Tori and essential dimension

Giordano Favi, Mathieu Florence

March 2007

Abstract. The present paper deals with algebraic tori and essential dimension in three unrelated contexts. After some preliminaries on essential dimension, versal torsors and tori, we explicitly construct a versal torsor for $\mathbf{PGL}_n$, $n \geq 5$ odd, defined over a field of transcendence degree $\frac{1}{2}(n-1)(n-2)$ over the base field. This recovers a result of Lorenz, Reichstein, Rowen and Saltman (found in [12]). We also discuss the so called "tori method" which gives a geometric proof of a result of Ledet on the essential dimension of a cyclic p-group (see [8, 9]). In the last section we compute the essential dimension of the functor $K \mapsto H^1(K, \mathbf{GL}_n(\mathbb{Z}))$, the latter set being in bijection with the isomorphism classes of n-dimensional K-tori.

Keywords and Phrases: Essential dimension, tori, versal torsors.

Introduction

The notion of essential dimension has been first defined by Buhler and Reichstein in [6] for finite groups and by Reichstein in [17] for algebraic groups. Since then many authors attempted to compute this number for specific algebraic groups. In this paper we are mainly concerned with upper bounds. The best known upper bounds for many algebraic groups have been performed by considering group actions on certain *lattices*. This can be seen in the work of Ledet ([8]), Lemire ([10]), and the joint work by Lorenz, Reichstein, Rowen and Saltman ([12]).

A portion of this paper is dedicated to a more geometrical approach to these results using the language of tori. This is not surprising since tori are dual to lattices, however, this has the advantage of treating geometric and arithmetic settings in a unified way. We discuss and reobtain here the result on the essential dimension of $\mathbf{PGL}_n$, for $n \geq 5$ odd, namely

$$\mathrm{ed}_k(\mathbf{PGL}_n) \leq \frac{(n-1)(n-2)}{2}$$

which was obtained in [12]. We also recover the inequality

$$\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/p^n\mathbb{Z}) \leq \varphi(p-1)p^{n-1}$$

where p is an odd prime (first proven in [9], see also [8], Proposition 8.3.5).

The last part of the paper is devoted to the computation of $\mathrm{ed}_k(\mathbf{GL}_n(\mathbb{Z}))$ and $\mathrm{ed}_k(\mathbf{SL}_n(\mathbb{Z}))$. It is well-known that $H^1(K, \mathbf{GL}_n(\mathbb{Z}))$ classifies n-dimensional K-tori up to isomorphism, hence we compute essential dimension of tori viewed as forms of $\mathbb{G}_m^n$. Note also that there is no versal torsor for $\mathbf{GL}_n(\mathbb{Z})$ and thus the standard techniques of essential dimension do not apply in this case.

In the following k will denote an arbitrary ground field. By a k-variety we mean a reduced separated scheme of finite type over k. An *algebraic group* is a group scheme over k which is smooth and of finite type.

Contents

1. Preliminaries on actions, torsors and essential dimension

Let G be a group scheme over a scheme S and let X be an S-scheme. A *(right) action* of G on X is a morphism of S-schemes

$$G \times_S X \longrightarrow X$$

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

which satisfy the categorical conditions of a usual (right) group 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. We 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 $X(T)$. If there exists a *dense* open G-invariant subset U of X such that G acts freely on U, we say that the action of G is *generically free*. Recall also that an action is said to be faithful if the induced map $G \to \mathrm{Aut}(X)$ is injective.

Lemma 1.1. *Let A be a finite algebraic group over a field k acting on a geometrically irreducible k-variety X. Then the action of A is generically free if and only if it is faithful.*

Proof. The implication $\Rightarrow$ is obvious and holds for any group A, not necessarly finite. Suppose that the action of A on X is faithful. To check that there exists an open set on which A acts freely is enough to find a point $x \in X$ such that A acts trivially on it since the subset of such points is open in X. We can thus suppose k algebraically closed. For any non identity element $a \in A(k)$, let X_a be the closed subvariety of X consisting of a-invariant elements. The X_a form a finite family of proper subvarieties of the irreducible variety X, hence their union cannot be the total space. □

Lemma 1.2. *Let G be a connected algebraic k-group, H a closed subgroup of G and A a finite k-group, acting on G by group automorphisms (say, on the left), and fixing H. Then, the action of $H \rtimes A$ on G is generically free if and only the action of A on $H\backslash G$ is faithful.*

Proof. It follows from the fact that $H \rtimes A$ acts generically freely on G if and only if A acts generically freely on $H\backslash G$ and from Lemma 1.1. □

In the sequel we will consider a base scheme S and we will deal with the finitely presented faithfully flat[1] topology on the category $\mathbf{Sch}/S$ of schemes over S.

Definition 1.3. *Let G be a fppf group scheme over Y. We say that a morphism of schemes $X \to Y$ is a G-*torsor over Y *if G acts on X, the morphism $X \to Y$ is fppf, 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 fppf topology on Y such that $X \times_Y U_i$ is isomorphic to $G \times_Y U_i$ for each i (see [14], Chapter III, Proposition 4.1). This means that X is locally isomorphic to G for the fppf 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.

The following concerns categorical quotients. More material on this subject can be found in [16] and [1]. 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 *versal 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 (see [1] Exposé V, Théorème 8.1) which asserts the existence of a versal quotient which is also a G-torsor.

Theorem 1.4. *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.

Definition 1.5. *Let G act on X. An open subscheme U which satisfies the conclusion of the above theorem will be called a* friendly *open subset of X.*

[1] fppf in the sequel according to the french tradition.

The important definition below is due to Merkurjev (see [13]) and can be found in [2] Definition 6.1 or [7].

