorname{Rep}^{(\chi)}(G)$ *such that* $\operatorname{ind} \beta^E(\chi) = \dim(V_\chi)$. (*By Theorem* 6.1, *this condition holds if the dimension of every irreducible representation of G over F is a power of p.*) *Let V be the direct sum of the spaces V_χ with χ in a minimal basis of $\widehat{C}$. Then*

1. *$V|_C$ is a faithful representation of C,*
2. $\operatorname{ed}_p(G) \geq \dim(V) - \dim(G)$*,*
3. *Moreover, if V is generically free, then*

$$\operatorname{ed}_p(G) = \operatorname{ed}(G) = \dim(V) - \dim(G).$$

7. Essential dimension of finite groups

7a. **Essential p-dimension.** Let G be a finite group. We view G as a constant algebraic group over a field F. By Example 3.1, to give a G-torsor is the same as to give a Galois G-algebra. Thus, the essential dimension of G measures the complexity of the class of Galois extensions with Galois group G.

Theorem 7.1. [47, Theorem 4.1] *Let p be a prime integer, G be a p-group and F a field of characteristic different from p containing a primitive p-th root of unity. Then*

$$\operatorname{ed}_p(G) = \operatorname{ed}(G) = \min \dim(V),$$

where the minimum is taken over all faithful representations V of G over F.

Proof. Let q be the order of G. By [91, Th. 24], every irreducible representation of G is defined over the field $F(\mu_q)$. Since F contains p-th roots of unity, the degree $[F(\mu_q) : F]$ is a power of p. Hence the dimension of any irreducible representation of G over F is a power of p.

Let C be the *socle* of G, i.e., the maximal elementary abelian p-group in the center of G, and V a G-representation in Corollary 6.3 such that the restriction $V|_C$ is faithful. It suffices to show that V is generically free. Let N be the kernel of V. As N is normal in G and $N \cap C = \{1\}$, by an elementary property of p-groups, N is trivial, i.e., V is faithful and hence generically free since G is finite. □

Remark 7.2. The proof of Theorem 7.1 and Remark 4.16 show how to compute the essential dimension of G over F. For every character $\chi \in \widehat{C}$ choose a nonzero representation $V_\chi \in \operatorname{Rep}^{(\chi)}(G)$ of the smallest dimension. It appears as an irreducible component of the smallest dimension of the induced representation $\operatorname{Ind}_C^G(\chi)$. We construct a basis $\chi_1, \dots, \chi_s$ of $\widehat{C}$ by induction as follows: Let χ_1 be a nonzero character with the smallest $\dim(V_{\chi_1})$. If the characters $\chi_1, \dots, \chi_{i-1}$ are already constructed for some $i \le s$, then we take for χ_i a character with minimal $\dim(V_{\chi_i})$ among all the characters outside of the subgroup generated by $\chi_1, \dots, \chi_{i-1}$. Then V is a faithful representation of the least dimension and $\operatorname{ed}(G) = \sum_{i=1}^s \dim(V_{\chi_i})$.

Remark 7.3. We can compute the essential p-dimension of an arbitrary finite group G over a field F of characteristic different from p. (We don't assume that F contains p-th roots of unity.) Let G_p be a Sylow p-subgroup of G. By [70, Proposition 4.10], Proposition 2.5 and Theorem 7.1, the integer $\operatorname{ed}_p(G) = \operatorname{ed}_p(G_p) = \operatorname{ed}_p\big((G_p)_{F_p}\big)$, where $F_p = F(\mu_p)$, coincides with the least dimension of a faithful representation of G_p over F_p.

Remark 7.4. Theorem 7.1 was extended in [59, Theorem 7.1] to the class of étale p-group schemes having a splitting field of degree a power of p. The case of a cyclic p-group G was considered earlier in [24].

Corollary 7.5. [47, Corollary 5.2] *Let F be a field as in Theorem 7.1. Then*

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

One can derive from Theorem 7.1 an explicit formula for the essential p-dimension of a finite p-group G as follows: For a finite group H, we denote the intersection of the kernels of all multiplicative characters $H \to F^\times$ by H'. For any $i \ge 0$, let K_i

be the intersection of the groups H' for all subgroups $H \subset G$ of index p^i and set $C_i = K_i \cap C$, where C is the socle of G. Set $C_{-1} = C$. Thus, we have a sequence of $\mathbb{F}_p$-spaces

$$C = C_{-1} \supset C_0 \supset \cdots \supset C_s$$

with $C_s = \{1\}$ for s large enough.

Theorem 7.6. [75, Theorem 1.2] *Let p be a prime integer, G be a p-group and F a field of characteristic different from p containing a primitive p-th root of unity. If $p = 2$, we assume that F contains a primitive 4-th root of unity. Then*

$$\mathrm{ed}_p(G) = \mathrm{ed}(G) = \sum_{i=0}^{s} \bigl(\dim(C_{i-1}) - \dim(C_i)\bigr) p^i.$$

7b. **Covariant dimension.** Let G be a finite group. A *covariant* of G is a G-equivariant morphism $\varphi : V \to W$, where V and W are finite-dimensional G-representations. We say that φ is faithful if G acts faithfully on the image $\varphi(V)$. The *covariant dimension* $\mathrm{covdim}(G)$ of G is the minimal value of $\dim(\varphi)$, as φ ranges over all possible faithful covariants of G (see [51] and [50]).

The essential and covariant dimensions of G are related as follows:

$$\mathrm{ed}(G) \le \mathrm{covdim}(G) \le \mathrm{ed}(G) + 1.$$

Theorem 7.7. [50, Theorem 3.1] *The equality* $\mathrm{covdim}(G) = \mathrm{ed}(G)$ *holds if and only if the center of G is not trivial.*

This result has since been used by A. Duncan in [21] (see Theorem 3.24) as a key ingredient in his classification of finite groups of essential dimension 2. Further applications can be found in [58] that generalizes the approach of [24] in the case of a cyclic group and gives another proof of the equality $\mathrm{ed}(G) = \min \dim(V)$ in the setup of Theorem 7.1. The approach replaces fibered categories by the homogenization method as follows:

Choose a minimal basis $\mathcal{B}$ for $\widehat{C}$. By Index Theorem 6.1, for any $\chi \in \mathcal{B}$ there is a G-representations $V_\chi \in \mathrm{Rep}^{(\chi)}(G)$ such that $\mathrm{ind}\, \beta^E(\chi) = \dim(V_\chi)$ for a generic G/C-torsor E. Let V be the direct sum of V_χ for all $\chi \in \mathcal{B}$ and $\varphi : V \dashrightarrow V$ a G-compression. It suffices to show that φ is dominant. It is shown in [58] that φ can be chosen homogeneous with respect to the components V_χ. In particular, φ can be thought of as a G/C-compression of the product of projective spaces $\mathbb{P}(V_\chi)$ for $\chi \in \mathcal{B}$. Therefore, twisting this compression by the generic G/C-torsor E, we get a compression of the product X of Severi-Brauer varieties $\mathrm{SB}(A_\chi)$, where $A\chi$ is a central division algebra of degree $\dim(V_\chi)$. By Proposition 4.17, X is incompressible, hence φ is dominant.

8. Essential dimension of groups of multiplicative type

The essential dimension of groups of multiplicative type was considered in [59].

8a. **Essential p-dimension.** Let G be an algebraic group of multiplicative type. Let L/F be the (finite) splitting field extension with Galois group Γ. The assignment

$$G \mapsto \widehat{G} := \mathrm{Hom}(G_L, \mathbf{G}_\mathrm{m})$$

yields an anti-equivalence between the category of groups of multiplicative type split by L and the category of finitely generated Γ-modules (see [48, 20.17]).

Let $\rho : G \to \mathbf{GL}(V)$ be a representation of G. By [48, §22], over the splitting field L of G, the L-space V_L has a basis $v_1, \dots, v_n$ consisting of eigenvectors of G_L in V_L. Moreover, the basis can be chosen Γ-invariant (see [59, Lemma 2.3]). The L-subalgebra $B \subset \operatorname{End}_L(V_L)$ consisting of all endomorphisms b such that $b(v_i) \in Lv_i$ for all i is canonically isomorphic to the product of n copies of L with the group Γ acting by permutations of the factors. It follows that the F-algebra $A := B^{\Gamma}$ is an étale algebra of dimension n. The isomorphism of B-modules $B \xrightarrow{\sim} V_L$ taking a b to $\sum b(v_i)$, is Γ-equivariant, hence it descends to an isomorphism of A-modules $A \xrightarrow{\sim} V$. It follows that the representation ρ is isomorphic to the composition

$$G \xrightarrow{\eta} \mathbf{GL}_1(A) \hookrightarrow \mathbf{GL}(A)$$

for a group homomorphism η. In particular, ρ factors through a quasisplit torus $\mathbf{GL}_1(A)$.

Clearly, the torus $\mathbf{GL}_1(A)$ acts generically freely on A. Therefore, if ρ is faithful, then η is injective and therefore, G acts generically freely on A. Thus, the classes of faithful and generically free representations of G coincide.

Note that the representation V is irreducible if and only if Γ acts transitively on the basis if and only if A is a field (and therefore, a subfield of L). In particular, $\dim(V)$ divides $[L : F] = |\Gamma|$.

A representations V of G over F is called *p-faithful* if the kernel of V is a finite group of order prime to p.

Theorem 8.1. [59, Theorem 1.1] *Let F be a field and p an integer different from* $\operatorname{char}(F)$. *Let G be a group of multiplicative type over F such that the splitting group Γ of G and the factor group G/T by the maximal subtorus T in G are p-groups. Then*

$$\operatorname{ed}_p(G) = \operatorname{ed}(G) = \min \dim(V),$$

where the minimum is taken over all p-faithful representations V of G over F.

Proof. The proof is parallel to the one of Theorem 7.1. First note that the dimension of an irreducible representation V of G over F is a p-power as Γ is a p-group and $\dim(V)$ divides $|\Gamma|$.

