Séminaire BOURBAKI juin 2015
67ème année, 2014-2015, n$^{\text{o}}$ 1101

ESSENTIAL DIMENSION

by **Alexander S. MERKURJEV**

INTRODUCTION

The essential dimension of an algebraic object is an integer that measures the complexity of the object. To motivate this notion, 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 $t^2 + at + b$ where $a, b \in K$, 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, up to isomorphism, over the field K_0 of transcendence degree at most 1 over F. On the other hand, the "generic" quadratic extension $F(t)/F(t^2)$, where t is a variable, cannot be defined over a subfield of $F(t^2)$ of transcendence degree 0. We say that the essential dimension of the class of quadratic extensions is equal to 1. Informally speaking, the essential dimension of an algebraic object is the minimal number of algebraically independent parameters one needs to define the object.

The notion of the essential dimension was introduced by J. Buhler and Z. Reichstein in [8] for the class of finite Galois field extensions with a given Galois group G and later in [35] was extended to the class of G-torsors for an arbitrary algebraic group G (see Section 2.4). Many classical algebraic objects such as simple algebras, quadratic and hermitian forms, algebras with involutions, etc., are closely related to the torsors of 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 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 $\mathsf{Fields}_F \to \mathsf{Sets}$ was defined in [5].

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

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 conjectural classification list) together with a morphism of functors $\mathcal{L} \to \mathcal{F}$, and the conjecture asserts that this morphism is surjective, i.e., the map $\mathcal{L}(K) \to \mathcal{F}(K)$ is surjective for every field extension K/F. 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 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 (Section 7.2) and in the theory of simple algebras (Corollaries 8.6 and 8.7).

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 variety 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 estimated by counting the number of algebraically independent parameters. But the essential dimension can be computed in some cases where no classification theorem is 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 (Section 3). The canonical dimension of a variety measures its compressibility. This can be studied by means of algebraic cycles and Chow motives (Section 8).

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 definitions of the essential dimension of algebraic varieties and algebraic groups. The essential dimension of special types of the categories fibered in groupoids such as stacks and gerbes can be computed (Section 4).

Essential dimension, which is defined in elementary terms, has surprising connections with many areas of algebra such as algebraic geometry, theory of Chow motives, algebraic K-theory, Galois cohomology, representation theory of algebraic groups, theory of fibered categories and valuation theory.

We use the following notation. The base field is always denoted by 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 $X \times_{\operatorname{Spec} F} \operatorname{Spec} K$.

1. DEFINITION AND SIMPLE PROPERTIES OF THE ESSENTIAL DIMENSION

1.1. Definition of the essential dimension

The essential dimension of a functor was defined in [5] as follows. 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 $\mathcal{F} : \mathsf{Fields}_F \to \mathsf{Sets}$ 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:

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

where the minimum is taken over all fields of definition K_0 of x. In other words, the essential dimension of x is the smallest transcendence degree of a field of definition of x.

We also define the *essential dimension of the functor* $\mathcal{F}$:

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

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

1.2. 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 $\mathcal{F} : \mathsf{Fields}_F \to \mathsf{Sets}$ be a functor, K/F a field extension, $x \in \mathcal{F}(K)$. We define the *essential p-dimension of* x:

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

where L runs over all prime to p extensions of K and the *essential p-dimension of the functor* $\mathcal{F}$:

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

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

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 $p = 0$.

1.3. Simple properties and examples

Let X be a scheme over F. We can view X as a functor from $\textsf{\textit{Fields}}_F$ to $\textsf{\textit{Sets}}$ taking a field extension K/F to the set of K-points $X(K) := \mathrm{Mor}_F(\mathrm{Spec}\, K, X)$.

Proposition 1.1 ([28], Corollary 1.4). — *For every variety X over F, we have $\mathrm{ed}_p(X) = \dim(X)$ for all $p \geq 0$.*

The following proposition is a straightforward consequence of the definition.

