On the Notion of Essential Dimension for Algebraic Groups

Zinovy Reichstein[1]

Department of Mathematics, Oregon State University,

Corvallis, OR 97331-4605

Abstract: We introduce and study the notion of essential dimension for linear algebraic groups defined over an algebraically closed fields of characteristic zero. The essential dimension is a numerical invariant of the group; it is often equal to the minimal number of independent parameters required to describe all algebraic objects of a certain type. For example, if our group G is S_n, these objects are field extensions, if $G = O_n$, they are quadratic forms, if $G = \mathrm{PGL}_n$, they are division algebras (all of degree n), if $G = G_2$, they are octonion algebras, if $G = F_4$, they are exceptional Jordan algebras. We develop a general theory, then compute or estimate the essential dimension for a number of specific groups, including all of the above-mentioned examples. In the last section we give an exposition of results, communicated to us by J.-P. Serre, relating essential dimension to Galois cohomology.

Contents

[1]Partially supported by NSA grant MDA904-9610022

1 Introduction

The purpose of this paper is to introduce and study the notion of essential dimension for linear algebraic groups. All algebraic groups we shall consider, along with all varieties, fields, etc., and all morphism between them will be defined over a fixed algebraically closed base field k of characteristic zero. The essential dimension $\mathrm{ed}(G)$ of an algebraic group G is the smallest integer d such that every principal G-bundle $X \longrightarrow B$ can be obtained (up to birational isomorphism) by pull-back from a diagram

$$\begin{array}{ccc} X \simeq B \times_C Y & \longrightarrow & Y \\ \downarrow & & \downarrow \\ B & \longrightarrow & C \end{array}$$

where $Y \longrightarrow C$ is a principal G-bundle, $B \longrightarrow C$ is a dominant map, and $\dim(C) \leq d$; cf. Definition 3.5 and Remark 2.17. The essential dimension naturally comes up in many interesting situations; several examples are given below.

(a) The essential dimension of the symmetric group S_n is the minimal number of parameters required to write down the general polynomial of degree n in one variable. (Here we allow Tschirnhaus transformations which do not involve radicals.) Equivalently, $\mathrm{ed}(S_n)$ is the smallest integer d with the following property: every field extension $K \subset L$ of degree n can be defined by (a degree n) polynomial with at most d algebraically independent coefficients (over k). The question of computing $\mathrm{ed}(S_n)$ is related to the algebraic form of Hilbert's 13th problem. For more on this we refer the reader to [BR_1] and [BR_2]; a discussion of essential dimensions of other finite groups can be found in [BR_1].

(b) Groups of essential dimension zero are precisely the "special groups" introduced by Serre [Se_1] and classified by Grothendieck [G] in the 1950s; see Section 5.

(c) Let D be a division algebra with center K. We say that D is defined over a subfield F of K if $D \simeq E \otimes_F K$ for some division algebra E with center F. The essential dimension of the projective linear group PGL_n is the smallest integer d such that every division algebra D of degree n is defined over some field F with $\mathrm{trdeg}_k(F) \leq d$. This number is of interest in the theory of division algebras; see [Pr_1, Thm. 2.1] and [Row]. We will discuss essential dimensions of projective linear groups in Section 9.

(d) The essential dimension of the orthogonal group O_n (resp. the special orthogonal group SO_n) is the smallest integer d such that every quadratic form (resp. every quadratic form of determinant 1) over every field F is equivalent to one with $\leq d$ algebraically independent coefficients (over k). We will determine these integers in Section 10.

(e) The essential dimensions of the exceptional group G_2 (resp. F_4) is the smallest integer d such that every octonion algebra (resp. every 27-dimensional exceptional simple Jordan algebra) can be defined over a field of transcendence degree $\leq d$. These numbers are discussed in Section 11.

The methods we use for computing, or at least estimating, the essential dimension of a given algebraic group G can be roughly divided into three categories: geometric, algebraic and cohomological. The geometric approach, based on (birational) invariant theory, is discussed in Sections 2-4. The algebraic approach, based on descent of "structured spaces" is developed in Sections 6-8; some applications are given in Sections 9-11. The cohomological approach is discussed in Sections 5 and 12; Section 5 is mostly concerned with the vanishing of H^1 and Section 12 deals with the relationship between the essential dimension of G and its cohomological invariants.

In order to illustrate the interplay among the geometric, algebraic, and cohomological methods, we will often prove the same result in several different ways, sometimes in different parts of the paper. For the convenience of the reader, we summarize most of what we now know about essential dimensions of specific groups in the table below and indicate where the proof of each result can be found.

Group	EssentialDimension	Proof
$(\mathbb{Z}/n)^r$	r	$[\mathrm{BR}_1, 6.1]$
S_n	$\geq [n/2]$	$[\mathrm{BR}_1, 6.5(\mathrm{b})], [\mathrm{BR}_2, 1.1]$, Ex. 12.8
	$\leq n-3$	$[\mathrm{BR}_1, 6.5(\mathrm{c})]$
$(k^*)^n$	$=0$	Thm. 5.4, Ex. 3.9(a)
GL_n	$=0$	Thm. 5.4, Ex. 3.9(b)
SL_n	$=0$	Thm. 5.4, Ex. 3.9(c), 8.9(a)
Sp_{2n}	$=0$	Thm. 5.4, Ex. 8.9(b)
PGL_n	$\leq n^2-2n$	Thm. 4.5
	$\leq n+\frac{(n-1)(n-2)}{2}$, n odd	Thm. 9.6
	$\geq 2r$ if $n=n_0^r$	Thm. 9.3
	$=2$ if $n=2, 3, 6$	Lemma 9.4(c)
	other results	Prop. 9.8, Rem. 9.9
O_n	$=n$	Thm. 10.3
	$\leq n$	Ex. 3.10(a), 4.2
	$\geq n$	Ex. 12.6
SO_n, $n \geq 3$	$=n-1$	Thm. 10.4
	$\leq n-1$	Ex. 3.10(b), 4.2
	$\geq n-1$	Ex. 12.7
G_2	$=3$	Thm. 11.2
	≤ 3	Rem. 11.4
	≥ 3	Rem. 11.3, Ex. 12.9, Thm. 12.12
F_4	≥ 5	Thm. 11.5, Ex. 12.10
E_6 (simply conn.)	≥ 3	Prop. 11.6, Thm. 12.12
	$\leq \mathrm{ed}(F_4)+1$	Prop. 11.7
E_7 (simply conn.)	≥ 3	Prop. 12.11(a), Thm. 12.12
E_8	≥ 3	Prop. 12.11(b), Thm. 12.12

For further results see the table in the appendix at the end of this paper.

Acknowledgements

We would like to thank J.-P. Serre for his help and encouragement and for allowing us to include an exposition of some of his unpublished results in this paper. In particular, Section 12 is based entirely on results he communicated to us. He also suggested the statements of Theorems 10.3, 10.4, 11.2 and 11.5; his proofs of these results are outlined in Section 12. (We give somewhat different proofs in Sections 10 and 11.)

The material of Section 5 was brought to our attention by V. L. Popov, who also made a number of other helpful comments after reading an earlier version of this paper. The results of Section 9.3 were suggested to us by L. H. Rowen and D. J. Saltman.

We would also like to express our gratitude to V. E. Kordonsky for sending us his preprints [Ko_1] and [Ko_2] along with a list of comments based on our earlier preprint (see Remark 3.6), to J. Buhler and B. Kahn for asking questions that got us interested in the subject matter of this paper, to R. S. Garibaldi, A. Vistoli, and N. Vonessen for stimulating discussions, and finally to H. Bass, P. Woit, and the Columbia University Mathematics Department for their hospitality during the summer of 1996, when some of the work on this paper was done.

2 Preliminaries

The purpose of this section is to introduce notation, terminology and a number of known results from birational invariant theory. Our emphasis will be on stating these results in a form suitable for subsequent use, not on developing the theory in a coherent and self-contained manner. For an excellent introduction to birational invariant theory we refer the reader to [PV, Sect 2]; see also [Po].

Our basic object of study will be primitive rather than irreducible G-varieties (see Definition 2.1); this (slightly) greater degree of generality will be needed the sequel.

2.1 Notation and terminology

The following notational conventions will be used throughout the paper.

k	algebraically closed base field of characteristic 0
F	usually a field extension of k
G	algebraic group defined over k
X	usually a G-variety
Gx	orbit of x under the action of G
$\mathrm{Stab}(x)$	stabilizer of x
$\mathrm{ed}(X)$	essential dimension X; see Definition 3.1
$\mathrm{ed}(G)$	essential dimension of G; see Definition 3.5
(W, β)	structured space over F; see Definition 6.1
(V, α)	structured space over k
$\mathrm{Aut}_k(V, \alpha)$	automorphism group of (V, α), usually denoted by G
$\tau(W, \beta)$	see Definition 8.7
$Z(A)$	center of the central simple algebra A
$\mathrm{UD}(m, n)$	universal division algebra of m $n \times n$-matrices
$<< a_1, \ldots, a_n >>$	n-fold Pfister form; see Section 10.1

Throughout this paper we shall work over a fixed base field k, which we assume to be algebraically closed and of characteristic 0. All algebraic objects we will consider (e.g., rings, fields, algebraic groups, algebraic varieties) and all maps between them will be defined over k.

If X is an algebraic variety, we shall denote the algebra of regular (resp. rational) functions on X by $k[X]$ (resp. $k(X)$). If X is irreducible then $k(X)$ is a field; in general, $k(X) = k(X_1) \oplus \ldots \oplus k(X_n)$ is a direct sum of fields; here $X_1, \ldots, X_n$ are the irreducible components of X. We shall say that a certain property holds for x in general position in X if it holds for all $x \in U$, where U is a dense open subset of X (i.e., an open subset which non-trivially intersects every irreducible component of X).

As usual, a rational map $X \dashrightarrow Y$ is an equivalence class of regular maps $U \longrightarrow Y$, where U is a dense open subset of X; $f_1 : U_1 \longrightarrow Y$ and $f_2 : U_2 \longrightarrow Y$ are considered equivalent if they agree on $U_1 \cap U_2$. The domain of a rational map $f : X \dashrightarrow Y$ is the union of all dense open subsets U where f is defined, and the range $f(X)$ is the union of $f(U)$. We will say that f is dominant if $f(X)$ is dense in Y.

We shall call an algebraic variety X a G-variety if X is equipped with a regular action of G (i.e., an action given by a regular morphism $G \times X \longrightarrow X$). If X and Y are G-varieties then by a regular map $X \longrightarrow Y$ of G-varieties we mean a regular G-equivariant map. The same applies to rational maps of G-varieties, biregular and birational isomorphisms of G-varieties, etc.

2.2 Primitive G-varieties

Definition 2.1 We shall call a G-variety X *primitive* if G transitively permutes the components of X.

Note that if G is connected then X is a primitive G-variety if and only if X is irreducible.

Lemma 2.2 *Let X be a G-variety. Then*

(a) X is birationally isomorphic to a disjoint union of primitive G-varieties.

(b) X is primitive if and only if $k(X)^G$ is a field.

Proof. (a) Write $X = X_1 \cup \ldots \cup X_n$, where each X_i is a union of components of X transitively permuted by G. Then each X_i is primitive and the natural projection from the disjoint union $\amalg_{i=1}^m X_i$ to X is a G-equivariant birational isomorphism.

(b) Suppose $k(X)^G$ is not a field. Then $k(X)^G$ has a zero-divisor $f \neq 0$. Let X_0 be the union of those irreducible components of X where $f = 0$ and X_1 be the union of the remaining irreducible components. Then X_0 and X_1 are G-invariant and non-empty. Since G cannot map a component in X_0 to a component in X_1, we conclude that X is not primitive. Conversely, suppose X is not primitive. By part (a) we may assume that X is a disjoint union of $m \geq 2$ primitive G-varieties $X_1, \ldots, X_m$. Let $f \in k(X)^G$ be given by $f_{|X_1} = 1$ and $f_{|X_i} = 0$ for all $i = 2, \ldots, m$. Then f is a zero divisor in $k(X)^G$ and thus $k(X)^G$ is not a field. □

2.3 Rational quotients

Theorem 2.3 (Rosenlicht [Ros$_1$], [Ros$_2$]) *Let X be a G-variety. Suppose $k(W) = k(X)^G$ and $\pi : X \dashrightarrow W$ is rational map induced by the inclusion $k(X)^G \hookrightarrow k(X)$. Then there exists an open dense subset U of X such that $\pi_{|U} : U \longrightarrow W$ is a regular map and for any $x, y \in U$, $\pi(x) = \pi(y)$ iff $Gx = Gy$.* $\square$

We shall denote W by X/G; this variety is uniquely defined up to birational equivalence. By Lemma 2.2(b), X is primitive if and only if X/G is irreducible. We will refer to the map $\pi : X \dashrightarrow X/G$ as *the rational quotient map* or simply *the quotient map*, since no other kind of quotient map will be considered in this paper.

