Essential Dimension: a Functorial Point of View (After A. Merkurjev)

Grégory Berhuy, Giordano Favi

Received: September 9, 2003

Communicated by Ulf Rehmann

Abstract. In these notes we develop a systematic study of the essential dimension of functors. This approach is due to A. Merkurjev and can be found in his unpublished notes [12]. The notion of essential dimension was earlier introduced for finite groups by J. Buhler and Z. Reichstein in [3] and for an arbitrary algebraic group over an algebraically closed field by Z. Reichstein in [14]. This is a numerical invariant depending on the group G and the field k. This number is denoted by $\mathrm{ed}_k(G)$. In this paper we insist on the behaviour of the essential dimension under field extension k'/k and try to compute $\mathrm{ed}_k(G)$ for *any* k. This will be done in particular for the group $\mathbb{Z}/n$ when $n \leq 5$ and for the circle group. Along the way we define the essential dimension of functor with versal pairs and prove that all the different notions of essential dimension agree in the case of algebraic groups. Applications to finite groups are given. Finally we give a proof of the so-called homotopy invariance, that is $\mathrm{ed}_k(G) = \mathrm{ed}_{k(t)}(G)$, for an algebraic group G defined over an infinite field k.

2000 Mathematics Subject Classification: 11E72, 12G05, 14L15, 14L30.

Keywords and Phrases: Essential dimension, algebraic groups, Galois cohomology, cohomological invariants, group scheme actions, torsors.

Acknowledgements

The authors would warmly thank P. Chabloz, R. Garibaldi, M. Ojanguren and J.-P. Serre for helpful comments and A. Merkurjev for providing us his private notes. The first named author also gratefully acknowledges support from the Swiss National Science Fundation, grant No 2100-065128.01/1.

Contents

Summary of the paper

In Section 1, we introduce the notion of essential dimension of a covariant functor from the category of field extensions over a base field k to the category of sets. This notion is due to A. Merkurjev and can be found in [12]. We then study the behaviour of this notion under products, coproducts and field extensions. Along the way, we define the notion of fibration of functors.

In Section 2, we introduce the essential dimension of an algebraic group G defined over an *arbitrary* field k. We then give some examples of computation of this essential dimension, including the case of the circle group.

In Section 3, we give an upper bound for the essential dimension of an algebraic group which acts linearly and generically freely on a finite-dimensional vector space. As an application, we show that the essential dimension of any algebraic group is finite. Compare this material with [14] where the essential dimension of G is defined taking the point of view of G-actions. Very sketchy proofs of these results can be found in [12]. For the convenience of the reader, we present complete proofs of them using the ideas of [12], filling in technical details. We then apply the previous results to estimate the essential dimension of finite abelian groups and dihedral groups when the base field is sufficiently large.

In Section 4, we introduce Merkurjev's notions of n-simple functors and non-constant morphisms (see [12]). We apply it to give lower bounds of essential dimension of some algebraic groups (e.g. symmetric groups) using non-trivial cohomological invariants always following [12].

In Section 5, inspired by Rost's definition of essential dimension for some sub-functors of Milnor's K-theory (see [16]), we define the notion of versal pair for functors from the category of commutative and unital k-algebras to the category of sets. We then define the (Rost's) essential dimension for functors having a versal pair, and compare it to Merkurjev's essential dimension.

In Section 6, we introduce the notion of generic torsor, following [9]. We then prove that the essential dimension of an algebraic group G is the essential dimension of a generic torsor. We also compare the essential dimension of an algebraic group G with that of any closed subgroup. Along the way the notion of compression of torsors is introduced following [14]. The present approach has the advantage that no hypothesis on the ground field is needed. Again, ideas of proofs of these results can be found in [12]. We use them, filling the details and reformulating them in terms of versal pairs.

In Section 7, we focus on essential dimension of finite constant group schemes. First of all, we prove that the essential dimension of such a group G is the minimum of the $\mathrm{trdeg}(E : k)$ for all the fields $E \subseteq k(V)$ on which G acts faithfully (see [3]). We then apply these results to compute essential dimension of cyclic and dihedral groups over the field of real numbers, and essential dimension of cyclic groups of order at most 5 over any base field.

Finally, in Section 8, we give the proof of the homotopy invariance for essential dimension of algebraic groups defined over an infinite field.

1. Introduction

Let k be a field. We denote by $\mathfrak{C}_k$ the category of field extensions of k, i.e. the category whose objects are field extensions K over k and whose morphisms are field homomorphisms which fix k. We write $\mathfrak{F}_k$ for the category of all *covariant* functors from $\mathfrak{C}_k$ to the category of sets. For such a functor $\mathbf{F}$ and for a field extension K/k we will write $\mathbf{F}(K)$ instead of $\mathbf{F}(K/k)$. If $K \to L$ is a morphism in $\mathfrak{C}_k$, for every element $a \in \mathbf{F}(K)$ we will denote by a_L the image of a under the map $\mathbf{F}(K) \longrightarrow \mathbf{F}(L)$. We shall say that a morphism $\mathbf{F} \longrightarrow \mathbf{G}$ between functors in $\mathfrak{F}_k$ is a SURJECTION if, for any field extension K/k, the corresponding map $\mathbf{F}(K) \longrightarrow \mathbf{G}(K)$ is a surjection of sets. If $\mathbf{F} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ is an object of $\mathfrak{F}_k$ and if K/k is a field extension we will sometimes denote by $\mathbf{F}_K$ the functor $\mathbf{F}$ viewed as a functor over the category $\mathfrak{C}_K$. By a scheme over k, we mean a k-scheme of finite type.

Examples 1.1.

(1) The forgetful functor, denoted by $\mathbf{O}$, which assigns to each field extension K/k the underlying set of K and to each morphism its underlying map of sets, is an object of $\mathfrak{F}_k$.

(2) The stupid functor, denoted by $*$, sending a field K to a one-point set is an object of $\mathfrak{F}_k$.

(3) Let X be a scheme over k. It defines a "point functor", still denoted by X, in this way :

$$K \mapsto X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X).$$

The set $X(K)$ is simply the set of all K-rational points of X.

(4) For any integer $n \geq 1$, we put $\mathbf{Q}_n(K)$ for the set of isomorphism classes of non-degenerate quadratic forms of dimension n over K. It is clear that $\mathbf{Q}_n$ defines an object of $\widetilde{\mathfrak{F}}_k$.

(5) A K-algebra is called primitive if it is isomorphic to a quotient of $K[X]$. Every such algebra is thus of the form $K[X]/{<}f{>}$ for a single polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. We denote by $\mathbf{Alg}_n(K)$ the set of isomorphism classes of n-dimensional primitive algebras. This also defines a functor $\mathbf{Alg}_n$ from $\mathfrak{C}_k$ to the category of sets.

(6) Let K be a field. We recall that an étale algebra over K is a finite dimensional commutative K-algebra A which satisfies the equality $\sharp\ \mathrm{Hom}_K(A, \overline{K}) = \dim_K A$, where $\overline{K}$ denotes an algebraic closure of K. This is equivalent to saying that $A \otimes_K \overline{K}$ is reduced or that A is a product of separable extensions of K. Moreover if K is infinite, A is étale over K if and only if $A \simeq K[X]/< f >$ where f has no multiple roots in $\overline{K}$. If A is étale over K and $K \to L$ is a field homomorphism then $A \otimes_K L$ is étale over L.
For any field extension K/k and any integer $n \geq 1$, let $\mathbf{\acute{E}t}_n(K)$ denote the set of isomorphism classes of n-dimensional étale algebras over K. It also defines an object of the category $\widetilde{\mathfrak{F}}_k$. When the base field k is infinite $\mathbf{\acute{E}t}_n$ is a subfunctor of $\mathbf{Alg}_n$ and these functors are closely related for the essential dimension.

(7) Let G be a finite abstract group of order n and let K be a field. By a Galois G-algebra over K (or Galois K-algebra with group G) we mean an étale K-algebra L of dimension n such that G acts on L as a group of K-automorphisms and such that $L^G = K$. We denote by G-$\mathbf{Alg}(K)$ the set of G-isomorphism classes of Galois G-algebras over K. The assignment $K \mapsto G$-$\mathbf{Alg}(K)$ from $\mathfrak{C}_k$ to the category of sets defines an object of $\widetilde{\mathfrak{F}}_k$.

(8) For every integer $d, n \geq 2$, define $\mathbf{F}_{d,n}(K)$ to be the set of all (non-trivial) homogenous forms over K of degree d in n variables modulo the $\mathbf{GL}_n(K)$-action and modulo the relation $f \sim \lambda f$ for $\lambda \in K^\times$. Once again $\mathbf{F}_{d,n}$ is an object of $\widetilde{\mathfrak{F}}_k$.

(9) Let S be a pointed set with at least two elements and $d \geq 1$ an integer. We shall define the functor $\mathbf{F}_S^d$ in the following way :

$$\mathbf{F}_S^d(K) = \begin{cases} S & \text{if } \operatorname{trdeg}(K:k) \geq d \\ \\ * & \text{otherwise} \end{cases}$$

and, for an extension K'/K, the obvious constant map of pointed sets $\mathbf{F}_S^d(K) \longrightarrow \mathbf{F}_S^d(K')$.

(10) Let L/k be an arbitrary field extension. Then, the (covariant) representable functor h_L given by $h_L(K) = \operatorname{Hom}(L, K)$ defines also an object of $\mathfrak{F}_k$.

One natural question is to ask how many parameters are needed to describe a given structure. For example, any n-dimensional quadratic form in characteristic not 2, is determined by n parameters since it can be reduced to a diagonal form.
A quadratic algebra will certainly be described by one parameter since it can always be written as $k[X]/< X^2 + a >$ when $\frac{1}{2}$ exists. The natural notion of functor shall replace the word "structure" and the following crucial definition, which is due to A. Merkurjev, shall make precise the concept of "how many parameters" are needed to describe it.

Definition 1.2. *Let* $\mathbf{F}$ *be an object of* $\mathfrak{F}_k$, K/k *a field extension and* $a \in \mathbf{F}(K)$. *For* $n \in \mathbb{N}$, *we say that the* ESSENTIAL DIMENSION OF a IS $\leq n$ *(and we write* $\operatorname{ed}(a) \leq n$*), if there exists a subextension* E/k *of* K/k *such that:*

i) $\operatorname{trdeg}(E:k) \leq n$,

ii) the element a *is in the image of the map* $\mathbf{F}(E) \longrightarrow \mathbf{F}(K)$.

We say that $\operatorname{ed}(a) = n$ *if* $\operatorname{ed}(a) \leq n$ *and* $\operatorname{ed}(a) \not\leq n-1$. *The* ESSENTIAL DIMENSION OF $\mathbf{F}$ *is the supremum of* $\operatorname{ed}(a)$ *for all* $a \in \mathbf{F}(K)$ *and for all* K/k. *The essential dimension of* $\mathbf{F}$ *will be denoted by* $\operatorname{ed}_k(\mathbf{F})$.

Examples 1.3.

(1) It is clear from the very definition that $\operatorname{ed}(*) = 0$ and $\operatorname{ed}(\mathbf{O}) = 1$. More generally, we may say that a functor $\mathbf{F}$ is FLASQUE if, for any field extension K'/K, the map $\mathbf{F}(K) \longrightarrow \mathbf{F}(K')$ is surjective. Clearly every flasque functor $\mathbf{F}$ satisfies $\operatorname{ed}(\mathbf{F}) = 0$ and every constant functor is flasque.

(2) We shall do some very easy computations on polynomials of degree 2,3 and 4 in order to compute the essential dimension of $\mathbf{Alg}_2, \mathbf{Alg}_3$ and $\mathbf{Alg}_4$. We start with simple considerations on the functor $\mathbf{Alg}_n$ for arbitrary n. Let $A = K[X]/ < f >$ and $B = K[Y]/ < g >$ two n-dimensional primitive algebras. We denote by x and y the classes of X and Y respectively. A homomorphism $\varphi : A \longrightarrow B$ is determined by the image of x, say

$$\varphi(x) = c_{n-1}y^{n-1} + c_{n-2}y^{n-2} + \cdots + c_1 y + c_0,$$

satisfying $f(\varphi(x)) = 0$. Saying that φ is an isomorphism is nothing but saying that $\varphi(x)$ generates B. In this case we say that $\varphi(x)$ is a nondegenerate Tschirnhaus transformation of f. Clearly a polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ is defined over $k(a_0, \dots, a_{n-1})$ and thus computing the essential dimension of (the isomorphism class of) $K[X]/ < f >$ is the same as reducing the number of coefficients appearing in f by means of nondegenerate Tschirnhaus transformations. (This is the starting point of the paper [3]). It clearly suffices to do this on the "generic element" $X^n + t_{n-1}X^{n-1} + \cdots + t_1 X + t_0$ (where the t_i's are algebraically independent over k) since every other polynomial is a specialization of this one.

Now, when the characteristic of the ground field k does not divide n, the substitution $Y = X - \frac{t_{n-1}}{n}$ drops the coefficient t_{n-1} and hence

$$\mathrm{ed}(\mathbf{Alg}_n) \leq n - 1.$$

For the polynomial $X^2 + aX + b$ this says that one can reduce it to the form $X^2 + c$. Now the algebra $k(t)[X]/ < X^2 + t >$ is clearly not defined over an algebraic extension of k and hence

$$\mathrm{ed}(\mathbf{Alg}_2) = 1.$$

Now $X^3 + aX^2 + bX + c$ can be reduced to $X^3 + b'X + c'$ and, setting $Y = \frac{c'}{b'}X$, one makes the second and the third coefficient equal. Thus one can reduce it to the form $X^3 + dX + d$. As before the algebra $k(t)[X]/ < X^3 + tX + t >$ is not defined over an algebraic extension of k and so

$$\mathrm{ed}(\mathbf{Alg}_3) = 1.$$

Similarly the generic polynomial of degree 4 can be reduced to the form $X^4 + sX^2 + tX + t$ and hence $\mathrm{ed}(\mathbf{Alg}_4) \leq 2$. We will see that it cannot be reduced, thus $\mathrm{ed}(\mathbf{Alg}_4) = 2$.

Remark 1.4. The notion of essential dimension depends on the ground field k. However, when the field k is fixed, there is no confusion by writing $\mathrm{ed}(\mathbf{F})$. When the context is not clear, or when we want to insist on some hypotheses made on the field, we shall write $\mathrm{ed}_k(\mathbf{F})$. In general, if k'/k is a field extension, every object $\mathbf{F}$ of $\mathfrak{F}_k$, can be viewed (by restriction) as an object of $\mathfrak{F}_{k'}$. The following proposition shows the behaviour of essential dimension under field extension.

Proposition 1.5. *Let k'/k a field extension and* $\mathbf{F}$ *an object of* $\mathfrak{F}_k$. *Then*

$$\mathrm{ed}_{k'}(\mathbf{F}) \leq \mathrm{ed}_k(\mathbf{F}).$$

Proof. If $\mathrm{ed}_k(\mathbf{F}) = \infty$, the result is obvious. Let $\mathrm{ed}_k(\mathbf{F}) = n$. Take K/k' a field extension and $a \in \mathbf{F}(K)$. There is a subextension $k \subseteq E \subseteq K$ with $\mathrm{trdeg}(E : k) \leq n$ such that a is in the image of the map $\mathbf{F}(E) \longrightarrow \mathbf{F}(K)$. The composite extension $E' = Ek'$ then satisfies $\mathrm{trdeg}(E' : k') \leq n$ and clearly a is in the image of the map $\mathbf{F}(E') \longrightarrow \mathbf{F}(K)$. Thus $\mathrm{ed}(a) \leq n$ and $\mathrm{ed}_{k'}(\mathbf{F}) \leq n$.

Remarks 1.6.

(1) The above proposition says that, for a fixed functor $\mathbf{F} \in \mathfrak{F}_k$, the map

$$\mathrm{ed}_{\_}(\mathbf{F}) : \mathfrak{C}_k \longrightarrow \mathbb{N} \cup \{\infty\}$$

is a contravariant functor where $\mathbb{N} \cup \{\infty\}$ is considered as a category by saying that there is a morphism $n \to m$ exactly when $n \leq m$. This implies that, if $\mathbf{F}$ is a functor defined over the category of *all* fields, to give an upper bound of $\mathrm{ed}_k(\mathbf{F})$ it is sufficient to give an upper bound over each prime field $\mathbb{F}_p$ when $\mathrm{char}(k) > 0$, and to give an upper bound over $\mathbb{Q}$ when $\mathrm{char}(k) = 0$.

(2) In general one does not have $\mathrm{ed}_k(\mathbf{F}) = \mathrm{ed}_{k'}(\mathbf{F})$ for any field extension k'/k. Example (9) above shows that the essential dimension can decrease considerably: one sees immediately that $\mathrm{ed}_{k'}(\mathbf{F}^d_S) = 0$ if $\mathrm{trdeg}(k' : k) \geq d$. This is due to the fact that the functor becomes constant over k' and hence its essential dimension is zero. On the other hand it is clear that $\mathrm{ed}_k(\mathbf{F}^d_S) = d$.

(3) Let L/k be an extension and H_L the corresponding representable functor of Example (10). Then one has $\mathrm{ed}_{k'}(\mathrm{H}_L) = \mathrm{trdeg}(L : k')$ if $k \subseteq k' \subseteq L$ and $\mathrm{ed}_{k'}(\mathrm{H}_L) = 0$ otherwise.

We shall see later on (Corollary 2.7 in Chapter II) an example of a functor for which the inequality of Proposition 1.5 is strict even if the extension k'/k is algebraic.

The behaviour of essential dimension with respect to subfunctors is not very clear. For example take for $\mathbf{G}$ the constant functor $\mathbf{G}(K) = S$ where S is a set with at least two elements. Then $\mathbf{F}^d_S$ is a subfunctor of $\mathbf{G}$ and the dimension of the former is d (which is arbitrarily large) whereas the dimension of $\mathbf{G}$ is zero. However there is a large class of subfunctors for which the essential dimension has a nice behaviour.

Definition 1.7. *Let* $\mathbf{G}$ *be an object of* $\mathfrak{F}_k$. *A subfunctor* $\mathbf{F} \subseteq \mathbf{G}$ *is called* SATURATED *if for any field extension* L/K *over* k *and any element* $a \in \mathbf{G}(K)$ *such that* $a_L \in \mathbf{F}(L)$ *there is an algebraic subextension* K'/K *such that* $a_{K'} \in \mathbf{F}(K')$.