Let C be the *p-cocle* of G, i.e., the maximal subgroup isomorphic to $(\boldsymbol{\mu}_p)^s$ for some s. The character Γ-module $\widehat{C}$ is canonically isomorphism to $\widehat{G}/(p\widehat{G} + I\widehat{G})$, where I is the augmentation ideal in $\mathbb{Z}[\Gamma]$. By Corollary 6.3, there exists a G-representation V such that the restriction $V|_C$ is faithful and

$$\operatorname{ed}_p(G) \geq \dim(V) - \dim(G).$$

The kernel N of the G-representation V is a normal subgroup of G with $N \cap C = \{1\}$. By Lemma [59, Lemma 2.2], N is a finite group of order prime to p, i.e., the G-representation V is p-faithful. Then V is a faithful (and hence generically free) representation of G/N, hence $\operatorname{ed}(G/N) \leq \dim(V) - \dim(G/N)$ by Proposition 3.13. As G is split over a p-extension of F and G/T is a p-group, the groups $H^1(K, G)$ and $H^1(K, G/N)$ are the p-primary torsion abelian groups for every field extension K/F. Since the order of N is prime to p, the natural homomorphism $H^1(K, G) \to H^1(K, G/N)$ is an isomorphism [59, Proposition 4.2]. It follows that $\operatorname{ed}(G) = \operatorname{ed}(G/N)$. Therefore,

$$\begin{aligned}\dim(V) - \dim(G) \leq \operatorname{ed}_p(G) \leq \operatorname{ed}(G) = \operatorname{ed}(G/N) \leq \\ \dim(V) - \dim(G/N) = \dim(V) - \dim(G).\end{aligned}$$

□

Theorem 8.1 can be restated in terms of Γ-modules. Recall that every representation of G factors through a quasisplit torus P, and the character Γ-module of a quasisplit torus is permutation. The representation ρ is p-faithful if and only if the cokernel of $f : \widehat{P} \to \widehat{G}$ is finite of order prime to p. A homomorphism of Γ-modules $A \to \widehat{G}$ with A a permutation Γ-module and the finite cokernel of order prime to p is called a *p-presentation* of $\widehat{G}$. A p-presentation of the smallest rank is called *minimal.*

Corollary 8.2. [59, Corollary 5.1] *Let $f : \widehat{P} \to \widehat{G}$ be a minimal p-presentation of $\widehat{G}$. Then* $\operatorname{ed}_p(G) = \operatorname{ed}(G) = \operatorname{rank}\big(\operatorname{Ker}(f)\big)$.

Remark 8.3. We can compute the essential p-dimension of an arbitrary group G of multiplicative type over a field F of characteristic different from p. Let G_p be the subgroup of G containing the maximal torus T of G such that G_p/T is a p-group and $[G : G_p]$ is relatively prime to p, and Γ_p a Sylow p-subgroup of Γ. Let $F_p = L^{\Gamma_p}$ be the fixed field of Γ_p.

For any field extension K/F, every element in the kernel and cokernel of the homomorphism

$$H^1(K, G_p) \to H^1(K, G)$$

are split over an extension of K of degree prime to p. It follows that the morphism of functors G_p-*torsors* $\to$ G-*torsors* is p-bijective. By Proposition 2.3 and Theorem 8.1,

$$\operatorname{ed}_p(G) = \operatorname{ed}_p(G_p) = \operatorname{ed}_p\big((G_p)_{F_p}\big)$$

is the rank of the kernel of a minimal p-presentation of $\widehat{G}_p$ (or equivalently, $\widehat{G}$) viewed as a Γ_p-module.

We derive an explicit formula for the essential p-dimension of a group G of multiplicative type.

The character Γ-module $\widehat{C}$ of the p-socle C is isomorphic to $\widehat{G}/(p\widehat{G} + I\widehat{G})$. For any subgroup $\Delta \subset \Gamma$, consider the composition $\widehat{G}^{\Delta} \hookrightarrow \widehat{G} \to \widehat{C}$. For every k, let V_k denote the image of the homomorphism

$$\coprod_{\Delta \subset \Gamma} \widehat{G}^{\Delta} \to \widehat{C},$$

where the coproduct is taken over all subgroups Δ with $[\Gamma : \Delta] \leq p^k$. We have the sequence of $\mathbb{F}_p$-subspaces

$$0 = V_{-1} \subset V_0 \subset \cdots \subset V_r = \widehat{C}. \tag{8.1}$$

Theorem 8.4. [72, Theorem 4.3] *We have the following explicit formula for the essential p-dimension of a group G of multiplicative type:*

$$\operatorname{ed}_p(G) = \sum_{k=0}^{r} \big(\dim(V_k) - \dim(V_{k-1})\big) p^k - \dim(G).$$

8b. **A conjecture on the essential dimension.** Let G be a group of multiplicative type over F split over a finite Galois extension L/F with Galois group Γ. Let

$$1 \to G \xrightarrow{\alpha} H \to S \to 1$$

be an exact sequence of groups of multiplicative type split by L. Suppose that α factors through a quasisplit torus. Then for any field extension K/F, the map α^* in the exact sequence

$$S(K) \to H^1(K, G) \xrightarrow{\alpha^*} H^1(K, H)$$

is trivial as quasisplit tori are special. It follows that S is a classifying variety for G and hence

$$\mathrm{ed}(G) \leq \dim(S) = \dim(H) - \dim(G).$$

The surjective Γ-homomorphism of the character groups $\hat{\alpha} : \widehat{H} \to \widehat{G}$ factors through a permutation Γ-module. A surjective homomorphism $f : A \to B$ of Γ-modules is called a *permutation representation of* B if A is a lattice and f factors through a permutation Γ-module. Thus, if $A \to \widehat{G}$ is a permutation representation of $\widehat{G}$, then $\mathrm{ed}(G) \leq \mathrm{rank}(A) - \dim(G)$.

A. Ruozzi posed the following conjecture in [87]:

Conjecture 8.5. *The essential dimension of a group G of multiplicative type is equal to* $\min\big(\mathrm{rank}(A) - \dim(G)\big)$*, where the minimum is taken over all permutation representations $A \to \widehat{G}$ of $\widehat{G}$.*

Proposition 8.6. [87, Theorem 14] Conjecture 8.5 holds for the groups G such that the splitting group Γ of G and the factor group G/T by the maximal subtorus T in G are p-groups for some prime integer p.

Proof. By Theorem 8.1, there is a Γ-homomorphism $f : P \to \widehat{G}$ with P a permutation Γ-module and the image M of f is of index $m := [\widehat{G} : M]$ prime to p such that $\mathrm{ed}(G) = \mathrm{rank}(P) - \mathrm{rank}\,\widehat{G})$. There is a Γ-homomorphism $j : \widehat{G} \to M$ such that both compositions of j with the inclusion $i : M \hookrightarrow \widehat{G}$ are multiplications by m.

As $|\widehat{G}_{\mathrm{tors}}| = p^k$ for some k, the multiple $p^k \cdot \mathrm{Id}$ of the identity of $\widehat{G}$ factors as the composition $\widehat{G} \to \mathbb{Z}^r \to \widehat{G}$ of group homomorphisms, where $r = \mathrm{rank}(\widehat{G}/\widehat{G}_{\mathrm{tors}})$. Since $|\Gamma| = p^n$ for some n, the multiple $p^{k+n} \cdot \mathrm{Id}$ factors as the composition

$$\widehat{G} \xrightarrow{f} \Lambda^r \xrightarrow{g} \widehat{G}$$

of Γ-module homomorphisms, where $\Lambda = Z[\Gamma]$.

Choose integers a and b such that $am + bp^{k+n} = 1$. Then the composition

$$\widehat{G} \xrightarrow{\begin{pmatrix} aj \\ f \end{pmatrix}} M \oplus \Lambda^r \xrightarrow{(i,\, bg)} \widehat{G}$$

is the identity, i.e., $\widehat{G}$ is a direct summand of $M \oplus \Lambda^r$.

Let A be the inverse image of $\widehat{G}$ under the homomorphism

$$f \oplus 1_{\mathbb{Z}[\Gamma]} : P \oplus \Lambda^r \to M \oplus \Lambda^r.$$

The surjection $A \to \widehat{G}$ is a permutation representation as it factors through $P \oplus \Lambda^r$ and $\mathrm{rank}(A) - \dim(\widehat{G}) = \mathrm{rank}(P) - \mathrm{rank}(M) = \mathrm{rank}(P) - \mathrm{rank}(\widehat{G}) = \mathrm{ed}(G)$. $\square$

Example 8.7. (see [52]) Let p be a prime integer different from $\mathrm{char}(F)$. The group $G = \mathbb{Z}/p\mathbb{Z}$ is a group of multiplicative type split by $F(\xi_p)$ with cyclic Galois group $\Gamma = \langle \gamma \rangle$ of order m dividing $p - 1$. The character Γ-module $\widehat{G}$ is cyclic of order p as an abelian group. Write $t^m - 1 = \Phi_m \cdot \Psi_m$ in the polynomial ring $\mathbb{Z}[t]$, where Φ_m is the m-th cyclotomic polynomial. The composition

$$h : \mathbb{Z}[t]/(\Phi_m) \xrightarrow{f} \mathbb{Z}[\Gamma] \xrightarrow{g} \widehat{G},$$

where γ acts on the first module by multiplication by t, $f(t^i) = \gamma^i \Psi_m(\gamma)$ and g takes 1 to a generator of $\widehat{G}$ is a permutation representation of $\widehat{G}$. Hence

$$\operatorname{ed}(\mathbb{Z}/p\mathbb{Z}) \leq \operatorname{rank} \mathbb{Z}[t]/(\Phi_m) = \varphi(m) = \varphi\big([F(\xi_p) : F]\big),$$

where φ is the Euler function. One can check that h is a minimal permutation representation of $\widehat{G}$, hence Conjecture 8.5 asserts that $\operatorname{ed}(\mathbb{Z}/p\mathbb{Z}) = \varphi\big([F(\xi_p) : F]\big)$. This is not known for $p \geq 11$ over $F = \mathbb{Q}$.