Definition 1.6. *Let k be a field, G be a linear algebraic group k and Y a k-scheme of finite type. A G-torsor $f : X \longrightarrow Y$ over Y is called* versal for G *(or* classifying*) if, for every extension k'/k, with k' infinite, and for every G-torsor $P' \longrightarrow \mathrm{Spec}(k')$, the set of points $y \in Y(k')$ such that $P' \simeq f^{-1}(y)$ is dense in Y.*

Remark 1.7. Such a torsor always exists : Indeed embed G in $S = \mathbf{GL}_n$ for n big enough. Then the exact sequence $1 \to G \to S \to S/G \to 1$ gives, for all k'/k, an exact sequence of pointed sets

$$G(k') \to S(k') \to S/G(k') \to H^1(k', G) \to 1.$$

The application $\partial : S/G(k') \to H^1(k', G)$ is given by taking the fiber of $S \to S/G$ at a k'-rational point of S/G. Thus any G-torsor over $\mathrm{Spec}(k')$ is isomorphic to the fiber of a point $y \in S/G(k')$. Moreover if $y', y \in S/G(k')$ are in the same $S(k')$-orbit, then $f^{-1}(y) = f^{-1}(y')$. If k' is infinite, $S(k')$ is dense in S and so is the $S(k')$-orbit of y in S/G.

The above remark is well known and can be found in [13] or [7] Example 5.4.

Definition 1.8. *Let G be a linear algebraic group over k. The smallest dimension* $\dim(Y)$ *of a versal G-torsor $X \longrightarrow Y$ is called the* essential dimension of G*.*

Definition 1.9. *Let $f : X \to Y$ and $f' : X' \to Y'$ two G-torsors. We say that f' is a* compression *of f if there is a commutative diagram*

$$\begin{array}{ccc} X & \overset{g}{\dashrightarrow} & X' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ Y & \underset{h}{\dashrightarrow} & Y' \end{array}$$

where g and h are G-equivariant, rational, dominant morphisms.

Lemma 1.10. *If $f : X \to Y$ is a versal G-torsor then so is any compression of f.*

Proof. See [2] Lemma 6.13. □

We would like to state a proposition that ensures the existence of versal torsors of "small" dimension, under certain conditions. We first need a general lemma which is better stated in a wider background.

Let $G \to S$ be a fppf group scheme. As before we consider the finitely presented faithfully flat topology (fppf-topology) on the category $\mathbf{Sch}/S$ of schemes over S. If $X \longrightarrow S$ is a S-scheme we will still denote by X the fppf-sheaf represented by X, that is the sheaf which sends $Y \longrightarrow S$ to $\mathrm{Hom}_S(Y, X)$. In this setting a (left) G-torsor is a fppf-sheaf $P : \mathbf{Sch}/S \to \mathbf{Sets}$, endowed with a (left) G-action, such that, locally for the fppf-topology, this sheaf is G-isomorphic to G itself. In particular, in this definition, we do not worry about torsors to be representable. However the usual properties of torsors hold, for example $P \simeq G$ if and only if P has an S-point. If $s : S' \longrightarrow S$ is a morphism of schemes there is the pullback functor s^* which sends G-torsors to $G \times_S S'$-torsors as usual. For the notions below and more about (bi)torsors in a general setting, see [4].

For a right G-torsor P and a left G-torsor Q, one defines the *contracted product* $P \overset{G}{\wedge} Q$ to be the sheaf associated to the presheaf defined by

$$T \mapsto (P(T) \times Q(T))/\{(xg, y) = (x, gy), g \in G(T)\}$$

for any S-scheme T. For any right G-torsor P we define its *opposite* (denoted by P^{o}) to be the left G-torsor where the action is given by $g * p = pg^{-1}$. For any right G-torsor P we have the following simple rules: $P \overset{G}{\wedge} P^{\mathrm{o}} \simeq G$ and $P \overset{G}{\wedge} G \simeq P$. Moreover, for any morphism $s : S' \to S$ one has $s^*(P \overset{G}{\wedge} Q) \simeq s^*(P) \overset{s^*(G)}{\wedge} s^*(Q)$.

Lemma 1.11. *Let S be a scheme and $G \to S$ be a faithfully flat group scheme of finite presentation over S. Let $f : S' \to S$ be a morphism of schemes. For any S-scheme T, let $T' = T \times_S S'$. Assume we are given a G-torsor $P \longrightarrow S$ and a G'-torsor $Q \longrightarrow S'$. Assume there exists a section $s : S \to S'$ of f. Then, P is G-isomorphic to $s^*(Q)$ if and only if the contracted product $Q \overset{G'}{\wedge} P'^{\mathrm{o}}$ has an $S \xrightarrow{s} S'$-point.*

Proof. We know that P is G-isomorphic to $s^*(Q)$ if and only if

$$(s^*(Q) \overset{G}{\wedge} P^{\mathrm{o}})(S) \neq \varnothing.$$

On the other hand, to say that $Q \overset{G'}{\wedge} P'^{\mathrm{o}}$ has an $S \xrightarrow{s} S'$-point is equivalent to saying that $s^*(Q \overset{G'}{\wedge} P'^{\mathrm{o}})$ has an S-point. But the S-sheaf $s^*(Q \overset{G'}{\wedge} P'^{\mathrm{o}})$ is canonically isomorphic to $s^*(Q) \overset{G}{\wedge} P^{\mathrm{o}}$, whence the claim. □

If now $G \to S$ acts on the left on some S-scheme X, for any (right) G-torsor P as above one can define the *twist* of X by P to be the fppf-sheaf associated to the presheaf

$$T \mapsto (P(T) \times X(T))/\{(pg, x) = (p, gx), g \in G(T)\}.$$

This will be denoted by ${}^P X$. Even in the case where $S = \mathrm{Spec}(k)$ and even if both P and X are representable this sheaf might not be representable. However, in the case where X is a quasi-projective k-variety and when P is a usual (representable) G-torsor, it is well-known that ${}^P X$ is representable by a k-variety (see [21] Chap. I, §3.1 for example).