Proposition 1.8. *Let* $\mathbf{F} \subseteq \mathbf{G}$ *be a saturated subfunctor. Then*

$$\mathrm{ed}(\mathbf{F}) \leq \mathrm{ed}(\mathbf{G}).$$

Proof. Let K/k be a field extension and $a \in \mathbf{F}(K)$. Assume that $\mathrm{ed}(\mathbf{G}) = n$. Then there is a subextension L/k and an element $b \in \mathbf{G}(L)$ such that $\mathrm{trdeg}\,(L : k) \leq n$ and $a = b_K$. Since $\mathbf{F}$ is saturated, there is an algebraic subextension E/L in K/L such that $b_E \in \mathbf{F}(E)$. Thus $a \in \mathrm{im}(\mathbf{F}(E) \longrightarrow \mathbf{F}(K))$ and since $\mathrm{trdeg}(E : k) \leq n$ this shows that $\mathrm{ed}(\mathbf{F}) \leq n$.

We continue our investigation with some very simple lemmas concerning the functorial properties of $\mathrm{ed} : \mathfrak{F}_k \longrightarrow \mathbb{N} \cup \{\infty\}$.

Lemma 1.9. *Let* $f : \mathbf{F} \twoheadrightarrow \mathbf{G}$ *be a surjection in* $\mathfrak{F}_k$. *Then*

$$\mathrm{ed}(\mathbf{G}) \leq \mathrm{ed}(\mathbf{F}).$$

Proof. Let K/k be an extension and $b \in \mathbf{G}(K)$. By assumption, there is an element $a \in \mathbf{F}(K)$ such that $f_K(a) = b$. Suppose that $\mathrm{ed}(\mathbf{F}) = n$. Take a subextension $k \subseteq E \subseteq K$ such that $\mathrm{trdeg}(E : k) \leq n$ and such that $a \in \mathrm{im}\big(\mathbf{F}(E) \longrightarrow \mathbf{F}(K)\big)$. The lemma now follows from the commutativity of the diagram

$$\begin{tikzcd}
\mathbf{F}(K) \arrow[r, two heads, "f_K"] & \mathbf{G}(K) \\
\mathbf{F}(E) \arrow[u] \arrow[r, two heads, "f_E"] & \mathbf{G}(E) \arrow[u]
\end{tikzcd}$$

Thus essential dimension is functorial (in a contravariant way) over the category of functors in $\mathfrak{F}_k$ with *surjections* as morphisms. Nevertheless we will not restrict ourselves to that category, since this would not be very natural. For instance, we will always consider products and coproducts in the category of functors with *all* morphisms. The next lemma shows that the essential dimension preserves coproducts.

Lemma 1.10. *Let* $\mathbf{F}$ *and* $\mathbf{G}$ *be two objects of* $\widetilde{\mathfrak{F}}_k$. *Then*

$$\mathrm{ed}(\mathbf{F}\coprod\mathbf{G}) = \max\{\mathrm{ed}(\mathbf{F}),\mathrm{ed}(\mathbf{G})\}.$$

Proof. Let K/k be an extension and $a \in \mathbf{F}(K)\coprod\mathbf{G}(K)$. Clearly $\mathrm{ed}(a) \leq \mathrm{ed}(\mathbf{F})$ or $\mathrm{ed}(a) \leq \mathrm{ed}(\mathbf{G})$ and hence $\mathrm{ed}(\mathbf{F}\coprod\mathbf{G}) \leq \max\{\mathrm{ed}(\mathbf{F}),\mathrm{ed}(\mathbf{G})\}$. The opposite inequality is clear since $\mathbf{F}$ and $\mathbf{G}$ are both saturated subfunctors of $\mathbf{F}\coprod\mathbf{G}$.

Lemma 1.11. *Let* $\mathbf{F}$ *and* $\mathbf{G}$ *be two objects of* $\widetilde{\mathfrak{F}}_k$. *Then*

$$\mathrm{ed}(\mathbf{F}\times\mathbf{G}) \leq \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{G}).$$

Proof. Take K/k a field extension and $(a,a') \in \mathbf{F}(K)\times\mathbf{G}(K)$. Take two extensions $k \subseteq E, E' \subseteq K$ with $\mathrm{trdeg}(E:k) \leq \mathrm{ed}(\mathbf{F}), \mathrm{trdeg}(E':k) \leq \mathrm{ed}(\mathbf{G})$ and such that a (respectively a') belongs to the image of $\mathbf{F}(E) \longrightarrow \mathbf{F}(K)$ (respectively $\mathbf{G}(E') \longrightarrow \mathbf{G}(K)$). So there exist $b \in \mathbf{F}(E)$ and $b' \in \mathbf{G}(E')$ such that $b_K = a$ and $b'_K = a'$. If we consider $L = EE'$ and denote by c (respectively c') the image of b in $\mathbf{F}(L)$ (respectively the image of b' in $\mathbf{G}(L)$) it is easily seen that (c,c') maps to (a,a'). Hence

$$\mathrm{ed}(a,a') \leq \mathrm{trdeg}(L:k) \leq \mathrm{trdeg}(E:k) + \mathrm{trdeg}(E':k) \leq \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{G}).$$

Thus $\mathrm{ed}(\mathbf{F}\times\mathbf{G}) \leq \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{G})$.

A slight generalization of the previous inequality can be performed for functors which are in some kind of "fibration position".

First recall that an action of a *set* Y over a set X is nothing but a map $Y \times X \to X$. If $y \in Y$ and $x \in X$ we shall write $y \cdot x$ for the image of (y,x) under this map. We say that a functor $\mathbf{F} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ acts over a functor $\mathbf{G} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ if, for every extension K/k, the set $\mathbf{F}(K)$ acts over $\mathbf{G}(K)$ and if the obvious compatibility condition holds: for each morphism $K \to L$ and for all elements $y \in \mathbf{F}(K)$ and $x \in \mathbf{G}(K)$, one has $(y\cdot x)_L = y_L \cdot x_L$. We shall say that the action of the functor $\mathbf{F}$ over the functor $\mathbf{G}$ is transitive if for every K/k the action of the set $\mathbf{F}(K)$ is transitive over $\mathbf{G}(K)$ (that is there is only one orbit). Recall also that, if $\pi : \mathbf{G} \longrightarrow \mathbf{H}$ is a morphism of functors in $\widetilde{\mathfrak{F}}_k$ and K/k is an extension, each element $a \in \mathbf{H}(K)$ gives rise to a functor $\pi^{-1}(a)$, defined over the category $\mathfrak{C}_K$, by setting $\pi_L^{-1}(a) = \{x \in \mathbf{G}(L) \mid \pi_L(x) = a_L\}$ for every extension L/K.

Definition 1.12. *Let* $\pi : \mathbf{G} \twoheadrightarrow \mathbf{H}$ *be a surjection in* $\widetilde{\mathfrak{F}}_k$. *We say that a functor* $\mathbf{F}$ *is in* fibration position *for* π *if* $\mathbf{F}$ *acts transitively on each fiber of* π. *More precisely, for every extension* K/k *and every* $a \in \mathbf{H}(K)$, *we require that the functor* $\mathbf{F}$ *(viewed over the category* $\mathfrak{C}_K$*) acts transitively on* $\pi^{-1}(a)$. *When* $\mathbf{F}$ *is in fibration position for* π *we simply write* $\mathbf{F} \rightsquigarrow \mathbf{G} \xrightarrow{\pi} \mathbf{H}$ *and call this a* fibration of functors.

In the following proposition we insist on the fact that all the functors involved *do not necessarly* take values in the category of groups.

Proposition 1.13. *Let* $\mathbf{F} \rightsquigarrow \mathbf{G} \xrightarrow{\pi} \mathbf{H}$ *be a fibration of functors. Then*

$$\mathrm{ed}(\mathbf{G}) \leq \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{H}).$$

Proof. Let K/k a field extension and $a \in \mathbf{G}(K)$. By definition there is a field extension E with $k \subseteq E \subseteq K$, satisfying $\mathrm{trdeg}(E:k) \leq \mathrm{ed}(\mathbf{H})$, and an element $b' \in \mathbf{H}(E)$ such that $b'_K = \pi_K(a)$. Since π_E is surjective there exists $a' \in \mathbf{G}(E)$ such that $\pi_E(a') = b'$. Now clearly $\pi_K(a'_K) = \pi_K(a)$ and thus a'_K and a are in the same fiber. By assumption there exists an element $c \in \mathbf{F}(K)$ such that $a'_K \cdot c = a$. Now there exists an extension E' with $k \subseteq E' \subseteq K$ and $\mathrm{trdeg}(E':k) \leq \mathrm{ed}(\mathbf{F})$ such that c is in the image of the map $\mathbf{F}(E') \longrightarrow \mathbf{F}(K)$. We take $c' \in \mathbf{F}(E')$ such that $c'_K = c$. Considering now the composite extension $E'' = EE'$ and setting $d = a'_{E''} \cdot c'_{E''} \in \mathbf{G}(E'')$ we have, since the action is functorial,

$$d_K = (a'_{E''} \cdot c'_{E''})_K = a'_K \cdot c'_K = a'_K \cdot c = a,$$

and thus

$$\mathrm{ed}(a) \leq \mathrm{trdeg}(E'':k) \leq \mathrm{trdeg}(E:k) + \mathrm{trdeg}(E':k) \leq \mathrm{ed}(\mathbf{H}) + \mathrm{ed}(\mathbf{F}).$$

Since this is true for an arbitrary element a the desired inequality follows.

Remark 1.14. The inequality $\mathrm{ed}(\mathbf{F} \times \mathbf{G}) \leq \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{G})$ is a consequence of this proposition. Indeed for $a \in \mathbf{G}(K)$ the fiber of the projection is $\mathbf{F}(K) \times \{a\}$ and the *set* $\mathbf{F}(K)$ acts transitively by simply setting $x \cdot (y, a) = (x, a)$.

Corollary 1.15. *Let* $1 \longrightarrow \mathbf{F} \longrightarrow \mathbf{G} \longrightarrow \mathbf{H} \longrightarrow 1$ *be a short exact sequence of group-valued functors. Then*

$$\mathrm{ed}(\mathbf{G}) \leq \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{H}).$$

Proof. This is clear since $\mathbf{H}(K) \cong \mathbf{G}(K)/\mathbf{F}(K)$ and the set $\mathbf{F}(K)$ acts transitively on equivalence classes by group multiplication.

Remarks 1.16.

a) One can have $\mathrm{ed}(\mathbf{G}) < \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{H})$ as is shown by the following example: For every field extension K let $\mathbf{F}(K) = K^{\times 2}$ be the subgroup of $\mathbf{G}(K) = K^{\times}$ consisting of all the squares and $\mathbf{H}(K) = K^{\times}/K^{\times 2}$ the corresponding quotient (as groups). It is not difficult to see that $\mathrm{ed}(\mathbf{F}) = \mathrm{ed}(\mathbf{G}) = \mathrm{ed}(\mathbf{H}) = 1$, and thus $1 = \mathrm{ed}(\mathbf{G}) < \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{H}) = 2$ (but note that $\mathbf{G} \ncong \mathbf{F} \times \mathbf{H}$ as functors).

b) For a product of functors, since $\mathbf{F} \times \mathbf{G}$ maps onto both $\mathbf{F}$ and $\mathbf{G}$, we have

$$\max\{\mathrm{ed}(\mathbf{F}), \mathrm{ed}(\mathbf{G})\} \leq \mathrm{ed}(\mathbf{F} \times \mathbf{G}) \leq \mathrm{ed}(\mathbf{F}) + \mathrm{ed}(\mathbf{G}).$$

However, even the behaviour of products with respect to essential dimension is not clear. Consider for instance the following two examples :

• Consider the functor $\mathbf{F}_S^d$ of example (9) above. Clearly $\mathbf{F}_S^d \times \mathbf{F}_S^d = \mathbf{F}_{S\times S}^d$ and hence

$$\mathrm{ed}(\mathbf{F}_S^d \times \mathbf{F}_S^d) = \mathrm{ed}(\mathbf{F}_{S\times S}^d) = d = \mathrm{ed}(\mathbf{F}_S^d).$$

Thus it is possible to have $\mathrm{ed}(\mathbf{F} \times \cdots \times \mathbf{F}) = \mathrm{ed}(\mathbf{F})$.

• In contrast with the previous example consider $\mathbf{O}$ the forgetful functor. Then

$$\mathrm{ed}(\underbrace{\mathbf{O} \times \cdots \times \mathbf{O}}_{n \text{ times}}) = n$$

and hence $\mathrm{ed}\big(\prod_{n\in\mathbb{N}} \mathbf{O}\big) = \infty$.

The geometric class of functors introduced in example (3) has an easy essential-dimensional behaviour. This is treated in the following

Proposition 1.17. *Let X be a scheme over k. Then*

$$\mathrm{ed}(X) = \dim(X).$$

Proof. Let K/k and $a \in X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$. If x denotes the corresponding point, we have an inclusion $k(x) \hookrightarrow K$, where $k(x)$ is the residue field at x. But

$$\dim(X) = \sup_{x\in X} \mathrm{trdeg}\,\big(k(x) : k\big),$$

hence $\dim(X) = \mathrm{ed}(X)$.

Definition 1.18. *Let $\mathbf{F}$ be an object of $\mathfrak{F}_k$. A* classifying scheme of $\mathbf{F}$ *is a k-scheme X such that there is a surjection $X \twoheadrightarrow \mathbf{F}$.*

Corollary 1.19. *If X is a classifying scheme of $\mathbf{F}$ then*

$$\mathrm{ed}(\mathbf{F}) \leq \dim(X).$$

Proof. This is clear from the definition and the previous considerations.

Examples 1.20.

• Consider $\mathbb{G}_m$ the multiplicative group scheme over k. If $\mathrm{char}(k) \neq 2$, then every quadratic form is diagonalizable, thus there is a surjective morphism of functors $\mathbb{G}_m^n \twoheadrightarrow \mathbf{Q}_n$ given by

$$\begin{aligned} \mathbb{G}_m^n(K) &\twoheadrightarrow \mathbf{Q}_n(K) \\ (a_1, \ldots, a_n) &\longmapsto \langle a_1, \ldots, a_n \rangle. \end{aligned}$$

Hence $\mathbb{G}_m^n$ is a classifying scheme of $\mathbf{Q}_n$. This shows that $\mathrm{ed}_k(\mathbf{Q}_n) \leq n$ if $\mathrm{char}(k) \neq 2$.

• For example (6) above, when k is infinite, there is also a classifying scheme X. Take $A = k[t_1, \ldots, t_n, \frac{1}{d(f)}]$ where $f = x^n + t_1 x^{n-1} + \cdots + t_n$ and $d(f)$ is the discriminant of f. It now suffices to take $X = \mathrm{Spec}(A)$. Hence $\mathrm{ed}_k(\mathbf{\acute{E}t}_n) \leq n$.

• In example (8) we easily see that every homogenous form of degree d with n variables can be written with at most $m = \binom{d+n-1}{n-1}$ coefficients. So one has a very rough classifying scheme $\mathbb{P}^{m-1}$ and thus

$$\mathrm{ed}(\mathbf{F}_{d,n}) \leq m - 1.$$

Moreover there is a fibration of functors

$$X_n \rightsquigarrow \mathbb{P}^{m-1} \twoheadrightarrow \mathbf{F}_{d,n}$$

where X_n is $\mathbf{PGL}_n$ viewed as a scheme over k. Thus, by Proposition 1.13, we have $\mathrm{ed}(\mathbb{P}^{m-1}) \leq \mathrm{ed}(X_n) + \mathrm{ed}(\mathbf{F}_{d,n})$. Since $\mathrm{ed}(\mathbb{P}^{m-1}) = m - 1$ and $\mathrm{ed}(X_n) = n^2 - 1$ it follows that

$$\mathrm{ed}(\mathbf{F}_{d,n}) \geq m - n^2.$$

In the case $n = 2$ one can easily show that $\mathrm{ed}(\mathbf{F}_{d,2}) \leq d - 2$ and the above inequality tells us that $\mathrm{ed}(\mathbf{F}_{d,2}) \geq d - 3$. Hence

$$d - 3 \leq \mathrm{ed}(\mathbf{F}_{d,2}) \leq d - 2.$$

For a discussion of the essential dimension of cubics in few variables, see a forthcoming paper of the authors.

• In example (8) one could have preferred considering homogenous forms only up to $\mathbf{GL}_n$ and not up to a scalar. Denote by $\mathbf{G}_{d,n}$ this new functor. There is a simple relationship between $\mathrm{ed}(\mathbf{F}_{d,n})$ and $\mathrm{ed}(\mathbf{G}_{d,n})$. Indeed there is an obvious surjection of functors

$$\mathbf{G}_{d,n} \twoheadrightarrow \mathbf{F}_{d,n}$$

sending a class modulo $\mathbf{GL}_n$ to its class in $\mathbf{F}_{d,n}$. But the fiber of a form $[f] \in \mathbf{F}_{d,n}(K)$ is clearly the subset $\{[\lambda f] \in \mathbf{G}_{d,n}(K) \,|\, \lambda \in K^\times\}$ and thus $K^\times$ acts transitively on each fiber. We hence obtain a fibration of functors

$$X \rightsquigarrow \mathbf{G}_{d,n} \twoheadrightarrow \mathbf{F}_{d,n}$$

where X is the scheme $\mathbb{A}^1 \setminus \{0\}$ viewed as a functor. This gives the inequality

$$\mathrm{ed}(\mathbf{G}_{d,n}) \leq \mathrm{ed}(\mathbf{F}_{d,n}) + \mathrm{ed}(X) = \mathrm{ed}(\mathbf{F}_{d,n}) + 1.$$

Remark 1.21. In this section all the basic concepts are introduced by Merkurjev in [12] with complete proofs. We have completed these results with Lemma 1.10, Definition 1.12, Corollary 1.15 and some trivial results. The discussion on $\mathbf{F}_{d,n}$ is also new.

2. Galois cohomology

We introduce an important class of functors using Galois cohomology. These functors will be the center of our considerations. Their essential dimension was first introduced by Reichstein, over an algebraically closed field, in terms of compressions. See [14] for details. The standard reference for Galois cohomology is Serre's book [19].

Let G be a k-group scheme (always of finite type). Take K/k a field extension and K_s a separable closure. The group $\Gamma_K = \mathrm{Gal}(K_s/K)$ acts on $G(K_s)$ compatibly with the G-action. The Galois cohomology set $H^1(\Gamma_K, G(K_s)) =: H^1(K,G)$ is then well defined, i.e. does not depend on the choice of the separable closure. Moreover $H^1(\_, G)$ is a functor in the first variable and thus is an object of $\mathfrak{F}_k$ (see [19] page 83). This allows us to set the following definition.

Definition 2.1. *Let G be a k-group scheme. The* essential dimension of *G is defined as*

$$\mathrm{ed}_k(G) = \mathrm{ed}_k(H^1(\_, G)).$$

A big portion of this paper is dedicated to the study of the essential dimension of certain group schemes. A certain number of techniques are developed in order to estimate it. In the sequel all group schemes are assumed for simplicity to be affine. We will mostly restrict ourselves to algebraic groups over k, that is smooth affine group schemes over k whose Hopf algebra is finitely generated.