Example 8.8. Let m be a positive integer and write $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $p_1, p_2, \dots, p^r$ are distinct primes. The cyclic group $G := \mathbb{Z}/m\mathbb{Z}$ is the product of cyclic groups $G_i := \mathbb{Z}/p_i^{k_i}\mathbb{Z}$. Let F be a field such that $\operatorname{char}(F) \neq p_i$ and $\xi_{p_i} \in F$ for every i. The Galois group Γ of $F(\xi_m)/F$ is the product of the p_i-groups $\Gamma_i := \operatorname{Gal}\big(F(\xi_{p_i^{k_i}})/F\big)$. Let I_i be the augmentation ideal in the group ring $\mathbb{Z}[\Gamma_i]$. Write A for the Γ-submodule of the permutation Γ-module $P := \coprod \mathbb{Z}[\Gamma_i]$ generated by $\coprod I_i$ and the element $(1, 1, \dots, 1)$. We have a surjective Γ_i-homomorphism $\mathbb{Z}[\Gamma_i] \to \widehat{G}_i$ taking 1 to a generator of $\widehat{G}_i$. The composition

$$A \hookrightarrow P \to \coprod \widehat{G}_i = \widehat{G}$$

is a permutation representation of $\widehat{G}$. Hence

$$\operatorname{ed}(\mathbb{Z}/m\mathbb{Z}) \leq \operatorname{rank}(A) = \sum [F(\xi_{p_i^{k_i}}) : /F] - r + 1$$

(see [58, Proposition 11] or [102]). One can check that this is a minimal permutation representation of $\widehat{G}$, hence Conjecture 8.5 asserts that the equality holds. The equality is also a consequence of Conjecture 4.23 [102, Theorem 4.4].

9. Essential dimension of spinor and even Clifford groups

9a. **Essential dimension of spinor groups.** The computation of the essential dimension of the spinor groups was initiated in [9] (the case $n \geq 15$ and n is not divisible by 4) and [27] (the case $n \leq 14$) and continued in [70] and [15] (the case $n \geq 15$ and n is divisible by 4). We write $\mathbf{Spin}_n$ for the split spinor group of a nondegenerate quadratic form of dimension n and maximal Witt index.

If $\operatorname{char}(F) \neq 2$, then the essential dimension of $\mathbf{Spin}_n$ has the following values for $n \leq 14$ (see [27, §23]):

n	≤ 6	7	8	9	10	11	12	13	14
$\operatorname{ed}_2(\mathbf{Spin}_n) = \operatorname{ed}(\mathbf{Spin}_n)$	0	4	5	5	4	5	6	6	7

The lower bounds for the essential dimension of $\mathbf{Spin}_n$ for $n \leq 14$ are obtained by providing nontrivial cohomological invariants and the upper bounds - by constructing classifying varieties. The lower and upper bounds match!

We write $\mathbf{Spin}_n^+$ for the semi-spinor group. We refer to [48] for various facts about spinor groups, their factor groups and Clifford algebras.

Lemma 9.1. [79] *If $n \geq 15$ then, over a field of characteristic 0, the following representations are generically free:*

(1) *The spin representation of* $\mathbf{Spin}_n$ *of dimension* $2^{(n-1)/2}$*, if* n *is odd,*
(2) *Either of the two half-spin representation of* $\mathbf{Spin}_n$ *of dimension* $2^{(n-2)/2}$*, if* $n \equiv 2$ $(mod\ 4)$
(3) *The half-spin representation of* $\mathbf{Spin}_n^+$*, of dimension* $2^{(n-2)/2}$*, if* $n \equiv 0$ $(mod\ 4)$ *and* $n \geq 20$*.*

In the following theorem we give the values of $\mathrm{ed}_p(\mathbf{Spin}_n)$ for $n \geq 15$ and $p = 0$ and 2. Note that $\mathrm{ed}_p(\mathbf{Spin}_n) = 0$ if $p \neq 0, 2$ as 2 is the only torsion prime of $\mathbf{Spin}_n$.

Theorem 9.2. *Let* F *be a field of characteristic zero. Then for every integer* $n \geq 15$ *we have:*

$$\mathrm{ed}_2(\mathbf{Spin}_n) = \mathrm{ed}(\mathbf{Spin}_n) = \begin{cases} 2^{(n-1)/2} - \frac{n(n-1)}{2}, & \textit{if } n \textit{ is odd;} \\ 2^{(n-2)/2} - \frac{n(n-1)}{2}, & \textit{if } n \equiv 2 \pmod 4; \\ 2^{(n-2)/2} + 2^m - \frac{n(n-1)}{2}, & \textit{if } n \equiv 0 \pmod 4, \end{cases}$$

where 2^m *is the largest power of* 2 *dividing* n*. Moreover,*

$$\mathrm{ed}_2(\mathbf{Spin}_n^+) = \mathrm{ed}(\mathbf{Spin}_n^+) = 2^{(n-2)/2} - \frac{n(n-1)}{2}, \quad \textit{if } n \equiv 0 \pmod 4 \text{ and } n \geq 20.$$

Proof. We start with the semi-spinor group $\mathbf{Spin}_n^+$ when $n \equiv 0 \pmod 4$ and $n \geq 20$ (see [9, Remark 3.10]). Let C be the center of $\mathbf{Spin}_n^+$. The factor group $H = \mathbf{Spin}_n^+ / C$ is the special projective orthogonal group. An H-torsor E over a field extension K/F determines a central simple algebra A with an orthogonal involution σ. The image of the map $\beta^E : \widehat{C} \to \mathrm{Br}(K)$ is equal to $\{0, [C^+]\}$, where C^+ is a simple components of the Clifford algebra $C(A, \sigma)$. By [67], there is a field extension K/F and an H-torsor (A, σ) over K such that $\mathrm{ind}(C^+) = 2^{(n-2)/2}$, i.e., $C^+(q)$ is a division algebra. The dimension of the semi-spinor representation V of G is also equal to $2^{(n-2)/2}$. By Lemma 9.1, V is generically free. It follows from Corollary 6.3 that

$$\mathrm{ed}_2(\mathbf{Spin}_n^+) = \mathrm{ed}(\mathbf{Spin}_n^+) = \dim(V) - \dim(\mathbf{Spin}_n^+) = 2^{(n-2)/2} - \frac{n(n-1)}{2}.$$

Let C be the 2-socle of the center $Z(G)$ of the group $G := \mathbf{Spin}_n$. Suppose first that n is odd. The group C is equal to $Z(G)$ and is isomorphic to $\boldsymbol{\mu}_2$. The factor group $H = G/C$ is the special orthogonal group. An H-torsor E over a field extension K/F is a nondegenerate quadratic form q of dimension n. The image of the map $\beta^E : \widehat{C} \to \mathrm{Br}(K)$ is equal to $\{0, [C_0(q)]\}$, where $C_0(q)$ is the even Clifford algebra of q. By [67], there is a field extension K/F and an H-torsor q over K such that $\mathrm{ind}\big(C_0(q)\big) = 2^{(n-1)/2}$, i.e., $C_0(q)$ is a division algebra. On the other hand, the dimension of the spinor representation V of G is also equal to $2^{(n-1)/2}$. By Lemma 9.1, V is generically free. It follows from Corollary 6.3 that

$$\mathrm{ed}_2(G) = \mathrm{ed}(G) = \dim(V) - \dim(G) = 2^{(n-1)/2} - \frac{n(n-1)}{2}.$$

Now suppose that $n \equiv 2 \pmod 4$. The group C is isomorphic to $\boldsymbol{\mu}_2$ (while $Z(G) \simeq \boldsymbol{\mu}_4$). As in the previous case, the factor group $H = G/C$ is the special orthogonal group and an H-torsor E over a field extension K/F is a nondegenerate quadratic form q of dimension n. The image of the map $\beta^E : \widehat{C} \to \mathrm{Br}(K)$ is equal to $\{0, [C(q)]\}$, where $C(q)$ is the Clifford algebra of q. As the center of the even Clifford algebra $C_0(q)$ is split, we have $C_0(q) \simeq C^+(q) \times C^-(q)$ with central simple

K-algebras $C^+(q)$ and $C^-(q)$ Brauer equivalent to $C(q)$. The degree of $C^\pm(q)$ is equal to $2^{(n-2)/2}$. By [67], there is a field extension K/F and an H-torsor q over K such that $\operatorname{ind}\big(C^\pm\big) = 2^{(n-2)/2}$, i.e., $C^\pm(q)$ are division algebras. The dimension of every semi-spinor representation V of G is also equal to $2^{(n-2)/2}$. By Lemma 9.1, V is generically free. It follows from Corollary 6.3 that

$$\operatorname{ed}_2(G) = \operatorname{ed}(G) = \dim(V) - \dim(G) = 2^{(n-2)/2} - \frac{n(n-1)}{2}.$$

Finally suppose that $n \equiv 0 \pmod 4$. The group $C = Z(G)$ is isomorphic to $\boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2$. The factor group $H = G/C$ is the special projective orthogonal group. An H-torsor E over a field extension K/F determines a central simple algebra A with an orthogonal involution σ. The image of the map $\beta^E : \widehat{C} \to \operatorname{Br}(K)$ is equal to $\{0, [A], [C^+], [C^-]\}$, where C^+ and C^- are simple components of the Clifford algebra $C(A, \sigma)$. By [67], there is a field extension K/F and an H-torsor (A, σ) over K such that $\operatorname{ind}(C^+) = \operatorname{ind}(C^-) = 2^{(n-2)/2}$ and $\operatorname{ind}(A) = 2^m$, the largest power of 2 dividing n. The image of a minimal basis of $\widehat{C}$ is equal to $\{[A], [C^+]\}$. It follows from Theorem 6.2 that

$$\operatorname{ed}_2(\mathbf{Spin}_n) \geq \operatorname{ind}(C^+) + \operatorname{ind}(A) - \dim(H) = 2^{(n-2)/2} + 2^m - \frac{n(n-1)}{2}.$$

In order to prove the opposite inequality apply Corollary 5.8 to the group homomorphism $G \to \mathbf{Spin}_n^+$:

$$\operatorname{ed}(G) \leq \operatorname{ed}(\mathbf{Spin}_n^+) + \max \operatorname{ed}(E/G),$$

where the maximum is taken over all $\mathbf{Spin}_n^+$-torsors E over all field extensions K/F. The image of the class of E under the map $H^1(K, \mathbf{Spin}_n^+) \to H^2(K, \boldsymbol{\mu}_2) = \operatorname{Br}_2(K)$ is the class of the algebra A_K, hence by Theorem 4.15 and Proposition 5.10, $\operatorname{ed}(E/G) \leq \operatorname{ind}(A_K)$. As $\operatorname{ind}(A_K)$ is a power of 2 dividing n, we have $\operatorname{ind}(A_K) \leq 2^m$, where 2^m is the largest power of 2 dividing n. The computation of the essential dimension of $\mathbf{Spin}_n^+$ in the first part of the proof yields the inequality

$$\operatorname{ed}(G) \leq 2^{(n-2)/2} + 2^m - \frac{n(n-1)}{2}$$

for $n \geq 20$.