Proposition 1.12. *Let k be a field and G be a linear algebraic group over k. Assume we are given a quasi-projective k-variety X, together with a generically free action of G on X. Suppose further that, for every extension k' of k with k' infinite, and for every G-torsor P over k', the twist of $X \times_k k'$ by P has a dense subset of k'-rational points. Let U be a friendly open subset of X for the action of G. Then the G-torsor $U \longrightarrow U/G$ is versal.*

Proof. This is an easy consequence of Lemma 1.11. Indeed, let k'/k be a field extension with k' infinite. Let $U' = U \times_k k'$. Let P be a G-torsor over k'. We apply the lemma to the case $S = \mathrm{Spec}(k')$, $S' = U'/G$ and $Q = U'$. Let V' be the twist of U' by P^{o}. The lemma tells us that, for any point $v \in V'(k')$, the pullback of the G-torsor $U' \longrightarrow U'/G$ by the image of v in $(U'/G)(k')$ is isomorphic to P. According to the hypothesis, there is a dense set of such points in $(U'/G)(k')$, which concludes the proof. □

Corollary 1.13. *The notations and hypothesis being those of Proposition 1.12, the torsor $U \longrightarrow U/G$ is versal if one of the following holds:*

i) *X is an affine space on which G acts linearly (this is well-known, see* [2] *Proposition 4.11 for example),*

ii) *X is a reductive linear algebraic group and $G = Y \rtimes H$ is the semi-direct product of an algebraic k-group H, acting by group automorphisms on X, by an H-invariant subgroup Y of X, acting on X by left translations, such that the following holds: for each field extension k'/k with k' infinite, and for each H-torsor P over k', if we denote by $\widetilde{Y}$ and $\widetilde{X}$ the respective twists of $Y \times_k k'$ and $X \times_k k'$ by P, the map $H^1(k', \widetilde{Y}) \mapsto H^1(k', \widetilde{X})$ is trivial.*

Proof. Case i) simply follows from Hilbert's Theorem 90 for $\mathbf{GL}_n$. To see ii) let k'/k be a field extension with k' infinite and let P/k' be a G-torsor. We would like to describe $\widehat{X}$, the twist of $X \times_k k'$ by P. It is obtained as follows. Let $G \xrightarrow{\pi} H$ be the natural projection, and s its canonical section. Consider the G-torsor $Q = (s \circ \pi)_*(P)$ (change of group). Its is immediate that $\pi_*(P)$ and $\pi_*(Q)$ are canonically isomorphic H-torsors. Let $\widetilde{Y}$ be the (outer) twist of $Y \times_k k'$ by Q. Then, there exists a $\widetilde{Y}$-torsor R such that P is G-isomorphic to $R \overset{\widetilde{Y}}{\wedge} Q$. Hence, by associativity of the twist, $\widehat{X}$ is obtained by first twisting X over G with Q (the result being a *group* $\widetilde{X}$), and then twisting $\widetilde{X}$ over $\widetilde{Y}$ with R. But by assumption, this last twist is isomorphic to $\widetilde{X}$ itself, and hence $\widehat{X} \simeq \widetilde{X}$ is a reductive group, with a dense set of k'-rational points, by [20] Corollary 13.3.9. □

We also recall here Merkurjev's definition of essential dimension which will be used in section 5.

Let k be a field. We denote by $\mathfrak{C}_k$ the category of field extensions of k. We will consider *covariant* functors $\mathbf{F} : \mathfrak{C}_k \to \mathbf{Sets}$ from $\mathfrak{C}_k$ to the category of sets.

Definition 1.14. *Let $\mathbf{F} : \mathfrak{C}_k \to \mathbf{Sets}$ be a covariant functor, 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 $\mathrm{ed}(a) \leq n$) if there exists a subextension E/k of K/k such that:*

i) *the transcendence degree of E/k is $\leq n$,*

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

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

Lemma 1.15. *For an algebraic group G defined over k, the essential dimension of the Galois cohomology functor $K \mapsto H^1(K, G)$ is equal to $\mathrm{ed}_k(G)$ as defined in Definition 1.8.*

Proof. See [2] Corollary 6.16. □

For a more detailed account on the notion of essential dimension of algebraic groups see for instance [2, 6, 13] or [17, 18].

2. Preliminaries on tori

Let G be any algebraic group over k. We will denote by G^* its character module and by G_* its cocharacter set. Recall that G^* is defined as

$$G^* = \mathrm{Hom}_{k_s}(G_{k_s}, \mathbb{G}_{\mathrm{m},k_s}),$$

where k_s denotes a separable closure of k. We will denote by Γ_k (or simply Γ) the absolute Galois group of k. There is a standard Γ-action on G^* and every character module will always be considered as a (continuous) Γ-module. Similarly G_* is defined as $G_* = \mathrm{Hom}_{k_s}(\mathbb{G}_{\mathrm{m},k_s}, G_{k_s})$ and will also be viewed as a Γ-set. When G is abelian G_* has a Γ-module structure as well.

Recall that an algebraic group T over k is called a *k-torus* if $T_{k_s} \simeq \mathbb{G}^n_{\mathrm{m},k_s}$ for some integer n. There is a well-known correspondence between k-tori and $\mathbb{Z}$-free continuous Γ_k-modules of finite rank (see [3]):

Theorem 2.1. *The correspondence $T \mapsto T^*$ establishes an anti-equivalence between the category of k-tori and the category of $\mathbb{Z}$-free continuous Γ_k-modules of finite rank. If M is such a module the corresponding torus is given by* $\mathrm{Spec}(A)$ *where $A = k_s[M]^{\Gamma_k}$. Moreover an exact sequence of k-tori*

$$1 \to T_1 \to T_2 \to T_3 \to 1$$

is exact if and only if the sequence of character modules

$$1 \to T_3^* \to T_2^* \to T_1^* \to 1$$

is exact.

For any algebraic group there is the well-known pairing $G_* \times G^* \to \mathbb{Z}$ given by composition

$$\mathrm{Hom}_{k_s}(\mathbb{G}_{\mathrm{m},k_s}, G_{k_s}) \times \mathrm{Hom}_{k_s}(G_{k_s}, \mathbb{G}_{\mathrm{m},k_s}) \to \mathrm{Hom}_{k_s}(\mathbb{G}_{\mathrm{m},k_s}, \mathbb{G}_{\mathrm{m},k_s}) \simeq \mathbb{Z}$$

which gives a duality between characters and cocharacters of k-tori. In particular, the statement of the above theorem holds also for cocharacter modules.

If T is a torus with character module T^* the torus those character module is $\bigwedge^k T^*$ will be denoted by $\bigwedge^k T$.
For any commutative finite dimensional k-algebra A and for an algebraic group G over A there is the so-called *Weil restriction* which is an algebraic group over k denoted by $\mathbf{R}_{A/k}(G)$. Recall that, by definition, for a commutative k-algebra R one has $\mathbf{R}_{A/k}(G)(R) = G(R \otimes_k A)$ and that the equality

$$H^1(A, G) = H^1(k, \mathbf{R}_{A/k}(G))$$

holds when A is *étale* (and for higher cohomology groups). One sees that if H is any subgroup of $\mathrm{Aut}_{k-alg}(A)$, then H acts on both A and $\mathbf{R}_{A/k}(G)$. For a finite dimensional étale algebra the group $\mathbf{R}_{A/k}(\mathbb{G}_m)$ is a k-torus. Tori of this kind are called *quasi-trivial*. They have trivial cohomology and moreover they correspond to so-called *permutation* modules, that is their character module has a $\mathbb{Z}$-basis which is permuted by the Galois group Γ_k.