Proposition 1.2 ([28], Proposition 1.3). — *Let $p \geq 0$ and $\alpha : \mathcal{F} \to \mathcal{F}'$ be a surjective morphism of functors from $\textsf{\textit{Fields}}_F$ to $\textsf{\textit{Sets}}$. Then $\mathrm{ed}_p(\mathcal{F}) \geq \mathrm{ed}_p(\mathcal{F}')$.*

Example 1.3. — 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 1.1 and 1.2, $\mathrm{ed}(\mathcal{F}) \geq \mathrm{ed}(\mathbb{A}^n_F) = \dim(\mathbb{A}^n_F) = n$, 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 problems of finding a lower and an upper bound for $\mathrm{ed}_p(\mathcal{F})$, and in some cases the bounds match.

Let $\mathcal{F} : \textsf{\textit{Fields}}_F \to \textsf{\textit{Sets}}$ be a functor. A variety X over F is called *classifying for $\mathcal{F}$* if there is a surjective morphism of functors $X \to \mathcal{F}$.

Classifying varieties are used to obtain upper bounds for the essential dimension. Propositions 1.1 and 1.2 yield:

Corollary 1.4. — *Let $\mathcal{F} : \textsf{\textit{Fields}}_F \to \textsf{\textit{Sets}}$ be a functor and X a classifying variety for $\mathcal{F}$. Then $\dim(X) \geq \mathrm{ed}(\mathcal{F})$.*

2. ESSENTIAL DIMENSION OF ALGEBRAIC GROUPS

Algebraic groups provide a variety of examples of functors given by classical algebraic objects.

2.1. Torsors

We will write "algebraic group over F" for a smooth affine group scheme of finite type over F.

The set of isomorphism classes of G-torsors of an algebraic group G over a variety X is in a bijection 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 $H^1_{\acute{e}t}\big(\mathrm{Spec}(F), G\big) = H^1\big(\mathrm{Gal}(F_{\mathrm{sep}}/F), G(F_{\mathrm{sep}})\big)$, where F_{sep} is a separable closure of F.

Example 2.1. — Let G be a finite (constant) group over F. A G-torsor over F is of the form $\mathrm{Spec}(L) \to \mathrm{Spec}(F)$, where L is a Galois G-algebra.

Example 2.2. — 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, $G(K) = \mathrm{Aut}_K(A_K)$ 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 $\mathbf{Aut}(C) = G_2$:

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

2.2. 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 [35] 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.

2.3. Cohomological invariants

Cohomological invariants provide lower bounds for the essential dimension (see [35]). 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 and for every $d \geq 0$, we have a *degree d cohomological functor*

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

A *degree d cohomological invariant u with values in M of a functor $\mathcal{F} : \mathsf{Fields}_F \to \mathsf{Sets}$* is a morphism of functors $u : \mathcal{F} \to H$, where we view H as a functor to 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 2.3 ([31], Theorem 3.4). — *Let $\mathcal{F} : \mathsf{Fields}_F \to \mathsf{Sets}$ 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 $\mathrm{ed}_p(\mathcal{F}) \geq d$.*

Example 2.4. — Write $\boldsymbol{\mu}_n$ for the group of n-th roots of unity over a field F such that n is not divisible by $\mathrm{char}(F)$. 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 $\mathbf{G}_{\mathrm{m}} := \mathrm{Spec}\, F[t, t^{-1}]$ is the *multiplicative group*. Hence $\mathrm{ed}(\boldsymbol{\mu}_n)^s \leq s$. On the other hand, if p is a prime divisor of n, then the cohomological degree s invariant

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

is not trivial [5, Corollary 4.9], hence $\mathrm{ed}_p(\boldsymbol{\mu}_n)^s = \mathrm{ed}(\boldsymbol{\mu}_n)^s = s$.