It remains to consider the case $n = 16$. Let V be the sum of the semi-spinor representation of $\mathbf{Spin}_{16}$ and the natural representation of the special orthogonal group $\mathbf{O}_{16}^+$, which we view as a $\mathbf{Spin}_{16}$-representation via the projection $\mathbf{Spin}_{16} \to \mathbf{O}_{16}^+$. Then V is a generically free representation of $\mathbf{Spin}_{16}$ (see [9, Theorem 3.3]). By Proposition 3.13,

$$\operatorname{ed}\big(\mathbf{Spin}_{16}\big) \leq \dim(V) - \dim\big(\mathbf{Spin}_{16}\big) = 24. \qquad \square$$

9b. **Essential dimension of the even Clifford group.** Let F be a field of characteristic different from 2 and K/F a field extension. We define:

$$I_n^1(K) := \boxed{\begin{array}{c}\text{Set of isomorphism classes of nondegenerate}\\ \text{quadratic forms over } K \text{ of dimension } n\end{array}}$$

There is a natural bijection $I_n^1(K) \simeq H^1(K, \mathbf{O}_n)$ (see [48, §29.E]).

Recall that the *discriminant* $\operatorname{disc}(q)$ of a form $q \in I^1_n(K)$ is equal to $(-1)^{n(n-1)/2}\det(q) \in K^\times/K^{\times 2}$. Set

$$I^2_n(K) := \{q \in I^1_n(K) \quad \text{such that} \quad \operatorname{disc}(q) = 1\}.$$

There is a natural bijection $I^2_n(K) \simeq H^1(K, \mathbf{O}^+_n)$ (see [48, §29.E]).

The *Clifford invariant* $c(q)$ of a form $q \in I^2_n(K)$ is the class in the Brauer group $\operatorname{Br}(K)$ of the Clifford algebra of q if n is even and the class of the even Clifford algebra if n is odd [48, §8.B]. Define

$$I^3_n(K) := \{q \in I^2_n(K) \quad \text{such that} \quad c(q) = 0\}.$$

Remark 9.3. Our notation of the functors I^k_n for $k = 1, 2, 3$ is explained by the following property: $I^k_n(K)$ consists of all classes of quadratic forms $q \in W(K)$ of dimension n such that $q \in I(K)^k$ if n is even and $q \perp \langle -1\rangle \in I(K)^k$ if n is odd, where $I(K)$ is the fundamental ideal of classes of even dimensional forms in the Witt ring $W(K)$ of K.

Let $\mathbf{\Gamma}^+_n$ be the split even Clifford group (see [48, §23]). We have $\mathbf{\Gamma}^+_n$-*torsors* $\simeq I^3_n$, hence $\operatorname{ed}_p(\mathbf{\Gamma}^+_n) = \operatorname{ed}_p(I^3_n)$ [15, §3].

The functor I^3_n is related to $\mathbf{Spin}_n$-torsors as follows: The short exact sequence

$$1 \to \boldsymbol{\mu}_2 \to \mathbf{Spin}_n \to \mathbf{O}^+_n \to 1$$

yields an exact sequence

$$K^\times/K^{\times 2} = H^1(K, \boldsymbol{\mu}_2) \to H^1(K, \mathbf{Spin}_n) \to H^1(K, \mathbf{O}^+_n) \xrightarrow{c} H^2(K, \boldsymbol{\mu}_2), \tag{9.1}$$

where c is the Clifford invariant. Thus $\operatorname{Ker}(c) = I^3_n(K)$.

The essential dimension of I^1_n and I^2_n was computed in [82, Theorems 10.3 and 10.4]: we have $\operatorname{ed}(I^1_n) = n$ and $\operatorname{ed}(I^2_n) = n - 1$. The Fiber Dimension Theorem 5.6 applied to (9.1) and Proposition 2.3 give the inequalities

$$\operatorname{ed}_p(I^3_n) \le \operatorname{ed}_p(\mathbf{Spin}_n) \le \operatorname{ed}_p(I^3_n) + 1$$

for every $p \ge 0$, thus either $\operatorname{ed}_p(I^3_n) = \operatorname{ed}_p(\mathbf{Spin}_n)$ or $\operatorname{ed}_p(I^3_n) = \operatorname{ed}_p(\mathbf{Spin}_n) - 1$.

It turns out that in order to decide which equality occurs, one needs to study the following problem in quadratic form theory. Note that this problem is stated entirely in terms of quadratic forms, while in its solution we use the essential dimension. We don't know how to solve the problem by means of quadratic form theory.

Problem 9.4. *For a field F, determine all pairs of integers (a, n) such that $0 < a < n$ and every form in $I^3_n(K)$ contains a nontrivial subform in $I^2_a(K)$ for every field extension K/F.*

All forms in $I^3_n(K)$ for $n \le 14$ are classified (see [27, Example 17.8, Theorems 17.13 and 21.3]). Inspection shows that for such n the problem has positive solution.

In general, for non-negative integers a, b and a field extension K/F set

$$I^3_{a,b}(K) := \big\{(q_a, q_b) \in I^2_a(K) \times I^2_b(K) \quad \text{such that} \quad q_a \perp q_b \in I^3_n(K)\big\}.$$

We have a morphism of functors $I^3_{a,b} \to I^3_n$ taking a pair (q_a, q_b) to $q_a \perp q_b$. It turns out that in the range $n \ge 15$ (with possibly two exceptions) we have the inequality $\operatorname{ed}(I^3_{a,b}) < \operatorname{ed}(I^3_n)$, thus, the morphism of functors is not surjective and hence the problem has negative solution.

Theorem 9.5. [15, Theorem 4.2] *Let F be a field of characteristic 0, $n \geq 15$ and a an even integer with $0 < a < n$. Then there is a field extension K/F and a form in $I_n^3(K)$ that does not contain a nontrivial subform in $I_a^2(K)$ (with possible exceptions: $(n,a) = (15,8)$ or $(16,8)$).*

Theorem 9.6. [15, Theorem 7.1] *Let F be a field of characteristic 0. Then for every integer $n \geq 15$ and $p = 0$ or 2 we have:*

$$\operatorname{ed}_p(\mathbf{\Gamma}_n^+) = \operatorname{ed}_p(I_n^3) = \begin{cases} 2^{(n-1)/2} - 1 - \frac{n(n-1)}{2}, & \text{if } n \text{ is odd;} \\ 2^{(n-2)/2} - \frac{n(n-1)}{2}, & \text{if } n \equiv 2 \pmod 4; \\ 2^{(n-2)/2} + 2^m - 1 - \frac{n(n-1)}{2}, & \text{if } n \equiv 0 \pmod 4, \end{cases}$$

where 2^m is the largest power of 2 dividing n.

If $char(F) \neq 2$, then the essential dimension of I_n^3 has the following values for $n \leq 14$:

n	≤ 6	7	8	9	10	11	12	13	14
$\operatorname{ed}_2(I_n^3) = \operatorname{ed}(I_n^3)$	0	3	4	4	4	5	6	6	7

Note that $\operatorname{ed}(I_{15}^3) = 22$. A jump of the value of $\operatorname{ed}(\mathbf{Spin}_n)$ when $n > 14$ is probably related to the fact that there is no simple classification of quadratic forms in I^3 of dimension greater than 14.

9c. **Pfister numbers.** Consider the following application in the algebraic theory of quadratic forms over a field F of characteristic different from 2 (see [9, §4]).

Recall that the quadratic form $a_0\langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \cdots \otimes \langle 1, a_m\rangle$ with $a_i \in F^\times$ is called a *general m-fold Pfister form* over F. Every form q in the m-th power $I^m(F)$ of the fundamental ideal in the Witt ring of F is the sum of several m-fold Pfister form. The m-Pfister number of q is the smallest number of m-fold Pfister forms appearing in a such sum. The Pfister number $\operatorname{Pf}_m(n)$ is the supremum of the m-Pfister number of q, taken over all field extensions K/F and all n-dimensional forms $q \in I^m(K)$.

One can easily check that $\operatorname{Pf}_1(n) = n/2$ and $\operatorname{Pf}_2(n) = n/2 - 1$, i.e., these values of the Pfister numbers are linear in n. The exponential lower bound for the essential dimension of the spinor groups implies that the value $\operatorname{Pf}_3(n)$ is at least exponential in n. It is not known whether $\operatorname{Pf}_m(n)$ is finite for $m \geq 4$.

10. Essential dimension of simple algebras

Let CSA_n be the functor taking a field extension K/F to the set of isomorphism classes $\mathsf{CSA}_n(K)$ of central simple K-algebras of degree n. By Example 3.2, the functors CSA_n and G-*torsors* for $G = \mathbf{PGL}_n$ are isomorphic, in particular, $\operatorname{ed}_p(\mathsf{CSA}_n) = \operatorname{ed}_p(\mathbf{PGL}_n)$ for every $p \geq 0$.