Lemma 2.2.

(1) *Let T be a k-torus, G be an algebraic group over k acting on T and P any G-torsor over k. Then for any integer $n \geq 0$ one has ${}^P(\bigwedge^n T) \simeq \bigwedge^n({}^P T)$.*

(2) *Let A be a finite dimensional étale k-algebra and G be a subgroup of* $\mathrm{Aut}_{k-alg}(A)$. *Then for any G-torsor P over k the twist of $\mathbf{R}_{A/k}(\mathbb{G}_m)$ by P is isomorphic to $\mathbf{R}_{A'/k}(\mathbb{G}_m)$ where A' is the k-algebra obtained by twisting A by P.*

Proof. Left to the reader. □

3. A versal torsor for $\mathbf{PGL}_n$, $n \geq 5$ odd

In this section, for n odd, we construct explicitely a versal $\mathbf{PGL}_n$-torsor which is defined over a field of transcendence degree $\frac{1}{2}(n-1)(n-2)$ over the ground field. The proof of the versality of such torsor relies on Corollary 1.13 *ii*) and is of a cohomological nature. The cohomology groups involved are that of some specific tori. As a corollary, we recover a result due to Lorenz, Rowen, Reichstein and Saltman (see [12] and also [11] Theorem 1.1). The torsors constructed here arise from the same lattices considered in [11] but their versality is established in a different way. To begin with, let us introduce some notations.

Let X be a finite set of cardinality n. Denote by $\mathbf{PGL}_X$ the group $\mathbf{PGL}(k^X)$. Let T_X be the diagonal maximal torus of $\mathbf{PGL}_X$ (with cocharacter module canonically isomorphic to $\mathbb{Z}^X/\mathbb{Z}$); its normalizer is the group $N_X = T_X \rtimes \mathfrak{S}_X$, where $\mathfrak{S}_X$ is the symmetric group of X. It is well-known that the map

$$H^1(K, N_X) \longrightarrow H^1(K, PGL_X)$$

is surjective for any K (this hold for any reductive group G, and follows from the existence of maximal K-tori in every inner twist of G, cf. [19], III.4, Lemme 6). Thus, in order to find a versal torsor for $\mathbf{PGL}_X$, it is enough to find one for N_X. Recall that we have the canonical Koszul complex (more precisely, its dual)

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}^X \longrightarrow \bigwedge^2 \mathbb{Z}^X \longrightarrow \cdots \longrightarrow \bigwedge^n \mathbb{Z}^X \longrightarrow 0,$$

where the maps are just given by wedging (say, on the right) by $\sum_{x\in X} x$. In particular, for any action of a group G on X, this complex is G-equivariant. Let us cut the first part of this complex in two short exact sequences

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}^X \longrightarrow (T_X)_* \longrightarrow 0$$

and

$$0 \longrightarrow (T_X)_* \longrightarrow \bigwedge^2 \mathbb{Z}^X \longrightarrow Q_X \longrightarrow 0.$$

Let R_X be the k-torus with cocharacter module Q_X and let S_X the k-torus with cocharacter module $\bigwedge^2 \mathbb{Z}^X$; i.e. $R_X = \mathrm{Spec}(k[Q_X])$ and $S_X = \mathrm{Spec}(k[\bigwedge^2 \mathbb{Z}^X])$. The last exact sequence gives a canonical sequence of k-tori

$$1 \longrightarrow T_X \longrightarrow S_X \longrightarrow R_X \longrightarrow 1.$$

Theorem 3.1. *Assume $n \geq 5$ is odd. Then, the natural action of N_X on S_X is generically free, and gives rise to a versal torsor for N_X.*

Proof. Let us check the first claim. By Lemma 1.2, it suffices to see that the action of $\mathfrak{S}_X$ on R_X is faithful. But the character module of R_X is just the kernel of the map

$$\bigwedge^2 \mathbb{Z}^X \longrightarrow \mathbb{Z}^X,$$

$$x \wedge y \longmapsto x - y.$$

Assume $\sigma \in \mathfrak{S}_X$ acts trivially on this kernel. Then, let $x, y, z \in X$ be three distinct elements. The element $x \wedge y + y \wedge z + z \wedge x$ (which lies in the kernel) must be σ-invariant. Hence, σ permutes x, y, z, for any choice of those three elements. But if $n \geq 4$, it is easily seen that this implies that σ is the identity. Thus, there exists $U \subset S_X$ a friendly open subset (for the action of N_X). To see that the torsor $U \longrightarrow U/N_X$ is versal, we use Corollary 1.13. We have to see that, for any field extension K/k, and for any $\mathfrak{S}_X$-torsor P, the map

$$H^1(K, {}^P T_X) \longrightarrow H^1(K, {}^P S_X)$$

is zero. Let L/K be the étale algebra obtained by twisting K^X by P. Then, the torus ${}^P T_X$ is nothing else than $\mathbf{R}_{L/K}(\mathbb{G}_m)/\mathbb{G}_m$ by Lemma 2.2. In the same way ${}^P S_X \simeq \bigwedge^2 \mathbf{R}_{L/K}(\mathbb{G}_m)$. Furthermore, by considering the exact cohomology sequence associated to the short exact sequence