We briefly recall the following interpretation of Galois cohomology (see [19] pages 128-129) which shows that many functors $\mathbf{F} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ can be viewed as Galois cohomology functors.

Proposition 2.2. *Let (V_0, x_0) be an algebraic structure over k (in the sense of* [19]*). For any field extension K/k let $G(K) = \mathrm{Aut}_K(V_0 \otimes_k K)$ be the group of K-automorphisms which preserve the structure. Then the set $H^1(k,G)$ classifies the k-isomorphism classes of algebraic structures over k which become isomorphic to (V_0, x_0) over a separable closure.*

First examples. It is well known that $H^1(K, \mathbf{GL}_n) = 1$ for every field K. For $n = 1$ this is the so-called *Hilbert 90 Theorem.* Thus $\mathrm{ed}_k(\mathbf{GL}_n) = 0$ for every field k. Moreover the short exact sequence

$$1 \longrightarrow \mathbf{SL}_n \longrightarrow \mathbf{GL}_n \longrightarrow \mathbb{G}_m \longrightarrow 1$$

induces an exact sequence in cohomology showing that $H^1(K, \mathbf{SL}_n) = 1$ for every field K. Thus one also has $\mathrm{ed}_k(\mathbf{SL}_n) = 0$ for every field k. It is also known that $H^1(K, \mathbb{G}_a)$ is trivial for every field K. It follows that $\mathrm{ed}_k(\mathbb{G}_a) = 0$.

Example of $H^1(k, \mathcal{S}_n)$. We consider the symmetric group $G = \mathcal{S}_n$ as a constant group scheme over k.

Take $V_0 = k \times \cdots \times k = k^n$ with its product k-algebra structure. It is easily computed that $\mathcal{S}_n = \mathrm{Aut}_{K\text{-alg}}(V_0 \otimes_k K)$. Thus, by the preceding proposition, we have that $H^1(k, \mathcal{S}_n)$ is the set of isomorphism classes of k-algebras A such that there exists a separable extension L/k with $A \otimes_k L \cong L^n$. It is then easily checked that $H^1(\_, \mathcal{S}_n) \cong \mathbf{\acute{E}t}_n$ as functors and thus

$$\mathrm{ed}_k(\mathcal{S}_n) = \mathrm{ed}_k(\mathbf{\acute{E}t}_n).$$

Galois algebras. Let G any arbitrary finite constant group scheme over k. For any field extension K/k there is a bijection from G-$\mathbf{Alg}(K)$ to $H^1(K, G)$ given as follows: let L be a Galois G-algebra over K. The set E_L of K-algebra homomorphisms $L \to K_s$ is finite with $\dim_K L$ elements. One shows easily that E_L is a principal homogenous space under Γ_K and G. Sending $[L]$ to $[E_L]$ yields a well defined map from G-$\mathbf{Alg}(K)$ to $H^1(K, G)$ which one can show to be a bijection (see [11] for details). Thus G-$\mathbf{Alg} \cong H^1(\_, G)$.

Examples 2.3.

• The group μ_n.

Let k be a field and consider $\mu_n = \mathrm{Spec}\big(k[X]/ < X^n - 1 > \big)$ the k-group scheme of the n-th roots of the unity.

– Suppose that n is prime to the characteristic of k. Then it is well known that for any field extension L/k one has a functorial isomorphism $H^1(L, \mu_n) \cong L^\times / L^{\times n}$. It thus follows that $\mathrm{ed}_k(\mu_n) = 1$.

– If $n = \mathrm{char}(k)$, then μ_n has trivial cohomology and thus $\mathrm{ed}_k(\mu_n) = 0$.

• The group $\mathbb{Z}/p$.

Let k be a field, p a prime number and denote by $\mathbb{Z}/p$ the constant k-group scheme represented by $\mathrm{Spec}(k^{\mathbb{Z}/p})$.
– If $\mathrm{char}(k) \neq p$ and k contains all the p-th roots of unity we can identify the group scheme $\mathbb{Z}/p$ with μ_p by choosing a primitive root of unity. In this case one finds $\mathrm{ed}_k(\mathbb{Z}/p) = 1$. When the field does not contain all the p-th roots of unity, the computation of $\mathrm{ed}_k(\mathbb{Z}/p)$ is much harder as we shall see later.
– When $\mathrm{char}(k) = p$ the situation is easier. The long exact sequence in cohomology induced by the short exact sequence

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow \mathbb{G}_a \longrightarrow \mathbb{G}_a \longrightarrow 0$$

gives a functorial isomorphism $H^1(L, \mathbb{Z}/p) \cong L/\wp(L)$ where $\wp(x) = x^p - x$ for $x \in L$. It now clearly follows that $\mathrm{ed}_k(\mathbb{Z}/p) = 1$.

Remark 2.4. When $\mathrm{char}(k) = p$, the group $\mathbb{Z}/p^n$ fits into a short exact sequence of k-group schemes analogous to the previous one, but using Witt vectors:

$$0 \longrightarrow \mathbb{Z}/p^n \longrightarrow W_n \longrightarrow W_n \longrightarrow 0$$

where $W_n(k)$ is the additive group of Witt vectors of length n (see [20]). Applying again cohomology and using the fact that $H^1(k, W_n) = 0$, one finds that W_n is a classifying scheme for $\mathbb{Z}/p^n$ and hence

$$\mathrm{ed}_k(\mathbb{Z}/p^n) \leq n.$$

Another proof of the inequality $\mathrm{ed}_k(\mathbb{Z}/p^n) \leq n$ is performed by looking at the exact sequence

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow \mathbb{Z}/p^n \longrightarrow \mathbb{Z}/p^{n-1} \longrightarrow 0.$$

It induces a long exact sequence in Galois cohomology but, when the base field k is of characteristic p one has $H^2(K, \mathbb{Z}/p) = 0$ for every extension K/k (see [19] page 86), and thus it reduces to a short exact sequence of group-valued functors

$$0 \longrightarrow H^1({}_-, \mathbb{Z}/p) \longrightarrow H^1({}_-, \mathbb{Z}/p^n) \longrightarrow H^1({}_-, \mathbb{Z}/p^{n-1}) \longrightarrow 0.$$

Then, by Corollary 1.15, one has

$$\mathrm{ed}_k(\mathbb{Z}/p^n) \leq \mathrm{ed}_k(\mathbb{Z}/p^{n-1}) + \mathrm{ed}_k(\mathbb{Z}/p)$$

and, since $\mathrm{ed}_k(\mathbb{Z}/p) = 1$, we are done by induction.

• The circle.

We are interested in the group scheme $S^1 = \mathrm{Spec}\left(k[X,Y]/< X^2 + Y^2 - 1>\right)$ with its usual group structure. We first notice that when -1 is a square and $\mathrm{char}(k) \neq 2$, the rings $k[X,Y]/ < X^2 + Y^2 - 1 >$ and $k[t, t^{-1}]$ are isomorphic. In that case it follows that the algebraic groups S^1 and $\mathbb{G}_m$ are isomorphic and hence $\mathrm{ed}_k(S^1) = 0$. When -1 is not a square we will see that the essential dimension increases.

Actually we will solve the problem for a wider class of algebraic groups.

Let k be a field and L an étale algebra over k. One defines the group scheme $\mathbb{G}^1_{m,L}$ by the exact sequence

$$1 \longrightarrow \mathbb{G}^1_{m,L} \longrightarrow \mathrm{R}_{L/k}(\mathbb{G}_{m,L}) \xrightarrow{N_{L/k}} \mathbb{G}_m \longrightarrow 1,$$

where $\mathrm{R}_{L/k}$ denotes the Weil restriction (see [11] p.329 where it is called corestriction).

In the sequel, we will prove the following result:

Theorem 2.5. *Let L/k be an étale algebra of dimension $n \geq 1$. Then*

$$\mathrm{ed}_k(\mathbb{G}^1_{m,L}) = \begin{cases} 0 & \text{if } L \text{ is isomorphic to a product of field} \\ & \text{extensions of relatively prime degrees} \\ 1 & \text{otherwise.} \end{cases}$$

The above sequence induces, for any extension K/k, the exact sequence in cohomology

$$(L \otimes K)^\times \xrightarrow{N_K} K^\times \longrightarrow H^1(K, \mathbb{G}^1_{m,L}) \longrightarrow 1$$

where N_K is a short notation for $N_{L\otimes K/K}$. This gives an isomorphism

$$H^1(K, \mathbb{G}^1_{m,L}) \simeq K^\times / N_{L\otimes K/K}(L \otimes K)^\times.$$

In particular one has $\mathrm{ed}_k(\mathbb{G}^1_{m,L}) \leq 1$ for every field k.

Since the case $n = 1$ is trivial, we may assume until the end of this section that $n \geq 2$.

We start with the following lemma:

Lemma 2.6. *Let k be a field, let L be a finite dimensional étale k-algebra of dimension $n \geq 2$, and let t be a transcendental element over k. Then t belongs to the norm group of $L \otimes k(t)/k$ if and only if L is isomorphic to a product of some finite separable field extensions of k those degrees are relatively prime.*

Proof. Assume that there exists $\alpha \in L \otimes k(t)$ such that $N_{L\otimes k(t)/k(t)}(\alpha) = t$. In the sequel, we will write $L(t)$ instead of $L \otimes k(t)$ in order to simplify notation. Write $\alpha = \dfrac{1}{Q(t)} \cdot \sum_{i=0}^{m} \lambda_i t^i$, for some $\lambda_i \in L$, with $\lambda_m \neq 0$ and some nonzero polynomial $Q(t) \in k[t]$ of degree $d \geq 0$. Assume first that L is a field. Then $L(t)/k(t)$ is again a separable field extension, and we have

$$Q(t)^n t = N_{L(t)/k(t)}(Q(t) \cdot \alpha) = \prod_\sigma \left(\sum_{i=0}^{m} \sigma(\lambda_i) \otimes t^i \right),$$

where σ describes $\mathrm{Hom}_k(L, k_s)$. Since L is a field and $\lambda_m \neq 0$, the leading coefficient of the right hand side term is equal to $N_{L/k}(\lambda_m) t^{mn}$. Since $Q(t)^n t$ is a polynomial of degree $nd + 1$ and $n \geq 2$, we get a contradiction.
Hence $L \simeq L_1 \times \cdots \times L_r$ for $r \geq 2$, where L_i/k is a finite separable field extension of degree n_i. We then have

$$t = N_{L_1(t)/k(t)}(\alpha_1) \cdots N_{L_r(t)/k(t)}(\alpha_r)$$

for some $\alpha_i \in L_i(t)^\times$. As above write $\alpha_i = \dfrac{1}{Q_i(t)} \cdot \sum_{j=0}^{m_i} \lambda_j^{(i)} \otimes t^j$, where $\lambda_{m_i}^{(i)} \neq 0$.

Since L_i is a field, the computation above shows that the leading coefficient of $Q_1(t)^{n_1}\cdots Q_r(t)^{n_r}t$ is

$$N_{L_1/k}(\lambda^{(1)}_{m_1})t^{m_1n_1}\cdots N_{L_r/k}(\lambda^{(r)}_{m_r})t^{m_rn_r},$$

which has degree $m_1n_1+\cdots+m_rn_r$. By assumption, this degree is equal to $1+n_1d_1+\cdots+n_rd_r$. It follows immediately that the n_i's are relatively prime. The converse is clear.

We now prove Theorem 2.5. Assume first that $\mathrm{ed}(\mathbb{G}^1_{m,L})=0$. Then the class of t in $H^1(k(t),\mathbb{G}^1_{m,L})$ is defined over k. That is there exist an element $a\in k$ such that $t=aN_{k(t)}(\alpha)$ for some $\alpha\in L\otimes k(t)$. Then $u=\frac{t}{a}$ is a transcendental element over k which belongs to the norm group of $L\otimes k(u)$. Applying the previous lemma shows that L is isomorphic to a product of some finite separable field extensions of k those degrees are relatively prime. Conversely, if L is isomorphic to a product of some finite separable field extensions of k those degrees are relatively prime, then one can easily see that N_K is surjective for any field extension K/k, so $\mathrm{ed}(\mathbb{G}^1_{m,L})=0$.

Corollary 2.7. *Let k be a field. Then*

$$\mathrm{ed}_k(S^1)=\begin{cases}1 & \textit{if } \mathrm{char}(k)\neq 2 \textit{ and } -1\notin k^{\times 2}\\ \\ 0 & \textit{otherwise.}\end{cases}$$

Proof. If $\mathrm{char}(k)\neq 2$, apply the previous theorem with $L=k[X]/(X^2-1)$. If $\mathrm{char}(k)=2$, it is easy to see that for any field extension K/k, we have $S^1(K_s)=\{(x,x+1)\mid x\in K_s\}$. In particular $S^1(K_s)\simeq K_s$ as Galois modules and $H^1(\_,S^1)=0$, showing that $\mathrm{ed}_k(S^1)=0$.

Remark 2.8. In this section new results are Remark 2.4, Theorem 2.5 and Corollary 2.7.

3. Cohomological invariants

One way of giving lower bounds of essential dimension of functors is to use cohomological invariants. This idea can be found in [14]. The advantage of Merkurjev's functorial point of view is that the definitions are natural and that one could in theory apply these methods to a broader class of invariants.

Definition 3.1. *Let $\mathbf{F}$ be an object of $\mathfrak{F}_k$ and $n\geq 1$ an integer. We say that $\mathbf{F}$ is n-*simple *if there exists a field extension $\tilde{k}/k$ such that for any extension $K/\tilde{k}$ with $\mathrm{trdeg}(K:\tilde{k})<n$ the set $\mathbf{F}(K)$ consists of one element.*

Example 3.2. Let M be a discrete torsion Γ_k-module and $n \geq 1$ an integer. Then it is known that $H^n(K, M) = 0$ if K contains an algebraically closed field and is of transcendence degree $< n$ over this field (see [19], Proposition 11, page 93). Taking for $\tilde{k}$ an algebraic closure of k one sees that $H^n(\_, M)$ is n-simple.

Definition 3.3. *A morphism of functors $f : \mathbf{F} \to \mathbf{G}$ is called* non-constant *if for any field extension K/k there exists an extension L/K and elements $a \in \mathbf{F}(K)$, $a' \in \mathbf{F}(L)$ such that $f_L(a_L) \neq f_L(a')$.*

Proposition 3.4. *Let $f : \mathbf{F} \to \mathbf{G}$ be a non-constant morphism and suppose that $\mathbf{G}$ is n-simple. Then $\mathrm{ed}_k(\mathbf{F}) \geq n$.*

Proof. Let $\tilde{k}$ be the field in the definition of n-simplicity of $\mathbf{G}$. Suppose that $\mathrm{ed}_k(\mathbf{F}) < n$. Since $\mathrm{ed}_{\tilde{k}}(\mathbf{F}) \leq \mathrm{ed}_k(\mathbf{F})$ one has $\mathrm{ed}_{\tilde{k}}(\mathbf{F}) < n$ too. Since f is non-constant there exists an extension $L/\tilde{k}$ and elements $a \in \mathbf{F}(\tilde{k})$, $a' \in \mathbf{F}(L)$ such that $f_L(a_L) \neq f_L(a')$. Since $\mathrm{ed}_{\tilde{k}}(\mathbf{F}) < n$ there exists a subextension $\tilde{k} \subseteq E \subseteq L$ of transcendence degree $< n$ over $\tilde{k}$ such that $a' \in \mathrm{im}(\mathbf{F}(E) \longrightarrow \mathbf{F}(L))$ that is $a' = a''_L$ for some $a'' \in \mathbf{F}(E)$.
Since the diagram

$$\begin{tikzcd}
\mathbf{F}(L) \arrow[r, "f_L"] & \mathbf{G}(L) \\
\mathbf{F}(E) \arrow[u] \arrow[r, "f_E"] & \mathbf{G}(E) \arrow[u] \\
\mathbf{F}(\tilde{k}) \arrow[u] \arrow[r, "f_{\tilde{k}}"] & \mathbf{G}(\tilde{k}) \arrow[u]
\end{tikzcd}$$

is commutative, and since $f_L(a_L) \neq f_L(a')$ it follows that $f_E(a_E) \neq f_E(a'')$. This contradicts the fact that $\mathbf{G}(E)$ consists of one element.

Definition 3.5. *Let k be a field and $\mathbf{F}$ be a covariant functor from $\mathfrak{C}_k$ to the category of pointed sets. A* cohomological invariant of degree n of $\mathbf{F}$ *is a morphism of pointed functors $\varphi : \mathbf{F} \longrightarrow H^n(\_, M)$, where M is a discrete torsion Γ_k-module. (Here $H^n(\_, M)$ is pointed by 0, the class of the trivial cocycle.) We say that it is* non-trivial *if for any extension K/k there exists $L \supseteq K$ and $a \in \mathbf{F}(L)$ such that $\varphi_L(a) \neq 0$ in $H^n(L, M)$.*

Corollary 3.6. *Let k be an arbitrary field and $\mathbf{F}$ be a functor from $\mathfrak{C}_k$ to the category of pointed sets. If $\mathbf{F}$ has a non-trivial cohomological invariant φ of degree n, then $\mathrm{ed}_k(\mathbf{F}) \geq n$.*

Proof. Clearly any non-trivial cohomological invariant is a non-constant morphism.

We will apply the above corollary to a special class of algebraic groups: finite constant abelian groups. Recall that such a group G can always be written as $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$ where $d_1 \mid d_2 \mid \cdots \mid d_n$. The number n is called the rank of G and is denoted by $\operatorname{rank}(G)$.

Proposition 3.7. *Let G be a finite abelian group and k a field such that $\operatorname{char}(k) \nmid \exp(G)$. Then $\operatorname{ed}_k(G) \geq \operatorname{rank}(G)$.*

Proof. For the proof one can suppose that k is algebraically closed. We will define a cohomological invariant φ of degree n for $H^1(\_, G)$. There is an isomorphism

$$H^1(K, G) \cong H^1(K, \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n) \cong H^1(K, \mathbb{Z}/d_1) \times \cdots \times H^1(K, \mathbb{Z}/d_n),$$
$$c \longmapsto (c_1, \ldots, c_n)$$

which, composed with the cup product

$$H^1(K, \mathbb{Z}/d_1) \times \cdots \times H^1(K, \mathbb{Z}/d_n) \to H^n(K, \mathbb{Z}/d_1 \otimes \cdots \otimes \mathbb{Z}/d_n)$$
$$(c_1, \ldots, c_n) \longmapsto c_1 \cup \cdots \cup c_n$$

defines a cohomological invariant

$$\varphi : H^1(\_, G) \longrightarrow H^n(\_, \mathbb{Z}/d_1)$$

since $\mathbb{Z}/d_1 \otimes \cdots \otimes \mathbb{Z}/d_n \cong \mathbb{Z}/d_1$. It suffices to show that it is non-trivial. We have to show that, for a field extension K/k, there exists $L \supseteq K$ and $a \in H^1(L, G)$ such that $\varphi_L(a) \neq 0$. We take $L = K(t_1, \ldots, t_n)$ and set (t_i)= class of t_i in $L^\times / L^{\times d_i} \cong H^1(L, \mathbb{Z}/d_i)$ (this isomorphism holds since k is algebraically closed). Then, the image of

$$a = \big((t_1), \ldots, (t_n)\big) \in H^1(L, \mathbb{Z}/d_1) \times \cdots \times H^1(L, \mathbb{Z}/d_n) \cong H^1(L, G)$$

is the element $\varphi(a) = (t_1) \cup \cdots \cup (t_n) \in H^n(L, \mathbb{Z}/d_1)$. We show that this element is $\neq 0$ by induction on n :

– For $n = 1$, $(t_1) \in K(t_1)^\times / K(t_1)^{\times d_1}$ is clearly non-zero.