Example 2.5. — Let $\mathbf{O}_n$ be the orthogonal group of a nondegenerate quadratic form of dimension n over a field F with $\mathrm{char}(F) \neq 2$. 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, $q \simeq \langle a_1, a_2, \ldots, a_n\rangle$ 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 $\mathrm{ed}(\mathbf{O}_n) \leq n$. On the other hand, the cohomological degree n invariant (the n-th Stiefel-Whitney class)

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

is well defined and nontrivial [14, §17], hence $\mathrm{ed}_2(\mathbf{O}_n) = \mathrm{ed}(\mathbf{O}_n) = n$.

2.4. Generically free and versal G-schemes

The original approach to the essential dimension of algebraic groups in [35] used the language of equivariant compressions of algebraic varieties.

Let G be an algebraic group over a field F. A G-variety 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 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 [10, 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.

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 [35], we write $\operatorname{ed}(X, G)$ for the smallest integer

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

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 2.2.

Lemma 2.6 ([5], §4). — *Let X be a generically free G-scheme and $E \to \operatorname{Spec}\big(F(X)^G\big)$ 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 every 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 G-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 $M_n(F)$ and the morphism $U \to U/G$ is a G-torsor.

Following [11], we call a G-scheme X *versal* if for every generically free G-scheme X' with the field $F(X')^G$ infinite and for 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 2.7 ([14], §5). — *Every G-representation V, viewed as a G-scheme, is versal.*

Proposition 2.8 ([31], Proposition 3.11). — *Let X be a versal generically free G-scheme (for example, a generically free representation of G). Then* $\mathrm{ed}(X, G) = \mathrm{ed}(G)$.

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 2.6 and Proposition 2.8 yield:

Corollary 2.9. — *Let E be a generic G-torsor. Then* $\mathrm{ed}(E) = \mathrm{ed}(G)$.

Proposition 2.8 also gives:

Proposition 2.10 (Upper bound). — *For an algebraic group G, we have*

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

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

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

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

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 2.12 ([6], Lemma 2.2). — *Let H be a subgroup of an algebraic group G. Then*

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

for every $p \geq 0$.

2.5. Symmetric groups

Let F be a field of characteristic zero. The study of the essential dimension of the symmetric group S_n was initiated in [8, Theorem 6.5]. An S_n-torsor over a field extension K/F is given by an S_n-Galois K-algebra or, equivalently, a degree n étale K-algebra.

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 2.7, 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

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

The lower bound $\mathrm{ed}(S_n) \geq \left[\frac{n}{2}\right]$ follows from Proposition 2.12 applied to a maximal 2-elementary subgroup $H \subset S_n$ and Example 2.4.

The lower bound $\mathrm{ed}(S_7) \geq 4$ was proved in [12] using the classification of rationally connected 3-folds with a faithful A_7-action given in [34, Theorem 1.5].

Theorem 2.13. — *All known values of the essential dimension of S_n are collected in the following table:*

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

Moreover, we have the following inequalities (for $n \geq 7$):

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

3. CANONICAL DIMENSION

The canonical dimension is a special case of the essential dimension of a functor.

3.1. Definition of the canonical dimension

The notion of canonical dimension of G-varieties was introduced in [4]. In this section we define the canonical p-dimension of a functor (see [22, §2] and [28, §1.6]).

Let $\mathcal{F} : \mathsf{Fields}_F \to \mathsf{Sets}$ 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:

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

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

For $p \geq 0$ we define

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

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

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

where the maximum is taken 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

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

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

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

by Proposition 1.2.

The functor $\widehat{\mathcal{F}}$ depends only on the class $\mathcal{C}$ of fields K in Fields_F such that $\mathcal{F}(K) \neq \emptyset$. The class $\mathcal{C}$ is closed under field extensions. We write $\mathrm{ed}_p(\mathcal{C}) := \mathrm{cdim}_p(\mathcal{F})$.

3.2. Canonical p-dimension and incompressibility of a variety

Let X be a variety over F. Viewing X as a functor from Fields_F to Sets, we have the *canonical p-dimension* $\mathrm{cdim}_p(X)$ of X defined. In other words, $\mathrm{cdim}_p(X)$ 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 1.1, $\mathrm{cdim}_p(X) \leq \mathrm{ed}_p(X) = \dim(X)$.