Remark 2.4 The identity $k(X/G) = k(X)^G$, which we used to define X/G, can be restated as a universal property of X/G as follows. Any rational map $f : X \dashrightarrow Y$ of G-varieties gives rise to a rational map $\overline{f} : X/G \dashrightarrow Y/G$ such that the diagram

$$\begin{array}{ccc} X & \overset{f}{\dashrightarrow} & Y \\ \pi_X \Big\downarrow & & \Big\downarrow \pi_Y \\ X/G & \overset{\overline{f}}{\dashrightarrow} & Y/G \end{array} \qquad (1)$$

commutes. Here π_X and π_Y are the rational quotient maps.

Remark 2.5 The rational quotient map $\pi : X \dashrightarrow X/G$ is unique in the following sense.

Let X be a primitive G-variety. Suppose $f : X \dashrightarrow X_0$ is a dominant rational map such that $f^{-1}(f(x)) = Gx$ for $x_0 \in X$ in general position. Then there exists a birational isomorphism $\overline{f} : X/G \overset{\simeq}{\dashrightarrow} X_0$ such that $f = \overline{f} \circ \pi$.

The map $\overline{f}$ is given by diagram (1) with $Y = X_0$, where X_0 is viewed as a G-variety with trivial G-action. Here $\pi_X = \pi$, $Y/G = X_0$ and $\pi_Y : Y \dashrightarrow Y/G$ is the identity map. Since X is primitive, both X_0 and X/G are irreducible. Moreover, by our assumption on f, the map $\overline{f} : X/G \dashrightarrow X_0$ is dominant and $\overline{f}^{-1}(x_0)$ is a single point for x_0 in general position in X_0. Thus $\overline{f}$ is a birational isomorphism; see, e.g., [H, 4.6]. $\square$

Remark 2.6 Suppose X is a G-variety and N is a closed normal subgroup of G. Then G/N has a naturally defined rational action on X/N; see [PV, Proposition 2.6]. In general, this action will not be regular; however, by a theorem of Rosenlicht (see [Ros$_1$, Theorem 1], [PV, Corollary 1.1]) there exists a model for X/N such that the induced G/N-action on it is regular, i.e., X/N is a G/N-variety. Moreover, this G-variety is uniquely defined up to birational isomorphism.

2.4 Generically free varieties

Definition 2.7 A G-variety X is said to be *generically free* if G acts freely (i.e., with trivial stabilizers) on a dense open subset of X.

Lemma 2.8 *Suppose a rational map $f : X \dashrightarrow Y$ of generically free G-varieties induces a birational isomorphism $\overline{f} : X/G \dashrightarrow Y/G$. Then f is a birational isomorphism.*

Proof. We may assume without loss of generality that X/G and Y/G are irreducible, i.e., X and Y are primitive G-varieties. In particular, every irreducible component of X has dimension $\dim(X)$ and every irreducible component of Y has dimension $\dim(Y)$. Moreover,

$$\dim(X) = \dim(X/G) + \dim(G) = \dim(Y/G) + \dim(G) = \dim(Y) .$$

Replacing X/G and Y/G by sufficiently small open subsets we may assume that all four maps in diagram (1) are regular, G acts freely on X and Y, and π_X separates the G-orbits in X. Then $f(X)$ is G-invariant subset of Y which intersects every G-orbit in Y; hence, $f(X) = Y$. On the other hand, $f(x_1) = f(x_2)$ means that $\pi_X(x_1) = \pi_X(x_2)$, i.e., $x_2 = g(x_1)$ for some $g \in G$. Consequently, $gf(x_1) = f(x_2) = f(x_1)$. Since G acts freely on Y, we conclude that $x_1 = x_2$.

We have therefore proved that f is bijective. Let $X = X_1 \cup \ldots \cup X_n$ be an irreducible decomposition of X. Let Y_i be the closure of $f(X_i)$ in Y. Since $\dim(Y_i) = \dim(X_i) = \dim(X) = \dim(Y)$, $Y_1, \ldots, Y_n$ are the irreducible components of Y. Moreover the injectivity of f implies that $Y_i \neq Y_j$ if $i \neq j$. For every $i = 1, \ldots, n$, the map $f_{|X_i} : X_i \longrightarrow Y_i$ is dominant and injective. Hence, each $f_{|X_i}$ is a birational isomorphism (see, e.g., [H, 4.6]) and therefore, so is f. □

2.5 (G, H)-sections

Definition 2.9 *(cf. [Ka$_1$, Sect. 1], [Po, 1.7.6], [Do, Sect. 3].)* Let G be an algebraic group, X be a G-variety, and H be a closed subgroup of G. An irreducible subvariety $S \subset X$ is called a (G, H)-section if

(a) GS is dense in X and

(b) there is a dense open subvariety $S_0 \subset S$ such that for any $s \in S_0$ we have $gs \in S$ if and only if $g \in H$.

Example 2.10 Let X be a primitive G-variety and let X_1 be an irreducible component of X. Then X_1 is a (G, G_1)-section, where $G_1 = \{g \in G \mid g(X_1) = X_1\}$.

Lemma 2.11 *Let X be a G-variety and S be a (G, H)-section of X. Then $k(S)^H = k(X)^G$.*

Proof. Let $\pi : X \dashrightarrow X/G$ be the rational quotient map. Then the restriction $\pi_{|S} : S \dashrightarrow X/G$ is well-defined and separates H-orbits in S_0. By Remark 2.5 $\pi_{|S}$ is the quotient map for the H-action on S. Equivalently, $k(S)^H = k(X/G)$, as claimed. $\square$

Definition 2.12 Let G be an algebraic group, H be a closed subgroup of G, and W be an H-variety. Then $G \times W$ is a $G \times H$-variety via

$$(g, h) : (g', w) \mapsto (gg'h^{-1}, hw) , \tag{2}$$

for any $g, g' \in G$, $h \in H$, and $w \in W$. By Remark 2.6 a model Y for $(G \times W)/H$ can be chosen so that the G-action on Y is regular and thus the quotient map $\pi : G \times W \dashrightarrow Y$ is a rational map of G-varieties. (Here we are identifying H with a normal subgroup $N = \{1_G\} \times H$ of $G \times H$ and G with $(G \times H)/N$).) We shall denote Y by $G *_H W$; this G-variety is well-defined up to birational isomorphism.

Remark 2.13 (a) If W is a generically free H-variety then it is easy to see that $G *_H W$ is a generically free G-variety.

(b) $W \hookrightarrow G *_H W$ given by $w \mapsto (1, w)$ is an H-equivariant embedding of H-varieties, whose image is a (G, H)-section of $G *_H W$. The following lemma shows that every (G, H)-section is of this form.

Lemma 2.14 *(cf. [Po, 1.7.5]) Let X be a G-variety and S be a (G, H)-section of X. Then $G *_H S$ and X are birationally isomorphic G-varieties.*

Proof. Consider the map $\phi : G \times S \longrightarrow X$ given by $(g, s) \mapsto gs$. Then ϕ is a morphism of $G \times H$ varieties, where $G \times H$ acts via (2) on $G \times S$ and H acts trivially on X. Moreover, this map is dominant and $\phi^{-1}(x)$ is a single H-orbit for x in general position in X. Thus by Remark 2.5, ϕ is the rational quotient map for the H-action on $G \times S$. In other words, we have the following commutative diagram:

$$\begin{tikzcd} G \times S \arrow[d, dashed, "\pi"'] \arrow[dr, "\phi"] & \\ G *_H S \arrow[r, dashed, "\simeq"] & X \end{tikzcd}$$

To complete the proof, note that since the G-action on $G \times S$ commutes with the H-action, every map in this diagram is G-equivariant. $\square$

2.6 Compressions and fiber products

Definition 2.15 Let X be a generically free G-variety. A *G-compression* of X is a dominant G-equivariant rational map $X \dashrightarrow Y$, where Y is another generically free G-variety.

Let Y be a primitive G-variety, $\pi : Y \dashrightarrow Y/G$ be the rational quotient map, and $\phi : X_0 \dashrightarrow Y/G$ be a dominant rational map. Recall that the fiber product $Y \times_{Y/G} X_0$ is defined as the closure of

$$\{(y, x_0) \mid \pi(y) = \phi(x_0)\}$$

in $Y \times X_0$. This variety inherits a G-action from Y. Clearly $Y \times_{Y/G} X_0$ is a generically free G-variety if an only if so is Y.

Lemma 2.16 *(a) Suppose Y and $\phi : X_0 \dashrightarrow Y/G$ are as above. Denote the fiber product $Y \times_{Y/G} X_0$ by X. Then the natural projection $pr : X = Y \times_{Y/G} X_0 \longrightarrow X_0$ is the rational quotient map for the G-action on X.*

(b) Conversely, suppose X is a generically free G-variety, $X_0 = X/G$, $\pi : X \dashrightarrow X_0$ is the rational quotient map and $\overline{f} : X_0 \dashrightarrow Y/G$ is the dominant rational map induced by a G-compression $f : X \dashrightarrow Y$. Then

$$\psi \stackrel{\text{def}}{=} f \times (\overline{f} \circ \pi) : X \stackrel{\simeq}{\dashrightarrow} Y \times_{Y/G} X_0$$

is a birational isomorphism of G-varieties.

Proof. (a) It is easy to see that $pr^{-1}(x_0) = Gx_0$ for x_0 in general position in X_0. Part (a) now follows from Remark 2.5.

(b) By part (a), the map $\overline{\psi} : X/G \stackrel{\simeq}{\dashrightarrow} X_0 = (Y \times_{Y/G} X_0)/G$ is a birational isomorphism. The desired conclusion now follows from from Lemma 2.8. □

Remark 2.17 Suppose X is a generically free G-variety. One can show that the rational quotient map $\pi : X \dashrightarrow X/G$ is a principal G-bundle over a dense open subset $U \subset X/G$. This means that there exists an etale cover $U' \longrightarrow U$ such that $U' \times_U \pi^{-1}(U)$ is isomorphic to $U' \times G$, as a G-variety. If X is primitive, this is equivalent to the following: there exists a finite rational cover $X_0 \dashrightarrow X/G$ of irreducible varieties such that $X_0 \times_{X/G} X$ is birationally isomorphic to $X_0 \times G$ (as a G-variety). The latter assertion follows from the existence of a rational quasisection for X; see [Po, 1.1.2]. Since we shall not use this result, except to motivate Definition 3.1, we omit the details of the argument.

2.7 The "no-name" lemma

Let Y be a G-variety and let $\phi : E \longrightarrow Y$ be a G-vector bundle of rank d. This means that ϕ is an algebraic vector bundle of rank d, G acts on both E and Y so that ϕ is a surjective morphism of G-varieties, and $g : \phi^{-1}(y) \mapsto \phi^{-1}(g(y))$ is a linear map for each $y \in Y$ and $g \in G$; see, e.g., [BK, Section 1].

Lemma 2.18 *Let Y be a generically free G-variety and let E be a G-vector bundle on Y. Then there exists a birational isomorphism α so that the diagram*

$$\begin{tikzcd} E/G \arrow[r, dashed, "\alpha"] \arrow[d, dashed, "\overline{\phi}"'] & Y/G \times k^d \arrow[dl] \\ Y/G & \end{tikzcd} \tag{3}$$

commutes. Here k^d is the d-dimensional affine space and $Y/G \times k^d \longrightarrow Y/G$ is projection to the first factor.

Proof. We may assume without loss of generality that Y is a primitive G-variety. Moreover, in view of Example 2.10 and Lemma 2.11, we may assume Y is irreducible (otherwise we can replace Y by an irreducible component Y_1, G by the stabilizer G_1 of Y_1, and E by $\phi^{-1}(Y_1)$).

If Y is irreducible then Lemma 2.18 is the usual form of the so-called "no-name lemma"; see [BK, Lemma 1.2], [Ka$_2$, p. 104], or [Do, p. 6]. □

In the sequel we will need the following variant of the no-name lemma.