– Suppose that $n > 1$:

We use a more general fact (see [1]). If K is a field equipped with a discrete valuation $\upsilon : K^\times \longrightarrow \mathbb{Z}$, then there is the so-called residue homomorphism

$$\partial_\upsilon : H^n(K, \mathbb{Z}/d) \longrightarrow H^{n-1}(\kappa(\upsilon), \mathbb{Z}/d)$$

where $\kappa(\upsilon)$ denotes the residue field of υ. This homomorphism has the following property :

If $\upsilon(a_1) = \cdots = \upsilon(a_{n-1}) = 0$ and $\upsilon(a_n) = 1$ (i.e. $a_i \in \mathcal{O}_\upsilon^\times$ for $i < n$) then

$$\partial_\upsilon\big((a_1) \cup \cdots \cup (a_{n-1}) \cup (a_n)\big) = (\overline{a}_1) \cup \cdots \cup (\overline{a}_{n-1}) \in H^{n-1}(\kappa(\upsilon), \mathbb{Z}/d)$$

where $\overline{a}_i$ is the class of a_i in $\mathcal{O}_\upsilon / \mathfrak{m}_\upsilon = \kappa(\upsilon)$.

In our case, we take for v the t_n-adic valuation on L. We thus have

$$\partial_v\big((t_1)\cup\cdots\cup(t_n)\big) = (t_1)\cup\cdots\cup(t_{n-1}) \in H^{n-1}\big(K(t_1,\ldots,t_{n-1}),\mathbb{Z}/d_1\big).$$

By induction hypothesis this element is non-zero, hence $(t_1)\cup\cdots\cup(t_n)\neq 0$ and $\mathrm{ed}(G)=n$.

Remark 3.8. This shows that $\mathrm{ed}_k(G)\geq \mathrm{rank}_p(G)$ for any field k with $\mathrm{char}(k)\neq p$. Here $\mathrm{rank}_p(G)$ denotes the rank of the largest p-elementary subgroup of G.

If $\mathrm{char}(k)=p$ this result is no longer true. Indeed, consider the group $\mathbb{Z}/p\times\cdots\times\mathbb{Z}/p$ (n copies). If one takes for k a field containing $\mathbb{F}_{p^n}$ there is a short exact sequence

$$0\to\mathbb{Z}/p\times\cdots\times\mathbb{Z}/p\to\mathbb{G}_a\to\mathbb{G}_a\to 0$$

where the map $\mathbb{G}_a\to\mathbb{G}_a$ is given by $x\mapsto x^p-x$. This gives in cohomology an exact sequence

$$\mathbb{G}_a(K)\to H^1(K,\mathbb{Z}/p\times\cdots\times\mathbb{Z}/p)\to\underbrace{H^1(K,\mathbb{G}_a)}_{=0}\to\cdots$$

Thus $\mathbb{G}_a$ is a classifying scheme for $\mathbb{Z}/p\times\cdots\times\mathbb{Z}/p$, when the field k contains $\mathbb{F}_{p^n}$, and it follows that $\mathrm{ed}_k(\mathbb{Z}/p\times\cdots\times\mathbb{Z}/p)=1$.

COROLLARY 3.9. *Let n be an integer and k a field with* $\mathrm{char}(k)\nmid n$. *Then*

$$\mathrm{ed}_k(\underbrace{\mu_n\times\cdots\times\mu_n}_{r\ times})=r.$$

PROOF. Since $H^1(K,\mu_n\times\cdots\times\mu_n)=K^\times/K^{\times n}\times\cdots\times K^\times/K^{\times n}$, one has a surjection of functors

$$\mathbb{G}_m\times\cdots\times\mathbb{G}_m\twoheadrightarrow H^1(\_,\mu_n\times\cdots\times\mu_n)$$

and thus $\mathrm{ed}_k(\mu_n\times\cdots\times\mu_n)\leq r$. For the opposite inequality it suffices to remark that over an algebraic closure the group $\mu_n\times\cdots\times\mu_n$ is isomorphic to the constant group $\mathbb{Z}/n\times\cdots\times\mathbb{Z}/n$ and apply Proposition 3.7.

Applying the same cohomological-invariant techniques to quadratic forms one can prove the following result which can be found in [14].

THEOREM 3.10. *Assume that* $\mathrm{char}(k)\neq 2$. *Then* $\mathrm{ed}_k(\mathbf{Q}_n)=n$.

PROOF. We have already shown that $\mathrm{ed}(\mathbf{Q}_n) \leq n$. We prove that $\mathrm{ed}(\mathbf{Q}_n) = n$ using a non-trivial cohomological invariant: the Delzant's Stiefel-Whitney class (see [5]) denoted by ω_n.

For any field extension K/k take $L = K(t_1, \ldots, t_n)$ and let $q = \langle t_1, \ldots, t_n \rangle$. One has $\omega_n(q) = (t_1) \cup \cdots \cup (t_n) \in H^n(L, \mathbb{Z}/2)$ which is non-zero, as it was checked before. Hence ω_n is a non-trivial cohomological invariant of degree n. It follows that $\mathrm{ed}(\mathbf{Q}_n) = n$.

One of the most interesting features of the use of cohomological invariants is the following application to the symmetric group. This was originally found in [3].

COROLLARY 3.11. *If* $\mathrm{char}(k) \neq 2$ *one has* $\mathrm{ed}(\mathcal{S}_n) \geq \left[\frac{n}{2}\right]$.

PROOF. We have already seen that $H^1(K, \mathcal{S}_n) = \acute{\mathbf{E}}\mathbf{t}_n(K)$. By Proposition 1.5, one can assume that k is algebraically closed. Consider now the functorial morphism

$$\acute{\mathbf{E}}\mathbf{t}_n(K) \longrightarrow \mathbf{Q}_n(K)$$

$$A \longmapsto \left(\mathcal{T}_{A/K} : x \mapsto \mathrm{Tr}_{A/K}(x^2)\right)$$

and $\omega_m : \mathbf{Q}_n(K) \longrightarrow H^m(K, \mathbb{Z}/2)$ with $m = \left[\frac{n}{2}\right]$. We show that the composite

$$\acute{\mathbf{E}}\mathbf{t}_n(K) \longrightarrow H^m(K, \mathbb{Z}/2)$$

is a non-trivial cohomological invariant. For any field extension K/k take $L = K(t_1, \ldots, t_m)$ and let

$$A \cong \begin{cases} L(\sqrt{t_1}) \times \cdots \times L(\sqrt{t_m}) & \text{if } n = 2m \\ L(\sqrt{t_1}) \times \cdots \times L(\sqrt{t_m}) \times L & \text{if } n = 2m+1. \end{cases}$$

Clearly the matrix of the trace form expressed in the basis $\{1, \sqrt{t}\}$ is $\begin{pmatrix} 2 & 0 \\ 0 & 2t_i \end{pmatrix}$. Hence

$$\begin{aligned} \mathcal{T}_{A/L} &\simeq \begin{cases} \langle 2, 2t_1, \ldots, 2, 2t_m \rangle & \text{if } n = 2m \\ \langle 2, 2t_1, \ldots, 2, 2t_m, 1 \rangle & \text{if } n = 2m+1 \end{cases} \\ &\simeq \langle t_1, \ldots, t_m \rangle \perp \langle 1, \ldots, 1 \rangle, \end{aligned}$$

since k is algebraically closed. Thus

$$\omega_m(\mathcal{T}_{A/L}) = \omega_m(\langle t_1, \ldots, t_m, 1, \ldots, 1 \rangle) = (t_1) \cup \cdots \cup (t_m) \neq 0.$$

4. Free actions and torsors

We recall here some facts about actions of group schemes and torsors in order to estimate $\mathrm{ed}(G)$. The main reference is the book of Demazure-Gabriel [6].

Let G be a group scheme over a scheme S and let X be an S-scheme. We say that G ACTS ON X if there is a morphism of S-schemes

$$\begin{aligned} G\times_S X &\longrightarrow X \\ (g,x) &\longmapsto x\cdot g \end{aligned}$$

which satisfy the categorical conditions of a usual group (right) action. It follows in particular that for any morphism $T\to S$ there is an action of the group $G(T)$ on the set $X(T)$.

Recall that a group G acts freely on a set X if the stabilizer of any point of X is trivial. One can mimic this and say that a group scheme G acts FREELY on a scheme X if for any S-scheme $T\longrightarrow S$ the group $G(T)$ acts freely on the set $X(T)$. One can also define the stabilizer of a point of X in the following way: Let $x\in X$ be any point. The SCHEME-THEORETIC STABILIZER OF x is the pull-back of the diagram

$$\begin{tikzcd} & G\times_S \{x\} \arrow[d] \\ \mathrm{Spec}(k(x)) \arrow[r, "x"] & X \end{tikzcd}$$

where the vertical map is the composite $G\times_S\{x\}\longrightarrow G\times_S X\longrightarrow X$. We denote it by G_x. It is a group scheme over $\mathrm{Spec}(k(x))$ and is a closed group subscheme of $G\times_S\{x\}$.

Once the vocabulary is established one has the following lemma.

Lemma 4.1. *Let X and G be as above, everything being of finite type over $S=\mathrm{Spec}(k)$. Then the following are equivalent*
(i) G acts freely,
(ii) $G_x=\{1\}$ for all points $x\in X$.

Proof. See [6], III, §2 Corollary 2.3.

One can also check these conditions on $\bar{k}$-points, where $\bar{k}$ is an algebraic closure of k.

Recall first that, for an algebraic group G over k, the Lie algebra can be defined as the kernel of the map $G(k[\tau])\to G(k)$ where $k[\tau]$ is the algebra $k[t]/t^2$ and the map $k[\tau]\to k$ is given by $\tau\mapsto 0$. Let x be a point of a scheme X and denoted by $K=k(x)$ its residue field. The point x is then viewed as an element of $X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$ and thus also as an element of $X(K[\tau])$ which we will denote by $x_{K[\tau]}$.

Lemma 4.2. *Let G be a group scheme of finite type over k acting on a k-scheme X of finite type.*

(i) *Suppose* $\mathrm{char}(k) = 0$. *Then G acts freely on X if and only if the group $G(\bar{k})$ acts freely on $X(\bar{k})$.*

(i') *Suppose* $\mathrm{char}(k) > 0$. *Then G acts freely on X if and only if the group $G(\bar{k})$ acts freely on $X(\bar{k})$, and for any closed point $x \in X$ the Lie algebra* $\mathrm{Lie}(G_x)$ *is trivial.*

Proof. See [6], III, §2 Corollary 2.5 and Corollary 2.8. The Lie algebra $\mathrm{Lie}(G_x)$ is called the Lie stabilizer of x.

Remark 4.3. The second part of condition (i') can checked easily using the following description of $\mathrm{Lie}(G_x)$ (see [6], III, §2, proof of Prop. 2.6.): let K be the residue field of x, and let $K[\tau]$ be the K-algebra $K[X]/(X^2)$. Then we have

$$\mathrm{Lie}(G_x) = \{g \in \mathrm{Lie}(G) \otimes K[\tau] \mid g \cdot x_{K[\tau]} = x_{K[\tau]}\}.$$

Remark 4.4. Let G act on X as above. For every scheme T consider the quotient map of sets $\pi : X(T) \longrightarrow Y(T) := X(T)/G(T)$. Sending a pair $(g, x) \in G(T) \times X(T)$ to $(x, x \cdot g)$ gives a mapping

$$G(T) \times X(T) \longrightarrow X(T) \times_{Y(T)} X(T).$$

If G acts freely this map is easily seen to be an isomorphism. It also says that the fibers of π are principal homogenous spaces under $G(T)$ (at least when they are non-empty). The notion of G-torsor generalizes this remark in the category of schemes and is the suitable definition for defining "parametrized" principal homogenous spaces.

Definition 4.5. *Let G be a group scheme over Y which is flat and locally of finite type over Y. We say that a morphism of schemes $X \to Y$ is a* (flat) G-torsor over Y *if G acts on X, the morphism $X \to Y$ is flat and locally of finite type, and the map $\varphi : G \times_Y X \to X \times_Y X$ defined by*

$$G \times_Y X \to X \times_Y X$$

$$(g, x) \mapsto (x, x \cdot g)$$

is an isomorphism.

This condition is equivalent to the existence of a covering $(U_i \to Y)$ for the flat topology on Y such that $X \times_Y U_i$ is isomorphic to $G \times_Y U_i$ for each i (see [13], Chapter III, Proposition 4.1). This means that X is "locally" isomorphic to G for the flat topology on Y. When the group G is smooth over Y it follows by faithfully flat descent that X is also smooth.

A morphism between two G-torsors $f : X \to Y$ and $f' : X' \to Y$ defined over the same base is simply a G-equivariant morphism $\varphi : X \to X'$ such that $f' \circ \varphi = f$. Again by faithfully flat descent it follows that any morphism between G-torsors is an isomorphism.

Remark 4.6. Notice that if $X \to Y$ is a G-torsor, then G acts freely on X. Indeed, take $x \in X$, then the fiber of the point $(x, x) \in X \times_Y X$ under the map $\varphi : G \times_Y X \to X \times_Y X$ is isomorphic to G_x. Since φ is an isomorphism it follows that G_x is trivial for every x.

We then consider the *contravariant* functor

$$G\text{-}\mathbf{Tors} : \text{Schemes} \longrightarrow \mathbf{Sets},$$

defined by

$$G\text{-}\mathbf{Tors}(Y) = \text{ isomorphism classes of } G\text{-torsors over } Y.$$

For every morphism $f : Y' \longrightarrow Y$ the corresponding map G-$\mathbf{Tors}(f)$ is defined as follows: if $X \to Y$ a G-torsor over Y, then the image of this torsor under G-$\mathbf{Tors}(f)$ is the pull-back of the diagram

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

which is easily checked to be a G-torsor over Y'.

When Y is a point, say $Y = \mathrm{Spec}(K)$, and G is smooth over K then any G-torsor $X \to \mathrm{Spec}(K)$ gives rise to a principal homogeneous space over K. Indeed X is smooth and thus $X(K_s) \neq \emptyset$ is a principal homogenous space under $G(K_s)$, thus an element of $H^1(K, G)$. We may thus consider G-$\mathbf{Tors}$ as a generalization of the first Galois cohomology functor over the category of fields.

Now that the notion of torsor is well-defined we have to overcome the problem of quotients.

Let G act on a S-scheme X. A morphism $\pi : X \longrightarrow Y$ is called a CATEGORICAL QUOTIENT of X by G if π is (isomorphic to) the *push-out* of the diagram

$$\begin{array}{ccc} G \times_S X & \longrightarrow & X \\ {\scriptstyle \mathrm{pr}_2}\downarrow & & \\ X & & \end{array}$$

In general such a quotient does not exist in the category of schemes. When it exists the scheme Y is denoted by X/G. We will not give a detailed account on the existence of quotients. We will only need the existence of a *generic quotient*, that is a G-invariant dense open subscheme U of X for which the quotient $U \longrightarrow U/G$ exists. Moreover, we will need one non-trivial fact due to P. Gabriel (which can be found in [7]) which asserts the existence of a generic quotient which is also a G-torsor.

THEOREM 4.7. *Let G act freely on a S-scheme of finite type X such that the second projection $G \times_S X \to X$ is flat and of finite type. Then there exists a (non-empty) G-invariant dense open subscheme U of X satisfying the following properties:*

i) There exists a quotient map $\pi : U \longrightarrow U/G$ in the category of schemes.

ii) π is onto, open and U/G is of finite type over S.

iii) $\pi : U \longrightarrow U/G$ is a flat G-torsor.

PROOF. This follows from [7], Exposé V, Théorème 8.1, p.281 where the statement is much more general and deals with groupoids. In order to recover it we make a translation: in our context the groupoid is that of §2 Exemple a) p.255 which simply defines the equivalence relation on the scheme X under the G-action. The fact that our action is free implies that the morphism $G \times_S X \longrightarrow X \times_S X$ is quasi-finite, which is one of the hypotheses of Théorème 8.1.

We thank J.-P. Serre for pointing out to us this result and an alternative proof which can be found in a paper of Thomason ([22]).

DEFINITION 4.8. *Let G act on X. An open subscheme U which satisfies the conclusion of the above theorem will be called a* FRIENDLY *open subscheme of X.*

From now on take $S = \mathrm{Spec}(k)$ where k is a field and G an algebraic group over k, that is we require G to be *smooth* and of finite type over k, and all the morphisms between schemes will be of finite type. Unless otherwise specified, when we say that $X \longrightarrow Y$ is a G-torsor we mean that $X \longrightarrow Y$ is a G_Y-torsor where G_Y is the group scheme obtained from G by base change $Y \to \mathrm{Spec}(k)$. In this case this says that there is an isomorphism $G \times_k X \simeq X \times_Y X$.

Definition 4.9. *Let $\pi : X \to Y$ be a G-torsor. For any field extension K/k we define a map*

$$\partial : Y(K) \longrightarrow H^1(K, G)$$

as follows: for any $y \in Y(K)$, the fiber X_y of $\pi : X \to Y$ at y is a twisted form of G (that is locally isomorphic to G for the flat topology) and thus smooth over K. Hence X_y has a K_s-rational point x. We then set $\partial(y) =$ isomorphism class of $X_y(K_s)$.

We can paraphrase the definition in terms of cocycles: for all $\gamma \in \Gamma_K$ we have

$$\pi(\gamma \cdot x) = \gamma \cdot \pi(x) = \gamma \cdot y = y.$$

Hence $\gamma \cdot x$ belongs to $X_y(K_s)$. Since $X \to Y$ is a G-torsor, there exists a unique $g(\gamma) \in G(K_s)$ such that $\gamma \cdot x = x \cdot g(\gamma)$. The assignment $\gamma \longmapsto g(\gamma)$ is then a 1-cocycle and the map ∂ sends y to the class of that cocycle in $H^1(K, G)$.