Let p be a prime integer and p^r the highest power of p dividing n. Then $\operatorname{ed}_p\big(\mathsf{CSA}_n\big) = \operatorname{ed}_p\big(\mathsf{CSA}_{p^r}\big)$ [86, Lemma 8.5.5]. Every central simple algebra of degree p is cyclic over a finite field extension of degree prime to p, hence $\operatorname{ed}_p\big(\mathsf{CSA}_p\big) = 2$ [86, Lemma 8.5.7].

10a. **Upper bounds.** Let G be an adjoint semisimple group over F. The adjoint action of G on the sum of two copies of the Lie algebra of G is generically free, hence by Proposition 3.13, $\operatorname{ed}(G) \leq \dim(G)$ (see [83, §4]). It follows that $\operatorname{ed}(\mathsf{CSA}_n) =$

$\mathrm{ed}(\mathbf{PGL}_n) \leq n^2 - 1$. This bound was improved in [56, Proposition 1.6] and [57, Theorem 1.1]:

$$\mathrm{ed}(\mathsf{CSA}_n) \leq \begin{cases} n^2 - 3n + 1, & \text{if } n \geq 4; \\ \frac{(n-1)(n-2)}{2}, & \text{if } n \geq 5 \text{ is odd.} \end{cases}$$

If p is a prime integer then $\mathrm{ed}_p(\mathsf{CSA}_n) = \mathrm{ed}_p(\mathsf{CSA}_{p^r})$, where p^r is the largest power of p dividing n. Upper bounds for $\mathrm{ed}_p(\mathsf{CSA}_{p^r})$ with $p > 0$ were obtained in [74], [76] and then improved in [88]. Let N be the normalizer of a maximal torus T of a semisimple group G. For any field extension K/F, the natural map

$$N\text{-}\mathsf{torsors}(K) \to G\text{-}\mathsf{torsors}(K) \tag{10.1}$$

is surjective by [93, III.4.3, Lemma 6]. It follows that $\mathrm{ed}_p(G) \leq \mathrm{ed}_p(N)$ for any $p \geq 0$. If $G = \mathbf{PGL}_{p^r}$, we have $N = T \rtimes S_{p^r}$, where T is the factor torus of $(\mathbf{G}_{\mathrm{m}})^{p^r}$ modulo $\mathbf{G}_{\mathrm{m}}$ embedded diagonally. Then $N\text{-}\mathsf{torsors}(K)$ is the set of isomorphism classes of pairs (A, L), where A is a central simple K-algebra of degree p^r and $L \subset A$ is an étale K-algebra of dimension p^r. The map (10.1) takes a pair (A, L) to A.

Structure theorems on maximal étale subalgebras of simple algebras allow us to replace the symmetric group S_{p^r} by a subgroup.

Lemma 10.1. [88, Corollary 3.3] *Let A be a central division algebra over a field F of degree $p^r \geq p$. Then there is a finite extension K/F of degree prime to p such that the K-algebra A_K contains a maximal subfield of the form $L_1 \otimes_K L_2$ with L_1 and L_2 of degree p and p^{r-1} over K respectively.*

Using the lemma one can replace the group S_{p^r} by the subgroup $S_p \times S_{p^{r-1}}$, hence $\mathrm{ed}_p(\mathsf{CSA}_{p^r}) \leq \mathrm{ed}_p\big(T \rtimes (S_p \times S_{p^{r-1}})\big)$. It turns out that there is generically free representation of the semidirect product of dimension $p^{2r-2} + p^r$.

Theorem 10.2. [88, Theorem 1.2] *For every $r \geq 2$, we have*

$$\mathrm{ed}_p(\mathsf{CSA}_{p^r}) \leq p^{2r-2} + 1.$$

10b. **Lower bounds.** In order to get a lower bound for $\mathrm{ed}_p\big(\mathsf{CSA}_{p^r}\big)$ one can use the valuation method. Using valuations we "degenerate" the group $\mathbf{PGL}_{p^r}$ to a torus as follows:

Let F be a field and p a prime integer different from $\mathrm{char}(F)$. Over a field extension L/F containing a primitive p-th root of unity, let $L' = L(a_1^{1/p}, a_2^{1/p}, \dots, a_r^{1/p})$ for some $a_i \in L^\times$ and choose a central simple L-algebra A of degree p^r that is split by L'. Over the rational function field $L(t) := L(t_1, t_2, \dots t_r)$, the algebra

$$B := A_{L(t)} \otimes (a_1, t_1) \otimes (a_2, t_2) \otimes \cdots \otimes (a_r, t_r),$$

where (a_i, t_i) are cyclic algebras of degree p, is split by $L'(t)$, hence there is a central simple algebra D of degree p^r over $L(t)$ Brauer equivalent to B.

Consider the functor $\mathcal{F} : \mathsf{Fields}_L \to \mathsf{Sets}$ that takes a field extension K/L to the factor group of the relative Brauer group $\mathrm{Br}(L' \otimes_L K/K)$ modulo the subgroup of decomposable elements of the form $(a_1, b_1) \otimes \cdots \otimes (a_r, b_r)$ with $b_i \in K^\times$. We can view the algebra A as an element of $\mathcal{F}(L)$, denoted $\widetilde{A}$. Using the theory of simple algebras over discrete valued fields, one obtains the key inequality

$$\mathrm{ed}_p\big(\mathsf{CSA}_{p^r}\big) \geq \mathrm{ed}_p(D) \geq \mathrm{ed}_p(\widetilde{A}) + r.$$

Note that the values of $\mathcal{F}$ are abelian groups, moreover, there is a torus T over L such that $\mathcal{F} \simeq T\text{-}\mathit{torsors}$. For a generic choice of A one has $\operatorname{ed}_p(\widetilde{A}) = \operatorname{ed}_p(T)$. This value can be computed using Theorem 8.4.

Theorem 10.3. [72, Theorem 6.1] *Let F be a field and p a prime integer different from* $\operatorname{char}(F)$. *Then*

$$\operatorname{ed}_p\big(\mathit{CSA}_{p^r}\big) \geq (r-1)p^r + 1.$$

Combining with the upper bound in Theorem 10.2 we get the following corollaries.

Corollary 10.4. [71, Theorem 1.1] *Let F be a field and p a prime integer different from* $\operatorname{char}(F)$. *Then* $\operatorname{ed}_p\big(\mathit{CSA}_{p^2}\big) = p^2 + 1$.

Note that M. Rost proved earlier that $\operatorname{ed}\big(\mathit{CSA}_4\big) = 5$.

Corollary 10.5. [88] *Let F be a field of characteristic different from* 2. *Then* $\operatorname{ed}_2\big(\mathit{CSA}_8\big) = 17$.

For every integers $n, m \geq 1$, any field extension K/F, let $\mathit{CSA}_{n,m}(K)$ denote the set of isomorphism classes of central simple K-algebras of degree n and exponent dividing m. Equivalently, $\mathit{CSA}_{n,m}(K)$ is the subset of the m-torsion part $\operatorname{Br}_m(K)$ of the Brauer group of K consisting of all elements a such that $\operatorname{ind}(a)$ divides n. In particular, $\mathit{CSA}_{n,n}(K) = \mathit{CSA}_n(K)$. We view $\mathit{CSA}_{n,m}$ as a functor $\mathit{Fields}_F \to \mathit{Sets}$.

Note that $\mathit{CSA}_{n,m} \simeq (\mathbf{GL}_n / \boldsymbol{\mu}_m)\text{-}\mathit{torsors}$.

We give upper and lower bounds for $\operatorname{ed}_p(\mathit{CSA}_{n,m})$ for a prime integer p different from $\operatorname{char}(F)$. Let p^r (respectively, p^s) be the largest power of p dividing n (respectively, m). Then $\operatorname{ed}_p(\mathit{CSA}_{n,m}) = \operatorname{ed}_p(\mathit{CSA}_{p^r,p^s})$ and (see [4, Section 6]). Thus, we may assume that n and m are the p-powers p^r and p^s respectively with $s \leq r$.

Every central simple algebra of degree 4 and exponent 2 is the tensor product $(a_1, b_1) \otimes (a_2, b_2)$ of two quaternion algebras. It follows from Example 3.7 that $\operatorname{ed}\big(\mathit{CSA}_{4,2}\big) = \operatorname{ed}_2\big(\mathit{CSA}_{4,2}\big) = 4$.

Theorem 10.6. [4, Theorem 6.1] *Let F be a field and p a prime integer different from* $\operatorname{char}(F)$. *Then, for any integers $r \geq 2$ and s with $1 \leq s \leq r$,*

$$p^{2r-2} + p^{r-s} \;\geq\; \operatorname{ed}_p(\mathit{CSA}_{p^r,p^s}) \;\geq\; \begin{cases} (r-1)2^{r-1} & \textit{if } p = 2 \textit{ and } s = 1, \\ (r-1)p^r + p^{r-s} & \textit{otherwise.} \end{cases}$$

Corollary 10.7. *Let p be an odd prime integer and F a field of characteristic different from p. Then*

$$\operatorname{ed}_p(\mathit{CSA}_{p^2,p}) = p^2 + p.$$

The corollary recovers a result in [97] that for p odd, there exists a central simple algebra of degree p^2 and exponent p over a field F which is not decomposable as a tensor product of two algebras of degree p over any finite extension of F of degree prime to p. Indeed, if every central simple algebra of degree p^2 and exponent p were decomposable, then the essential p-dimension of $\mathit{CSA}_{p^2,p}$ would be at most 4.

Corollary 10.8. *Let F be a field of characteristic different from* 2. *Then*

$$\operatorname{ed}_2(\mathit{CSA}_{8,2}) = \operatorname{ed}(\mathit{CSA}_{8,2}) = 8.$$

The corollary recovers a result in [1] that there is a central simple algebra of degree 8 and exponent 2 over a field F which is not decomposable as a tensor product of three quaternion algebras over any finite extension of F of odd degree. Indeed, if every central simple algebra of degree 8 and exponent 2 were decomposable, then the essential 2-dimension of $\mathsf{CSA}_{8,\,2}$ would be at most 6.