Lemma 2.19 *Let Y be a generically free G-variety and let $\phi : E \longrightarrow Y$ be a G-vector bundle of dimension d. Then E is birationally isomorphic to $Y \times k^d$ (as a G-variety), where k^d is the affine d-space with trivial G-action.*

Proof. By Lemma 2.16, E is birationally isomorphic to $Y \times_{Y/G} (E/G)$. Let α be as in (3). Then we have the following birational isomorphisms of G-varieties:

$$E \simeq Y \times_{Y/G} E/G \overset{1\times\alpha}{\simeq} Y \times_{Y/G} (Y/G \times k^d) \simeq Y \times k^d. \qquad \square$$

Corollary 2.20 *Let Y be a primitive generically free G-variety and let V be a d-dimensional linear representation of G. Then there exists a G-equivariant dominant rational map $f : Y \times k^d \dashrightarrow V$. Here G acts on $Y \times k^d$ via $g(y, a) = (gy, a)$, as in the previous lemma.*

Proof. Let $E = Y \times V$ and let $\phi : Y \times k^d \overset{\simeq}{\dashrightarrow} Y \times V$ be the birational isomorphism of Lemma 2.19. Now set $f = pr \circ \phi$, where $pr : Y \times V \longrightarrow V$ is projection to the second component. □

3 Definition of essential dimension

3.1 The essential dimension of a G-variety

Recall that that, up to birational isomorphism, a generically free G-variety X can be viewed as a principal G-bundle over the base X/G; see Remark 2.17. Moreover, Lemma 2.16(b) says that if $X \dashrightarrow Y$ is a compression then X is obtained from Y by a (dominant) base extension $X/G \dashrightarrow Y/G$. Informally speaking, the G-bundle structure of $X \dashrightarrow X/G$ is completely determined by the G-bundle structure of $Y \dashrightarrow Y/G$; the base extension $X/G \dashrightarrow Y/G$ simply "spreads" this structure over a larger base. Thus given a generically free G-variety X one can ask for a "minimal possible" base space $B = Y/G$ over which it is defined. Of course, such a base space cannot be expected to be unique, so we will limit ourselves to studying its dimension.

Definition 3.1 The essential dimension of a primitive generically free G-variety X is the smallest possible value of $\dim(Y/G)$, where $X \dashrightarrow Y$ is a compression; see Definitions 2.1 and 2.15. We shall denote this number by $\mathrm{ed}(X, G)$ or simply $\mathrm{ed}(X)$ if the reference to G is clear from the context.

Remark 3.2 If X is primitive and $X \dashrightarrow Y$ is a G-compression then Y is primitive as well. Indeed, $k(Y)^G$ is contained in $k(X)^G$, which is a field; see Lemma 2.2(b).

Note also that $\dim(Y/G) = \dim(Y) - \dim(G)$, where $\dim(Y)$ is the dimension of any irreducible component of Y. Thus we could have defined $\mathrm{ed}(X, G)$ as the minimal value of $\dim(Y)$ rather than of $\dim(Y/G) = \dim(Y) - \dim(G)$. Subtracting $\dim(G)$ is simply a matter of convention; we will later find it useful.

We now record several simple observations for future reference.

Lemma 3.3 *Let X and Y be primitive generically free G-varieties. Then*

(a) $\mathrm{ed}(X, G) \leq \dim(X) - \dim(G)$.

(b) Suppose there exists a G-compression $X \dashrightarrow Y$. Then $\mathrm{ed}(X, G) \leq \mathrm{ed}(Y, G)$.

(c) Let Y_0 be the union of $\phi(X)$, as ϕ ranges over all G-equivariant rational maps $\phi : X \dashrightarrow Y$. (As usual, $\phi(X)$ is defined as $\phi(U)$, where U is the domain of ϕ.) Suppose Y_0 is dense in Y. Then $\mathrm{ed}(X, G) \leq \mathrm{ed}(Y, G)$.

(d) Let S be a G-variety with trivial G-action. Then $\mathrm{ed}(X \times S, G) = \mathrm{ed}(X, G)$.

(e) If $G = \{1\}$ then $\mathrm{ed}(X, G) = 0$ *for any X.*

Proof. Parts (a) and (b) are immediate consequences of the definition.

(c) Let $f : Y \dashrightarrow Z$ be a G-compression with $\dim(Z/G) = \mathrm{ed}(Y, G)$. Suppose G acts freely on a dense G-invariant open subset V of Z. Let $U = \phi^{-1}(V) \subset Y$. By our assumption $Y_0 \cap U \neq \emptyset$. In other words, there exists a rational G-equivariant map $\phi : X \dashrightarrow Y$ such that $\phi(X) \cap U \neq \emptyset$. Then $f \circ \phi : X \dashrightarrow Z$ is a well-defined G-equivariant rational map. Denote the closure of the image of this map in Z by Z_0. By our choice of U, Z_0 is a generically free G-variety. Thus $f \circ \phi$ can be viewed as a compression $X \dashrightarrow Z_0$. Consequently, $\mathrm{ed}(X, G) \leq \dim(Z_0/G) \leq \dim(Z/G) = \mathrm{ed}(Y, G)$, as claimed.

(d) Since the natural projection $X \times S \longrightarrow X$ is a G-compression, part (b) says that $\mathrm{ed}(X \times S, G) \leq \mathrm{ed}(X, G)$. On the other hand, given $s \in S$, let $\phi_s : X \longrightarrow X \times S$ be the (regular) G-equivariant map given by $\phi_s(x) = (x, s)$. Since the images of ϕ_s cover $X \times S$, as s ranges over S, part (c) implies $\mathrm{ed}(X, G) \leq \mathrm{ed}(X \times S, G)$.

(e) If $G = \{1\}$ then we can (G-equivariantly) compress X to a point. $\square$

3.2 The essential dimension of a group

Theorem 3.4 *Let G be an algebraic group, X be a generically free primitive G-variety, $E \longrightarrow X$ be a G-vector bundle over X and V, V' be two generically free linear representations of G. Then*

(a) $\mathrm{ed}(E, G) = \mathrm{ed}(X, G)$,

(b) $\mathrm{ed}(V, G) = \mathrm{ed}(V', G)$ *and*

(c) $\mathrm{ed}(X, G) \le \mathrm{ed}(V, G)$.

Proof. (a) By Lemma 2.19, E is birationally equivalent to $X \times k^d$, as a G-variety. Thus $\mathrm{ed}(E, G) = \mathrm{ed}(X \times k^d, G) = \mathrm{ed}(X, G)$; see Lemma 3.3(d).

(b) Let $E = V \times V'$. Applying part (a) to the vector bundle $E \longrightarrow V$ given by projection to the first factor, we obtain the equality $\mathrm{ed}(E, G) = \mathrm{ed}(V, G)$. Similarly, $\mathrm{ed}(E, G) = \mathrm{ed}(V', G)$, and thus $\mathrm{ed}(V, G) = \mathrm{ed}(V', G)$.

(c) By Corollary 2.20 there exists a G-compression $X \times k^d \dashrightarrow V$, where $d = \dim(V)$. Now combining parts (b) and (d) of Lemma 3.3, we obtain

$$\mathrm{ed}(X, G) = \mathrm{ed}(X \times k^d, G) \le \mathrm{ed}(V, G) \, ,$$

as claimed. For an alternative proof, see Remark 7.2. □

Note that every linear algebraic group can be embedded in some GL_n and thus has a generically free linear representation. Thus we can now give the following definition.

Definition 3.5 The *essential dimension* of an algebraic group G is defined to be the essential dimension of a generically free linear G-representation. By Theorem 3.4(b) this number is is independent of the choice of the representation; we shall denote it by $\mathrm{ed}(G)$. Note that $\mathrm{ed}(G) = \max\{\mathrm{ed}(X, G)\}$, as X ranges over all primitive generically free G-varieties; see Theorem 3.4(c).

Remark 3.6 In an earlier version of this paper the inequality $\mathrm{ed}(G, X) \le \mathrm{ed}(G)$ was only established for reductive groups G. Theorem 3.4(c) in its current form was first pointed out to us by V. E. Kordonsky, who proved it by reducing the general case to one where G is reductive and then appealing to our earlier result. His argument also yields the following theorem [Ko_1, Theorem 1]:

If G is an algebraic group and L is the Levi subgroup of G then $\mathrm{ed}(G) = \mathrm{ed}(L)$. □

3.3 First properties

Lemma 3.7 *Suppose an algebraic subgroup G is an (algebraic) semidirect product of its subgroups N and H, with $N \lhd G$. Then* $\mathrm{ed}(G) \ge \mathrm{ed}(H)$.

Proof. Let V be a generically free linear representation of G and let $\phi : V \dashrightarrow Y$ be a G-compression with $\dim(Y/G) = \mathrm{ed}(G)$. Then we can choose a regular model for Y/N which is a generically free H-variety; see Remark 2.6 We can thus view V as a generically free linear representation of H and the composite map $V \dashrightarrow Y/N$ below as an H-compression:

$$\begin{array}{ccc} V & \dashrightarrow & Y \\ & & \downarrow \\ & & Y/N \\ & & \downarrow \\ & & Y/G \end{array}$$

Thus $\mathrm{ed}(G) = \dim(Y) - \dim(G) = \dim(Y/N) - \dim(H) \geq \mathrm{ed}(H)$. $\square$

Lemma 3.8 $\mathrm{ed}(G_1 \times G_2) \leq \mathrm{ed}(G_1) + \mathrm{ed}(G_2)$ *for any two algebraic groups* G_1 *and* G_2.

Proof. For $i = 1, 2$ let V_i be a generically free linear representation of G_i and let $\phi_i : V_i \dashrightarrow Y_i$ be a G_i-compression such that $\mathrm{ed}(G_i) = \dim(Y_i) - \dim(G_i)$. Then $V_1 \times V_2$ is a generically free linear representation of $G_1 \times G_2$ and

$$\phi_1 \times \phi_2 : V_1 \times V_2 \dashrightarrow Y_1 \times Y_2$$

is a $G_1 \times G_2$-compression. Thus $\mathrm{ed}(G) \leq \dim(Y_1 \times Y_2) - \dim(G) = \dim(Y_1) + \dim(Y_2) - \dim(G_1) - \dim(G_2) = \mathrm{ed}(G_1) + \mathrm{ed}(G_2)$, as claimed. $\square$

3.4 Examples

Example 3.9 *(a) Let* $T_d = (k^*)^d$ *be a* d*-dimensional torus. Then* $\mathrm{ed}(T_d) = 0$ *for any* $d \geq 1$.

(b) $\mathrm{ed}(\mathrm{GL}_n) = 0$,

(c) $\mathrm{ed}(\mathrm{SL}_n) = 0$.

Proof. (a) The natural representation of T_d on $V = k^d$ is generically free. Hence by Lemma 3.3(a), $\mathrm{ed}(T_d) = \mathrm{ed}(V, T_d) \leq \dim(V) - \dim(T_d) = 0$.

(b) Consider the linear representation of GL_n on $V = \mathrm{M}_n(k)$ given by left multiplication. By Lemma 3.3(a), $\mathrm{ed}(\mathrm{GL}_n) \leq \dim(V) - \dim(\mathrm{GL}_n) = 0$.

(c) Let SL_n act on $V = \mathrm{M}_n(k)$ by left multiplication, as above. Let $Y \subset V$ be the set of matrices of determinant 1 and let $f : V \dashrightarrow Y$ be given by

$$f(A) = \left(\frac{1}{\det(A)} v_1, v_2, \dots, v_n \right),$$

where $A = (v_1, \dots, v_n)$ is the matrix whose columns are $v_1, \dots, v_n$. It is easy to see that f is a SL_n-compression; thus $\mathrm{ed}(\mathrm{SL}_n) \leq \dim(Y) - \dim(SL_n) = 0$. $\square$

Example 3.10 *(a)* $\mathrm{ed}(O_n) \le n$*, (b)* $\mathrm{ed}(SO_n) \le n-1$.

Proof. Let $W = k^n$, $q : W \times W \longrightarrow k$ be a non-degenerate symmetric bilinear form, and O_n be the group of q-preserving linear transformations $W \longrightarrow W$. If $v \in W$ and $0 \ne v_1, \ldots, v_r \in W$, we define $P(v; v_1, \ldots, v_r)$ by

$$P(v; v_1, \ldots, v_r) = v - \sum_{i=1}^{r} \frac{q(v_i, v)}{q(v_i, v_i)}\, v_i \tag{4}$$

Note that if $v_1, \ldots v_i$ are mutually orthogonal then $P(v, v_1, \ldots, v_i)$ is just the component of v orthogonal to $v_1, \ldots, v_r$.

For $d = 1, \ldots, n$ let $Y_d \subset W^d$ be the set of elements $(w_1', \ldots, w_d')$ such that $q(w_i', w_j') = 0$ and $q(w_i', w_i') \ne 0$ for any $1 \le i < j \le d$. Note that Y_d is a locally closed O_n-invariant subvariety of W^d. An easy induction argument, using the projection $Y_{d+1} \longrightarrow Y_d$ to the first d components, shows that Y_d is an irreducible variety of dimension $n + (n-1) + \ldots + (n-d+1) = d(2n-d+1)/2$.

(a) Consider the linear representation of O_n on $V = W^n$. Both W^n and Y_n are generically free O_n-varieties. We now observe that the usual diagonalization process gives rise to a compression $f : W^n \dashrightarrow Y_n$. That is, we define $f(w_1, \ldots, w_n) = (w_1', \ldots, w_n')$, where $w_1' = w_1$ and

$$w_i' = P(w_i; w_1', \ldots, w_{i-1}') \tag{5}$$

for $i = 2, \ldots, n$. Thus $\mathrm{ed}(O_n) \le \dim(Y_n/O_n) = \dim(Y_n) - \dim(O_n) = n(n+1)/2 - n(n-2)/2 = n$, as claimed.