Definition 4.10. *We say that G acts* generically freely *on X if there exists a non-empty G-stable open subscheme U of X on which G acts freely.*

The previous considerations show in particular that, if G acts generically freely on X, then there exists a friendly open subscheme $U \subset X$ on which G acts freely (take for U the intersection of a dense open subset on which G acts freely and a friendly open subscheme). Hence the statement of the following proposition is consistent.

Proposition 4.11. *Let G be an algebraic group over k acting linearly and generically free on an affine space $\mathbb{A}(V)$, where V is a finite dimensional k-vector space. Let U be a non-empty friendly open subscheme of $\mathbb{A}(V)$ on which G acts freely. Then U/G is a classifying scheme of $H^1(\_, G)$. In particular we have*

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

Proof. It is sufficient to show that, for any field extension K/k, the map $\partial : U/G(K) \longrightarrow H^1(K, G)$ is surjective. Let $g \in Z^1(K, G)$. We twist the action of Γ_K over $V(K_s)$ by setting

$$\gamma * v = \gamma \cdot v \cdot g(\gamma)^{-1}$$

for all $\gamma \in \Gamma_K$ and $v \in V(K_s)$. Clearly this action is Γ_K-semilinear, that is $\gamma * (\lambda v) = \gamma(\lambda)(\gamma * v)$ for all $\lambda \in K_s$. Hence $V(K_s)^{(\Gamma_K, *)}$ is Zariski-dense in $V(K_s)$. Since U is open, there exists an invariant point $v_0 \in U(K_s)$ for the new action $*$. We thus have

$$v_0 = \gamma * v_0 = \gamma \cdot v_0 \cdot g(\gamma)^{-1}$$

and hence $v_0 \cdot g(\gamma) = \gamma \cdot v_0$. In particular, we have for any $\gamma \in \Gamma_K$

$$\gamma \cdot \pi(v_0) = \pi(\gamma \cdot v_0) = \pi(v_0 \cdot g(\gamma)) = \pi(v_0),$$

hence $\pi(v_0) \in U/G(K)$ and maps to g under ∂.

Remark 4.12. Any algebraic group G acts linearly and generically freely over some vector space. Indeed, since G is isomorphic to a closed subgroup of some $\mathbf{GL}_n$, one can assume that $G \subset \mathbf{GL}_n$. Let $V = \mathrm{M}_n(k)$. The group G then acts linearly on $\mathbb{A}(V)$ by (right) matrix multiplication. Now let $U = \mathbf{GL}_n$, viewed as an open subscheme of $\mathbb{A}(V)$. Clearly, the stabilizer of any matrix $M \in U(\bar{k})$ is trivial. Moreover, since the action of $\mathrm{Lie}(G)$ is obtained by restriction of the action of $G(k[\tau])$ (where $\tau^2 = 0$), the Lie stabilizer of any closed point of U is also trivial. Hence G acts freely on U. The previous proposition then shows that the essential dimension of G is finite.

Our next aim is to deal with finite group schemes. Recall that a group scheme over k is called ÉTALE if its Hopf algebra is a finitely generated separable algebra over k (see [6] p.234–238 for an account on étale group schemes).

Proposition 4.13. *Let G be an étale group scheme over k and let V be a finite dimensional k-vector space. Then*
i) G acts linearly and generically freely on $\mathbb{A}(V)$ if and only if G is isomorphic to a closed subgroup of $\mathbf{GL}(V)$.
ii) G acts linearly and generically freely on $\mathbb{P}(V)$ if and only if G is isomorphic to a closed subgroup of $\mathbf{PGL}(V)$.

Proof. We only prove the statement ii) since i) is similar. We have to find an open subscheme U of $\mathbb{P}(V)$ such that the group G acts freely on U. We first consider the action of $G(k_s)$ on $\mathbb{P}(V)(k_s)$. For each $g \in G(k_s)$ consider the linear subspace $S_g = \{x \in \mathbb{P}(V)(k_s) \mid g \cdot x = x\}$ and let $S = \bigcup_{g \in G(k_s)} S_g$. This is an algebraic subvariety of $\mathbb{P}(V)(k_s)$ which is invariant under the absolute Galois group Γ_k. By descent theory (see [23] pp.131-138) there exists a closed subscheme X of $\mathbb{P}(V)$ defined over k such that $X(k_s) = S$. Moreover, always by descent theory, the group scheme G acts on X since $G(k_s)$ acts on $X(k_s) = S$. The desired open subscheme is then $U = \mathbb{P}(V) \setminus X$. To prove this, by Lemma 4.1, we have to check that for all points $x \in U$ the stabilizer G_x is trivial. By construction we have that $G_x(k_s) = 1$ for all $x \in U$. But G is étale and hence G_x too. It then follows that $G_x = 1$.

We now study more carefully the case of finite *constant* group schemes. The following lemma is probably well-known, but we have not found any reference for it, so we give a proof for the convenience of the reader.

Lemma 4.14. *Let G be a constant group scheme, and let H be any algebraic group scheme defined over k. Then the map*

$$\mathrm{Hom}(G, H) \to \mathrm{Hom}(G(k), H(k))$$

sending $\Phi \in \mathrm{Hom}(G, H)$ to Φ_k is a bijection. Moreover, Φ is injective if and only if Φ_k is injective.

Proof. Given a morphism $\varphi : G(k) \longrightarrow H(k)$, we have to show that there exists a unique morphism of group schemes $\Phi : G \longrightarrow H$ such that $\Phi_k = \varphi$. We thus have to define, in a natural way, a group homomorphism $\Phi_R : G(R) \longrightarrow H(R)$ for every k-algebra R. Since $G(\prod R_i) = \prod G(R_i)$ and since every commutative ring is product of connected rings one may assume that R is connected. In this case, since G is constant, one has $G(R) = G = G(k)$ and one then defines Φ_R to be the composite $G(R) = G(k) \to H(k) \to H(R)$. This proves the first part of the statement.

Since Φ is a natural map and $G(\bar{k}) = G(k)$, it follows that $\Phi_{\bar{k}}$ is the composite of Φ_k and of the inclusion $H(k) \hookrightarrow H(\bar{k})$. Hence, if Φ_k is injective, then $\Phi_{\bar{k}}$ is also injective. Since the Lie algebra of a constant group scheme is trivial, Proposition 22.2 of [11] implies that Φ is injective.

Proposition 4.15. *Let V be a finite dimensional k-vector space, and let G be a finite constant group scheme over k. Then G acts linearly and generically freely on $\mathbb{A}(V)$ if and only if the abstract group G is isomorphic to a subgroup of $\mathbf{GL}(V)(k)$. In this case, we have*

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

Proof. If G is isomorphic to a subgroup of $\mathbf{GL}(V)(k)$, then there exists a group morphism $\varphi : G(k) \hookrightarrow \mathbf{GL}(V)(k)$. By Lemma 4.14 above there exists a unique injective morphism of group schemes $\Phi : G \longrightarrow \mathbf{GL}(V)$ extending φ. Proposition 4.13 then shows that G acts linearly and generically freely on $\mathbb{A}(V)$. The converse is clear. The inequality $\mathrm{ed}_k(G) \leq \dim(V)$ is then a direct application of the Proposition 4.11.

Proposition 4.15 helps in the computation of the essential dimension of finite abelian groups over sufficiently big fields.

Corollary 4.16. *Let G be a finite abelian group and k a field with $\mathrm{char}(k) \nmid \exp(G)$. If the field k contains all the $\exp(G)$-th roots of unity, then*

$$\mathrm{ed}_k(G) = \mathrm{rank}(G).$$

In particular, if G is cyclic then $\mathrm{ed}_k(G) = 1$.

Proof. By Proposition 3.7 we only have to prove that $\mathrm{ed}_k(G) \leq \mathrm{rank}(G)$. Let $n = \mathrm{rank}(G)$ and write $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$ where $d_1 \mid d_2 \mid \cdots \mid d_n$. By hypothesis, we have $k \supset \mu_{d_m} \supset \cdots \supset \mu_{d_1}$. We then have the following injection

$$\begin{aligned} G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n &\longrightarrow \mathbf{GL}_n(k) \\ ([m_1], \ldots, [m_n]) &\mapsto \begin{pmatrix} \zeta_1^{m_1} & & 0 \\ & \ddots & \\ 0 & & \zeta_n^{m_n} \end{pmatrix} \end{aligned}$$

where ζ_i denotes a primitive d_i-th root of unity. Now apply the above proposition.

We will see later on that the computation is much more complicated when no roots of unity are assumed to be in the base field.

An action of an algebraic group G on a scheme X is called FAITHFUL if G is isomorphic to a subgroup of $\mathrm{Aut}(X)$ via this action. Proposition 4.15 above then shows that for a finite constant group G, faithful actions on a vector space V correspond to generically free actions on V.

As a little application of faithful actions we give some bounds on the essential dimension of dihedral groups $D_n = \mathbb{Z}/n \rtimes \mathbb{Z}/2$. We will use the classical presentation $D_n = < \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} >$.

Corollary 4.17. *Let k be a field of characteristic $p \geq 0$. Let n be a natural integer such that $p \nmid n$ and suppose that $\mu_n \subset k^\times$. Then $\mathrm{ed}_k(D_n) \leq 2$.*

Proof. Let ζ a n-th primitive root of unity and define an homomorphism $D_n \longrightarrow \mathbf{GL}_2(k)$ by sending σ to $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ and τ to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. One can easily show that this gives an injective group homomorphism, and then apply Proposition 4.15.

For the groups D_4 and D_6, one can even drop the assumptions on the field at least when $\mathrm{char}(k) \neq 2$. Actually,

$$\begin{aligned} D_4 &\longrightarrow \mathbf{GL}_2(k) \\ \sigma &\longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ \tau &\longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} D_6 &\longrightarrow \mathbf{GL}_2(k) \\ \sigma &\longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \\ \tau &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

are both faithful representations. Hence $\mathrm{ed}_k(D_4) \leq 2$ and $\mathrm{ed}_k(D_6) \leq 2$ for any field k of characteristic $\neq 2$.

In the sequel we will not only deal with faithful linear representations but also with projective ones. The following lemma is an immediate consequence of Proposition 4.13 and Lemma 4.14. We state it here for further reference.

Lemma 4.18. *Let G be a finite constant group scheme over k. Then G acts generically freely on $\mathbb{P}(V)$ if and only if the abstract group G is isomorphic to a subgroup of $\mathbf{PGL}(V)(k)$.*

Remark 4.19. This section is directly inspired by the work of Merkurjev. In particular Propositions 4.11, 4.15 and Corollary 4.16 can be found in [12]. However, all the previous presentation takes care of many technical details which were not pointed out in Merkurjev's paper. Proofs are consequently a little bit longer and a great attention is given to working without any assumption on the characteristic of the ground field. Some trivial results about dihedral groups have been added. Proposition 4.13 has been proved for a future computation on cubics (see the forthcoming paper of the authors: "Essential dimension of cubics").

5. Versal pairs and Rost's definition

In this section we define another notion of essential dimension and compare it with the one introduced at the beginning. The ideas described below are based on the paper [16] where Rost computes $\mathrm{ed}(\mathbf{PGL}_4)$. We therefore call it Rost's essential dimension.

Let k be a field and $\mathfrak{A}_k$ be the category of *all* (associative and unital) commutative k-algebras with homomorphism of k-algebras (sending 1 to 1) as morphisms. Every functor $\mathbf{F} : \mathfrak{A}_k \longrightarrow \mathbf{Sets}$ by restriction defines a functor $\mathfrak{C}_k \longrightarrow \mathbf{Sets}$ hence an object of $\mathfrak{F}_k$. We shall define the notion of essential dimension for a special class of functors $\mathbf{F} : \mathfrak{A}_k \longrightarrow \mathbf{Sets}$.

Let K/k be an object of $\mathfrak{C}_k$. For a local k-subalgebra $\mathcal{O}$ of K, with maximal ideal $\mathfrak{m}$, we will write $\kappa(\mathcal{O}) = \mathcal{O}/\mathfrak{m}$ for its residue field and $\pi : \mathcal{O} \longrightarrow \kappa(\mathcal{O})$ for the quotient map.

Definition 5.1. *Let K and L be two extensions of k. A* pseudo k-place *$f : K \rightsquigarrow L$ is a pair $(\mathcal{O}_f, \alpha_f)$ where $\mathcal{O}_f$ is a local k-subalgebra of K and $\alpha_f : \kappa(\mathcal{O}_f) \to L$ is a morphism in $\mathfrak{C}_k$.*
Let $\mathbf{F} : \mathfrak{A}_k \longrightarrow \mathbf{Sets}$ be a functor and take $f : K \rightsquigarrow L$ a pseudo k-place. We say that an element $a \in \mathbf{F}(K)$ is unramified *in f if a belongs to the image of the map $\mathbf{F}(\mathcal{O}_f) \longrightarrow \mathbf{F}(K)$. In this case we define the* set of specializations of *a to be*

$$f^*(a) = \big\{\mathbf{F}(\alpha_f \circ \pi)(c) \mid c \in \mathbf{F}(\mathcal{O}_f) \text{ with } c_K = a\big\}.$$

We say that a pair (a, K) with $a \in \mathbf{F}(K)$ is a versal pair for $\mathbf{F}$ *(over k) if for every extension L/k and every element $b \in \mathbf{F}(L)$ there exists a pseudo k-place $f : K \rightsquigarrow L$ such that a is unramified in f and such that $b \in f^*(a)$.*

Here is a picture of the situation:

$$\begin{tikzcd} \mathcal{O} \arrow[r] \arrow[d, "\pi"'] & K \\ \kappa(\mathcal{O}) \arrow[r, "\alpha_f"] & L \end{tikzcd} \quad \Rightarrow \quad \begin{tikzcd} \mathbf{F}(\mathcal{O}) \arrow[r] \arrow[d] & \mathbf{F}(K) \ni a \\ \mathbf{F}(\kappa(\mathcal{O})) \arrow[r] & \mathbf{F}(L) \ni b \end{tikzcd}$$

Example 5.2. Let X be an irreducible k-scheme, $k(X)$ its function field and denote by $\eta : \mathrm{Spec}(k(X)) \longrightarrow X$ the unique morphism whose image is the generic point of X. Then $(\eta, k(X))$ is a versal pair for X.
Indeed, take $x : \mathrm{Spec}(L) \to X$ an element in $X(L)$. Then the local ring $\mathcal{O}_{X,x}$ at the point x is naturally a subring of $k(X)$ and there is a canonical morphism from the residue field $k(x)$ to L giving a pseudo k-place $k(X) \rightsquigarrow L$ with the desired property.

Definition 5.3. *Let* $\mathbf{F} : \mathfrak{A}_k \longrightarrow \mathbf{Sets}$ *be a functor which has a versal pair. We define its* (Rost's) essential dimension *(denoted by* $\mathrm{ed}'(\mathbf{F})$*) to be the minimum of the transcendence degree of the field of definition for versal pairs. More precisely* $\mathrm{ed}'(\mathbf{F}) = \min \mathrm{trdeg}(K : k)$ *for all* K/k *such that there exists an element* $a \in \mathbf{F}(K)$ *making* (a, K) *into a versal pair for* $\mathbf{F}$.

Remark 5.4. In the paper of Rost ([16]) the notion is a little bit different. What is called k-place in his context is a pseudo k-place where $\mathcal{O}$ is required to be a valuation ring. Every k-place is then trivially a pseudo k-place. However the converse is not true in general. Indeed for a local ring $\mathcal{O}$ in a field K one can always find a valuation whose local ring $\mathcal{O}_v$ dominates it but there is no control on the residue field.

Definition 5.5. *Let* $\mathbf{F} : \mathfrak{A}_k \longrightarrow \mathbf{Sets}$ *be a functor which has a versal pair. We say that a versal pair* (a, K) *is* nice *if for any* $L \subset K$ *and* $a' \in \mathbf{F}(L)$ *such that* $a = a'_K$*, the pair* (a', L) *is versal. We say that* $\mathbf{F}$ *is* nice *if it has a nice versal pair.*

Proposition 5.6. *Let* $\mathbf{F} : \mathfrak{A}_k \longrightarrow \mathbf{Sets}$ *be a functor which has a versal pair. Then we have*

$$\mathrm{ed}_k(\mathbf{F}) \leq \mathrm{ed}'_k(\mathbf{F})$$

where on the left $\mathbf{F}$ *is viewed as a functor on* $\mathfrak{C}_k$*. Moreover, if* $\mathbf{F}$ *is nice, then*

$$\mathrm{ed}'_k(\mathbf{F}) = \mathrm{ed}_k(\mathbf{F}) = \mathrm{ed}(a),$$

where (a, K) *is any nice versal pair.*

Proof. Let L/k be any field extension, and let $b \in \mathbf{F}(L)$. Let (a, K) be a versal pair such that $\mathrm{trdeg}(K : k) = \mathrm{ed}'_k(\mathbf{F})$. Since (a, K) is versal, then b comes from an element of $\mathbf{F}(\kappa(\mathcal{O}))$ for some local ring $\mathcal{O}$. Then

$$\mathrm{ed}(b) \leq \mathrm{trdeg}(\kappa(\mathcal{O}) : k) \leq \mathrm{trdeg}(K : k).$$

This proves the first assertion.

Let now (a, K) be a nice versal pair (notice that $\mathrm{trdeg}(K : k)$ is not necessarily minimal). Take a subextension $k \subset L \subset K$ with an element $a' \in \mathbf{F}(L)$ such that $a = a'_L$ and $\mathrm{trdeg}(L : k) = \mathrm{ed}(a)$. By assumption, (a', L) is versal, so $\mathrm{ed}'_k(\mathbf{F}) \leq \mathrm{trdeg}(L : k) = \mathrm{ed}(a) \leq \mathrm{ed}_k(\mathbf{F})$. This concludes the proof.

Remark 5.7. All the present section is new but is inspired by the work of Rost which can be found in [16].

6. Generic torsors and compressions

Now that we have seen the notion of versal pairs we want to apply it to $H^1(\_, G)$ when viewed as a functor over $\mathfrak{A}_k$. That is we consider the functor G-**Tors** over the category of affine k-schemes. This section deals with compressions of torsors and is closely related to Reichstein's original discussion. Compare with [14] where everything is done over an algebraically closed field. For the definition of generic torsors we follow [9].

Let G be an algebraic group over k. If G acts linearly and generically freely on a vector space V, there exists an open subscheme $U \subseteq \mathbb{A}(V)$ such that $\pi : U \longrightarrow U/G = Y$ is a G-torsor. We have defined a map (see Definition 4.9)

$$\partial : Y(K) \longrightarrow H^1(K, G)$$

and proved that ∂ is surjective (see Proposition 4.11). Actually, we have shown a little more: for every torsor $P \in H^1(K, G)$, there exists a non-empty subset S of Y such that the isomorphism class of $\pi^{-1}(y)$ is equal to P for every $y \in S(K)$. Such an S is a Zariski-dense subset of Y if K is infinite.