Write n_X for the $\gcd \deg(x)$ over all closed points $x \in X$.

Lemma 3.1 ([31], 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 $\mathrm{cdim}_p(X) = 0$.*
2. *If $\mathrm{cdim}_p(X) = 0$ and X is geometrically integral, then $(n_X, p) = 1$.*

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

Lemma 3.2 ([31], Lemma 4.2). — *Let X be a variety over F and $p \geq 0$. Then $\mathrm{cdim}_p(x_{gen})$ 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, $\mathrm{cdim}(x_{gen})$ is the least dimension of the image of a rational morphism $X \dashrightarrow X$.*

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

Proposition 3.3 ([31], 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.*

Proposition 3.4 ([21], 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 $X \dashrightarrow X$.*

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 $\alpha \in \mathrm{CH}_d(X \times Y)$ 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 $\mathrm{CH}_d(X \times Y) \simeq \mathrm{CH}_d(Y \times X)$.

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

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

is defined [13, § 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 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 3.5 ([20], 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.*

Example 3.6. — Proposition 3.5 can be used to prove the following (see [17] or [18]). Let A be a central simple 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 K/F if and only if the algebra A_K is split. Then $\operatorname{cdim}(X) = \operatorname{cdim}_p(X) = p^m - 1$, where $p^m \leq p^n$ is the index of A. In particular, X is p-incompressible if and only if A is a division algebra.

3.3. Incompressibility of products of varieties

In general, the product of incompressible varieties may not be incompressible.

Theorem 3.7 ([19], Corollary 12). — *Let $X_1, X_2, \ldots, X_n$ be projective homogeneous varieties, $\widehat{X}_k$ the product of all the X_i's but X_k. Then the product $X_1 \times X_2 \times \cdots \times X_n$ is p-incompressible for a prime p if and only if X_k is p-incompressible over the function field $F(\widehat{X}_k)$ for all k.*

The following example is used in the proof of Theorem 5.1.

Example 3.8. — Let p be a prime integer and $D \subset \mathrm{Br}_p(F)$ a finite subgroup, where $\mathrm{Br}_p(F)$ is the subgroup of elements of exponent dividing p in the Brauer group $\mathrm{Br}(F)$ of F. Let $A_1, A_2, \ldots, A_n$ be central simple algebras such that the classes $[A_i]$ form a basis of D. Let X_i be the Severi-Brauer variety of A_i. By Theorem 3.7, the product $X_1 \times X_2 \times \cdots \times X_n$ is p-incompressible if and only if the algebra A_k is a division algebra over the field $F(\widehat{X}_k)$ for all k. This was originally shown in [22, Theorem 2.1] with the help of algebraic K-theory.

By the index reduction formula, the latter condition is equivalent to $\mathrm{ind}(A^\alpha) \geq \mathrm{ind}(A_k)$ for all k and $\alpha = (j_1, j_2, \ldots, j_n)$ with $j_k \neq 0$, where A^α is the tensor product of $A_i^{\otimes j_i}$ over all i. The algebras A_i satisfying this condition can be constructed by induction as follows. Let $[A_1]$ be a nonzero class of D of the smallest index. If the classes $[A_1], \ldots, [A_{i-1}]$ are already chosen for some i, we take $[A_i]$ the class of D of the smallest index among the classes in $D \setminus \mathrm{span}([A_1], \ldots, [A_{i-1}])$.

4. FIBER DIMENSION THEOREM

The essential dimension of a fibered category was defined in [7]. The language of fibered category unites the two seemingly different cases of the essential dimension of an algebraic variety and an algebraic group.

4.1. Categories fibered in groupoids

In many examples of functors $\mathcal{F} : \mathit{Fields}_F \to \mathit{Sets}$, 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 $\mathit{Schemes}_F$ be the category of schemes over F, $\pi : \mathcal{X} \to \mathit{Schemes}_F$ 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 $\mathit{Schemes}_F$ 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 $\mathit{Schemes}_F$ 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.