In the case $p = 2$ one can get a better upper bound.

Theorem 10.9. [2, Theorem 1.1] *Let F be a field of characteristic different from 2. Then, for any integer $n \geq 3$,*

$$\operatorname{ed}_p(\mathsf{CSA}_{2^n,\,2}) \leq 2^{2n-4} + 2^{n-1}.$$

Corollary 10.10. *Let F be a field of characteristic different from 2. Then*

$$\operatorname{ed}_2(\mathsf{CSA}_{16,\,2}) = 24.$$

Some bounds for the essential p-dimension in characteristic p were obtained in [2] and [3].

10c. **Essential dimension of split simple groups of type A.** A split simple group of type A_{n-1} is isomorphic to $\mathbf{SL}_n/\boldsymbol{\mu}_m$ for a divisor m of n. The exact sequence

$$1 \to \mathbf{SL}_n/\boldsymbol{\mu}_m \to \mathbf{GL}_n/\boldsymbol{\mu}_m \to \mathbf{G}_{\mathrm{m}} \to 1$$

allows us to compare the essential dimension of $\mathbf{SL}_n/\boldsymbol{\mu}_m$ and $\mathbf{GL}_n/\boldsymbol{\mu}_m$.

Theorem 10.11. [14, Theorem 1.1] *Let n be a natural number, m a divisor of n and p a prime integer. Let p^r and p^s be the largest powers of p dividing n and m respectively. Then over a field of characteristic not p,*

$$\operatorname{ed}_p(\mathbf{SL}_n/\boldsymbol{\mu}_m) = \begin{cases} 0, & \text{if } s = 0; \\ \operatorname{ed}_p\big(\mathsf{CSA}_{p^r,\,p^r}\big), & \text{if } s = r; \\ \operatorname{ed}_p\big(\mathsf{CSA}_{p^r,\,p^s}\big) + 1, & \text{if } 0 < s < r. \end{cases}$$

11. ESSENTIAL DIMENSION OF OTHER FUNCTORS

11a. **Essential dimension of forms and hypersurfaces.** Define the functors taking a field extension K/F to the set of isomorphism classes $\mathsf{Forms}_{n,\,d}(K)$ of forms (homogeneous polynomials) in n variables of degree d and to the factor set $\mathsf{Hypersurf}_{n,\,d}(K) = \mathsf{Forms}_{n,\,d}(K)/K^\times$ by the natural scalar action of the multiplicative group, viewed as the set of isomorphism classes of hypersurfaces in $\mathbb{P}^{n-1}_K$ of degree d.

Theorem 11.1. [85, Theorem 1.1] *Let F be a field of characteristic 0. Assume that $n \geq 2$ and $d \geq 3$ are integers and $(n, d) \neq (2, 3), (2, 4)$ or $(3, 3)$. Then*

(1) $\operatorname{ed}\big(\mathsf{Forms}_{n,\,d}\big) = \binom{n+d-1}{d} - n^2 + \operatorname{cdim}\big(\mathsf{CSA}_{n,\,d}\big) + 1.$

(2) $\operatorname{ed}\big(\mathsf{Hypersurf}_{n,\,d}\big) = \binom{n+d-1}{d} - n^2 + \operatorname{cdim}\big(\mathsf{CSA}_{n,\,d}\big).$

The values of $\operatorname{ed}\big(\mathsf{Forms}_{n,\,d}\big)$ and $\operatorname{ed}\big(\mathsf{Hypersurf}_{n,\,d}\big)$ for $n, d \geq 1$ not covered by Theorem 11.1 are summarized in the following table.

n	d	$\operatorname{ed}\big(\mathsf{Forms}_{n,\,d}\big)$	$\operatorname{ed}\big(\mathsf{Hypersurf}_{n,\,d}\big)$
arbitrary	1	0	0
1	≥ 2	1	0
arbitrary	2	n	$n - 1$
2	3	2	1
3	4	3	2
4	3	4	3

Write $\gcd(n,d) = q_1 q_2 \cdots q_t$, where the q_i are powers of distinct primes p_i. Let $p_i^{k_i}$ be the largest power of p_i dividing n. Conjecture 4.23 would imply that

$$\operatorname{cdim}\bigl(\mathsf{CSA}_{n,\,d}\bigr) = \sum_{i=1}^{t} (p_i^{k_i} - 1).$$

11b. **Essential dimension of abelian varieties.**

Theorem 11.2. [8, Theorem 1.2], [11, Theorem 1.2] *Let A be an abelian variety of dimension $g > 0$ over a field F. Then*

1. *If F is algebraically closed of characteristic 0, then $\operatorname{ed}(A) = 2g$;*
2. *If F is a number field, then $\operatorname{ed}(A) = \infty$.*

11c. **Essential dimension of moduli of curves.** The essential dimension of fibered categories (stacks) technique (see Section 5) is used in the proof of the following theorem.

Theorem 11.3. [10] *Let $\mathcal{M}_{g,n}$ be the stack of n-pointed smooth algebraic curves of genus g over a field of characteristic 0. Then*

$$\operatorname{ed}\bigl(\mathcal{M}_{g,n}\bigr) = \begin{cases} 2, & \textit{if } (g,n) = (0,0) \textit{ or } (1,1); \\ 0, & \textit{if } (g,n) = (0,1) \textit{ or } (0,2); \\ \infty, & \textit{if } (g,n) = (1,0) \\ 5, & \textit{if } (g,n) = (2,0) \\ 3g-3+n, & \textit{otherwise} \end{cases}$$

11d. **Essential dimension of some subfunctors.** In this section we consider certain subfunctors of Y for an algebraic variety Y over F. More specifically, let $f : X \to Y$ be a dominant morphism of varieties over F. We consider the functor $\mathcal{I}_f : \mathsf{Fields}_F \to \mathsf{Sets}$ defined by

$$\mathcal{I}_f(K) = \operatorname{Im}\bigl(X(K) \xrightarrow{f_K} Y(K)\bigr) \subset Y(K)$$

for a field extension K/F. Thus, $\mathcal{I}_f$ is a subfunctor of Y.

Theorem 11.4. *Let $f : X \to Y$ be a dominant morphism of varieties over a field F and X' the generic fiber of f. Then*

$$\dim(Y) + \operatorname{cdim}_p(X') \le \operatorname{ed}_p(\mathcal{I}_f) \le \operatorname{ed}(\mathcal{I}_f) \le \dim(X)$$

for every $p \ge 0$.

Proof. As there is a surjection $X \to \mathcal{I}_f$, we have $\operatorname{ed}_p(\mathcal{I}_f) \le \operatorname{ed}(\mathcal{I}_f) \le \dim(X)$.

Let $K = F(Y)$, E/K a field extension and $x' \in X'(E)$. Write x for the image of x' in $X(E)$ and set $y := f_E(x)$ in $Y(E)$. We view y as a point in $\mathcal{I}_f(E)$. By the definition of the essential dimension of $\mathcal{I}_f(E)$, there is a prime to p field extension L/E, a subfield $L_0 \subset L$ over F and an element $y_0 \in \mathcal{I}_f(L_0)$ such that $(y_0)_L = y_L$ and $\operatorname{tr.deg}(L_0/F) \le \operatorname{ed}_p(\mathcal{I}_f)$. It follows that the images of y_0 and y in Y coincide with the generic point of Y, hence K can be viewed as a subfield of L_0.

As $y_0 \in \mathcal{I}_f(L_0)$, there is a point $x_0 \in X(L_0)$ such that $f_{L_0}(x_0) = y_0$. We can view x_0 as a point in $X'(L_0)$. Thus, $(x')_L$ is detected by L_0 and by the definition of the canonical p-dimension of X', we have

$$\operatorname{cdim}_p(x') \le \operatorname{tr.deg}(L_0/K) = \operatorname{tr.deg}(L_0/F) - \operatorname{tr.deg}(K/F) \le \operatorname{ed}_p(\mathcal{I}_f) - \dim(Y).$$

It follows that $\operatorname{cdim}_p(X') \le \operatorname{ed}_p(\mathcal{I}_f) - \dim(Y)$. □

Corollary 11.5. *If the generic fiber X' is p-incompressible, then* $\operatorname{ed}_p(\mathcal{I}_f)=\operatorname{ed}(\mathcal{I}_f)=\dim(X)$.

Proof. As X' is p-incompressible, we have $\operatorname{cdim}_p(X')=\dim(X')$. Note that $\dim(X)=\dim(Y)+\dim(X')$. ☐

Example 11.6. Let F be a field of characteristic zero and $\alpha\in H^n\big(F,\mu_p^{\otimes(n-1)}\big)$ a non-zero symbol. Consider the functor

$$\mathcal{F}_\alpha(K)=\Big\{a\in K^\times \quad\text{such that}\quad (a)\cup\alpha_K=0 \quad\text{in}\quad H^{n+1}\big(K,\mu_p^{\otimes n}\big)\Big\}\subset K^\times.$$

Let Z_α be a p-generic splitting norm variety of α of dimension $p^{n-1}-1$ (see Example 4.13). Write $\widetilde{S}^p(Z_\alpha)$ for the symmetric p-th power of Z_α with all the diagonals removed. A geometric point of $\widetilde{S}^p(Z_\alpha)$ is a zero-cycle $z=z_1+\dots+z_p$ of degree p with all z_i distinct. There is a vector bundle $E\to\widetilde{S}^p(Z_\alpha)$ with the fiber over a point z as above the degree p algebra $F(z):=F(z_1)\times\dots\times F(z_p)$ (see [95, §2]). Leaving only invertible elements in each fiber we get an open subvariety X in E. Note that $\dim(X)=p\dim(Z_\alpha)+p=p^n$. A K-point of X is a pair (z,u), where z is an effective zero-cycle on Z_α over K of degree p and $u\in K(z)^\times$.