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathbf{R}_{L/K}(\mathbb{G}_m) \longrightarrow \mathbf{R}_{L/K}(\mathbb{G}_m)/\mathbb{G}_m \longrightarrow 1,$$

we find that $H^1(K, \mathbf{R}_{L/K}(\mathbb{G}_m)/\mathbb{G}_m) = \ker(\mathrm{Br}(K) \longrightarrow \mathrm{Br}(L))$. This implies, by the standard restriction-corestriction argument, that $H^1(K, \mathbf{R}_{L/K}(\mathbb{G}_m)/\mathbb{G}_m)$ is killed by n. Because n is odd, to prove that the map

$$H^1(K, \mathbf{R}_{L/K}(\mathbb{G}_m)/\mathbb{G}_m) \longrightarrow H^1(K, \bigwedge^2 \mathbf{R}_{L/K}(\mathbb{G}_m))$$

is zero, it is enough to show that the group on the right is killed by 2. This is seen as follows. Consider the injection

$$i : \bigwedge^2 \mathbb{Z}^X \longrightarrow \mathbb{Z}^{X^2}.$$

$$x \wedge y \longmapsto (x, y) - (y, x)$$

Define $r : \mathbb{Z}^{X^2} \longrightarrow \bigwedge^2 \mathbb{Z}^X$ by $r((x, y)) = x \wedge y$. We have $r \circ i = 2\,\mathrm{Id}$. Viewing $\mathbb{Z}^{X^2}$ as the cocharacter module of $\mathbf{R}_{L \otimes_K L/K}(\mathbb{G}_m)$, we can see i as an injection $1 \longrightarrow \bigwedge^2 \mathbf{R}_{L/K}(\mathbb{G}_m) \longrightarrow \mathbf{R}_{L \otimes_K L/K}(\mathbb{G}_m)$. The composite

$$r \circ i : \bigwedge^2 \mathbf{R}_{L/K}(\mathbb{G}_m) \longrightarrow \bigwedge^2 \mathbf{R}_{L/K}(\mathbb{G}_m)$$

is multiplication by 2, and induces the trivial map on the H^1 level, because of Hilbert's Theorem 90 applied to $\mathbf{R}_{L \otimes_K L/K}(\mathbb{G}_m)$. This finishes the proof. □

Corollary 3.2 (see [12], Theorem 1.1). *Assume $n \geq 5$ is odd. Then,*

$$\mathrm{ed}_k(\mathbf{PGL}_n) \leq \frac{(n-1)(n-2)}{2}.$$

Proof. This follows from the fact that $\dim(R_X) = \frac{(n-1)(n-2)}{2}$, which is an easy calculation left to the reader. □

4. The "tori method" for cyclic groups

In this section, we give a geometric proof of a result originally due to Ledet (see [9]) which can also be found in [8] Theorem 8.3.1. The proof of the case $r = 1$ of the theorem below was communicated to us by J.-P. Serre and goes back to a result of Lenstra. We also owe him the terminology "tori method".

Theorem 4.1 (see [8] Theorem 8.3.1). *Let k be a field, $p > 2$ a prime number and r a positive integer. Assume p is not the characteristic of k. Let l/k be the field generated by p^r-th roots of unity, and G its Galois group, of order $t = p^d q$, where q divides $p-1$. We then have*

$$\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z} \rtimes G) \leq \varphi(q)p^d.$$

Proof. Choose a primitive p^r-th root of unity ξ, which enables us to identify μ_{p^r} with $\mathbb{Z}/p^r\mathbb{Z}$. Choose also a generator g of the cyclic group G. Consider the torus $T = \mathbf{R}_{l/k}(\mathbb{G}_m)$. Its character module is isomorphic to $\mathbb{Z}[X]/(X^t - 1)$, where g acts by multiplication by X. We have an obvious action of $\mathbb{Z}/p^r\mathbb{Z} \rtimes G$ on T. We will see later that this action is generically free. For a field extension k'/k, the twist of $T \times_k k'$ by a G-torsor P is just $\mathbf{R}_{l'/k'}(\mathbb{G}_m)$, where l'/k' is the G-Galois étale k'-algebra obtained by twisting $l \otimes_k k'$ by P. Hence this twist is a quasi-trivial torus with trivial H^1 according to Hilbert's Theorem 90. We therefore see that the hypothesis of Corollary 1.13 *ii*) hold. Thus, if $U \subset T$ is a friendly open subset for the action of $\mathbb{Z}/p^r\mathbb{Z} \rtimes G$ on T; the $\mathbb{Z}/p^r\mathbb{Z} \rtimes G$-torsor

$$U \longrightarrow U/(\mathbb{Z}/p^r\mathbb{Z} \rtimes G)$$

is versal. We will find a compression of this torsor. To do this, define

$$\Psi(X) = \prod_{i=0}^{d} \Phi_{p^i q}(X),$$

where $\Phi_n(X)$ is the n-th cyclotomic polynomial, and consider the k-torus T' with character module $\mathbb{Z}[X]/\Psi(X)$. As before, the action of g on this module is just multiplication by X. The natural injection

$$\mathbb{Z}[X]/\Psi(X) \longrightarrow \mathbb{Z}[X]/(X^t - 1)$$

which is multiplication by $(X^t - 1)/\Psi(X)$, gives a surjection $T \longrightarrow T'$. To finish the proof, it remains to show that the action of $\mathbb{Z}/p^r\mathbb{Z} \rtimes G$ on T' (and hence on T) is generically free. We first check that the composite map $\mathbb{Z}/p^r\mathbb{Z} \longrightarrow T \longrightarrow T'$ is injective. Denote by α the element of $(\mathbb{Z}/p^r\mathbb{Z})^*$ such that the action of g on $\mathbb{Z}/p^r\mathbb{Z}$ is given by multiplication by α. At the level of characters, we have to see that the map

$$\mathbb{Z}[X]/\Psi(X) \longrightarrow \mathbb{Z}/p^r\mathbb{Z},$$

given by $1 \mapsto ((X^t - 1)/\Psi(X))(\alpha)$, is a surjection. Let β be the image of α in $\mathbb{Z}/p\mathbb{Z}$ via the natural map $\mathbb{Z}/p^r\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$; this is an element of multiplicative order q. It remains to check that β is not a root (in $\mathbb{Z}/p\mathbb{Z}$) of the polynomial

$$(X^t - 1)/\Psi(X) = \prod_{i,u} \Phi_{p^i u}(X),$$

where i ranges from 0 to d and u ranges over the divisors of q distinct from q itself. But in $\mathbb{Z}/p\mathbb{Z}$, we have