This leads naturally to the following definition:

Definition 6.1. *Let $f : X \to Y$ be a G-torsor with Y irreducible. We say that it is* classifying for *G if, for any field extension k'/k with k' infinite and for any principal homogenous space P' of G over k'/k, the set of points $y \in Y(k')$ such that P' is isomorphic to the fiber $f^{-1}(y)$ is dense in Y. In particular we have a surjection of functors $Y \twoheadrightarrow H^1(\_, G)$ showing that Y is a classifying scheme of G.*

Remark 6.2. Proposition 4.11 and Remark 4.12 show that a classifying G-torsor always exist for any algebraic group G. Moreover one can always find a reduced classifying torsor for G. Indeed take $X \to Y$ a classifying torsor for G and let $\varphi : Y_{\mathrm{red}} \to Y$ the reduced scheme of Y with its canonical map. Then pulling back $X \to Y$ along φ gives a torsor which is isomorphic to $X_{\mathrm{red}} \to Y_{\mathrm{red}}$ and which is also classifying.

Definition 6.3. *We call* generic torsor over G *the generic fiber of a classifying G-torsor $X \to Y$, i.e. the pullback of*

$$\begin{tikzcd} & X \arrow[d] \\ \mathrm{Spec}(k(Y)) \arrow[r] & Y \end{tikzcd}$$

where $\mathrm{Spec}(k(Y)) \to Y$ *is the generic point. If* $P \longrightarrow \mathrm{Spec}(k(Y))$ *is such a generic torsor it can be viewed as an element of* $H^1(k(Y), G)$.

*More precisely one can restate the definition in the following way. Let G be an algebraic group over k, K a field extension of k and $P \longrightarrow \mathrm{Spec}(K)$ a G-torsor. We say that P is k-*versal *or k-*generic *if*

i) there exists an irreducible scheme Y (whose generic point is denoted by η) with function field $k(Y) \simeq K$ (such a scheme is called a model of K) and a G-torsor $f : X \longrightarrow Y$ whose generic fiber $f^{-1}(\eta) \longrightarrow \mathrm{Spec}(K)$ is isomorphic to $P \longrightarrow \mathrm{Spec}(K)$. In other words

$$\begin{tikzcd} P \arrow[r] \arrow[d] & X \arrow[d] \\ \mathrm{Spec}(K) \arrow[r] & Y \end{tikzcd}$$

is a pull-back.

ii) For every extension k'/k with k' infinite, for every non-empty open set U of Y and for every G-torsor $P' \longrightarrow \mathrm{Spec}(k')$, there exists a k'-rational point $x \in U$ such that $f^{-1}(x) \simeq P'$.

Remark 6.4. If $f : X \to Y$ is a classifying G-torsor, then, for any non-empty open subset U of Y, the map $f : f^{-1}(U) \to U$ is also a classifying torsor. This says that generic torsors over G correspond bijectively to birational classes of classifying torsors for G.

LEMMA 6.5. *Let $P \to \mathrm{Spec}(k(Y))$ be a generic torsor. Then $(P, k(Y))$ is a versal pair for G-**Tors**.*

PROOF. Take $T \to \mathrm{Spec}(L)$ any torsor defined over L/k. Since $X \to Y$ is a classifying torsor there exist a L-rational point $y : \mathrm{Spec}(L) \to Y$ such that $T \to \mathrm{Spec}(L)$ fits into a pull-back

$$\begin{tikzcd} T \arrow[r] \arrow[d] & X \arrow[d] \\ \mathrm{Spec}(L) \arrow[r] & Y \end{tikzcd}$$

Take $\mathcal{O}_{Y,y}$ the local ring at the point y and let $\varphi : \mathrm{Spec}(\mathcal{O}_{Y,y}) \to Y$ be the canonical morphism. Consider $P' \to \mathrm{Spec}(\mathcal{O}_{Y,y})$ the torsor obtained by pulling-back $X \to Y$ along φ. The local ring $\mathcal{O}_{Y,y}$ is naturally a sub-k-algebra of $k(Y)$ and we have a diagram

$$\begin{tikzcd} P \arrow[rr] \arrow[dr, dashed] \arrow[dd] & & X \arrow[dd] \\ & P' \arrow[ur] \arrow[dd] & \\ \mathrm{Spec}(k(Y)) \arrow[rr] \arrow[dr] & & Y \\ & \mathrm{Spec}(\mathcal{O}_{Y,y}) \arrow[ur, "\varphi"'] & \end{tikzcd}$$

showing that $P \to \mathrm{Spec}(k(Y))$ comes from a torsor over $\mathrm{Spec}(\mathcal{O}_{Y,y})$. Moreover the morphism $y : \mathrm{Spec}(L) \to Y$ factorizes through $\mathrm{Spec}(k(y))$ and, if we denote by $P'' \to \mathrm{Spec}(k(y))$ the torsor obtained by pulling-back $P' \to \mathrm{Spec}(\mathcal{O}_{Y,y})$ along the morphism $\mathrm{Spec}(k(y)) \to \mathrm{Spec}(\mathcal{O}_{Y,y})$, one has the following diagram

$$\begin{tikzcd} & T \arrow[rr] \arrow[dl, dashed] \arrow[dd] & & X \arrow[dl] \arrow[dd] \\ P'' \arrow[rr] \arrow[dd] & & P' \arrow[dd] & \\ & \mathrm{Spec}(L) \arrow[rr, "y"] \arrow[dl] & & Y \arrow[dl, "\varphi"] \\ \mathrm{Spec}(k(y)) \arrow[rr] & & \mathrm{Spec}(\mathcal{O}_{Y,y}) & \end{tikzcd}$$

This shows that $T \to \mathrm{Spec}(L)$ comes from $P'' \to \mathrm{Spec}(k(y))$. Thus the local ring $\mathcal{O}_{Y,y}$ toghether with the morphism $k(y) \to L$ form the desired pseudo k-place showing that $(P, k(Y))$ is a versal pair.

Remark 6.6. In the proof of the preceeding lemma the density hypothesis in the definition of a classifying torsor is not used. This hypothesis will be used when talking about compressions.

Remark 6.7. Notice that when Y is smooth over k, the local ring $\mathcal{O}_{Y,y}$ of any point of Y is dominated by a valuation ring whose residue field is equal to $k(y)$. It follows in this case that any pseudo k-place defines a k-place in the sense of Rost (see [16]). Since we do not have a precise reference for this result we have decided to deal only with pseudo k-places.

Actually we will see that a generic torsor give rise to a nice versal pair for the functor G-**Tors**. We first need a definition

Definition 6.8. *Let $f : X \longrightarrow Y$ and $f' : X' \longrightarrow Y'$ be two G-torsors. We say that f' is a* compression *of f if there is a diagram*

$$\begin{tikzcd} X \arrow[r, dashed, "g"] \arrow[d, "f"'] & X' \arrow[d, "f'"] \\ Y \arrow[r, dashed, "h"'] & Y' \end{tikzcd}$$

where g is a G-equivariant rational dominant morphism and h is a rational morphism too. The essential dimension *of a G-torsor f is the smallest dimension of Y' in a compression f' of f. We still denote this by* $\mathrm{ed}(f)$.

Remark 6.9. Take as above a compression of $f : X \longrightarrow Y$ and let $U \subseteq Y$ the open subscheme on which h is defined. Taking the pull-back of $X' \longrightarrow Y'$ along h one obtains a G-torsor $f'' : P \longrightarrow U$ which fits into a diagram

$$\begin{tikzcd} X \arrow[r, dashed] \arrow[d, "f"'] & P \arrow[r] \arrow[d, "f''"] & X' \arrow[d, "f'"] \\ Y \arrow[r, dashed] & U \arrow[r] & Y' \end{tikzcd}$$

and f'' is a compression too.

The following simple result will be helpful in the sequel.

Lemma 6.10. *Let $g : X \dashrightarrow X'$ be a rational dominant G-equivariant morphism between generically free schemes. Then there exist X_0 (resp. X'_0) a friendly open subscheme of X (resp. of X') such that g induces a compression of torsors*

$$\begin{tikzcd} X_0 \arrow[r, dashed, "g"] \arrow[d] & X'_0 \arrow[d] \\ X_0/G \arrow[r, dashed, "h"'] & X'_0/G \end{tikzcd}$$

Proof. Take U some friendly open subscheme of X. Since g is dominant one can find U', open subscheme of X', which lies in the image of g. Intersecting U' with some friendly open set of X' gives a friendly open set X'_0 in the image of U. Then $X_0 = g^{-1}(X'_0)$ is the desired open set.

Lemma 6.11. *Let $f : X \longrightarrow Y$ be a G-torsor with Y irreducible and reduced. Let $T \longrightarrow \operatorname{Spec}(k(Y))$ be its generic fiber. Then* $\operatorname{ed}(f) = \operatorname{ed}(T)$.

Proof. Let f and T be as above. Let $f' : X' \longrightarrow Y'$ be a compression of f and $T' \longrightarrow \operatorname{Spec}(k(Y'))$ its generic fiber. By Remark 6.9 above, and since the generic fiber of f is isomorphic to the generic fiber of f'', one can suppose that the compression is a pull-back. The cube

$$\begin{tikzcd}
& T \arrow[rr] \arrow[dl] \arrow[dd] & & X \arrow[dl] \arrow[dd] \\
T' \arrow[rr, crossing over] \arrow[dd] & & X' & \\
& \operatorname{Spec}(k(Y)) \arrow[rr] \arrow[dl] & & Y \arrow[dl] \\
\operatorname{Spec}(k(Y')) \arrow[rr] & & Y' \arrow[from=uu, crossing over] &
\end{tikzcd}$$

then shows that T' maps to T under $H^1(k(Y'), G) \longrightarrow H^1(k(Y), G)$. This shows that $\operatorname{ed}(T) \leq \operatorname{ed}(f)$.

Conversely suppose there is a subextension $k \subseteq K' \subseteq K := k(Y)$ together with a principal homogenous space T' over K' such that T' maps to T under $H^1(K', G) \longrightarrow H^1(k(Y), G)$. We have to find a G-torsor $f' : X' \longrightarrow Y'$ such that T' is isomorphic to its generic fiber and a compression from f to f'.

First remark that one can suppose everything to be affine. Indeed the generic point of Y lies in some open affine subset U and T is also the generic fiber of the G-torsor $f^{-1}(U) \longrightarrow U$.

Now rewrite the problem in terms of rings: say $Y = \operatorname{Spec}(A)$, $X = \operatorname{Spec}(B)$, $T = \operatorname{Spec}(P)$, $T' = \operatorname{Spec}(P')$ and let $k[G]$ denote the algebra of G. We know that K is the field of fractions of A (since Y is reduced), that $P \simeq B \otimes_A K$ and $P \simeq P' \otimes_{K'} K$. We have to find a subring A' of K' whose field of fractions is K', a G-torsor B'/A' such that $P' \simeq B' \otimes_{A'} K'$ and a rational compression from B'/A' to B/A.

Since K is of finite type over k we can write it as $K = k(\alpha)$ where (α) is a short notation for $(\alpha_1, \ldots, \alpha_n)$. Similarly, since P is of finite type over K we write it $P = K[\beta]$ for some $\beta_1, \ldots, \beta_m$. In the same way we write $K' = k(\alpha')$ and $P' = K'[\beta']$.

We will take for A' a localisation of the ring $k[\alpha']$ for which the isomorphism $P' \otimes_{K'} P' \simeq P' \otimes_k k[G]$ is defined. More precisely, since both $P' \otimes_{K'} P'$ and $P' \otimes_k k[G]$ are finitely generated algebras over K' one can find a polynomial f in the α'_i such that $B' \otimes_{A'} B' \simeq B' \otimes_k k[G]$ where $A' = k[\alpha']_f$ and $B' = A'[\beta']$

(since there is only a finite number of polynomials to invert in order to define the isomorphism).

Now obviously $P' \simeq B' \otimes_{A'} K'$ and we just have to find a rational morphism from A' to A and this will induce a rational compression from B'/A' to B/A. This is easily done since the image of A' under the map $A' \subset K' \subset K$ lies in a subring of the form $k[\alpha]_g$ for some polynomial g in the α_i (again one has only to invert the polynomials that appear in the image of the α'_i which are only finite in number). Now $A = k[\alpha]_h$ for some polynomial h and we have a natural map $A' \to k[\alpha]_g \to (k[\alpha]_g)_h = A_g$. In the same way one finds a rational map $B' \to B_p$ compatible with the previous one.

It follows that $\mathrm{ed}(f) \leq \mathrm{ed}(T)$ and the proof is complete.

Remark 6.12. The hypothesis "reduced" on Y can be dropped easily arguing with $A/\mathrm{Nil}(A)$ rather then A. Since Remark 6.2 tells that one can always find a reduced classifying torsor this will not be proved.

Lemma 6.13. *Let $f' : X' \longrightarrow Y'$ be a compression of a classifying torsor $f : X \longrightarrow Y$. Then f' is also classifying.*

Proof. Let

$$\begin{tikzcd} X \arrow[r, dashed, "g"] \arrow[d, "f"'] & X' \arrow[d, "f'"] \\ Y \arrow[r, dashed, "h"'] & Y' \end{tikzcd}$$

be such a compression. Let k'/k be a field extension with k' infinite and let $P' \in H^1(k', G)$. Since f is classifying one can find a k'-rational point $y \in Y(k')$ which lies in U, the open set on which h is defined, such that $f^{-1}(y) \simeq P'$. Then the fiber of f' at $h(y)$ clearly gives a torsor isomorphic to P'.

Corollary 6.14. *Let $T \to \mathrm{Spec}(K)$ be a generic G-torsor, $K' \subset K$ and $T' \to \mathrm{Spec}(K')$ such that $T'_K = T$. Then T' is also a generic torsor.*

Proof. Take a classifying G-torsor $X \longrightarrow Y$ which is a model for T. Then, by the proof of Lemma 6.11, defining T over a smaller field means compressing the torsor $X \longrightarrow Y$. Since the compression of a classifying torsor is again classifying it follows that T comes from a generic torsor.

Corollary 6.15. *The functor G-**Tors** is nice.*

Proof. We have to show G-**Tors** has a nice versal pair. But a generic torsor defines a versal pair and niceness is ensured by the previous corollary.

Corollary 6.16. *Let G be an algebraic group over k and let $T \in H^1(K, G)$ be a generic torsor. Then $\mathrm{ed}'_k(G) = \mathrm{ed}_k(G) = \mathrm{ed}(T)$.*

Proof. As pointed out above, any generic torsor gives rise to a nice versal pair and we can apply Proposition 5.6.

Proposition 6.17. *Let G be an algebraic group acting linearly and generically freely on $\mathbb{A}(V)$ where V is some vector space. Suppose that the G-action induced on $\mathbb{P}(V)$ is again generically free. Then*

$$\mathrm{ed}(G) \leq \dim(V) - \dim(G) - 1.$$

Proof. The map $\mathbb{A}(V) \setminus \{0\} \to \mathbb{P}(V)$ gives a rational G-equivariant map from $\mathbb{A}(V) \to \mathbb{P}(V)$ which gives a compression of the corresponding torsors in view of Lemma 6.10 above.

Corollary 6.18. *Let G be a finite constant group scheme over k. Suppose that, for an integer $n \geq 2$, there is an injective map $\rho : G \hookrightarrow \mathbf{GL}_n(k)$ such that $\pi \circ \rho$ stays injective where $\pi : \mathbf{GL}_n(k) \to \mathbf{PGL}_n(k)$ is the canonical projection. Then $\mathrm{ed}(G) \leq n - 1$.*

Proof. Indeed G acts generically freely on $\mathbb{A}^n$ by Proposition 4.15 and by Lemma 4.18 on $\mathbb{P}^{n-1}$ too. We can thus apply the above result.

Using compressions we are able to explain the behaviour of the essential dimension of G with respect to a closed subgroup.

Theorem 6.19. *Let G be an algebraic group and H a closed algebraic subgroup of G. Then*

$$\mathrm{ed}(H) + \dim(H) \leq \mathrm{ed}(G) + \dim(G).$$

In particular, if G is finite, we have

$$\mathrm{ed}(H) \leq \mathrm{ed}(G).$$

Proof. Let $\mathbb{A}(V)$ be an affine space on which G acts generically freely. Take U open in $\mathbb{A}(V)$ such that U/G and U/H both exist and are torsors. Now take

$$\begin{tikzcd} U \arrow[r, dashed, "g"] \arrow[d] & X \arrow[d] \\ U/G \arrow[r, dashed, "h"'] & Y \end{tikzcd}$$

a G-compression such that $\dim(Y) = \mathrm{ed}(G)$. Since the stabilizer in H of a point x is a subgroup of G_x it follows that H acts generically freely on U and on X too. Now g is also H-equivariant and by the Lemma 6.10 above g gives rise to an H-compression of $U \longrightarrow U/H$. It then follows that

$$\begin{aligned} \mathrm{ed}(H) &\leq \dim(X) - \dim(H) \\ &= \dim(Y) + \dim(G) - \dim(H) \\ &= \mathrm{ed}(G) + \dim(G) - \dim(H). \end{aligned}$$

This provides another proof of the following

Corollary 6.20. *If* $\mathrm{char}(k) \neq 2$ *one has* $\mathrm{ed}(\mathcal{S}_n) \geq [\frac{n}{2}]$.

Proof. We have $H = \underbrace{\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2}_{[\frac{n}{2}] \text{ times}} \subset \mathcal{S}_n$. But we have seen (Corollary 4.16) that the essential dimension of a finite 2-torsion elementary abelian group is equal to its rank if $\mathrm{char}(k) \neq 2$. One concludes using the preceeding theorem.

Proposition 6.21. *Let* G *be an algebraic group over* k *and denote by* G^0 *its connected component. If* $\mathrm{ed}_k(G) = 1$ *then* G/G^0 *is isomorphic to a finite subgroup of* $\mathbf{PGL}_2$.

Proof. The fact that the group G/G^0 is finite is well-known. Assume now that $\mathrm{ed}_k(G) = 1$. Let $\mathbb{A}(V)$ be an affine space on which G acts generically freely. Let $U \subseteq \mathbb{A}(V)$ be a friendly open subscheme and let $X \longrightarrow Y$ a G-torsor together with a compression of the generic torsor $U \longrightarrow U/G$

$$\begin{tikzcd} U \arrow[r, dashed] \arrow[d] & X \arrow[d] \\ U/G \arrow[r, dashed] & Y \end{tikzcd}$$

Now G acts freely on X (by Remark 4.6) and hence G^0 too. Then the quotient X/G^0 exists and G/G^0 acts freely on it. It follows that there is a monomorphism of group schemes $G/G^0 \to \mathrm{Aut}(X/G^0)$. Now $\mathbb{A}(V)$ is rational and thus X/G^0 is unirational. But

$$\dim(X/G^0) = \dim(X) - \dim(G^0) = \dim(X) - \dim(G) = \dim(Y) = 1$$

and then by a theorem of Lüroth X/G^0 is birationnaly equivalent to $\mathbb{P}^1$. It follows that $\mathrm{Aut}(X/G^0) \cong \mathbf{PGL}_2$. Thus G/G^0 is isomorphic to a subgroup of $\mathbf{PGL}_2$.