(b) Note that W^{n-1} is a generically free linear representation of SO_n (but not of O_n) and Y_{n-1} is a generically free SO_n-variety of W^{n-1}. Moreover, the map $W^{n-1} \dashrightarrow Y_{n-1}$ given by $(w_1, \ldots, w_{n-1}) \mapsto (w_1', \ldots, w_{n-1}')$, with $w_1', \ldots, w_{n-1}'$ as in (5), is an SO_n-compression. Thus

$\mathrm{ed}(SO_n) \le \dim(Y_{n-1}) - \dim(SO_n) = (n-1)(n+2)/2 - n(n-1)/2 = n-1$. □

4 $(G-H)$-sections and essential dimension

4.1 The essential dimension of a section

Lemma 4.1 *Let X be a generically free G-variety and let $S \subset X$ be a (G,H)-section; see Definition 2.9. Then* $\mathrm{ed}(X, G) \le \mathrm{ed}(S, H)$.

Proof. Recall that $X \simeq G *_H S$; see Definition 2.12 and Lemma 2.14.

Choose a generically free H-variety Y and an H-compression $\alpha : S \dashrightarrow Y$ such that $\dim(Y/H) = \mathrm{ed}(S, H)$. Then $G *_H Y$ is a generically free G-variety; see Remark 2.13(a). It is easy to see that α lifts to a G-compression $\beta : X \simeq G *_H S \dashrightarrow G *_H Y$ given by $\beta : (g, s) \mapsto (g, \alpha(s))$. Thus $\mathrm{ed}(X, G) = \mathrm{ed}(G *_H S, G) \le \dim(G *_H Y) - \dim(G) = \dim(Y) - \dim(H) = \mathrm{ed}(S, H)$. □

Example 4.2 To illustrate Lemma 4.1 we will give an alternative proof of the inequalities $\mathrm{ed}(O_n) \leq n$ and $\mathrm{ed}(SO_n) \leq n-1$ of Example 3.10.

Let $W = k^n$, q be a non-degenerate symmetric bilinear form of W, $e_1, \ldots, e_n$ be an orthonormal basis with respect to q, and $V = W^n$ be a generically free linear O_n-variety as in Example 3.10. Set $V_i = \mathrm{Span}(e_1, \ldots, e_i)$. Then $S = V_1 \times \ldots \times V_n$ is a $(O_n, (\mathbb{Z}/2)^n)$-section of $V = W^n$. Thus by Lemma 4.1

$$\mathrm{ed}(O_n) = \mathrm{ed}(V, O_n) \leq \mathrm{ed}(S, (\mathbb{Z}/2)^n) = \mathrm{ed}((\mathbb{Z}/2)^n) \leq n\ .$$

Note that $\mathrm{ed}(S, (\mathbb{Z}/2)^n) = \mathrm{ed}((\mathbb{Z}/2)^n)$ because S is a linear space with a generically free $(\mathbb{Z}/2)^n$-action. The last inequality follows from the fact that the group $(\mathbb{Z}/2)^n$ has a generically free n-dimensional representation. (We remark that, in fact, $\mathrm{ed}((\mathbb{Z}/2)^n) = n$ by [BR_1, Theorem 6.1]; however, all we need here is the inequality $\mathrm{ed}((\mathbb{Z}/2)^n) \leq n$, which is immediate from the definition of essential dimension.)

Note that S can also be viewed as a $(SO_n, (\mathbb{Z}/2)^{n-1})$-section for the SO_n-action on V. Applying Lemma 4.1 to this section yields the inequality $\mathrm{ed}(SO_n) \leq n-1$ of Example 3.10(b). $\square$

Another application of Lemma 4.1 can be found in the proof of Proposition 11.7.

Proposition 4.3 *Let G be a connected semisimple group whose center is trivial. Let N be the normalizer of a maximal torus in G. Then* $\mathrm{ed}(G) \leq \mathrm{ed}(N)$.

Proof. Let T be a maximal torus of G and let $Lie(G)$ and $Lie(T)$ be the Lie algebras of G and T respectively. Then the linear representation of G on

$$V = Lie(G) \times Lie(G)$$

given by the adjoint action in each component is generically free and

$$S = Lie(T) \times Lie(G)$$

is a (G, N)-section for this action; see [Po, 1.7.17]. Thus $\mathrm{ed}(N) = \mathrm{ed}(S, N)$; see Definition 3.5. By Lemma 4.1 we have $\mathrm{ed}(G) = \mathrm{ed}(V, G) \leq \mathrm{ed}(S, N) = \mathrm{ed}(N)$, as claimed. $\square$

Remark 4.4 Note that $\mathrm{ed}(G)$ can be strictly less than $\mathrm{ed}(N)$. Indeed, let $G = \mathrm{SL}_n$. Then $\mathrm{ed}(G) = 0$; see Example 3.9. On the other hand, $\mathrm{ed}(N) > 0$, since N is not connected; see Theorem 5.4.

We also remark that the group N cannot be replaced by the Weyl group W of G in the statement of Proposition 4.3. In other words, the inequality $\mathrm{ed}(G) \leq \mathrm{ed}(W)$ is false in general. For example, if $G = \mathrm{PGL}_4$ then $W = S_4$ and thus $\mathrm{ed}(W) = 2$; see [BR_1, Thm. 6.5]. On the other hand, $\mathrm{ed}(\mathrm{PGL}_4) \geq 4$; see Theorem 9.3. $\square$

4.2 An application

Theorem 4.5 $\mathrm{ed}(\mathrm{PGL}_n) \leq n^2 - 2n$ *for every* $n \geq 4$.

Proof. Let T be a maximal torus in PGL_n and let N be the normalizer of T. By Proposition 4.3 it is sufficient to show that $\mathrm{ed}(N) \leq n^2 - 2n$. We therefore take a closer look at N. The maximal torus T can be thought of as $(k^*)^n/\Delta$, where $\Delta \simeq k^*$ is the diagonal subgroup of $(k^*)^n$. Then N can be written as a semidirect product $T \times_\phi S_n$, where $\phi : S_n \longrightarrow \mathrm{Aut}(T)$ is given by permuting the n factors of k^*.

We will now construct a linear representation V of N. Let V be the k-vector space freely spanned by the $n(n-1)$ basis vectors e_{ij}, where $i, j = 1, \ldots, n$ and $i \neq j$. We shall denote $\sum x_{ij} e_{ij}$ by (x_{ij}). The action of N on V is defined as follows. Write an element of N as (t, σ), where $t = (t_1, \ldots, t_n)$ (modulo Δ) and $\sigma \in S_n$. Then

$$(t, \sigma) : e_{ij} \mapsto t_{\sigma(i)} t^{-1}_{\sigma(j)} e_{\sigma(i)\sigma(j)} \ .$$

One can check that this action is generically free and thus

$$\mathrm{ed}(N) = \mathrm{ed}(V, N) \leq \dim(V/N) = \dim(V) - \dim(N) = n^2 - 2n + 1 \ .$$

We shall, instead, derive the slightly better bound of Theorem 4.5 by considering the N-action on the projective space $P(V)$.

Lemma 4.6 *The action of* N *on* $P(V)$ *is generically free.*

Proof. Let a, a', b, b are four distinct integers between 1 and n. Define a rational function $z_{(a,a')(b,b')}$ on $P(V)$ by

$$z_{(a,a')(b,b')} = \frac{x_{ab} x_{a'b'}}{x_{ab'} x_{a'b}} \ .$$

Note that $z_{(a,a')(b,b')} = z_{(c,c')(d,d')}$ implies $\{a, a'\} = \{c, c'\}$ and $\{b, b'\} = \{d, d'\}$. Let U be the dense N-invariant open subset of V consisting of those $p \in P(V)$ satisfying
(i) $x_{ij}(p) \neq 0$ for every distinct $i, j = 1, \ldots, n$, and
(ii) $z_{(a,a')(b,b')}(p) \neq z_{(c,c')(d,d')}(p)$ whenever $\{a, a'\} \neq \{c, c'\}$ or $\{b, b'\} \neq \{d, d'\}$.

We claim that N acts freely on U. Indeed, let $p \in U$ and suppose $(t, \sigma)p = p$ for some $(t, \sigma) \in N$. Note that the functions $z_{(a,a')(b,b')}$ are T-invariant and

$$(t, \sigma) z_{(a,a')(b,b')} = z_{(\sigma(a),\sigma(a'))(\sigma(b)\sigma(b'))} \ .$$

Thus if $p \in U$, then $\{\sigma(a), \sigma(a')\} = \{a, a'\}$ and $\{\sigma(b), \sigma(b')\} = \{b, b'\}$ for every 4-tuple a, a', b, b' of distinct integers between 1 and n. If $n \geq 4$ then the only $\sigma \in S_n$ with this property is the identity element.

We have thus proved that if $p \in U$ and $(t, \sigma)p = p$ then $\sigma = 1$ in S_n. We now want to show that $t = 1$ in T. Indeed, since every coordinate x_{ij} of p is assumed to be non-zero, $(t,1)p = p$ implies $t_a t_b^{-1} = t_c t_d^{-1}$ for every $1 \le a,b,c,d \le n$ with $a \ne b$ and $c \ne d$. Letting $b = d = 1$, we see that $t_2 = t_3 = \ldots = t_n$. Similarly for $b = d = 2$ we obtain $t_1 = t_3 = \ldots = t_n$. Thus $t_1 = \ldots = t_n$, i.e., $t = 1$ in T. This completes the proof of the lemma. □

To finish the proof of the theorem, consider the natural (N-equivariant) projection map $V \dashrightarrow P(V)$. By Lemma 4.6 this map is an N-compression. Thus by Lemma 3.3(a-b) $\mathrm{ed}(N) \le \dim(P(V)) - \dim(N) = (n^2 - n - 1) - (n - 1) = n^2 - 2n$, as claimed. □

Remark 4.7 In Section 9 we will strengthen the upper bound of Theorem 4.5 for every n which is not a power of 2; see Theorem 9.6 and Remark 9.9.

5 Groups of low essential dimension

The results of this section have been suggested to us by V. L. Popov.

5.1 Rational sections

Let X be a primitive G-variety (see Definition 2.1) and let $\pi : X \dashrightarrow X/G$ be the rational quotient map for the G-action on X. A subvariety $S \subset X$ is said to be a *rational section* if $\pi_{|S} : S \dashrightarrow X/G$ is a birational isomorphism.

Remark 5.1 *S is a rational section of X if and only if S is a (G,H)-section with $H = \{1_G\}$.* Indeed, if S is a $(G,\{1\})$-section then $\pi_{|S} : S \dashrightarrow X/G$ is a birational isomorphism by Lemma 2.11. The opposite implication follows from Theorem 2.3. □

Lemma 5.2 *Let X be a primitive generically free G-variety. Then* $\mathrm{ed}(X,G) = 0$ *if and only if X has a rational section.*

Proof. Suppose $\mathrm{ed}(X,G) = 0$. Then there exists a G-compression $f : X \dashrightarrow Y$, where Y/G is a point. In other words, there is a point $y \in Y$ such that Gy is dense in Y and $\mathrm{Stab}(y) = \{1_G\}$. It is now easy to see that $S = f^{-1}(y)$ is a $(G,\{1\})$-section, and, hence, a rational section; see Remark 5.1.

Conversely, suppose $S \subset X$ is a rational section. Then S is a $(G,\{1\})$-section; hence, by Lemmas 4.1 and 3.3(e), $\mathrm{ed}(X,G) \le \mathrm{ed}(S,\{1\}) = 0$. □

5.2 Special groups

Let G be an algebraic group defined over k. Recall that G is called *special* if $H^1(K,G) = \{1\}$ for every field K containing k. Special groups were introduced by Serre [Se_1] and classified by Grothendieck [G].

Proposition 5.3 *The following conditions are equivalent:*

(a) G is a special group,

(b) $\mathrm{ed}(X,G)=0$ *for every primitive generically free G-variety X,*

(c) $\mathrm{ed}(G)=0$.

Proof. By Lemma 5.2 condition (b) is equivalent to

(b′) every primitive generically free G-variety has a rational section

and (c) is equivalent to

(c′) every generically free linear representation of G has a rational section.

It is well known that conditions (a), (b') and (c') are equivalent; see e.g., [Po, 1.4], [PV, Section 2.6], or [Do, Sect. 7]. Hence, so are (a), (b), and (c). □

Combining Proposition 5.3 with Grothendieck's classification, of special groups (see [G, Section 5] or [PV, Theorem 2.8]), we obtain the following result.

Theorem 5.4 *Let G be an algebraic group defined over k. Then* $\mathrm{ed}(G)=0$ *if and only if G is connected and its maximal connected semisimple subgroup is a direct product $G_1\times\ldots\times G_r$, where each G_i is of type* SL *or* Sp. □

5.3 n-special groups

Definition 5.5 We will say that an algebraic group G defined over k is n-special if $H^1(K,G)=\{1\}$ for any extension K/k of transcendence degree $\le n$.

Note that a special group is n-special for every n.