Consider the morphism $f:X\to\mathbf{G}_{\mathrm{m}}$ taking a pair (z,u) to $N_{K(z)/K}(u)$ and the functor $\mathcal{I}_f$.

Lemma 11.7. *For any field extension K/F we have:*

1. $\mathcal{I}_f(K)\subset\mathcal{F}_\alpha(K)$.
2. *If K has no nontrivial field extensions of degree prime to p, then* $\mathcal{F}_\alpha(K)=\mathcal{I}_f(K)$.

Proof. (1) Suppose $a\in\mathcal{I}_f(K)$, i.e., $a=N_{K(z)/K}(u)$ for a point $(z,u)\in X(K)$. We have

$$(a)\cup\alpha_K=N_{E/K}\big((u)\cup\alpha_{K(z)}\big)=0$$

as $\alpha_{K(z)}=0$ since Z_α is a splitting field of α. Thus, $a\in\mathcal{F}_\alpha(K)$.

(2) Let $a\in\mathcal{F}_\alpha(K)$, i.e., $(a)\cup\alpha_K=0$ for an element $a\in K^\times$. By [95], there is a degree p field extension E/K and an element $u\in E^\times$ such that $a=N_{E/K}(u)$ and $\alpha_E=0$. It follows that $Z(E)\neq\emptyset$ and therefore, Z has a closed point z of degree p with $F(z)=E$. We have $(z,u)\in X(K)$ and $f(z,u)=a$, hence $a\in\mathcal{I}_f(K)$. ☐

It follows from the lemma that the inclusion of functors $\mathcal{I}_f\hookrightarrow\mathcal{F}_\alpha$ is a p-bijection, hence $\operatorname{ed}_p(\mathcal{I}_f)=\operatorname{ed}_p(\mathcal{F}_\alpha)$ by Proposition 2.3.

The generic fiber X' of f is a p-generic splitting variety for the $(n+1)$-symbol $(t)\cup\alpha$ over the rational function field $F(t)$ (see [95]). As the symbol $(t)\cup\alpha$ is not trivial, the variety X' is p-incompressible by Example 4.13. By Corollary 11.5, $\operatorname{ed}_p(\mathcal{I}_f)=\dim(X)=p^n$. It follows that

$$\operatorname{ed}_p(\mathcal{F}_\alpha)=p^n.$$

Example 11.8. Let (V,q) be a non-degenerate quadratic form over F of characteristic different from 2 and $D(q)$ the functor of values of q, i.e.,

$$D(q)(K)=\big\{q(v),\quad v\in V_K\quad\text{is an anisotropic vector}\big\}\subset K^\times.$$

If the form q is isotropic, then $D(q)(K)=K^\times$ for all K and hence $\operatorname{ed}_2\big(D(q)\big)=\operatorname{ed}\big(D(q)\big)=1$.

Let $X \subset V$ be the open subscheme of anisotropic vectors in V. The restriction of q on X yields a morphism $f : X \to \mathbf{G}_{\mathrm{m}}$. The generic fiber X' of f is the affine quadric given by the quadratic form $h := q \perp \langle -t \rangle$ over the rational function field $F(t)$.

Lemma 11.9. *The first Witt index of* h *(see Example 4.14) is equal to* 1.

Proof. Over the function field $F(t)(h)$ of h, we have:

$$q_{F(t)(h)} \perp \langle -t \rangle = h_{F(t)(h)} = h' \perp \langle t, -t \rangle$$

for a quadratic form h' over $F(t)(h)$. Then the form h' is a subform of $q_{F(t)(h)}$. As the field extension $F(t)(h)/F$ is purely transcendental, the form $q_{F(t)(h)}$ is anisotropic, hence so is h'. ☐

It follows from the lemma and Example 4.14 that the generic fiber X' is 2-incompressible. By Corollary 11.5,

$$\mathrm{ed}_2\big(D(q)\big) = \mathrm{ed}\big(D(q)\big) = \dim(q).$$

Corollary 11.10. *Let* $q(x) = q(x_1, \dots, x_n)$ *be an anisotropic quadratic form over a field* F *with* $\mathrm{char}(F) \neq 2$. *Let* L *be a subfield of the rational function field* $F(x)$ *containing* $F\big(q(x)\big)$. *Then the generic value* $q(x)$ *of* q *is a value of* q *over* L *if and only if the degree* $[F(x) : L]$ *is finite and odd.*

Proof. Suppose $[F(x) : L]$ is finite and odd. Since $q(x)$ is a value of q over $F(x)$, by Springer's Theorem, $q(x)$ of q is a value of q over L.

Conversely, suppose $q(x)$ is a value of q over L, i.e., $q(x)$ is defined over L. As $\mathrm{ed}\big(D(q)\big) = n$, we have $\mathrm{tr.deg}_F(L) = n$, hence $[F(x) : L]$ is finite. By [35, Theorem 6.4], the degree of every rational morphism of the generic fiber X' to itself is odd. It follows that $[F(x) : L]$ is odd. ☐

Example 11.11. Let L/F be a finite separable field extension. Let $f : R_{L/F}(\mathbf{G}_{\mathrm{m},L}) \to \mathbf{G}_{\mathrm{m}}$ be the norm map. Consider the functor $\mathcal{I}_f$. The set $\mathcal{I}_f(K)$ is the group of all non-zero norms for the extension $K \otimes_F L/K$. The generic fiber X' of f is the generic torsor for the norm one torus $T = R^{(1)}_{L/F}(\mathbf{G}_{\mathrm{m},L})$.

It was proved in [44] that the variety X' is p-incompressible if $[L : F]$ is a power of a prime integer p. In this case, $\mathrm{ed}_p(\mathcal{I}_f) = \mathrm{ed}(\mathcal{I}_f) = [L : F]$.

References

[1] S. Amitsur, L. Rowen, and J.-P. Tignol, *Division algebras of degree* 4 *and* 8 *with involution*, Israel J. Math. **33** (1979), no. 2, 133–148.

[2] S. Baek, *Essential dimension of simple algebras with involutions*, To appear in Bull. Lond. Math. Soc.

[3] S. Baek, *Essential dimension of simple algebras in positive characteristic*, C. R. Math. Acad. Sci. Paris **349** (2011), no. 7-8, 375–378.

[4] S. Baek and A. Merkurjev, *Essential dimension of central simple algebras*, Acta Mathematica **209** (2012), no. 1, 1–27.

[5] A. Beauville, *On finite simple groups of essential dimension* 3, arXiv:1101.1372v2 [math.AG] (18 Jan 2011), 3 pages.

[6] G. Berhuy and Z. Reichstein, *On the notion of canonical dimension for algebraic groups*, Adv. Math. **198** (2005), no. 1, 128–171.

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

[8] P. Brosnan, *The essential dimension of a g-dimensional complex abelian variety is $2g$*, Transform. Groups **12** (2007), no. 3, 437–441.

[9] P. Brosnan, Z. Reichstein, and A. Vistoli, *Essential dimension, spinor groups, and quadratic forms*, Ann. of Math. (2) **171** (2010), no. 1, 533–544.

[10] P. Brosnan, Z. Reichstein, and A. 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.

[11] P. Brosnan and R. Sreekantan, *Essential dimension of abelian varieties over number fields*, C. R. Math. Acad. Sci. Paris **346** (2008), no. 7-8, 417–420.

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

[13] V. Chernousov, S. Gille, and A. Merkurjev, *Motivic decomposition of isotropic projective homogeneous varieties*, Duke Math. J. **126** (2005), no. 1, 137–159.

[14] V. Chernousov and A. Merkurjev, *Essential p-dimension of split simple groups of type A_n*, Linear Algebraic Groups and Related Structures (preprint server) 429 (2011, Apr 15), 8 pages.

[15] V. Chernousov and A. Merkurjev, *Essential dimension of spinor and Clifford groups*, Linear Algebraic Groups and Related Structures (preprint server) 455 (2012, Jan 2), 13 pages.

[16] V. Chernousov and J.-P. Serre, *Lower bounds for essential dimensions via orthogonal representations*, J. Algebra **305** (2006), no. 2, 1055–1070.

[17] H. Chu, S.-J. Hu, M.-C. Kang, and J. Zhang, *Groups with essential dimension one*, Asian J. Math. **12** (2008), no. 2, 177–191.

[18] J.-L. Colliot-Thélѐne, N. Karpenko, and A. Merkurjev, *Rational surfaces and the canonical dimension of the group* PGL_6, Algebra i Analiz **19** (2007), no. 5, 159–178.

[19] M. Demazure and A. Grothendieck, *Schémas en groupes*, SGA 3, vol. 1, Springer-Verlag, Berlin, 1970.

[20] A. Duncan and Z. Reichstein, *Versality of algebraic group actions and rational points on twisted varieties*, preprint, 2012.

[21] A. Duncan, *Finite groups of essential dimension* 2, to appear in Comment. Math. Helv.

[22] A. Duncan, *Essential dimensions of A_7 and S_7*, Math. Res. Lett. **17** (2010), no. 2, 263–266.

[23] R. Elman, N. Karpenko, and A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society Colloquium Publications, vol. 56, American Mathematical Society, Providence, RI, 2008.

[24] M. Florence, *On the essential dimension of cyclic p-groups*, Invent. Math. **171** (2008), no. 1, 175–189.

[25] W. Fulton, *Intersection theory*, Springer-Verlag, Berlin, 1984.

[26] R. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in Galois cohomology*, American Mathematical Society, Providence, RI, 2003.

[27] R. Garibaldi, *Cohomological invariants: exceptional groups and spin groups*, Mem. Amer. Math. Soc. **200** (2009), no. 937, xii+81, With an appendix by Detlev W. Hoffmann.

[28] Ph. Gille and Z. Reichstein, *A lower bound on the essential dimension of a connected linear group*, Comment. Math. Helv. **84** (2009), no. 1, 189–212.

[29] I. Herstein, *Noncommutative rings*, Mathematical Association of America, Washington, DC, 1994, Reprint of the 1968 original, With an afterword by Lance W. Small.