Assume that $\mathcal{X}(X)$ 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 4.1. — 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 4.2. — 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 the 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 4.3. — 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 2.1, $E \simeq \operatorname{Spec}(L)$, 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 [16]).

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

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

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

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

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 4.4. — 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.

4.2. 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 $x_0 : \operatorname{Spec}(K_0) \to \mathcal{X}$.

Define

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

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

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

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

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

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

If the fiber category $\mathcal{X}(X)$ is small for every X, we have the functor $\mathcal{F}_{\mathcal{X}} : \mathsf{Fields}_F \to \mathsf{Sets}$ (see Section 4.1). 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 [7, Theorem 3.2].

Theorem 4.5 ((Fiber Dimension Theorem), [26], Theorem 1.1)
Let $f : \mathcal{X} \to \mathcal{Y}$ be a morphism of CFG's over F. Then for every $p \geq 0$,

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

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.

Theorem 4.5 and Example 4.4 give:

Corollary 4.6 ([7], Corollary 3.3). — *Let G be an algebraic group and X a G-scheme. Then*

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

for every $p \geq 0$.

Corollary 4.7. — *Let $G \to H$ be a homomorphism of algebraic groups over F. Then*

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

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

4.3. 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

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

making $\mathrm{B}C$ a "group object" in the category of *CFG*'s.

We set $H = G/C$ and let E be an H-torsor over $\mathrm{Spec}(F)$. Consider the fibered category $\mathcal{X} := E/G$. This is a *gerbe banded by* C. 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

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

for a scheme X implies that $\mathcal{X}$ has an object over X if and only if the image of $\theta(\mathcal{X})$ in $H^2_{\text{ét}}(X, C)$ 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 [23, §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 so that $\mathrm{B}C$ "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 $E \to \mathrm{Spec}(F)$ 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".

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

Proposition 4.8. — *Let $\mathcal{X}$ be a 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 $p \geq 0$.

The following theorem (which is used in the proof of Theorem 5.1) shows 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. The case $s = 1$ was proved in [7, Theorem 4.1]. Recall that $\mathrm{ed}_p(\mathrm{B}C) = s$ in this case by Example 2.4.

Theorem 4.9 ([22], Theorem 3.1). — *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*

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

5. ESSENTIAL DIMENSION OF FINITE GROUPS

5.1. Essential p-dimension

Let G be a finite group. We view G as a constant algebraic group over a field F. By Example 2.1, 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. The main ingredients of the proof of the following theorem are Theorems 3.7 (Example 3.8) and 4.9.

Theorem 5.1 ([22], 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*

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

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

Remark 5.2. — The proof of Theorem 5.1 and Example 3.8 shows how to compute the essential dimension of G over F. For every character $\chi \in \widehat{C}$ choose a nonzero representation V_χ of the smallest dimension such that the restriction to C is multiplication by the character χ. It appears as an irreducible component of the smallest dimension of the induced representation $\mathrm{Ind}_C^G(\chi)$. We construct a basis $\chi_1, \dots, \chi_s$ of $\widehat{C}$ 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, then we take χ_i a character with minimal $\dim(V_{\chi_i})$ among all characters outside of the subgroup generated by $\chi_1, \dots, \chi_{i-1}$. Then V is a faithful representation of the least dimension and $\mathrm{ed}(G) = \sum_{i=1}^s \dim(V_{\chi_i})$.

Corollary 5.3 ([22], Corollary 5.2). — *Let F be a field as in Theorem* 5.1*. Then*

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

6. ESSENTIAL DIMENSION OF GROUPS OF MULTIPLICATIVE TYPE

The essential dimension of groups of multiplicative type was considered in [27].

6.1. Essential p-dimension

Let G be an algebraic group of multiplicative type (a twisted form of a diagonalizable group). A representation V of G over F is called *p-faithful* if the kernel of V is a finite group of order prime to p.