Proposition 5.6 *Let G be an n-special algebraic group and let X be a generically free primitive G-variety. Then*

(a) either $\mathrm{ed}(X,G)=0$ *or* $\mathrm{ed}(X,G)\ge n+1$ *and*

(b) either $\mathrm{ed}(G)=0$ *or* $\mathrm{ed}(G)\ge n+1$.

Proof. (a) Assume the contrary: $\mathrm{ed}(X,G)=i$, where $1\le i\le n$. Then there exists a compression $\alpha : X \dashrightarrow Y$ such that $\mathrm{trdeg}_k\, k(Y)^G=\dim(Y/G)=i$. Recall that the generically free action of G on Y determines an element of $H^1(k(Y/G),G)$; following Popov [Po, 1.3], we shall denote this class by $cl(G:Y)$. By our assumption $H^1(k(Y/G),G)=\{1\}$ and thus $cl(G,Y)=1$. Consequently, Y has a rational section; see [Po, 1.4.1]. By Lemma 5.2, this implies that $\mathrm{ed}(Y,G)=0$. Thus $\mathrm{ed}(X,G)\le \mathrm{ed}(Y,G)=0$ (see Lemma 3.3(b)), contradicting our assumption.

Part (b) is an immediate consequence of (a) and Definition 3.5. □

Corollary 5.7 *Let G be a connected algebraic group. Then*

(a) $\mathrm{ed}(X, G) \neq 1$ *for any irreducible G-variety X.*

(b) $\mathrm{ed}(G) \neq 1$.

Proof. By a theorem of Steinberg [St, Thm. 1.9] every connected group is 1-special. □

Remark 5.8 Note that Corollary 5.7 fails if G is not assumed to be connected. For example, $\mathrm{ed}(G) = 1$ if G is a (finite) cyclic or odd dihedral group; see [BR_1, 6.2].

Remark 5.9 A conjecture of Serre [Se_3, III.3.1] (often referred to as "Conjecture II") says that every simply connected semisimple group G is 2-special. This conjecture has been verified for all simple groups other than E_8; see [Se_3, Sect 5], [Se_4, III.3], [BP], [Ko_2], and [Gi].

6 Structured spaces I

6.1 Definition and examples

Definition 6.1 Let F be a field.

(a) A structured space over F is a pair (W, β), where W is a finite-dimensional F-vector space and β is a tensor on W, i.e., $\beta \in T(W) \otimes T(W^*)$. If F'/F is a field extension then $(W, \beta) \otimes_F F'$ is defined to be the structured space (W', β'), where $W' = W \otimes_F F'$ and $\beta' = \beta \otimes 1 \in T(W) \otimes T(W^*) \otimes F' = T(W') \otimes T(W'^*)$.

(b) Two structured spaces (W, β) and (W', β') over F are isomorphic if there exists an isomorphism $\phi : W \longrightarrow W'$ of F-vector spaces such that $\phi^*(\beta) = \beta'$, where ϕ^* is the isomorphism $T(W) \otimes T(W^*) \longrightarrow T(W') \otimes T(W'^*)$ induced by ϕ.

(c) In the special case where A is a finite-dimensional F-algebra, W is the underlying F-vector space of A and the multiplicative structure is given by a tensor $\beta \in W^* \otimes W^* \otimes W$, we will write $A = (W, \beta)$. Note that here the algebra A is not assumed to be commutative or associative, or to have an identity element.

Remark 6.2 The above definition is essentially the same as the one in [Se_2, X.2] or [Se_4, III.1.1]. The only difference is that we do not require α to be homogeneous, i.e., to lie in $T^p(W) \otimes T^q(W^*)$ for some $p, q \geq 0$; see Example 6.3(e) below.

We will always assume (as we do elsewhere in this paper) that F is a field extension of k; if $F = k$ we will usually denote our structured spaces by (V, α). In this case we will be interested in the algebraic group $\mathrm{Aut}_k(V, \alpha) \overset{\text{def}}{=} \{g \in \mathrm{GL}(V) \mid g^*(\alpha) = \alpha\}$. The following examples will be of special interest to us in the sequel.

Example 6.3 (a) $V = k^n$ and $\alpha = 0$. Then $\mathrm{Aut}_k(V, \alpha) = \mathrm{GL}_n$.

(b) $V = k^n$ and $0 \neq \alpha \in \Lambda^n(V^*)$ is a volume form on V. Then $\mathrm{Aut}_k(V, \alpha) = \mathrm{SL}_n$.

(c) $V = k^{2n}$ and $\alpha \in \Lambda^2(V^*)$ is a symplectic (i.e., non-degenerate skew-symmetric bilinear) form. Then $\mathrm{Aut}_k(V, \alpha) = \mathrm{Sp}_{2n}$.

(d) $V = k^n$ and $\alpha \in S^2(V^*)$ is a non-degenerate symmetric bilinear form. Then $\mathrm{Aut}_k(V, \alpha) = O_n$.

(e) $V = k^n$ and $\alpha = \alpha_1 + \alpha_2$, where $\alpha_1 \in \Lambda^n(W^*)$ is a volume form and $\alpha_2 \in S^2(W^*)$ is a non-degenerate symmetric bilinear form. Then any element $g \in \mathrm{GL}(V)$ preserving α has to preserve both α_1 and α_2. Thus $\mathrm{Aut}_k(V, \alpha) = \mathrm{SL}_n \cap O_n = SO_n$.

(f) (V, α) is the algebra $k \oplus \ldots \oplus k$ (n times); see Definition 6.1(c). Then $\mathrm{Aut}_k(V, \alpha)$ is the symmetric group S_n.

(g) $(V, \alpha) = \mathrm{M}_n(k)$ is the algebra of $n \times n$-matrices over k. Then $\mathrm{Aut}_k(V, \alpha) = \mathrm{PGL}_n$.

(h) $(V, \alpha) = \mathbf{O}$, where $\mathbf{O}$ is the (split) octonion algebra over k; see Section 11.1. Then $\mathrm{Aut}_k(\mathbf{O})$ is the exceptional group G_2.

(i) $(V, \alpha) = \mathbf{A}$, where $\mathbf{A}$ is the (split) Albert algebra over k; see Section 11.3. Then $\mathrm{Aut}_k(V, \alpha)$ is the exceptional group F_4.

(j) $V = k^{27}$ is the underlying vector space of the Albert algebra $\mathbf{A}$ and $\alpha \in V^* \otimes V^* \otimes V^*$ be the trilinear form associated to the cubic norm on $\mathbf{A}$; see Sections 11.3 and 11.5. Then $\mathrm{Aut}(V, \alpha)$ is the (simply connected) exceptional group E_6.

6.2 First properties

Let (W, β) be a structured space defined over a field F containing k. Suppose $B = \{b_1, \ldots, b_n\}$ is an F-basis of W. Denote the dual basis of W^* by $B^* = \{(b_1)^*, \ldots, (b_n)^*\}$. Then the tensors $b_I = b_{i_1} \otimes \ldots \otimes b_{i_r}$ form an F-basis of $T(W)$, as r ranges over the positive integers, $I = (i_1, \ldots, i_r)$, and each i_j ranges over $\{1, \ldots, n\}$. Similarly, the tensors $(b_J)^* = (b_{j_1})^* \otimes \ldots \otimes (b_{j_s})^*$ form an F-basis of $T^*(W)$. Thus we can write

$$\beta = \sum_{I,J} \beta_I^J(B)\, b_I \otimes b_J^* \,, \tag{6}$$

where each coefficient $\beta_I^J(B)$ lies in F. Note that only finitely many of these coefficients are non-zero.

Let $(V = k^n, \alpha)$ be a structured space and $G = \mathrm{Aut}_k(V, \alpha)$. Note that the G-action on V may not be generically free; however, the (diagonal) G-action on V^n is always free on the open subset $(V^n)'$ consisting of n-tuples of linearly independent elements. (We prefer the notation $(V^n)'$ to $\mathrm{GL}(V)$, since we view this set as a Zariski open subset of V^n and ignore the group structure.)

Let $B \in (V^n)'$ be a basis of V. Write $\alpha = \sum_{I,J} \alpha_I^J(B)\, b_I \otimes b_J^*$, as in (6). Then each α_I^J can be viewed as a function $(V^n)' \longrightarrow k$, which takes $B \in (V^n)'$ to $\alpha_I^J(B)$. It is easy to see that the functions α_I^J are regular on $(V^n)'$ and thus rational on V^n.

Lemma 6.4 *Let $V = k^n$, $\alpha \in T(V) \otimes T(V^*)$, $G = \mathrm{Aut}_k(\alpha)$ and $(V^n)' \subset V^n$ be as above. Suppose $B, B' \in (V^n)'$. Then*

(a) $B' = gB$ for some $g \in G$ if and only if $\alpha_I^J(B) = \alpha_I^J(B')$ for every I and J.

(b) If Z is a G-invariant subvariety of V^n such that $Z \cap (V^n)' \neq \emptyset$ then $k(Z)^G = k(\alpha_I^J{}_{|Z})$, where I ranges over $\{1, \ldots, n\}^r$ and J ranges over $\{1, \ldots, n\}^s$.

Proof. (a) Write $B' = gB$ for some $g \in GL(V)$ and observe that $g \in G = \mathrm{Aut}_k(V, \alpha)$ if and only if $\alpha_I^J(B) = \alpha_I^J(B')$ for every I and J.

(b) Each α_I^J defines a regular map $(V^n)' \longrightarrow k$; together they define a regular map $f : (V^n)' \longrightarrow k^N$, where N is the number of non-zero α_I^J's. Denote $f(Z \cap (V^n)')$ by Z_0. By part (a) f separates the G-orbits in $(V^n)'$ and, hence, in $Z \cap (V^n)'$. Thus by Remark 2.5, Z_0 is birationally isomorphic to Z/G; hence, $k(Z)^G = k(Z/G) = k(Z_0) = k(\alpha_I^J{}_{|Z})$, as claimed. $\square$

7 Spaces of rational maps

7.1 Equivariant maps into vector spaces

Proposition 7.1 *Let G be an algebraic group and let V be a linear representation of G. Then for every generically free G-variety X and every $v \in V$, there exists a G-equivariant rational map $f : X \dashrightarrow V$ whose image contains v.*

Proof. Suppose the action of G on V is given by the group homomorphism $\phi : G \longrightarrow \mathrm{GL}_n$, where $n = \dim(V)$. We may assume without loss of generality that ϕ is injective. Indeed, otherwise we can replace V by $V' = V \oplus W$, where W is a generically free linear representation of G. If we can construct a G-equivariant rational map $X \dashrightarrow V'$ whose image contains $(v, 0)$, then the composition of this map with the projection $V' = V \oplus W \longrightarrow V$ will have the desired properties.

Note that we may also assume without loss of generality that X is primitive. Indeed, by Lemma 2.2 X is isomorphic to a disjoint union of primitive varieties. It is enough to define f on one of them; after that the others can be sent to 0.

Thus we can think of G as a subgroup of $\mathrm{GL}_n = \mathrm{GL}(V)$; the G-action on V is then given by left multiplication. Let $X' = \mathrm{GL}_n *_G X$; see Definition 2.12. Recall that X' is a generically free GL_n-variety; see Remark 2.13. Since GL_n is a special group, Proposition 5.3 tells us that $\mathrm{ed}(X', \mathrm{GL}_n) = 0$. This means that there exists a GL_n-compression $\alpha : X' \dashrightarrow O$, where O is a single GL_n-orbit with trivial stabilizer. In other words, up to birational isomorphism of GL_n-varieties, $O \simeq V^n \simeq \mathrm{M}_n$, where GL_n acts on M_n by left multiplication.

Note that the image of α contains every non-singular matrix in M_n (these matrices form a single dense GL_n-orbit). In particular, there exists an $x' = (g, x) \in X'$ such that $\alpha(x') = I_n = n \times n$-identity matrix. Then $\alpha(1_G, x) = g^{-1}$. Let $v_1, \ldots, v_n$ be the columns of g^{-1}; since they are linearly independent, we can write

$$v = c_1 v_1 + \ldots + c_n v_n$$

for some $c_1, \dots, c_n \in k$. Let $\beta : \mathrm{M}_n \longrightarrow V$ be the linear map given by

$$\beta(A) = A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} .$$

Note that β is GL_n-equivariant and $\beta(g^{-1}) = v$. Now the desired map $f : X \dashrightarrow V$ is obtained as a composition

$$X \hookrightarrow X' = \mathrm{GL}_n *_G X \overset{\alpha}{\dashrightarrow} \mathrm{M}_n \overset{\beta}{\longrightarrow} V \ ,$$

where the inclusion $X \hookrightarrow X'$ is given by $x \mapsto (1_G, x)$; see Remark 2.13. This inclusion is clearly G-equivariant; the maps α and β are GL_n-equivariant (and, hence, G-equivariant) by our construction. Hence, f is G-equivariant and $f(x) = v$, as desired. $\square$

Remark 7.2 Let G be an algebraic group, X be a generically free primitive G-variety and V be a generically free linear representation of G. Then combining Proposition 7.1 with Lemma 3.3(c), we obtain the inequality $\mathrm{ed}(X, G) \leq \mathrm{ed}(V, G) \overset{\mathrm{def}}{=} \mathrm{ed}(G)$. This gives another proof of Theorem 3.4(c). $\square$

Definition 7.3 Let G be an algebraic group, $G \longrightarrow \mathrm{GL}(V)$ be a linear representation of G and X be a G-variety. We shall denote the $k(X)^G$-vector space of G-equivariant rational maps $X \dashrightarrow V$ by $RMaps_G(X, V)$.