$$\Phi_{p^i u}(X) = \prod_{\lambda} (X - \lambda)^{\varphi(p^i)},$$

where λ ranges over the elements of $\mathbb{Z}/p\mathbb{Z}$ of order u. Therefore β, being of order q, is not a root of $(X^t - 1)/\Psi(X)$. This proves that the map $\mathbb{Z}/p^r\mathbb{Z} \longrightarrow T'$ is indeed an injection. We check that the action of $\mathbb{Z}/p^r\mathbb{Z} \rtimes G$ on T' is generically free using Lemma 1.2, that is we only have to check that G acts faithfully on $T'/(\mathbb{Z}/p^r\mathbb{Z})$. We first show that the action of G is faithful on T' and reduce to this case. If the G-action on T' was not faithful, then $\Psi(X)$ (and hence $\Phi_t(X)$) would divide $X^u - 1$ for some divisor u of t distinct from t itself, which does not hold. Suppose now that there is $\gamma \in G$ such that $\gamma x = \xi_x x$ for all $x \in T'$, where ξ_x is a p^r-th root of unity. For a p^r-th root of unity ξ let X_ξ be the closed subvariety of T' defined by

$$X_\xi = \{x \in T' \mid \gamma x = \xi x\}.$$

Since T' is irreducible and since the finite union of X_ξ covers T', there exists ξ such that $X_\xi = T'$. But taking $x = 1$ this gives $\xi = 1$ and it contradicts the fact that the action of G on T' is faithful. We have thus proved that the action of $\mathbb{Z}/p^r\mathbb{Z} \rtimes G$ on T' gives rise to a versal torsor; we therefore have

$$\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z} \rtimes G) \leq \dim T' = \deg \Psi = \varphi(q) + \sum_{i=1}^{d} \varphi(q)(p^i - p^{i-1}) = \varphi(q)p^d.$$

□

5. The essential dimension of $\mathbf{GL}_n(\mathbb{Z})$

In this section, we compute the essential dimension of the functor

$$K \mapsto H^1(K, \mathbf{GL}_n(\mathbb{Z})).$$

Recall that $H^1(k, \mathbf{GL}_n(\mathbb{Z}))$ classifies the isomorphism classes of n-dimensional k-tori. In a similar way $H^1(k, \mathbf{SL}_n(\mathbb{Z}))$ classifies isomorphisms classes of pairs (T, ϕ) where T is an n-dimensional k-torus and ϕ is an isomorphism $\bigwedge^n T \to \mathbb{G}_m$. Let K/k be a field extension. In this section, by the essential dimension (over k) of a K-torus T, we understand the essential dimension of the class of T in $H^1(K, \mathbf{GL}_{\dim T}(\mathbb{Z}))$ as defined in Section 1, Definition 1.14. This number will be denoted by $\mathrm{ed}([T])$ where $[T]$ denotes the isomorphism class of the torus T. Unfolding the definition, $\mathrm{ed}([T])$ is the minimal transcendance degree over k of an intermediate extension $K/K'/k$ such that there exists a K'-torus T' together with an isomorphism $T' \times_{K'} K \simeq T$. Notice that K' can always be chosen to be algebraically closed in K; this will be important in the sequel. We shall first need a little lemma.

Lemma 5.1. *Let $\Gamma \longrightarrow \Gamma'$ be a surjection of profinite groups, with kernel H. Let M, N be two free abelian groups of finite rank, endowed with a continuous action of Γ'. We have $\mathrm{Hom}_\Gamma(M,N) = \mathrm{Hom}_{\Gamma'}(M,N)$ and $\mathrm{Ext}^1_\Gamma(M,N) = \mathrm{Ext}^1_{\Gamma'}(M,N)$.*

Proof. The first assertion is a triviality. For the second, we may assume that Γ is finite. Then, embed N (viewed as a Γ-module) into an exact sequence

$$0 \longrightarrow N \longrightarrow F \longrightarrow Q \longrightarrow 0,$$

where F is Γ-free. Because $H^1(H, N) = \mathrm{Hom}(H, N) = 0$, we also have the exact sequence

$$0 \longrightarrow N \longrightarrow F^H \longrightarrow Q^H \longrightarrow 0,$$

where F^H is Γ'-free. Looking at the associated long exact sequences in cohomology, we find that:

$$\begin{aligned} \mathrm{Ext}^1_\Gamma(M,N) &= \mathrm{Hom}_\Gamma(M,Q)/\mathrm{Hom}_\Gamma(M,F) \\ &= \mathrm{Hom}_{\Gamma'}(M,Q^H)/\mathrm{Hom}_{\Gamma'}(M,F^H) \\ &= \mathrm{Ext}^1_{\Gamma'}(M,N). \end{aligned}$$

□

In terms of essential dimension of tori, this lemma has the following nice consequence:

Proposition 5.2. *Let K/k be a field extension, and $1 \longrightarrow T' \longrightarrow T \longrightarrow T'' \longrightarrow 1$ an exact sequence of K-tori. We then have* $\mathrm{ed}([T]) \leq \mathrm{ed}([T']) + \mathrm{ed}([T''])$.

Proof. Let $K/K'/k$ be an intermediate field extension, with K' algebraically closed in K. It is enough to show that, if T' and T'' can be defined over K', then so can T. But this is exactly the content of Lemma 5.1, with Γ (resp. Γ') the absolute Galois group of K (resp. of K'), and M (resp. N) the character module of T' (resp. of T''). □

Let K/k be a field extension. For a separable field extension L/K of degree n we will consider its essential dimension (denoted by $\mathrm{ed}(L/K)$) to be the essential dimension of its class in $H^1(K, \mathfrak{S}_n)$, where $\mathfrak{S}_n$ stands for the symmetric group.

We recall that for a k-torus T there is a minimal finite Galois extension l/k which splits T, i.e. such that $T \times_k l \simeq \mathbb{G}_m^n \times_k l$. Such an extension is given as follows: take the homomorphism $\Gamma_k \to \mathbf{GL}(T^*)$ given by the Γ-action on T^* and let H be its kernel. Then $l = k_s^H$. This extension is called the *minimal Galois splitting field* of T.

Lemma 5.3. *Let K/k be a field extension.*

1. *Let T be a K-torus. Then* $\mathrm{ed}([T]) = \mathrm{ed}(L/K)$ *where L/K is the minimal Galois splitting field of T.*
2. *Let (T, ϕ) be a pair consisting of an n-dimensional K-torus and an isomorphism $\phi : \bigwedge^n T \to \mathbb{G}_m$. Then* $\mathrm{ed}([T, \phi]) = \mathrm{ed}([T])$.