Theorem 6.1 ([27], Theorem 1.1). — *Let F be a field and p an integer different from* $\mathrm{char}(F)$*. 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*

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

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

Theorem 6.1 can be restated in terms of Γ-modules. Every representation ρ 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 6.2 ([27], Corollary 5.1). — *Let $f : \widehat{P} \to \widehat{G}$ be a minimal p-presentation of $\widehat{G}$. Then* $\mathrm{ed}_p(G) = \mathrm{ed}(G) = \mathrm{rank}\big(\mathrm{Ker}(f)\big)$.

7. ESSENTIAL DIMENSION OF SPINOR GROUPS

7.1. Spinor groups

The torsors of the split spinor group $\mathbf{Spin}_n$ are essentially the nondegenerate quadratic forms of dimension n with trivial discriminant and Clifford invariant.

The computation of the essential dimension of the spinor groups was initiated in [6] (the case $n \geq 15$ and n is not divisible by 4) and [15] (the case $n \leq 14$) and continued in [28] and [9] (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 $\mathrm{char}(F) \neq 2$, then the essential dimension of $\mathbf{Spin}_n$ has the following values for $n \leq 14$ (see [15, §23]):

n	≤ 6	7	8	9	10	11	12	13	14
$\mathrm{ed}_2(\mathbf{Spin}_n) = \mathrm{ed}(\mathbf{Spin}_n)$	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!

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 $p \neq 0, 2$.

The theorem below shows the exponential growth of the essential dimension of $\mathbf{Spin}_n$ when n goes to infinity. This is not predicted by the table of small values of $\mathrm{ed}(\mathbf{Spin}_n)$!

Theorem 7.1. — *Let F be a field of characteristic zero. Then for every integer $n \geq 15$ we have:*

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

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

Remark 7.2. — We have $\mathrm{ed}(\mathbf{Spin}_{15}) = 23$ and $\mathrm{ed}(\mathbf{Spin}_{16}) = 24$. A jump of the value of $\mathrm{ed}(\mathbf{Spin}_n)$ when $n > 14$ is probably related to the fact that there is no simple classification of quadratic forms with trivial discriminant and Clifford invariant of dimension greater than 14 or that the classifying space of $\mathbf{Spin}_n$ is not stably rational.

7.2. Pfister numbers

Consider the following application in the algebraic theory of quadratic forms over a field F of characteristic different from 2 (see [6, §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 $I(F)$ in the Witt ring of F is the sum of several m-fold Pfister forms. The m-Pfister number of q is the smallest number of m-fold Pfister forms appearing in a such sum. The Pfister number $\mathrm{Pf}_m(n)$ 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 check that $\mathrm{Pf}_1(n) = \frac{n}{2}$ and $\mathrm{Pf}_2(n) = \frac{n}{2} - 1$, 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 $\mathrm{Pf}_3(n)$ is at least exponential in n. It is not known whether $\mathrm{Pf}_m(n)$ is finite for $m \geq 4$.

8. 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 2.2, the functors CSA_n and G-$\mathsf{torsors}$ for $G = \mathbf{PGL}_n$ are isomorphic, in particular, $\mathrm{ed}_p(\mathsf{CSA}_n) = \mathrm{ed}_p(\mathbf{PGL}_n)$ for every $p \geq 0$.

Let p be a prime integer and p^r the highest power of p dividing n. Then $\mathrm{ed}_p\big(\mathsf{CSA}_n\big) = \mathrm{ed}_p\big(\mathsf{CSA}_{p^r}\big)$ [36, Lemma 8.5.5]. Every central simple algebra of degree p is cyclic over a finite field extension of degree prime to p, hence $\mathrm{ed}_p\big(\mathsf{CSA}_p\big) = 2$ [36, Lemma 8.5.7].