Equivalently, $RMaps_G(X, V) = (V \otimes_k k(X))^G$.

Lemma 7.4 *Let $V = k^n$, let $G \longrightarrow \mathrm{GL}(V)$ be a linear representation of G, and let X be a primitive G-variety. Then*

(a) $b_1, \dots, b_m \in RMaps_G(X, V)$ are linearly independent over $k(X)^G$ if and only if $b_1(x), \dots, b_m(x)$ are linearly independent over k for x in general position in X.

(b) If X is generically free then $\dim_{k(X)^G}(RMaps_G(X, V)) = n$.

Proof. (a) Suppose $b_1(x), \dots, b_m(x)$ are linearly independent for $x \in X$ in general position and $\sum_{i=1}^m f_i b_i = 0$ for some $f_1, \dots, f_m \in k(X)^G$. Then evaluating both sides at $x \in X$ in general position, we conclude that $f_1 = \ldots = f_m = 0$ in $k(X)^G$ and thus $b_1, \dots, b_m$ are $k(X)^G$-linearly independent.

Conversely, suppose $b_1(x), \dots, b_m(x)$ are k-linearly dependent for $x \in X$ in general position. Then we may assume without loss of generality that $b_1(x), \dots, b_{m-1}(x)$ are linearly independent for x in general position; otherwise, we can simply replace $b_1, \dots, b_m$ by $b_1, \dots, b_{m-1}$. Thus for each x in general position in X, there exist uniquely defined $f_1(x), \dots, f_{m-1}(x) \in k$ such that

$$b_m = f_1 b_1 + \ldots + f_{m-1} b_{m-1} \ . \tag{7}$$

It remains to prove that $f_1, \ldots, f_{m-1} \in k(X)^G$. By Cramer's rule $f_1, \ldots, f_{m-1} \in k(X)$. To prove these functions are G-invariant, choose $x \in X$ and $g \in G$, then substitute gx into (7) and apply g^{-1} to both sides. Since each b_i is a G-equivariant map $X \dashrightarrow V$, we have $g^{-1}b_i(gx) = b_i(x)$ and thus

$$b_m(x) = f_1(gx)b_1(x) + \ldots + f_{m-1}(gx)b_{m-1}(x) .$$

By uniqueness of $f_i(x)$, we conclude that $f_i(gx) = f_i(x)$, i.e., $f_i \in k(X)^G$, as claimed.

(b) The inequality $\dim_{k(X)^G} RMaps(X, V) \leq n$ is a direct consequence of part (a). To prove the opposite inequality, let $v_1, \ldots, v_n$ be a k-basis of V, $v = (v_1, \ldots, v_n) \in V^n$. By Proposition 7.1 there exists a rational G-equivariant map $b : X \dashrightarrow V^n$ whose image contains v. Write $b = (b_1, \ldots, b_n)$, where each b_i is a rational G-equivariant map $X \dashrightarrow V$, i.e., and element of $RMaps_G(X, V)$. In order to complete the proof of part (b), it is enough to show that $b_1, \ldots, b_n$ are $k(X)^G$-linearly independent. Let S be the set of $x \in X$ such that $b_1(x), \ldots, b_n(x)$ are k-linearly independent. Clearly S is an open G-invariant subset of X; moreover, since the image of b contains v, $S \neq \emptyset$. Thus S is open and dense in X; the desired conclusion now follows from part (a). $\square$

7.2 Structured spaces of rational maps

Let $(V = k^n, \alpha)$ be a structured space, let $G = \mathrm{Aut}_k(V, \alpha)$, and let H be an algebraic subgroup of G, as above. In this setting $RMaps_H(X, V)$ carries a naturally defined tensor, which we shall denote by α_H^X. To define α_H^X, choose a $k(X)^H$-basis $B = \{b_1, \ldots, b_n\}$ of $RMaps_H(X, V)$. Then

$$\alpha_H^X \stackrel{\text{def}}{=} \sum_{I,J} (\alpha_H^X)_I^J \, b_I \otimes (b^*)_J ,$$

where we define $(\alpha_H^X)_I^J \in k(X)^H$ (as a rational function on X) by

$$(\alpha_H^X)_I^J(x) = \alpha_I^J(B(x)) . \tag{8}$$

Here $B(x) = \{b_1(x), \ldots, b_n(x)\}$ is a basis of V (for x in general position in X). Note that since H is a subgroup of $G = \mathrm{Aut}_k(V, \alpha)$, each function $x \mapsto \alpha_I^J(B(x))$ is, indeed, an element of $k(X)^H$. Moreover, it is easy to see that our definition of α_H^X does not depend on the choice of B.

Example 7.5 Suppose $\alpha \in V^* \otimes V^* \otimes V$ defines the structure of an algebra A on V, i.e., $(V, \alpha) = A$; see Definition 6.1(c). Then the structured space $(RMaps_H(X, V), \alpha_H^X)$ is the algebra of H-equivariant rational maps $X \dashrightarrow V$, with pointwise multiplication.

Lemma 7.6 *Let $(V = k^n, \alpha)$ be a structured space, H be an algebraic subgroup of $G = \mathrm{Aut}_k(V, \alpha)$, and X be a generically free primitive G-variety.*

(a) Suppose $f : X \dashrightarrow Y$ is an H-compression. Then

$$(RMaps_H(X,V), \alpha_H^X) \simeq (RMaps_H(Y,V), \alpha_H^Y) \otimes_{k(Y)^H} k(X)^H ,$$

where the field extension $k(X)^H/k(Y)^H$ is induced by f.

(b) Suppose S is an (H, H')-section of X. Then

$$(RMaps_H(X,V), \alpha_H^X) \simeq (RMaps_{H'}(S,V), \alpha_{H'}^S) .$$

(c) Suppose $X = H \times X_0$, where X_0 is an irreducible variety and H acts on X by $h(h', x_0) = (hh', x_0)$. Then $(RMaps_H(X,V), \alpha_H^X) \simeq (V, \alpha) \otimes_k k(X_0)$.

Proof. (a) Let $\phi : RMaps_H(Y,V) \otimes_{k(Y)^H} k(X)^H \longrightarrow RMaps_H(X,V)$ be $k(X)^H$-linear map given by $a \otimes 1 \longrightarrow a \circ f$. If $C = \{c_1, \dots, c_n\}$ is a $k(Y)^H$-basis of $RMaps_H(Y,V)$ then Lemma 7.4 shows that $\phi(C)$ is a $k(X)^H$-basis of $RMaps_H(Y,V)$. This proves that ϕ is an isomorphism of $k(X)^H$-vector spaces. Comparing the coefficients of α_H^X in the basis C to the coefficients of α_H^Y in the basis $\phi(C)$, we conclude that ϕ is an isomorphism of structured spaces.

(b) Let $B = \{b_1, \dots, b_n\}$ be a $k(X)^H$-basis of $RMaps_H(X,V)$. Recall that by Lemma 2.11, the restriction $a \mapsto a_{|S}$ induces an isomorphism between the fields $k(X)^H$ and $k(S)^{H'}$. We will therefore identify these fields. Moreover, by Lemma 7.4, $B_{|S} = \{(b_1)_{|S}, \dots, (b_n)_{|S}\}$ is a basis of $RMaps_{H'}(S,V)$. Hence, $\phi : a \mapsto a_{|S}$ gives rise to an isomomorphism $\phi : RMaps_H(X,V) \longrightarrow RMaps_{H'}(S,V)$ of $k(X)^H$-vector spaces. To show that ϕ induces the desired isomorphism of structured spaces, observe that if we restrict the coefficients of α_H^X in the basis B to S, we obtain the coefficients of $\alpha_{H'}^S$; see (8).

(c) Note that $\{1\} \times X_0$ is an $(H, \{1\})$-section of X. Thus by part (b), we may assume $H = \{1\}$ and $X = X_0$. Now apply part (a) to the $\{1\}$-compression $X \longrightarrow \{pt\}$, where $\{pt\}$ is a single point. Since $(RMaps_{\{1\}}(\{pt\}, V), \alpha_{\{1\}}^{\{pt\}}) = (V, \alpha)$, this completes the proof. □

8 Structured spaces II

8.1 Structured spaces of type (V, α)

Definition 8.1 Let F be a field containing k and let $(V = k^n, \alpha)$ be a structured space. We shall say that $(W = F^n, \beta)$ is a structured space of type (V, α) if

$$(W, \beta) \otimes_F E \simeq (V, \alpha) \otimes_k E \tag{9}$$

for some field extension E/F.

Remark 8.2 A structured space $(W = F^n, \beta)$ of type (V, α) is usually called "an F/k-form of (V, α)"; see e.g., [Se$_4$, III.1]. We will use the term "structured space" in order to avoid linguistic confusion in those cases where α and β are themselves multilinear forms, as in, e.g., Example 6.3(b), (c), (d), (j).

Remark 8.3 If (W, β) is a structured space of type (V, α) then we can always choose the field extension E/F in Definition 8.1 to be finitely generated. Indeed, if $v_1, \ldots, v_n$ is a k-basis of V, $w_1, \ldots, w_n$ is an F-basis of W and the isomorphism (9) is given by $w_i \mapsto \sum_j a_{ij} v_{ij}$ with $a_{ij} \in E$ then we can replace E by $F(a_{ij})$.

Example 8.4 (a) Suppose $V = k^n$ and α is a volume (resp. non-degenerate symmetric bilinear) form on V. Then (W, β) is of type (V, α) if and only if $W = F^n$ and β is a a volume (resp. non-degenerate symmetric bilinear) form on W.

(b) Let $V = k^n$, let $e_1, \ldots, e_n$ be a k-basis of V, $\alpha_1 = e_1^* \wedge \ldots \wedge e_n^* \in \Lambda^n(V)$, $\alpha_2 = (e_1^*)^2 + \ldots + (e_n^*)^2 \in S^2(V)$, and $\alpha = \alpha_1 + \alpha_2$. Recall that $\mathrm{Aut}_k(V, \alpha) = SO_n$; see Example 6.3(e). Now let F be a field extension of k and $W = F^n$. Then an easy linear algebra argument shows that $\beta_2 \mapsto (W, \alpha_1 \otimes_k F + \beta_2)$ defines a bijection between equivalence classes of bilinear forms of determinant 1 on W (modulo $\mathrm{SL}(W)$) and isomorphism classes of structured spaces (W, β) of type (V, α); cf. [KMRT, (29.29), p. 407].

(c) Suppose (V, α) is the algebra $k \oplus \ldots \oplus k$ (n times), as in Example 6.3(f). Then (W, β) is of type (V, α) if and only if β defines the structure of an n-dimensional etale algebra over F, i.e., a direct sum of field extensions of F; cf. [KMRT, (29.9), p. 395].

(d) Suppose $(V = k^{27}, \alpha) = \mathbf{A}$, where $\mathbf{A}$ is the (split) Albert algebra; see Section 11.3. Then (W, β) is structured spaces of type (V, α) if and only if $W = F^{27}$ and β defines the structure of a central simple exceptional Jordan algebra on W; see [J, Sect V.7].

For other examples see Lemma 9.1 and Remark 11.4.

Lemma 8.5 *Suppose $(V = k^n, \alpha)$ is a structured space with automorphism group $G = \mathrm{Aut}_k(V, \alpha)$. Let H be an algebraic subgroup of G, and let X be a primitive generically free H-variety. Then $(RMaps_H(X, V), \alpha_H^X)$ is a structured space of type (V, α).*

Proof. We may assume without loss of generality that X is irreducible. Indeed, otherwise an irreducible component X_1 of X is an (H, H_1)-section (see Example 2.10); we can thus replace X by X_1, H by H_1 and then appeal to Lemma 7.6(b).

For irreducible X, consider the H-compression $f : H \times X \longrightarrow X$, where H acts on $H \times X$ by $h'(h, x) = (h'h, x)$ and $f(h, x) = hx$. Now apply Lemma 7.6(a) to this compression; the desired conclusion then follows from Lemma 7.6(c). □

Proposition 8.6 *Let $(V = k^n, \alpha)$ be a structured space with automorphism group $G = \mathrm{Aut}_k(V, \alpha)$, and let F be a finitely generated field extension of k. Then*

(a) a structured space $(W = F^n, \beta)$ is of type (V, α) if and only if there exists a generically free primitive G-variety X such that $(W, \beta) \simeq (RMaps_G(X, V), \alpha_G^X)$.