Proof. (1) Recall that the Galois group G of L/K is the quotient of Γ_K by the kernel of the map $f_T : \Gamma_K \longrightarrow \mathbf{GL}(T^*)$. Assume there exists a subextension $K/K'/k$, with K' algebraically closed in K, and a K'-torus T', such that $T' \times_{K'} K$ is isomorphic to T. Let L'/K' be the minimal Galois splitting field of T' of Galois group G'. Then $(L' \otimes_{K'} K)/K$ is a Galois field extension, with Galois group G', which splits T. By minimality of L/K, we have that L is isomorphic to a subfield of $(L' \otimes_{K'} K)/K$, and G is a quotient of G'. By Galois theory, there exists an intermediate field $L'/M'/K'$, with Galois group G, such that $(M' \otimes_{K'} K)/K$ is isomorphic to L/K. This proves that $\mathrm{ed}_k(L/K) \leq \mathrm{ed}_k([T])$.
For the converse inequality, assume there exists an intermediate field extension $K/K'/k$, and a Galois field extension L'/K', of group G, such that $(L' \otimes_{K'} K)/K$ is isomorphic to L/K. Consider the map f' which is obtained by composing the map $f_T : G \longrightarrow \mathbf{GL}(T^*)$ with the projection $\Gamma_{K'} \longrightarrow G$. Let T'/K' be the torus defined by f'. It is clear that $T' \times_{K'} K$ is isomorphic to T. The desired inequality follows.
(2) Let (T, ϕ) be a pair, with T an n-dimensional K-torus and ϕ an isomorphism $\bigwedge^n T \longrightarrow \mathbb{G}_m$. Assume there exists an intermediate field extension $K/K'/k$, with K' algebraically closed in K, and a K'-torus T', together with an isomorphism $T' \times_{K'} K \longrightarrow T$. Because of Lemma 5.1 (applied to $M = \mathbb{Z}$ and $N = \bigwedge^n(T'^*)$), we see that ϕ is already defined over K'. This implies that $\mathrm{ed}([T, \phi]) \leq \mathrm{ed}([T])$. The converse inequality is obvious. □

Theorem 5.4. *For any field k, we have*

$$\mathrm{ed}_k(\mathbf{GL}_n(\mathbb{Z})) = \max\{\mathrm{ed}_k(G) \mid G \text{ finite subgroup of } \mathbf{GL}_n(\mathbb{Z})\}.$$

The same equality holds for $\mathbf{SL}_n(\mathbb{Z})$. Moreover, If k has characteristic not 2, we have $\mathrm{ed}_k(\mathbf{GL}_n(\mathbb{Z})) = n$, and $n - 1 \leq \mathrm{ed}_k(\mathbf{SL}_n(\mathbb{Z})) \leq n$. If n is odd one has $\mathrm{ed}_k(\mathbf{SL}_n(\mathbb{Z})) = n - 1$.

Proof. Let K/k be a field extension. Let T be a K-torus and let G be the Galois group of its minimal splitting field. By point (1) of the above lemma one has $\mathrm{ed}(T) \leq \mathrm{ed}_k(G)$, whence the inequality $\mathrm{ed}_k(\mathbf{GL}_n(\mathbb{Z})) \leq \max\{\mathrm{ed}_k(G) \mid G \text{ finite subgroup of } \mathbf{GL}_n(\mathbb{Z})\}$. For the converse inequality, let G be a finite subgroup of $\mathbf{GL}_n(\mathbb{Z})$ and let P be a G-torsor over K. Consider the K-torus T obtained by twisting $\mathbb{G}_{m,K}^n$ by P. The preceeding lemma yields the equality $\mathrm{ed}([T]) = \mathrm{ed}(P)$. Therefore $\mathrm{ed}(P) \leq \mathrm{ed}_k(\mathbf{GL}_n(\mathbb{Z}))$. The desired inequality follows. The similar equality for $\mathbf{SL}_n(\mathbb{Z})$ follows from Lemma 5.3 2).
Suppose now that $\mathrm{char}\, k \neq 2$ and let us show that $\mathrm{ed}_k(\mathbf{GL}_n(\mathbb{Z})) = n$. We know in this case that $\mathrm{ed}_k((\mathbb{Z}/2\mathbb{Z})^n) = n$ (see [2] Corollary 3.9 for example). By the first part of the theorem it then follows $\mathrm{ed}_k(\mathbf{GL}_n(\mathbb{Z})) \geq n$. Let us prove the reverse inequality. It suffices to show that, if G is a finite subgroup of $\mathbf{GL}_n(\mathbb{Z})$, we have $\mathrm{ed}_k(G) \leq n$. So let $G \subset \mathbf{GL}_n(\mathbb{Z})$ be such a group and consider the action of G on the torus $\mathbb{G}_m^n$. It is generically free, let U be a friendly subset for this action. The torsor $U \to U/G$ is then versal by Corollary 1.13 *ii*) and hence $\mathrm{ed}_k(G) \leq \dim(U/G) = n$. It remains to be shown that

$$n - 1 \leq \mathrm{ed}_k(\mathbf{SL}_n(\mathbb{Z})) \leq n.$$

The right hand inequality is obvious from what has been shown so far. For the other inequality, consider the natural diagonal embedding

$$\ker\left((\mathbb{Z}/2\mathbb{Z})^n \xrightarrow{\text{aug}} \mathbb{Z}/2\mathbb{Z}\right) \longrightarrow \mathbf{SL}_n(\mathbb{Z}),$$

and use the first part of the theorem. Assume now that n is odd and let us prove the equality $\mathrm{ed}_k(\mathbf{SL}_n(\mathbb{Z})) = n - 1$. Assume first that k has characteristic zero. Let G be a finite subgroup of $\mathbf{SL}_n(\mathbb{Z})$. Then G is a subgroup of $\mathbf{SL}_n(k)$ since $\mathrm{char}\, k = 0$. It follows that G acts faithfully on $\mathbb{P}^{n-1}$ and that the natural projection $\mathbb{A}^n \setminus \{0\} \to \mathbb{P}^{n-1}$ is a G-compression. This shows that $\mathrm{ed}_k(G) \leq n - 1$, whence the desired equality in this case. If k has finite characteristic $p \neq 2$, by a lemma of Minkowski (see [15] p. 213), the composite

$$G \longrightarrow \mathbf{GL}_n(\mathbb{Z}) \longrightarrow \mathbf{GL}_n(\mathbb{Z}/p\mathbb{Z})$$

is still an injection, and hence G is a subgroup of $\mathbf{SL}_n(k)$ as well. The result then follows as before. □

Remarks 5.5.