Remark 6.22. The above discussion is longer than Merkurjev's one. Many details are given and proofs are completed. However the philosophy introduced here is due to Merkurjev which was himself inspired by Reichstein's work. The discussion about the niceness of G-**Tors** is new. Proposition 6.21 is a new result which was pointed out to us by J.-P. Serre.

7. Some finite groups

In this section we will compute the essential dimension of some constant group schemes. We first deal with some generalities and an application to the symmetric group (which can originally be found in [3]). Groups of the form $\mathbb{Z}/n$ and dihedral groups are then studied more carefully.

In what follows G will denote a finite constant group scheme over k.

We first recall that if G is such a group, then any linear generically free action on a vector space V is actually a faithful representation (see Proposition 4.15). Since G is finite and acts faithfully on the field of functions $k(V)$, this gives rise to a Galois extension $k(V)/k(V)^G$. This is indeed a generic torsor for G by our previous considerations. Now any subfield $E \subseteq k(V)$ on which G acts faithfully gives rise in the same way to a Galois extension E/E^G. From this remark we have the following proposition which is the definition of essential dimension in [3]

Proposition 7.1. *Let G be a finite constant group scheme over k acting faithfully on a k-vector space V. Then the essential dimension of G is the minimum of the* $\operatorname{trdeg}(E:k)$ *for all the fields $E \subseteq k(V)$ on which G acts faithfully.*

Application to $\mathcal{S}_n$.

In this example we suppose that $\operatorname{char}(k) \neq 2$.

With this assumption on the ground field, $\mathcal{S}_n$ acts faithfully on the hyperplane $H = \{\ x \in \mathbb{A}^n_k \mid x_1 + \cdots + x_n = 0\ \}$ and thus on $k(x_1, \ldots, x_{n-1})$. But on $k(x_1, \ldots, x_{n-1})$ we have a multiplicative action, i.e. a $\mathbb{G}_m$-action, given by $\lambda \cdot x_i = \lambda x_i$ for all $\lambda \in \mathbb{G}_m(k)$ and all $i = 1, \ldots, n-1$. This action commutes with the action of $\mathcal{S}_n$. We easily see that

$$k(x_1, \ldots, x_{n-1})^{\mathbb{G}_m} = k\big(x_1/x_{n-1}, \ldots, x_{n-2}/x_{n-1}\big).$$

Now, if $n \geq 3$, the group $\mathcal{S}_n$ acts faithfully on the latter field. The transcendence degree of $k\big(x_1/x_{n-1}, \ldots, x_{n-2}/x_{n-1}\big)$ being equal to $n-2$, one concludes that $\operatorname{ed}(\mathcal{S}_n) \leq n-2$ for $n \geq 3$.

In particular we find $\operatorname{ed}(\mathcal{S}_3) = 1$ and $\operatorname{ed}(\mathcal{S}_4) = 2$.

If now we suppose $n \geq 5$, we show that $\operatorname{ed}(\mathcal{S}_n) \leq n-3$.

The group $\mathbf{PGL}_2(k)$ acts on $k(x_1, \ldots, x_n)$ in the following way :

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \cdot x_i = \frac{a x_i + b}{c x_i + d} \qquad \forall\ i = 1, \ldots, n.$$

If now i, j, k, ℓ are distinct, the cross-sections $[x_i, x_j, x_k, x_\ell] = \frac{(x_i - x_k)(x_j - x_\ell)}{(x_j - x_k)(x_i - x_\ell)}$ are $\mathbf{PGL}_2$-invariant. Hence we have

$$k([x_i, x_j, x_k, x_\ell]) \subset k(x_1, \ldots, x_n)^{\mathbf{PGL}_2(k)}$$

where $k([x_i, x_j, x_k, x_\ell])$ is a short notation for the field generated by the biratios $[x_i, x_j, x_k, x_\ell]$ for i, j, k, l all distinct. But $k([x_i, x_j, x_k, x_\ell])$ is generated by the biratios $[x_1, x_2, x_3, x_i]$ with $i = 4, \dots, n$.
Hence $k([x_i, x_j, x_k, x_\ell]) \cong k(y_1, \dots, y_{n-3})$. But, if $n \geq 5$, every $\sigma \in \mathcal{S}_n \setminus \{1\}$ moves at least one of the $[x_i, x_j, x_k, x_\ell]$'s. Consequently, since the above action commutes with the $\mathcal{S}_n$-action, $\mathcal{S}_n$ acts faithfully on $k(y_1, \dots, y_{n-3})$.

This shows that $\mathrm{ed}(\mathcal{S}_n) \leq n-3$ for all $n \geq 5$.

In particular we have $\mathrm{ed}(\mathcal{S}_5) = 2$ and $\mathrm{ed}(\mathcal{S}_6) = 3$.

The question is still open concerning $\mathcal{S}_7$. Do we have $\mathrm{ed}(\mathcal{S}_7) = 3$ or 4 ?

The following lemma is an immediate consequence of Proposition 6.21. We restate it here in the case of finite groups and reprove it using an algebraic argument. Compare with [3] Theorem 6.2.

Lemma 7.2 (Useful Lemma). *Let G be a finite constant group. If $\mathrm{ed}_k(G) = 1$, then G is isomorphic to a subgroup of $\mathbf{PGL}_2(k)$.*

Proof. Let G act faithfully on a vector space V and let $k(V)/k(V)^G$ be the corresponding Galois extension. Saying that $\mathrm{ed}_k(G) = 1$ means that there is a subextension K/k where $\mathrm{trdeg}(K : k) = 1$ with G acting faithfully on K. Since K is a subextension of $k(V)$, which is rational, and since $\mathrm{trdeg}(K : k) = 1$, by Lüroth's theorem K is also rational. Thus $K \cong k(t)$. Since G acts faithfully on $k(t)$ this means that G is a subgroup of $\mathrm{Aut}(k(t)) \cong \mathbf{PGL}_2(k)$.

We continue this section studying more carefully the groups $\mathbb{Z}/n$ and D_n.

We recall first of all that, if the field k contains the n-th roots of unity, one has $\mathrm{ed}_k(\mathbb{Z}/n) = 1$ and that the inequality $\mathrm{ed}_k(\mathbb{Z}/n) \geq 1$ holds for any field. Upper bounds are usually given by actions or representations and these will essentially depend on the ground field. Furthermore lower bounds are generally difficult to find. We begin with some easy considerations in order to understand the problem.

Consider $\mathbb{Z}/n$ as a constant $\mathbb{R}$-group scheme. Then one has a faithful representation

$$\mathbb{Z}/n \longrightarrow \mathrm{SL}_2(\mathbb{R})$$

given by sending the generator of $\mathbb{Z}/n$ to the matrix

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

representing the rotation of angle $\theta = 2\pi/n$. Hence $\mathrm{ed}_{\mathbb{R}}(\mathbb{Z}/n) \leq 2$ for every n. Clearly this holds for an arbitrary field k containing $\mathbb{R}$. The question becomes particularly interesting when the field is $\mathbb{Q}$. For a better results on the essential dimension of cyclic and dihedral groups over $\mathbb{Q}$ see the work of A. Ledet in [10] where for example the equality $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/7) = 2$ is proven.

But linear representations do not always give the best possible upper bounds. Recall that if G is a finite subgroup of $\mathbf{GL}_n(k)$ for some n and if its image in $\mathbf{PGL}_n(k)$ is still G then $\mathrm{ed}_k(G) \leq n-1$ (see Corollary 6.18).

As we shall see, in the study of cyclic groups there is a gap between groups of odd and even order.

Lemma 7.3 (Simple Lemma). *Let n be an integer, k a field such that $\mathrm{char}(k) \nmid n$ and $\zeta \in \overline{k}$ a primitive n-th root of the unity. Suppose that $\zeta + \zeta^{-1} \in k$. Let $S = \begin{pmatrix} \zeta+\zeta^{-1} & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then the order of S in $\mathbf{GL}_2(k)$ equals n and the subgroup generated by S and T is isomorphic to the dihedral group D_n. Moreover, if n is odd, the same holds in $\mathbf{PGL}_2(k)$ for the classes of S and T.*

Proof. Let $P = \begin{pmatrix} 1 & \zeta^{-1} \\ 1 & \zeta \end{pmatrix}$. Then $S = P^{-1}\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} P$ showing that S has order n. Moreover easily $TST^{-1} = S^{-1}$.
Now assume that n is odd. We only have to check that $S^i \neq \lambda I$ for all $\lambda \in k$ and all $i = 1, \dots, n-1$. Suppose that $S^i = \lambda I$ for some $\lambda \in k$ and some $i = 1, \dots, n-1$. This would mean that $\zeta^i = \lambda$ and $\zeta^{-i} = \lambda$. Thus $\zeta^{2i} = 1$. This means that $n \mid 2i$ which is impossible.

This lemma gives us already the exact value of $\mathrm{ed}_k(\mathbb{Z}/n)$, with n odd, when the field contains $\zeta + \zeta^{-1}$.

Proposition 7.4. *Let n be an odd integer, k a field such that $\mathrm{char}(k) \nmid n$ and ζ a primitive n-th root of the unity. If $\zeta + \zeta^{-1} \in k$ then*

$$\mathrm{ed}_k(\mathbb{Z}/n) = 1.$$

Proof. We only have to prove that $\mathrm{ed}_k(\mathbb{Z}/n) \leq 1$. But the lemma above shows that $\mathbb{Z}/n$ injects into $\mathbf{GL}_2(k)$ and that this map stays injective when passing to $\mathbf{PGL}_2(k)$. Thus $\mathrm{ed}_k(G) \leq 2-1 = 1$ by Corollary 6.18.

This gives the essential dimension of $\mathbb{Z}/3$:

Corollary 7.5. *For any field k one has $\mathrm{ed}_k(\mathbb{Z}/3) = 1$.*

Proof. Clearly every field contains $\zeta + \zeta^{-1} = -1$ and hence, if the characteristic of k is $\neq 3$, one can apply the above argument. In characteristic 3 we already know the result (see Examples 2.3).

The tough problem is to deal with groups of the form $\mathbb{Z}/2n$ where n is even. The following theorem gives an answer for $n = 2$. We postpone its proof until the end of the present section.

Theorem 7.6. *Let k be a field of characteristic $\neq 2$. Then*

$$\mathrm{ed}_k(\mathbb{Z}/4) = \begin{cases} 1 & \textit{if } -1 \textit{ is a square in } k \\ \\ 2 & \text{otherwise.} \end{cases}$$

The result was already known by Serre in [21] (see Exercice 1.2) even though the notion of essential dimension was not defined. More recently in [17] Rost computed the essential dimension of a twisted form of $\mathbb{Z}/4$ generalizing the present result.

The above Simple Lemma has a converse statement when n is prime.

Lemma 7.7. *Let $p > 2$ a prime, k a field of characteristic $\neq p$ and $\zeta \in \overline{k}$ a primitive p-th root of unity. If $\mathbf{PGL}_2(k)$ has an element of order p then $\zeta + \zeta^{-1} \in k$.*

Proof. Let $M \in \mathbf{GL}_2(k)$ of order p in $\mathbf{PGL}_2(k)$. There is a $\lambda \in k^\times$ such that $M^p = \lambda I$, thus the minimal polynomial m_M divides $X^p - \lambda$. Hence $X^p - \lambda$ is not irreducible (otherwise $p = \deg(m_M) \leq 2$) and therefore $\lambda = \mu^p$ for some $\mu \in k^\times$. Thus we can suppose that $\lambda = 1$. In that case, the eigenvalues of M are of the form ζ^i. Let ζ^i and ζ^j be the two eigenvalues of M. We have $\det(M) = \zeta^{i+j} \in k^\times$. Suppose that $i+j \not\equiv 0 \mod p$, then $< \zeta^{i+j} >= \mu_p \subset k^\times$ and hence $\zeta + \zeta^{-1} \in k^\times$. Suppose that $i + j \equiv 0 \mod p$, then $j \equiv -i$. If $i \equiv 0$ then $M = I$ which is impossible, hence $i \not\equiv 0$ and the eigenvalues are disctinct. Thus

$$M = P^{-1} \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix} P \in \mathbf{GL}_2(k)$$

for some invertible matrix P. But since $i \not\equiv 0$, there exists j such that $ij \equiv 1 \mod p$. Then $M^j = P^{-1} \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} P$ belongs to $\mathbf{GL}_2(k)$ and it follows that $\zeta + \zeta^{-1} = \mathrm{Tr}(M^j) \in k$.

Corollary 7.8. *Let p be a prime, k a field such that $\mathrm{char}(k) \neq p$ and suppose that $\zeta + \zeta^{-1} \notin k$. Then*

$$\mathrm{ed}_k(\mathbb{Z}/p) \geq 2.$$

Proof. Suppose that $\mathrm{ed}(\mathbb{Z}/p) = 1$, then by the Useful Lemma we would have an injection $\mathbb{Z}/p \longrightarrow \mathbf{PGL}_2(k)$ which is impossible by the above lemma.

We now have the exact value of the essential dimension of $\mathbb{Z}/5$.

Corollary 7.9. *Let k a field such that* $\mathrm{char}(k) \neq 5$ *and ζ a primitive 5-th root of unity. Then*

$$\mathrm{ed}_k(\mathbb{Z}/5) = \begin{cases} 1 & \text{if } \zeta + \zeta^{-1} \in k \\ \\ 2 & \text{otherwise.} \end{cases}$$

Proof. If $\zeta + \zeta^{-1} \in k$ apply Proposition 7.4. If $\zeta + \zeta^{-1} \notin k$ then by the above corollary we have $\mathrm{ed}_k(\mathbb{Z}/5) \geq 2$. It then suffices to show that $\mathrm{ed}_k(\mathcal{S}_5) \leq 2$ since $\mathbb{Z}/5$ is a subgroup of $\mathcal{S}_5$ and thus $\mathrm{ed}_k(\mathbb{Z}/5) \leq \mathrm{ed}_k(\mathcal{S}_5) = 2$. If $\mathrm{char}(k) \neq 2$ this has been proven at the beginning of this section.
Assume now that $\mathrm{char}(k) = 2$. It suffices to show that the generic torsor for $\mathcal{S}_5$ is defined over a field of transcendence degree at most 2. By [2] Proposition 4.4, the generic polynomial defining the generic torsor can be reduced to the form $X^5 + aX^2 + bX + c$. If $b = 0$ we are done. If $b \neq 0$ replacing X by $\frac{c}{b}X$ gives the conclusion.

Another application of the Useful Lemma concerns $\mathbb{Z}/p^2$ in characteristic p. Recall that we already know that $\mathrm{ed}_k(\mathbb{Z}/p^2) \leq 2$ in that case as it was shown in Section 2.

Proposition 7.10. *If* $\mathrm{char}(k) = p$ *then* $\mathrm{ed}_k(\mathbb{Z}/p^2) = 2$.

Proof. By the Useful Lemma we know that if $\mathrm{ed}_k(G) = 1$ then G is isomorphic to a subgroup of $\mathbf{PGL}_2(k)$. Thus it suffices to show that, if $\mathrm{char}(k) = p$, there are no elements of order p^2 in $\mathbf{PGL}_2(k)$. We leave it as an easy exercise to the reader.

One can handle in a similar way the computation of some essential dimensions for the dihedral groups D_n.

Corollary 7.11. *Let n be odd, k a field such that* $\mathrm{char}(k) \nmid n$ *and ζ a primitive n-th root of the unity. If $\zeta + \zeta^{-1} \in k$ then* $\mathrm{ed}_k(D_n) = 1$.

Proof. It readily follows from Simple Lemma above and Corollary 6.18.

Corollary 7.12. *Let n be an integer. Then*

$$\mathrm{ed}_{\mathbb{R}}(D_n) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ \\ 2 & \text{if } n \text{ is even.} \end{cases}$$

Proof. By the Simple Lemma, there is a real 2-dimensional faithful representation of D_n for every n. Hence $\mathrm{ed}_{\mathbb{R}}(D_n) \leq 2$. Moreover, when n is even D_n contains $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$ as a subgroup, according to whether n is congruent to 0 or 2 modulo 4. Thus the statement is a consequence of Theorem 7.6 and Proposition 3.7.

One very interesting result for finite groups can be found in [10] and concerns the essential dimension of $G \times \mathbb{Z}/2$. We give here this result without proof.

Theorem 7.13 (Jensen, Ledet, Yui). *Let k be a field of characteristic 0 containg the primitive pth roots of unity, for a prime p, and let G be a finite group. Assume that k does not contain the primitive rth root of unity for any prime $r \neq p$ dividing $|Z(G)|$. Then*

$$\mathrm{ed}_k(G \times \mathbb{Z}/2) = \mathrm{ed}_k(G) + 1.$$

This result gives for example $\mathrm{ed}_{\mathbb{Q}}(G \times \mathbb{Z}/2) = \mathrm{ed}_{\mathbb{Q}}(G)+1$ for any finite group G. The same holds for $\mathbb{R}$.

Corollary 7.14. *Let n be an odd integer. Then*

$$\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/2n) = \mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/n) + 1.$$

The same holds for $\mathbb{R}$.

Using this result and Theorem 7.6 the computation over the real numbers for cyclic groups is complete:

Corollary 7.15. *Let $n \neq 2$ be an integer. Then*

$$\mathrm{ed}_{\mathbb{R}}(\mathbb{Z}/n) = \begin{cases} 1 & \textit{if } n \textit{ is odd} \\ 2 & \textit{if } n \textit{ is even} \end{cases}$$

Proof. We already know that $\mathrm{ed}_{\mathbb{R}}(\mathbb{Z}/n) \leq 2$. If n is odd, Proposition 7.4 tells that $\mathrm{ed}_{\mathbb{R}}(\mathbb{Z}/n) = 1$. If n is even, two cases arise: either $n = 2m$ with m odd and one applies the above corollary, or $n = 4m$ and in this case $\mathbb{Z}/n$ contains $\mathbb{Z}/4$ as a subgroup. Then Theorem 7.6 shows that $\mathrm{ed}_{\mathbb{R}}(\mathbb{Z}/n) \geq 2$.

As promised, we finish the section with a proof of Theorem 7.6 which gives the essential dimension of $\mathbb{Z}/4$.

Notice first that when -1 is a square in k (and $\mathrm{char}(k) \neq 2$) then Corollary 4.16 tells that $\mathrm{ed}_k(\mathbb{Z}/4) = 1$.