8.1. 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 2.10, $\mathrm{ed}(G) \leq \dim(G)$ (see [35, §4]). It follows that $\mathrm{ed}(\mathsf{CSA}_n) = \mathrm{ed}(\mathbf{PGL}_n) \leq n^2 - 1$. This bound was improved in [24, Proposition 1.6] and [25, Theorem 1.1]:

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

Upper bounds for $\mathrm{ed}_p(\mathsf{CSA}_{p^r})$ with $p > 0$ were obtained in [32], [33] and then improved in [37].

Theorem 8.1 ([37], Theorem 1.2). — *For every $r \geq 2$, we have*

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

8.2. 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.

Theorem 8.2 ([30], Theorem 6.1). — *Let F be a field and p a prime integer different from* $\mathrm{char}(F)$. *Then*

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

Combining with the upper bound in Theorem 8.1 we get the following corollaries.

Corollary 8.3 ([29], Theorem 1.1). — *Let F be a field and p a prime integer different from* $\mathrm{char}(F)$. *Then* $\mathrm{ed}_p\big(\mathsf{CSA}_{p^2}\big) = p^2 + 1$.

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

Corollary 8.4 ([37]). — *Let F be a field of characteristic different from 2. Then* $\mathrm{ed}_2\big(\mathsf{CSA}_8\big) = 17$.

For every integers $n, m \geq 1$, m dividing n, a field extension K/F, let $\mathsf{CSA}_{n,m}(K)$ denote the set of isomorphism classes of central simple K-algebras of degree n and exponent dividing m.

We give upper and lower bounds for $\mathrm{ed}_p(\mathsf{CSA}_{n,m})$ for a prime integer p different from $\mathrm{char}(F)$. Let p^r (respectively, p^s) be the largest power of p dividing n (respectively, m). Then $\mathrm{ed}_p(\mathsf{CSA}_{n,m}) = \mathrm{ed}_p(\mathsf{CSA}_{p^r,p^s})$ and (see [3, 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 that $\mathrm{ed}\big(\mathsf{CSA}_{4,2}\big) = \mathrm{ed}_2\big(\mathsf{CSA}_{4,2}\big) = 4$.

Theorem 8.5 ([3], Theorem 6.1). — *Let F be a field and p a prime integer different from* $\mathrm{char}(F)$. *Then, for any integers $r \geq 2$ and s with $1 \leq s \leq r$,*

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

Corollary 8.6. — *Let p be an odd prime integer and F a field of characteristic different from p. Then*

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

The corollary recovers a result in [38] 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 $\mathsf{CSA}_{p^2,p}$ would be at most 4.

Corollary 8.7. — *Let F be a field of characteristic different from 2. Then*

$$\mathrm{ed}_2(\mathsf{CSA}_{8,2}) = \mathrm{ed}(\mathsf{CSA}_{8,2}) = 8.$$

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 8.8 ([2], Theorem 1.1). — *Let F be a field of characteristic different from 2. Then, for any integer $n \geq 3$,*

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

Corollary 8.9. — *Let F be a field of characteristic different from 2. Then*

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

REFERENCES

[1] S.A. AMITSUR, L.H. 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*, Bull. Lond. Math. Soc. **44** (2012), no. 3, 578–590.

[3] S. BAEK and A. MERKURJEV – *Essential dimension of central simple algebras*, Acta Math. **209** (2012), no. 1, 1–27.

[4] G. BERHUY and Z. REICHSTEIN – *On the notion of canonical dimension for algebraic groups*, Adv. Math. **198** (2005), no. 1, 128–171.

[5] G. BERHUY and G. FAVI – *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330 (electronic).

[6] P. BROSNAN, Z. REICHSTEIN and A. VISTOLI – *Essential dimension, spinor groups, and quadratic forms*, Ann. of Math. (2) **171** (2010), no. 1, 533–544.

[7] 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.

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

[9] V. CHERNOUSOV and A. MERKURJEV – *Essential dimension of spinor and Clifford groups*, Algebra Number Theory **8** (2014), no. 2, 457–472.

[10] M. DEMAZURE and A. GROTHENDIECK – *Schémas en groupes*, SGA 3, vol. 1, Springer-Verlag, Berlin, 1970.