(b) Suppose X and X' are generically free primitive G-varieties such that $k(X)^G = k(X')^G$ and $(RMaps_G(X, V), \alpha_G^X) \simeq (RMaps_G(X', V), \alpha_G^{X'})$ (as structured spaces). Then $X \simeq X'$ (as G-varieties).

Proof. (a) The "if" assertion follows from Lemma 8.5. To prove the converse, assume $(W = F^n, \beta)$ is a structured space of type $(V = k^n, \alpha)$. Choose E/F as in Definition 8.1. By Remark 8.3 we may assume that E is finitely generated over F and, hence, over k. Thus there exist irreducible varieties X_0 and Y_0 such that $E = k(Y_0)$, $F = k(X_0)$, and the field extension E/F is induced by a dominant rational morphism $\phi : Y_0 \dashrightarrow X_0$.

Let $B = \{b_1, \ldots, b_n\}$ be an F-basis of W. Then B is also an E-basis of $V \otimes_k E$; see (9). Recall that $(V, \alpha) \otimes_k E \simeq (RMaps_G(Y, V), \alpha_G^Y)$, where $Y = G \times Y_0$; see Lemma 7.6(c). Thus we can view $b_1, \ldots, b_n$ as G-equivariant rational maps $Y \dashrightarrow V$; together they define a G-equivariant rational map $b : Y \dashrightarrow V^n$. Let Z be the closure of $b(Y)$ in V^n. Note that $Z \cap (V^n)' \neq \emptyset$ (see Lemma 7.4) and thus the rational map $\overline{b} : Y_0 \dashrightarrow Z_0 = Z/G$ induced by $b : Y \dashrightarrow Z$ is given by $(\alpha_I^J)_{|Z} \mapsto \beta_I^J(B)$; see Remark 2.4 and Lemma 6.4(b). Since every $\beta_I^J(B)$ lies in F, $\overline{b}$ factors through X_0 (via ϕ). Consequently b factors through $X = X_0 \times_{Z_0} Z$. These maps are shown in the following diagram.

$$\begin{array}{ccccccc} b & : & Y = G \times Y_0 & \dashrightarrow & X = X_0 \times_{Z_0} Z & \overset{c}{\dashrightarrow} & Z \subset V^n \\ & & \downarrow & & \downarrow & & \downarrow \\ \overline{b} & : & Y_0 & \overset{\phi}{\dashrightarrow} & X_0 & \overset{\overline{c}}{\dashrightarrow} & Z_0 \subset (V^n)/G \end{array}$$

Here the vertical arrows represent quotient maps and c (resp. $\overline{c}$) is the map $X \dashrightarrow Z \subset V^n$ (resp. $X_0 \dashrightarrow Z_0 \subset V^n/G$) induced by b (resp. $\overline{b}$). Let $c = (c_1, \ldots, c_n)$, where each c_i is a G-equivariant rational map $X \dashrightarrow V$ and let $C = \{c_1, \ldots, c_n\}$. Since $Z \cap (V^n)' \neq \emptyset$, C is an F-basis of $RMaps_G(X, V)$; see Lemma 7.4. By our construction $(\alpha_G^X)_I^J(C) = \beta_I^J(B)$ for every I and J. This means that the structured spaces (W, β) and $RMaps_G(X, V)$ are isomorphic via the linear map $W \longrightarrow RMaps_G(X, V)$ which takes b_i to c_i.

(b) Denote the structured space $(RMaps_G(X, V), \alpha_G^X)$ by (W, β). We want to show that X can be uniquely recovered from (W, β). Let $C = \{c_1, \ldots, c_n\}$ be a basis of $W = RMaps_G(X, V)$, $c = (c_1, \ldots, c_n)$ be the rational map $X \dashrightarrow V^n$ defined by C, and Z be the closure of $c(X)$ in V^n. Then by Lemma 7.4, $Z \cap (V^n)' \neq \emptyset$; thus c induces a rational map $\overline{c} : X_0 \dashrightarrow Z_0$, where $Z_0 = \pi(Z) \simeq Z/G$ and $\pi : V^n \longrightarrow V^n/G$ is the quotient map. The maps c and $\overline{c}$ are shown in the diagram below.

$$\begin{array}{ccl} X & \overset{c}{\dashrightarrow} & Z \subset V^n \\ \downarrow & & \downarrow \ \pi \\ X_0 & \overset{\overline{c}}{\dashrightarrow} & Z_0 \subset (V^n)/G \end{array}$$

Here the vertical maps are quotient maps and $\overline{c}$ is given by $\alpha_I^J \mapsto \beta_I^J(C)$. (Recall that $k(V^n/G) = k(\alpha_I^J)$; see Lemma 6.4(b).) Now note that $X \simeq X_0 \times_{Z_0} Z$ (see Lemma 2.16(b)) and $Z = \pi^{-1}(Z_0)$.

This shows that X can be uniquely recovered from (W, β). More precisely, suppose

$$(RMaps_G(X, V), \alpha_G^X) \overset{\text{def}}{=} (W, \beta) \simeq (RMaps_G(X', V), \alpha_G^{X'})$$

via a map which sends the basis C of (W,β) to a basis D of $(RMaps_G(X',V),\alpha_G^{X'})$. Denote the G-equivariant rational morphism $(d_1,\dots,d_n) : X' \dashrightarrow V^n$ by d. Then the induced map $\overline{d} : X'/G = X_0 \dashrightarrow V^n/G$ of quotient spaces is the same as $\overline{c}$; thus $X' \simeq X_0 \times_{Z_0} Z \simeq X$, as claimed. □

8.2 Structured spaces and essential dimension

Definition 8.7 Let F be a field, $(W = F^n, \beta)$ be a structured space and F_0 be a subfield of F.

(a) We say that (W,β) is defined over F_0 if there exists an F-basis B of W such that every coefficient $\beta_I^J(B)$ of β with respect to this basis lies in F_0. Equivalently, (W,β) is defined over F_0 if and only if it is isomorphic to $(W_0,\beta_0)\otimes_{F_0} F$ for some structured space $(W_0 = F_0^n, \beta_0)$.

(b) $\tau(W,\beta) \stackrel{\text{def}}{=} \min\{\mathrm{trdeg}_k(F_0)\}$, where (W,β) is defined over F_0. Equivalently, $\tau(W,\beta) = \min\{\mathrm{trdeg}_k k(\beta_I^J(B) \mid I,J)\}$, as B ranges over all F-bases of W.

Theorem 8.8 *Let (V,α) be a structured space and $G = \mathrm{Aut}_k(V,\alpha)$.*

(a) If X is a generically free primitive G-variety then

$$\mathrm{ed}(X,G) = \tau(RMaps_G(X,V),\alpha_G^X).$$

(b) $\mathrm{ed}(G) = \max\{\tau(W,\beta)\}$*, where the maximum is taken over all structured spaces (W,β) of type (V,α).*

Proof. (a) Denote the structured space $(RMaps_G(X,V),\alpha_G^X)$ by (W,β).

If $X \dashrightarrow Y$ is a G-compression then by Lemma 7.6(a) the structured space (W,β) is defined over $k(Y)^G$. If we choose Y to be of minimal possible dimension, then $\mathrm{trdeg}_k k(Y)^G = \dim(Y/G) = \mathrm{ed}(X,G)$. This proves that $\tau(W,\beta) \le \mathrm{ed}(X,G)$.

To prove the opposite inequality, write $(W,\beta) \simeq (\tilde{W},\tilde{\beta}) \otimes_{\tilde{F}} F$, where $(\tilde{W},\tilde{\beta})$ is a structured space over $\tilde{F}$ and $\mathrm{trdeg}_k(\tilde{F}) = \tau(W,\beta)$. Note that since (W,β) is a structured space of type (V,α), so is $(\tilde{W},\tilde{\beta})$. Thus by Proposition 8.6(a),

$$(\tilde{W},\tilde{\beta}) \simeq (RMaps_G(\tilde{X}),\alpha_G^{\tilde{X}})$$

for some primitive generically free G-variety $\tilde{X}$ with $k(\tilde{X})^G = \tilde{F}$. On the other hand, the extension $F/\tilde{F}$ is given by a rational morphism $X/G \dashrightarrow \tilde{X}/G$ of algebraic varieties. Using this morphism we can construct the fiber product $Y = X/G \times_{\tilde{X}/G} \tilde{X}$. By Lemma 7.6(a),

$$\begin{gathered}(RMaps_G(Y,V),\alpha_G^Y) \simeq (RMaps_G(\tilde{X},V),\alpha_G^{\tilde{X}}) \otimes k(X)^G \simeq \\ (\tilde{W},\tilde{\beta}) \otimes_{\tilde{F}} F = (W,\beta) = (RMaps_G(X,V),\alpha_G^X)\,.\end{gathered}$$

Hence, by Proposition 8.6(b), X is birationally isomorphic to $Y = X/G \times_{\tilde{X}/G} \tilde{X}$. Since the natural projection $Y \longrightarrow \tilde{X}$ is a G-compression, we conclude that

$$\mathrm{ed}(X,G) = \mathrm{ed}(Y,G) \le \dim(\tilde{X}/G) = \mathrm{trdeg}_k\, k(\tilde{X}/G) = \mathrm{trdeg}_k\, \tilde{F} = \tau(W,\beta)\,,$$

as claimed.

(b) Recall that $\mathrm{ed}(G) = \max\{\mathrm{ed}(X, G)\}$, as X ranges over all generically free primitive G-varieties; see Definition 3.5. The desired conclusion now follows from part (a) and Proposition 8.6. $\square$

We conclude this section with two simple applications of Theorem 8.8. Other applications will be given in Sections 9-11.

Example 8.9 (a) Suppose $V = k^n$ and α be a volume form on V, so that $\mathrm{Aut}_k(V, \alpha) = \mathrm{SL}_n$. Then every volume β form on $W = F^n$ can be written as $b_1 \wedge \ldots \wedge b_n$ for some basis $b_1, \ldots, b_n$ of W. Thus every structured space (W, β) of type (V, α) is isomorphic to $(V, \alpha) \otimes_k F$, and, consequently, $\tau(W, \alpha) = 0$. Applying Theorem 8.8, we conclude that $\mathrm{ed}(\mathrm{SL}_n) = 0$; cf. Example 3.9(c) and Theorem 5.4.

(b) (cf. [Se_4, III.1.2(a)]) Suppose $V = k^{2n}$ and $\alpha \in \Lambda^2(V^*)$ is symplectic form on V. Then every symplectic form β form on $W = F^n$ can be written as

$$\beta = b_1^* \wedge b_2^* + \ldots + b_{2n-1}^* \wedge b_{2n}^*$$

in some basis $b_1, \ldots, b_n$ of W. This means that every structured space (W, β) of type (V, α) is isomorphic to $(V, \alpha) \otimes_k F$ and thus $\tau(W, \alpha) = 0$. By Theorem 8.8, we conclude that $\mathrm{ed}(\mathrm{Sp}_{2n}) = 0$; cf. Theorem 5.4.

9 Projective linear groups

9.1 Central simple algebras

Recall that $\mathrm{PGL}_n = \mathrm{Aut}_k(\mathrm{M}_n)$, where we view the matrix algebra $\mathrm{M}_n = \mathrm{M}_n(k)$ as a structured space (k^{n^2}, α); see Definition 6.1(c).

Lemma 9.1 *(Wedderburn; see e.g., [Se_2, X.5 Proposition 7] or [KMRT, 1.1]) Let F be a field containing k and let $W = F^{n^2}$. Then (W, β) is a structured space of type M_n if and only if $\beta \in W^* \otimes W^* \otimes W$ defines the structure of a central simple F-algebra on W.* $\square$

If A is a central simple algebra, we will denote the center of A by $Z(A)$. Division algebras will usually be denoted by D. Recall that $\mathrm{UD}(m, n)$ is the division algebra generated by m generic $n \times n$ matrices $X_1 = (x_{ij}^{(1)}), \ldots, X_m = (x_{ij}^{(m)})$. For a more detailed discussion of these algebras we refer the reader to [Pr_1, Part II] or [Pi, 20.8].