Notice also that one always has $\mathrm{ed}_k(\mathbb{Z}/4) \leq 2$. Indeed let k be a field of characteristic $\neq 2$ and let $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Since A is of order 4, this gives a faithful representation $\mathbb{Z}/4 \longrightarrow \mathbf{GL}_2$ and one concludes that $\mathrm{ed}_k(\mathbb{Z}/4) \leq 2$ using Proposition 4.15.

It thus suffices to prove that $\mathrm{ed}_k(\mathbb{Z}/4) \geq 2$ when $-1 \notin k^{\times 2}$. Our proof is based on the following parametrization of cyclic extensions of degree 4 (see [8]).

Proposition 7.16. *Let K be a field of characteristic $\neq 2$. Let $D \in K^\times \setminus K^{\times 2}$. Then $K(\sqrt{D})/K$ is contained in a cyclic field extension of degree 4 if and only if D is a sum of two squares in K. Let $D = a^2 + b^2, a, b \in K$. Then $K(\sqrt{q(D + a\sqrt{D})})$, $q \in K^\times$ is a parametrization of all cyclic extensions of degree 4 with discriminant D. The trace form of $K(\sqrt{q(D + a\sqrt{D})})$ over K is $\langle 1, D, q, q\rangle$.*

This result tells us that the trace form essentially "depends on two parameters". Let L_0 be the Galois algebra $K(\sqrt{q(D + a\sqrt{D})})$ described in the above proposition. Let $K = k(s,t)$ the function field in two variables and set $D = s^2 + 1, q = t$ (here $a = s, b = 1$ in the notation of the proposition). Now the algebra L_0 can be viewed as an element of $H^1(k(s,t), \mathbb{Z}/4)$. To prove $\mathrm{ed}(L_0) = 2$ it is sufficient to show that the trace form $q = \langle 1, s^2+1, t, t\rangle$ is not defined over a subfield $K \subset k(s,t)$ of transcendence degree 1. We will show that this is the case when k is a field in which -1 is not a square using an idea of Rost.

We begin by making some easy observations on the first residue map of quadratic forms. For convenience we recall briefly its definition following [18].

Let (F, υ) be a field of characteristic different from 2 equipped with a discrete valuation, and let π denotes a prime element (i.e. an element such that $\upsilon(\pi) = 1$). We denote by $\mathcal{O}_\upsilon$ the valuation ring of υ and by $\kappa(\upsilon)$ the residue field.

Any quadratic form q defined over F can be diagonalized as

$$q \simeq \langle a_1, \ldots, a_m, \pi a_{m+1}, \ldots, \pi a_n\rangle,$$

with $a_i \in \mathcal{O}_\upsilon^\times$. Then the map $\partial_\upsilon : W(F) \longrightarrow W(\kappa(\upsilon))$ defined by

$$\partial_\upsilon(q) := \langle \bar{a}_1, \cdots, \bar{a}_m\rangle$$

is a well-defined group homomorphism which is independent of the choice of π, called the first residue map.

Now let $K \subset F$, and let $\omega = \upsilon_{|K}$. If ω is trivial over K, then $K \subset \kappa(\upsilon)$ and it follows from the definition that for any $q \in W(K)$ we have $\partial_\upsilon(q_F) = q_{\kappa(\upsilon)}$.

If ω is non-trivial over K, then any prime element π' of (K, ω) can be written as $\pi' = u\pi^e$ for some $u \in \mathcal{O}_\upsilon^\times$ and some non-negative integer e. The integer e is well-defined and called the ramification index of (K, ω) in (F, υ). If $e = 1$, we say that the extension $(F, \upsilon)/(K, \omega)$ is unramified. Moreover in this case, we have an inclusion $\kappa(\omega) \subset \kappa(\upsilon)$.

If e is odd, then for any $q \in W(K)$, one easily checks that in $W(\kappa(\upsilon))$ the equality $\partial_\upsilon(q_F) = \partial_\upsilon(q)_{\kappa(\upsilon)}$ holds.

Let now k a field in which -1 is not a square. We consider υ the t-adic valuation on the field $F = k(s,t)$ and υ' the (s^2+1)-adic valuation on $\kappa(\upsilon) \cong k(s)$ (note that since -1 is not a square we can consider this valuation).

Suppose now that q is defined over a subfield $K \subset k(s,t)$ with $\mathrm{trdeg}(K:k) = 1$, and write $q = q'_F$ for some quadratic form q' defined over K. Notice that, since $\mathrm{trdeg}(K:k) = 1$, then $\mathrm{trdeg}(F:K) = 1$, and it follows that F/K is a purely transcendental extension.

If the valuation $\omega = \upsilon_{|K}$ is trivial we have

$$\partial_\upsilon(q) = \partial_\upsilon(q'_F) = q'_{\kappa(\upsilon)}.$$

Since $\kappa(\upsilon) = k(s) \subset F$, by scalar extension we obtain the following equality in $W(F)$

$$\partial_\upsilon(q)_F = q.$$

It follows that $\langle 1, 1+s^2\rangle = \langle 1, 1+s^2, t, t\rangle$, showing that $\langle t, t\rangle$ is hyperbolic over F. Then, comparing discriminants, one finds that -1 is a square in $F = k(s,t)$, hence in k, which is a contradiction. Thus the valuation ω is non-trivial over K.

Notice now that $\kappa(\omega)$ is a finite extension of k, since any discrete k-valuation over a field extension of transcendence degree 1 over k is associated to some irreducible polynomial with coefficients in k. Since $\kappa(\omega) \subset k(s)$, this implies that $\kappa(\omega) = k$. It follows, by [4], Prop. 2, p. 327, that ω and υ has same value group, that is $(F,\upsilon)/(K,\omega)$ is unramified. In particular, we have

$$\partial_\upsilon(q) = \partial_\upsilon(q'_F) = \partial_\omega(q')_{\kappa(\upsilon)}.$$

Since $\partial_\omega(q') \in W(\kappa(\omega)) = W(k)$, we then get $\partial_{\upsilon'}(\partial_\upsilon(q)) = \partial_\omega(q')$, so we finally obtain the equality

$$\partial_{\upsilon'}(\partial_\upsilon(q))_{\kappa(\upsilon)} = \partial_\upsilon(q),$$

that is $\langle 1\rangle = \langle 1, 1+s^2\rangle$ in $W(k(s))$, which is a contradiction.

This shows that $\mathrm{ed}(\langle 1, s^2+1, t, t\rangle) = 2$ when -1 is not a square. It follows that $\mathrm{ed}(L_0) = 2$ and consequently $\mathrm{ed}_k(\mathbb{Z}/4) \geq 2$ in that case. This completes the proof of Theorem 7.6.

Remark 7.17. Most of the results of the present section were known to Buhler and Reichstein over an algebraically closed field of characteristic 0. Emphasis is given here to the computation of the essential dimension over arbitrary fields.

8. Homotopy invariance

In this section we shall prove the so-called *homotopy invariance* (that is $\mathrm{ed}_k(G) = \mathrm{ed}_{k(t)}(G)$) for algebraic groups defined over infinite fields. We first begin with some considerations on places of the form $k(t) \rightsquigarrow k$. Unadorned $\otimes$ will always mean $\otimes_k$.

Let k be any field, $a(t) \in k(t)$ and $\tau \in k$. We say that $a(t)$ is UNRAMIFIED at τ if $a(t) \in k[t]_{\mathfrak{m}_\tau}$ where $\mathfrak{m}_\tau$ denotes the maximal ideal $< t-\tau >$ of $k[t]$. When $a(t)$ is unramified at τ one can evaluate or specialize it at τ by simply replacing t by τ. Actually every $\tau \in k$ defines a pseudo k-place $k(t) \rightsquigarrow k$ denoted by $(\mathcal{O}_\tau, \alpha_\tau)$ where the local ring $\mathcal{O}_\tau$ is $k[t]_{\mathfrak{m}_\tau}$ and the morphism α_τ is the isomorphism $k[t]/\mathfrak{m}_\tau \simeq k$. Saying that $a(t)$ is unramified at τ is then the same than saying that $a(t)$ (viewed as an element of $\mathbf{F}(k(t))$ where $\mathbf{F}$ is the forgetful functor) is unramified in the place $(\mathcal{O}_\tau, \alpha_\tau)$ and $a(\tau)$ the specialization of $a(t)$ at τ is nothing but the image of $a(t)$ under the map

$$s_\tau : \mathcal{O}_\tau = k[t]_{\mathfrak{m}_\tau} \to k[t]_{\mathfrak{m}_\tau}/\mathfrak{m}_\tau \simeq k[t]/\mathfrak{m}_\tau \simeq k.$$

These considerations extend naturally to vector spaces as follows:

Definition 8.1. *Let A be a k-vector space (not necessarily finite dimensional). Let t be an indeterminate over k, and let $\tau \in k$. We say that an element $a(t) \in A \otimes k(t)$ is* UNRAMIFIED *at τ if $a \in A \otimes \mathcal{O}_\tau$. Let $s_\tau : \mathcal{O}_\tau \longrightarrow k$ be the above morphism.The* SPECIALIZATION *of $a(t)$, denoted by $a(\tau)$, is the image of $a(t)$ under the map $\mathrm{Id}_A \otimes s_\tau : A \otimes \mathcal{O}_\tau \to A \otimes k \simeq A$.*

Let $B \subset A$ be a k-subspace. Recall that the maps $B \otimes k(t) \to A \otimes k(t)$, $B \otimes \mathcal{O}_\tau \longrightarrow B \otimes k(t)$ etc are injective.

We need the following result:

Lemma 8.2. *Let $b(t) \in B \otimes k(t)$. Assume that $b(t)$, viewed as an element of $A \otimes k(t)$ is unramified at τ. Then $b(t)$, viewed as an element of $B \otimes k(t)$, is unramified at τ, and the two corresponding specializations coincide. In particular $b(\tau)$ is in B.*

Proof. This follows from the formula $(A \otimes \mathcal{O}_\tau) \cap (B \otimes k(t)) = B \otimes \mathcal{O}_\tau$.

We continue with some considerations on torsors. Let $X \longrightarrow Y$ be a G-torsor over k and let E/k be any field extension. Pulling back everything along

$\mathrm{Spec}(E) \to \mathrm{Spec}(k)$ one obtains $X_E \longrightarrow Y_E$ a G-torsor over E:

$$\begin{tikzcd}
X_E \arrow[r] \arrow[d] & X \arrow[d] \\
Y_E \arrow[r] \arrow[d] & Y \arrow[d] \\
\mathrm{Spec}(E) \arrow[r] & \mathrm{Spec}(k)
\end{tikzcd}$$

Now, for any field extension L/E and any G-torsor $T \to \mathrm{Spec}(L)$ there is a one-to-one correspondence between the set of L-rational points of Y having T as a fiber and the set of L-rational points of Y_E having T as a fiber. Indeed if $y : \mathrm{Spec}(L) \to Y$ is such a point, we have a diagram

$$\begin{tikzcd}
T \arrow[d] \arrow[dr, dashed] \arrow[drr, bend left] & & \\
\mathrm{Spec}(L) \arrow[dr, dashed] \arrow[drr, bend left=10, "y"] \arrow[ddr, bend right] & X_E \arrow[r] \arrow[d] & X \arrow[d] \\
& Y_E \arrow[r] \arrow[d] & Y \arrow[d] \\
& \mathrm{Spec}(E) \arrow[r] & \mathrm{Spec}(k)
\end{tikzcd}$$

by the universal property of the pull-backs involved.

From now on we will deal with $E = k(t)$ and we shall write $X(t) \longrightarrow Y(t)$ instead of $X_{k(t)} \longrightarrow Y_{k(t)}$.

Lemma 8.3. *Let $X \to Y$ be a classifying torsor over an infinite field k. Then the torsor $X(t) \to Y(t)$ is a classifying torsor over $k(t)$.*

Proof. First notice that one can suppose Y to be affine. Let now $L/k(t)$ be a field extension and $T \to \mathrm{Spec}(L)$ be any G-torsor. Let $Z \subset Y$ be the dense subset of Y such that for every $y : \mathrm{Spec}(L) \to Z$ the fiber of $X \to Y$ at y is T. Denote by $Z(t)$ the corresponding subset of $Y(t)$. We have to show that $Z(t)$ is dense. Write $Y = \mathrm{Spec}(A)$ for some k-algebra A. We have that $Y(t) = \mathrm{Spec}(A \otimes k(t))$ and the bijection between the sets Z and $Z(t)$ says that every point $\mathfrak{p}(t) \in Z(t)$ is of the form $\mathfrak{p} \otimes k(t)$ for exactely one $\mathfrak{p} \in Z$. Saying that $Z \subset Y$ is dense means that for every non-zero element f of A there exists $\mathfrak{p} \in Z$ such that $f \notin \mathfrak{p}$. Take $f(t) \in A \otimes k(t)$ a non-zero element and suppose that $Z(t)$ is not dense, that is $f(t) \in \mathfrak{p}(t)$ for all $\mathfrak{p}(t) \in Z(t)$. Since k is infinite one can find $\tau \in k$ such that $f(t)$ is unramified at τ and $f(\tau) \neq 0$. Now Lemma 8.2 tells that $f(\tau) \in \mathfrak{p}$ for all $\mathfrak{p} \in Z$ contradicting the fact that Z is dense in Y.

Theorem 8.4 (Homotopy invariance).
Let G be an algebraic group over an infinite field k. Then

$$\mathrm{ed}_k(G) = \mathrm{ed}_{k(t)}(G).$$

Proof. We only have to prove $\mathrm{ed}_k(G) \leq \mathrm{ed}_{k(t)}(G)$. Let $X \longrightarrow Y$ a classifying G-torsor over k with Y minimal for the dimension (that is $\dim(Y) = \mathrm{ed}_k(G)$). Pulling back everything along $\mathrm{Spec}(k(t))$ one obtains $X(t) \longrightarrow Y(t)$ which is again a classifying torsor in view of the preceeding lemma.

Suppose now that $\mathrm{ed}_{k(t)}(G) < \mathrm{ed}_k(G)$. This means that the torsor $X(t) \longrightarrow Y(t)$ can be further compressed over $k(t)$. That means that there exists a G-torsor $X' \longrightarrow Y'$ with $\dim\ Y' < \dim\ Y(t) = \dim\ Y$ fitting into a pull-back

$$\begin{tikzcd} X(t) \arrow[r] \arrow[d] & X' \arrow[d] \\ Y(t) \arrow[r] & Y' \end{tikzcd}$$

But now, one can find $\varphi \in k[t]$ such that the above pull-back is defined over $\mathrm{Spec}\big(k[t, \frac{1}{\varphi}]\big)$. Now take $\xi : \mathrm{Spec}(k) \to \mathrm{Spec}\big(k[t, \frac{1}{\varphi}]\big)$ a k-rational point. Such a point exists since k is infinite. Now Y'_ξ, the fiber of Y' over ξ, is closed in Y' and thus satisfies $\dim\ Y'_\xi \leq \dim\ Y'$. Pulling back the above square along ξ one has

$$\begin{tikzcd} X(t)_\xi \arrow[r] \arrow[d] & X'_\xi \arrow[d] \\ Y(t)_\xi \arrow[r] & Y'_\xi \end{tikzcd}$$

But $X(t)_\xi \simeq X$, so the torsor $X \longrightarrow Y$ can be compressed into a torsor $X'_\xi \longrightarrow Y'_\xi$ with $\dim\ Y'_\xi \leq \dim\ Y' < \dim\ Y$ contradicting the minimality of Y.

For the moment we do not know if homotopy invariance holds for finite fields.

Remark 8.5. To our knowledge the homotopy invariance is a new result.

References

[1] J. Arason, *Cohomologische Invarianten quadratischer Formen.* J. of Algebra 36 (1975), 446–491

[2] A.–M. Bergé, J. Martinet, *Formes quadratiques et extensions en caractéristique 2.* Ann. Inst. Fourier (2), 35 (1985) 57–77

[3] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group.* Comp. Math. 106 (1997), 159–179

[4] P.M. Cohn, *Algebra, vol. 2.* John Wiley & Sons Ed., London (1977)

[5] A. Delzant, *Définition des classes de Stiefel-Whitney d'un module quadratique sur un corps de caractéristique différente de* 2. C.R Acad. Sci. Paris 255 (1962), 1366–1368

[6] M. Demazure, P. Gabriel, *Groupes algébriques, vol. 1.* Ed. Masson & Cie (1970)

[7] M. Demazure, A. Grothendieck, *Schémas en groupes vol. 1.* SGA 3, Springer-Verlag (1970)

[8] C. Drees, M. Epkenhans, M. Krüskemper, *Computation of the trace form of Galois extensions.* J. of Algebra 192 (1997), 209–234

[9] R. Garibaldi, A. Merkurjev, J.-P. Serre, *Cohomological invariants in Galois cohomology.* AMS University Lecture Series 28 (2003)

[10] C Jensen, A Ledet, N Yui, *Generic Polynomials* MSRI Publ. 45, Cambridge University Press (2002)

[11] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions.* AMS Coll. Pub. 44 (1998)

[12] A. Merkurjev, *Essential dimension.* Private notes (1999), Lecture notes (2000)

[13] J.S. Milne, *Étale Cohomology.* Princeton Math. Series 33, Princeton University Press, Princeton, N.J. (1980)

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

[15] M. Rosenlicht, *Some basic theorems on algebraic groups.* American J. of Math. 78 (1963), 401–443

[16] M. Rost, *Computation of some essential dimensions.* Preprint (2000). Available on http://www.math.ohio-state.edu/˜rost/ed.html

[17] M. Rost, *Essential dimension of twisted* C_4. Preprint (2000). Available on http://www.math.ohio-state.edu/˜rost/ed.html

[18] W. Scharlau, *Quadratic and hermitian forms.* Grund. Math. Wiss. 270, Springer-Verlag, Berlin-Heidelberg (1985)

[19] J.-P. Serre, *Cohomologie Galoisienne.* Cinquième éd. Lecture Notes 5, Springer-Verlag (1997)

[20] J.-P. Serre, *Corps locaux.* Hermann, Paris (1962)

[21] J.-P. Serre, *Topics in Galois Theory.* Research notes in Math. 1, Jones and Bartlett Pib., Boston, MA (1992)

[22] R. W. Thomason, *Comparison of equivariant algebraic and topological K-theory.* Duke Math. J. 53, No 3, (1986), 795–825

[23] W. C. Waterhouse. *Introduction to Affine Group Schemes.* GTM 66, Springer-Verlag (1979)

Grégory Berhuy
University of British Columbia
Department of Mathematics
1984 Mathematics Road
V6T 1Z2 Vancouver BC, Canada
berhuy@math.ubc.ca

Giordano Favi
Université de Lausanne
IMA-Dorigny
CH-1015 Lausanne Switzerland
giordano.favi@ima.unil.ch
giordano.favi@epfl.ch