[30] V. Ishkhanov, B. Lur'e, and D. Faddeev, *The embedding problem in Galois theory*, Translations of Mathematical Monographs, vol. 165, American Mathematical Society, Providence, RI, 1997, Translated from the 1990 Russian original by N. B. Lebedinskaya.

[31] V. Iskovskih, *Minimal models of rational surfaces over arbitrary fields*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 1, 19–43, 237.

[32] B. Kahn, *Comparison of some field invariants*, J. Algebra **232** (2000), no. 2, 485–492.

[33] M.-C. Kang, *A central extension theorem for essential dimensions*, Proc. Amer. Math. Soc. **136** (2008), no. 3, 809–813 (electronic).

[34] N. Karpenko, *Grothendieck Chow motives of Severi-Brauer varieties*, Algebra i Analiz **7** (1995), no. 4, 196–213.

[35] N. Karpenko, *On anisotropy of orthogonal involutions*, J. Ramanujan Math. Soc. **15** (2000), no. 1, 1–22. MR 1 751 923

[36] N. Karpenko, *Canonical dimension of orthogonal groups*, Transform. Groups **10** (2005), no. 2, 211–215.

[37] N. Karpenko, *A bound for canonical dimension of the (semi)spinor groups*, Duke Math. J. **133** (2006), no. 2, 391–404.

[38] N. Karpenko, *Canonical dimension of (semi-)spinor groups of small ranks*, Pure Appl. Math. Q. **4** (2008), no. 4, part 1, 1033–1039.

[39] N. Karpenko, *Canonical dimension*, Proceedings of the International Congress of Mathematicians. Volume II (New Delhi), Hindustan Book Agency, 2010, pp. 146–161.

[40] N. Karpenko, *Incompressibility of orthogonal grassmannians*, C. R. Math. Acad. Sci. Paris **349** (2011), no. 21-22, 1131–1134.

[41] N. Karpenko, *Incompressibility of quadratic Weil transfer of generalized Severi-Brauer varieties*, J. Inst. Math. Jussieu **11** (2012), no. 1, 119–131.

[42] N. Karpenko, *Upper motives of algebraic groups and incompressibility of Severi-Brauer varieties*, To apper in J. Reine Angew. Math.

[43] N. Karpenko, *Unitary grassmannians*, Linear Algebraic Groups and Related Structures (preprint server) 424 (2011, Mar 17), 17 pages, To appear in J. Pure Appl. Algebra.

[44] N. Karpenko, *Incompressibility of generic torsors of norm tori*, Linear Algebraic Groups and Related Structures (preprint server) 475 (2012, Aug 8), 5 pages.

[45] N. Karpenko and A. Merkurjev, *Essential dimension of quadrics*, Invent. Math. **153** (2003), no. 2, 361–372.

[46] N. Karpenko and A. Merkurjev, *Canonical p-dimension of algebraic groups*, Adv. Math. **205** (2006), no. 2, 410–433.

[47] N. Karpenko and A. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508.

[48] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits.

[49] V. È. Kordonskiĭ, *On the essential dimension and Serre's conjecture II for exceptional groups*, Mat. Zametki **68** (2000), no. 4, 539–547.

[50] H. Kraft, R. Lötscher, and G. Schwarz, *Compression of finite group actions and covariant dimension. II*, J. Algebra **322** (2009), no. 1, 94–107.

[51] H. Kraft and G. Schwarz, *Compression of finite group actions and covariant dimension*, J. Algebra **313** (2007), no. 1, 268–291.

[52] A. Ledet, *On the essential dimension of some semi-direct products*, Canad. Math. Bull. **45** (2002), no. 3, 422–427.

[53] A. Ledet, *On p-groups in characteristic p*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), Springer, Berlin, 2004, pp. 591–600.

[54] A. 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.

[55] A. Ledet, *Finite groups of essential dimension one*, J. Algebra **311** (2007), no. 1, 31–37.

[56] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transform. Groups **9** (2004), no. 4, 337–379.

[57] M. Lorenz, Z. Reichstein, L. Rowen, and D. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670.

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

[59] R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein, *Essential p-dimension of algebraic tori*, To apper in J. Reine Angew. Math.

[60] R. Lötshcer, *A fiber dimension theorem for essential and canonical dimension*, Linear Algebraic Groups and Related Structures (preprint server) 454 (2011, Dec 16) , 28 pages.

[61] M. MacDonald, *Essential p-dimension of the normalizer of a maximal torus*, Transform. Groups **16** (2011), no. 4, 1143–1171.

[62] M. MacDonald, *Upper bounds for the essential dimension of E_7*, Linear Algebraic Groups and Related Structures (preprint server) 449 (2011, Nov 16), 5 pages.

[63] Ju. Manin, *Rational surfaces over perfect fields. II*, Mat. Sb. (N.S.) **72 (114)** (1967), 161–192.

[64] B. Mathews, *Canonical dimension of projective* $\mathrm{PGL}_1(A)$*-homogeneous varieties*, Linear Algebraic Groups and Related Structures (preprint server) 332 (2009, Mar 30), 7 pages.

[65] B. Mathews, *Incompressibility of orthogonal Grassmannians of rank* 2, J. Algebra **349** (2012), no. 1, 353–363.

[66] B. Mathews, *Canonical dimension of projective homogeneous varieties of inner type A and type B*, ProQuest LLC, Ann Arbor, MI, 2009, Thesis (Ph.D.)–University of California, Los Angeles.

[67] A. Merkurjev, *Maximal indexes of Tits algebras*, Doc. Math. **1** (1996), No. 12, 229–243 (electronic).

[68] A. Merkurjev, *Steenrod operations and degree formulas*, J. Reine Angew. Math. **565** (2003), 13–26.

[69] A. Merkurjev, *R-equivalence on three-dimensional tori and zero-cycles*, Algebra Number Theory **2** (2008), no. 1, 69–89.

[70] A. Merkurjev, *Essential dimension*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 299–325.

[71] A. Merkurjev, *Essential p-dimension of* $\mathrm{PGL}(p^2)$, J. Amer. Math. Soc. **23** (2010), no. 3, 693–712.

[72] A. Merkurjev, *A lower bound on the essential dimension of simple algebras*, Algebra Number Theory **4** (2010), no. 8, 1055–1076.

[73] A. Merkurjev and A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136.

[74] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra Number Theory **3** (2009), no. 4, 467–487.

[75] A. Meyer and Z. Reichstein, *Some consequences of the Karpenko-Merkurjev theorem*, Doc. Math. (2010), no. Extra volume: Andrei A. Suslin sixtieth birthday, 445–457.

[76] A. Meyer and Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, J. Algebra **329** (2011), 213–221.

[77] J. Milne, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980.

[78] J. Milnor, *Algebraic K-theory and quadratic forms*, Invent. Math. **9** (1969/1970), 318–344.

[79] A. Popov, *Finite stationary subgroups in general position of simple linear Lie groups*, Trudy Moskov. Mat. Obshch. **48** (1985), 7–59, 263.

[80] Yu. Prokhorov, *Simple finite subgroups of the cremona group of rank 3*, J. Algebraic Geom. **21** (2012), 563–600.

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

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

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

[84] Z. Reichstein, *Essential dimension*, Proceedings of the International Congress of Mathematicians. Volume II (New Delhi), Hindustan Book Agency, 2010, pp. 162–188.

[85] Z. Reichstein and A. Vistoli, *A genericity theorem for algebraic stacks and essential dimension of hypersurfaces*, To apper in JEMS.

[86] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, With an appendix by János Kollár and Endre Szabó.

[87] A. Ruozzi, *Algebraic tori and essential dimension*, Thesis (Ph.D.)–University of California, Los Angeles.

[88] A. Ruozzi, *Essential p-dimension of* PGL_n, J. Algebra **328** (2011), 488–494.

[89] N. Semenov and K. Zainoulline, *Essential dimension of Hermitian spaces*, Math. Ann. **346** (2010), no. 2, 499–503.

[90] J.-P. Serre, *Cohomologie galoisienne: progrès et problèmes*, Astérisque (1995), no. 227, Exp. No. 783, 4, 229–257, Séminaire Bourbaki, Vol. 1993/94.

[91] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[92] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[93] J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.

[94] J.-P. Serre, *Le groupe de Cremona et ses sous-groupes finis*, Astérisque (2010), no. 332, Exp. No. 1000, vii, 75–100, Séminaire Bourbaki. Volume 2008/2009. Exposés 997–1011.

[95] A. Suslin and S. Joukhovitski, *Norm varieties*, J. Pure Appl. Algebra **206** (2006), no. 1-2, 245–276.

[96] R. Thomason, *Algebraic K-theory of group scheme actions*, Algebraic topology and algebraic K-theory (Princeton, N.J., 1983), Ann. of Math. Stud., vol. 113, Princeton Univ. Press, Princeton, NJ, 1987, pp. 539–563.

[97] J.-P. Tignol, *Algèbres indécomposables d'exposant premier*, Adv. in Math. **65** (1987), no. 3, 205–228.

[98] D. Tossici and A. Vistoli, *On the essential dimension of infinitesimal group schemes*, arXiv:1101.3988v3 [math.AG] (25 Oct 2010), 11 pages.

[99] B. Totaro, *Birational geometry of quadrics in characteristic* 2, J. Algebraic Geom. **17** (2008), no. 3, 577–597.

[100] A. Vishik, *On the Chow groups of quadratic Grassmannians*, Doc. Math. **10** (2005), 111–130 (electronic).

[101] A. Vishik, *Direct summands in the motives of quadrics*, Preprint, 1999, 13 pages. Available on the web page of the author `http://www.maths.nott.ac.uk/personal/av/papers.html`.

[102] W. Wong, *On the essential dimension of cyclic groups*, J. Algebra **334** (2011), 285–294.

[103] K. Zainoulline, *Canonical p-dimensions of algebraic groups and degrees of basic polynomial invariants*, Bull. Lond. Math. Soc. **39** (2007), no. 2, 301–304.

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

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

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