[11] A. DUNCAN and Z. REICHSTEIN – *Versality of algebraic group actions and rational points on twisted varieties*, To appear in Journal of Algebraic Geometry.

[12] A. DUNCAN – *Essential dimensions of A_7 and S_7*, Math. Res. Lett. **17** (2010), no. 2, 263–266.

[13] W. FULTON – *Intersection theory*, Springer-Verlag, Berlin, 1984.

[14] R. GARIBALDI, A. MERKURJEV, and J-P. SERRE – *Cohomological invariants in Galois cohomology*, Amer. Math. Soc., Providence, RI, 2003.

[15] 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.

[16] V.V. ISHKHANOV, B. B. LURÉ and D. K. FADDEEV – *The embedding problem in Galois theory*, Translations of Mathematical Monographs, vol. 165, Amer. Math. Soc., Providence, RI, 1997, translated from the 1990 Russian original by N. B. Lebedinskaya.

[17] N.A. KARPENKO – *Grothendieck Chow motives of Severi-Brauer varieties*, Algebra i Analiz **7** (1995), no. 4, 196–213.

[18] N.A. KARPENKO – *On anisotropy of orthogonal involutions*, J. Ramanujan Math. Soc. **15** (2000), no. 1, 1–22.

[19] N.A. KARPENKO – *Incompressibility of products*, Preprint (2015).

[20] N.A. KARPENKO – *Canonical dimension*, Proceedings of the International Congress of Mathematicians. Volume II (New Delhi), Hindustan Book Agency, 2010, pp. 146–161.

[21] N.A. KARPENKO and A. MERKURJEV – *Canonical p-dimension of algebraic groups*, Adv. Math. **205** (2006), no. 2, 410–433.

[22] N.A. KARPENKO and A. MERKURJEV – *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508.

[23] M-A. KNUS, A. MERKURJEV, M. ROST and J-P. TIGNOL – *The book of involutions*, Amer. Math. Soc., Providence, RI, 1998, With a preface in French by J. Tits.

[24] N. LEMIRE – *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transform. Groups **9** (2004), no. 4, 337–379.

[25] M. LORENZ, Z. REICHSTEIN, L.H. ROWEN and D.J. SALTMAN – *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670.

[26] R. LÖTSCHER – *A fiber dimension theorem for essential and canonical dimension*, Compositio Math. **149** (2013), no. 1, 148–174.

[27] R. LÖTSCHER, M. MACDONALD, A. MEYER and Z. REICHSTEIN – *Essential dimension of algebraic tori*, J. reine angew. Math. **677** (2013), 1–13.

[28] A. MERKURJEV – *Essential dimension*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 299–325.

[29] A. MERKURJEV – *Essential p-dimension of* $\mathrm{PGL}(p^2)$, J. Amer. Math. Soc. **23** (2010), no. 3, 693–712.

[30] A. MERKURJEV – *A lower bound on the essential dimension of simple algebras*, Algebra Number Theory **4** (2010), no. 8, 1055–1076.

[31] A. MERKURJEV – *Essential dimension: a survey*, Transform. Groups **18** (2013), no. 2, 415–481.

[32] 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.

[33] A. MEYER and Z. REICHSTEIN – *An upper bound on the essential dimension of a central simple algebra*, J. Algebra **329** (2011), 213–221.

[34] Yu. PROKHOROV – *Simple finite subgroups of the cremona group of rank 3*, J. Algebraic Geom. **21** (2012), 563–600.

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

[36] 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.

[37] A. RUOZZI – *Essential p-dimension of* PGL_n, J. Algebra **328** (2011), 488–494.

[38] J-P. TIGNOL – *Algèbres indécomposables d'exposant premier*, Adv. in Math. **65** (1987), no. 3, 205–228.

Alexander S. MERKURJEV

Department of Mathematics
University of California at Los Angeles
Los Angeles, California, 90095-1555, U.S.A.
E-mail : merkurev@math.ucla.edu