(1) Since for finite groups $H \leq G$ one has $\mathrm{ed}_k(H) \leq \mathrm{ed}_k(G)$, in order to compute $\mathrm{ed}_k(\mathbf{SL}_n(\mathbb{Z}))$ it is enough to know $\mathrm{ed}_k(G)$ for all G finite *maximal* subgroups of $\mathbf{SL}_n(\mathbb{Z})$. Moreover it is enough to consider only maximal finite subgroups up to isomorphism (and not up to conjugacy) since essential dimension is invariant under isomorphism.

(2) The maximal finite subgroups of $\mathbf{SL}_2(\mathbb{Z})$ are isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$. The essential dimension of these groups is well known: over $\mathbb{Q}$ for example one has $\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/4\mathbb{Z}) = \mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/6\mathbb{Z}) = 2$ (see [2] and [8] for more detailed results) and thus $\mathrm{ed}_{\mathbb{Q}}(\mathbf{SL}_2(\mathbb{Z})) = 2$. One the other hand, if $\mu_{12} \subset k$ then $\mathrm{ed}_k(\mathbf{SL}_2(\mathbb{Z})) = 1$ since $\mathrm{ed}_k(\mathbb{Z}/4\mathbb{Z}) = \mathrm{ed}_k(\mathbb{Z}/6\mathbb{Z}) = 1$ in this case. For n even, bigger than 2, we do not know the exact value of $\mathrm{ed}_k(\mathbf{SL}_n(\mathbb{Z}))$, even when $k = \mathbb{C}$.

(3) In [5], for a complex abelian variety A, Brosnan shows that $\mathrm{ed}_{\mathbb{C}}(A) = \max\{\mathrm{ed}_{\mathbb{C}}(G) \mid G \text{ finite subgroup of } A\}$. We do not know yet if there is a deeper connection between this result and the above.

Corollary 5.6. *Let K/k be a field extension, and L/K a finite separable field extension. We have*

$$\mathrm{ed}([\mathbf{R}_{L/K}(\mathbb{G}_m)]) = \mathrm{ed}([\mathbf{R}^1_{L/K}(\mathbb{G}_m)]) = \mathrm{ed}([\mathbf{R}_{L/K}(\mathbb{G}_m)/\mathbb{G}_m]) = \mathrm{ed}(L/K).$$

Proof. Considering the two exact sequences

$$1 \longrightarrow \mathbf{R}^1_{L/K}(\mathbb{G}_m) \longrightarrow \mathbf{R}_{L/K}(\mathbb{G}_m) \longrightarrow \mathbb{G}_m \longrightarrow 1$$

and

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathbf{R}_{L/K}(\mathbb{G}_m) \longrightarrow \mathbf{R}_{L/K}(\mathbb{G}_m)/\mathbb{G}_m \longrightarrow 1,$$

this is an easy consequence of Proposition 5.2 and of Theorem 5.4. □

Acknowledgements

The authors warmly thank the University of Bielefeld in Germany where this work was born. We specially thank Ulf Rehmann for giving us the possibility to work in Bielefeld's Math Departement. We also would like to thank the anonymous referee for helpful comments which improved the exposition and sharpened some of our results.

References

[1] *Schémas en groupes. I: Propriétés générales des schémas en groupes.* Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151. Springer-Verlag, Berlin, 1970.

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

[3] A. Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[4] L. Breen. Bitorseurs et cohomologie non abélienne. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 401–476. Birkhäuser Boston, Boston, MA, 1990.

[5] P. Brosnan. The essential dimension of a g-dimensional complex variety is $2g$. `http://www.math.ubc.ca/ brosnan/`, pages 1–5, 2007.

[6] J. Buhler and Z. Reichstein. On the essential dimension of a finite group. *Compositio Math.*, 106(2):159–179, 1997.

[7] S. Garibaldi, A. Merkurjev, and J.-P. Serre. *Cohomological invariants in Galois cohomology*, volume 28 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2003.

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

[9] A. Ledet. On the essential dimension of some semi-direct products. *Canad. Math. Bull.*, 45(3):422–427, 2002.

[10] N. Lemire. Essential dimension of algebraic groups and integral representations of Weyl groups. *Transform. Groups*, 9(4):337–379, 2004.

[11] M. Lorenz and Z. Reichstein. Lattices and parameter reduction in division algebras. `http://arxiv.org/abs/math.RA/0001026`, pages 1–18, 2000.

[12] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman. Fields of definition for division algebras. *J. London Math. Soc. (2)*, 68(3):651–670, 2003.

[13] A. Merkurjev. Essential dimension. *Private Notes*, pages 1–11, 1999.

[14] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[15] H. Minkowski. *Gesammelte Abhandlungen*, volume I. Springer, 1968.

[16] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]*. Springer-Verlag, Berlin, third edition, 1994.

[17] Z. Reichstein. On the notion of essential dimension for algebraic groups. *Transform. Groups*, 5(3):265–304, 2000.

[18] Z. Reichstein and B. Youssin. Essential dimensions of algebraic groups and a resolution theorem for G-varieties. *Canad. J. Math.*, 52(5):1018–1056, 2000. With an appendix by János Kollár and Endre Szabó.

[19] J.-P. Serre. *Cohomologie galoisienne*, volume 1962 of *Cours au Collège de France*. Springer-Verlag, Berlin, 1962/1963.

[20] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, second edition, 1998.

[21] V. E. Voskresenskiĭ. *Algebraic groups and their birational invariants*, volume 179 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1998. Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ].

Giordano Favi, Mathematisches Institut, Rheinsprung 21, 4057 Basel, Switzerland
E-mail address: giordano.favi@gmail.com
URL: http://www.math.unibas.ch/∼giordano

Mathieu Florence, CSAG, EPFL, CH-1015 Lausanne, Switzerland
E-mail address: mathieu.florence@gmail.com