Lemma 9.2 *(a)* $\mathrm{ed}(\mathrm{PGL}_n) = \max\{\tau(A)\}$, *as A ranges over all central simple algebras of degree n whose center contains k.*

(b) $\mathrm{ed}(\mathrm{PGL}_n) = \tau(\mathrm{UD}(m, n))$ *for any $m \geq 2$.*

(c) $\mathrm{ed}(\mathrm{PGL}_n) = \max\{\tau(D)\}$, *as D ranges over all division algebras of degree n whose center contains k.*

Proof. Part (a) follows from Lemma 9.1 and Theorem 8.8(b). To prove part (b), consider the representation of PGL_n on $V_m = (\mathrm{M}_n)^m$ given by

$$g(a_1, \ldots, a_m) = (ga_1g^{-1}, \ldots, ga_mg^{-1}) \,.$$

The structured space $(RMaps_{\mathrm{PGL}_n}(V_m, V_1), \alpha^{V_m}_{\mathrm{PGL}_n})$ is the algebra of rational PGL_n-equivariant maps $V_m \longrightarrow V_1 = M_n$; see Example 7.5. By a theorem of Procesi this algebra is isomorphic to $\mathrm{UD}(m,n)$; see [Pr$_2$, Thm. 2.1]. (The isomorphism identifies $X_i \in \mathrm{UD}(m,n)$ with the projection map $\pi_i : V_m = (M_n)^m \longrightarrow M_n$ given by $\pi_i(a_1, \ldots, a_m) = a_i$). Now part (b) follows from Theorem 8.8(a). Part (c) is an immediate consequence of (a) and (b). $\square$

Theorem 9.3 $\mathrm{ed}(\mathrm{PGL}_{n^r}) \geq 2r$ *for any* $n \geq 2$ *and* $r \geq 1$.

Proof. [Re, Theorem 16.1(b)] shows that $\tau(\mathrm{UD}(2, n^r)) \geq 2r$. The desired conclusion now follows from Lemma 9.2(b). $\square$

9.2 Cyclic algebras

Lemma 9.4 *(a) If D is a division algebra of degree $n \geq 2$ then $\tau(D) \geq 2$.*

(b) If D is a cyclic division algebra then $\tau(D) = 2$.

(c) $\mathrm{ed}(\mathrm{PGL}_n) = 2$ *if* $n = 2$, 3, *and* 6.

Proof. (a) Assume the contrary: $D = D_0 \otimes_{K_0} K$, where K is the center of D and K_0 is the center of D_0 and $\mathrm{trdeg}_k(K_0) \leq 1$. Then D_0 cannot be a division algebra by Tsen's theorem (see e.g., [Pi, 19.4]), a contradiction. Another proof of part (a) can be deduced from Corollary 5.7(a) (with $G = \mathrm{PGL}_n$).

(b) Since D is cyclic, there are elements $x, y \in D$ such that $x^n = u \in K$, $y^n = v \in K$, $xy = \zeta yx$ where ζ is a primitive n-th root of unity. (Recall that we are assuming k is algebraically closed and of characteristic 0; in particular, $\zeta \in k$.) Examining the structure constants of D in the basis $B = \{x^iy^j \mid i, j = 0, \ldots, n-1\}$, we see that D is defined over the field $k(u, v)$. Thus $\tau(D) \leq \mathrm{trdeg}_k(u, v) \leq 2$. Part (b) follows from this inequality and part (a).

(c) Follows from part (b) and Lemma 9.2(c), since every division algebra of degree 2, 3, or 6 is cyclic; see e.g., [Pi, 15.6]. $\square$

9.3 Algebras of odd degree

In this section we use a theorem of Rowen [Row] to give an upper bound on $\mathrm{ed}(\mathrm{PGL}_n)$ for odd n.

Recall that by a theorem of Wedderburn every central simple algebra A with center F is of the form $A = \mathrm{M}_d(D)$, where D is a division algebra with center F. The algebra D is unique up to isomorphism (of F-algebras); we shall refer to it as the underlying division algebra of A. The degree of D is called the index of A and is denoted by $\mathrm{Ind}(A)$. Two central simple algebras with center F are called Brauer equivalent if they have F-isomorphic underlying division algebras. Brauer equivalence classes of central simple algebras form an abelian group under tensor products; this group is called the Brauer group of F and is denoted by $\mathrm{Br}(F)$. For a more detailed discussion of the structure theory of central simple algebras and the Brauer group we refer the reader to [Pi].

Lemma 9.5 *Let D_1 and D_2 be division algebras with center F. Suppose D_1 and D_2 generate the same cyclic subgroup of* $\mathrm{Br}(F)$. *Then $\tau(D_1) = \tau(D_2)$.*

Proof. By symmetry it is enough to show

$$\tau(D_1) \geq \tau(D_2) \tag{10}$$

Note that our assumption forces D_1 and D_2 to have the same degree, which we shall denote by n; see [Pi, Proposition 13.4(viii)]. Write $D_1 = E_1 \otimes_K F$, where E_1 is a subalgebra of D_1 of degree n, K is the center of E_1 and $\mathrm{trdeg}_k(K) = \tau(D_1)$. Suppose $D_1^{\otimes i} = \mathrm{M}_{n^{i-1}}(D_2)$, where i relatively prime to n. We claim that the central simple algebra $E_1^{\otimes i}$ has index n. Indeed, on the one hand, $\mathrm{Ind}(E_1^{\otimes i}) \leq \mathrm{Ind}(E_1) = n$ and, on the other hand, $\mathrm{Ind}(E_1^{\otimes i}) \geq \mathrm{Ind}(D_1^{\otimes i}) = n$. Thus we can write $E_1^{\otimes i} = \mathrm{M}_{n^{i-1}}(E_2)$ for some division algebra E_2 of degree n, with center K. We now claim that

$$D_2 = E_2 \otimes_K F \ . \tag{11}$$

Note that (11) immediately implies (10), since it says that D_2 is defined over K. To prove (11), observe that $\mathrm{M}_{n^{i-1}}(E_2) \otimes_K F = E_1^{\otimes i} \otimes_K F = D_1^{\otimes i} = \mathrm{M}_{n^{i-1}}(D_2)$. Now (11) follows from the uniqueness part of Wedderburn's theorem; see [Pi, Section 3.5]. □

Theorem 9.6 *Let $n \geq 3$ be an odd integer. Then* $\mathrm{ed}(\mathrm{PGL}_n) \leq n + \frac{(n-1)(n-2)}{2}$.

Proof. Let $D_1 = \mathrm{UD}(2, n)$ and D_2 be the underlying division algebra of $D_1^{\otimes 2}$. By a theorem of Rowen [Row], $\tau(D_2) \leq n + \frac{(n-1)(n-2)}{2}$. Combining Lemma 9.5 with Lemma 9.2(b), we obtain $\mathrm{ed}(\mathrm{PGL}_n) = \tau(D_1) = \tau(D_2) \leq n + \frac{(n-1)(n-2)}{2}$, as claimed. □

9.4 Algebras of composite degree

Lemma 9.7 *Suppose n_1 and n_2 are relatively prime positive integers. For $i = 1, 2$ let D_i be a division algebra of degree n_i with center F and let $D = D_1 \otimes_F D_2$. Then*

(a) $\tau(D_i) \leq \tau(D)$ for $i = 1, 2$.

(b) $\tau(D) \leq \tau(D_1) + \tau(D_2)$.

Proof. (a) Let E be a division subalgebra of D of degree n_1n_2 such that $\mathrm{trdeg}_k\, Z(E)$ is as small as possible, i.e., is equal to $\tau(D)$. Then we can write E as $E_1 \otimes_{Z(E)} E_2$, where $\deg(E_i) = n_i$ for $i = 1, 2$. Thus $D = E \otimes_{Z(E)} F = (E_1 \otimes_{Z(E)} F) \otimes_{Z(D)} (E_2 \otimes_{Z(E)} F)$. Since the decomposition $D = D_1 \otimes_{Z(D)} D_2$ is unique, we have $D_1 \simeq E_1 \otimes_{Z(E)} F$ and $D_2 \simeq E_2 \otimes_{Z(E)} F$. This means that D_1 and D_2 are both defined over $Z(E)$; consequently, $\tau(D_i) \le \tau(D)$ for $i = 1, 2$.

(b) Suppose the algebra D_i is defined over $F_i \subset F$ with $\mathrm{trdeg}_k(F_i) = \tau(D_i)$; here $i = 1, 2$. In other words, D_i has a subalgebra E_i of degree n_i whose center is F_i. Let $E = E_1E_2$ be the division subalgebra generated by E_1 and E_2 inside D. Then $D = E \otimes_{Z(E)} F$ and therefore D is defined over $Z(E)$. Note that $Z(E)$ is the subfield of F generated (over k) by F_1 and F_2. Hence, $\mathrm{trdeg}_k\, Z(E) \le \mathrm{trdeg}_k\, F_1 + \mathrm{trdeg}_k\, F_2 \le \tau(D_1) + \tau(D_2)$, as claimed. □

Proposition 9.8 *Let $n_1, n_2 \ge 2$ be relatively prime integers. Then*

(a) $\mathrm{ed}(\mathrm{PGL}_{n_i}) \le \mathrm{ed}(\mathrm{PGL}_{n_1n_2})$ *for $i = 1, 2$.*

(b) $\mathrm{ed}(\mathrm{PGL}_{n_1n_2}) \le \mathrm{ed}(\mathrm{PGL}_{n_1}) + \mathrm{ed}(\mathrm{PGL}_{n_2})$.

Proof. (a) It is enough to show that $\mathrm{ed}(\mathrm{PGL}_{n_1}) \le \mathrm{ed}(\mathrm{PGL}_{n_1n_2})$. Let $D_1 = \mathrm{UD}(Z(D_1))$, $D_2 = \mathrm{M}_{n_2}(Z(D_1))$, and $D = D_1 \otimes_{Z(D_1)} D_2 = M_{n_2}(D_1)$. The desired inequality now follows from Lemmas 9.2 and 9.7(a).

(b) The algebra $D = \mathrm{UD}(2, n_1n_2)$ can be written as $D_1 \otimes_{Z(D)} D_2$, where D_1 and D_2 are subalgebras of D of degrees n_1 and n_2 respectively; see, e.g., [Pi, 14.4]. Applying Lemmas 9.2 and 9.7(b), we obtain

$$\mathrm{ed}(\mathrm{PGL}_{n_1n_2}) = \tau(D) \le \tau(D_1) + \tau(D_2) \le \mathrm{ed}(\mathrm{PGL}_{n_1}) + \mathrm{ed}(\mathrm{PGL}_{n_2}) \ ,$$

as claimed. □

Remark 9.9 Proposition 9.8(b) can often be used to strengthen the upper bounds on $\mathrm{ed}(\mathrm{PGL}_n)$ given by Theorem 4.5, Lemma 9.4(c) and Theorem 9.6. For example, since $\mathrm{ed}(\mathrm{PGL}_5) \le 11$ (by Theorem 9.6) and $\mathrm{ed}(\mathrm{PGL}_6) = 2$ (by Lemma 9.4(c)), we have

$$\mathrm{ed}(\mathrm{PGL}_{30}) \le \mathrm{ed}(\mathrm{PGL}_6) + \mathrm{ed}(\mathrm{PGL}_5) \le 13 \ .$$

On the other hand, a direct application of Theorem 4.5 with $n = 30$ gives a much weaker bound $\mathrm{ed}(\mathrm{PGL}_{30}) \le 840$.

More generally, Proposition 9.8, in combination with Theorem 9.6, allows us to strengthen the bound given by Theorem 4.5 for every n which is not a power of 2.

10 Orthogonal groups

The main results of the next two sections (namely, Theorems 10.3, 10.4, 11.2, and 11.5) were communicated to us by J.-P. Serre. The proofs we present here are based on Tsen-Lang theory; they are somewhat different from Serre's original proofs, which will be given in Section 12.

10.1 Pfister forms

Let F be a field. As usual, we shall denote the quadratic form $\sum_{i=1}^n a_i x_i^2$ on F^n by $< a_1, \ldots, a_n >$; the n-fold Pfister form $< 1, a_1 > \otimes \ldots \otimes < 1, a_n >$ will be denoted by $<< a_1, \ldots, a_n >>$.

Lemma 10.1 *(see, e.g., [Pf, Ch. 8, Ex. 1.2.6]) Suppose $a_1, \ldots, a_n$ are independent indeterminates over k and $F = k(a_1, \ldots, a_n)$. Then the Pfister form $<< a_1, \ldots, a_n >>$ is anisotropic over F.* □

Remark 10.2 Pfister forms naturally arise in the following context. Suppose β is a symmetric bilinear form on W. Recall that β gives rise to the symmetric bilinear $\Lambda^i(\beta)$ on $\Lambda^i(W)$ given by

$$\Lambda^i(\beta)(w_1 \otimes \ldots \otimes w_i, w_1' \otimes \ldots \otimes w_i') = \sum_{\sigma \in S_n} (-1)^\sigma \beta(w_1, w'_{\sigma(1)}) \ldots \beta(w_i, w'_{\sigma(i)}) \,. \tag{12}$$

Then $\Lambda(\beta) \stackrel{\text{def}}{=} \Lambda^1(\beta) \oplus \ldots \oplus \Lambda^n(\beta)$ is a symmetric bilinear form on $\Lambda(W) = \Lambda^1(W) \oplus \ldots \oplus \Lambda^n(W)$. An easy direct computation shows that if $\beta(x, x) =< a_1, \ldots, a_n >$ then $< 1 > \oplus \Lambda(\beta)(x, x) =<< a_1, \ldots, a_n >>$.

10.2 The essential dimension of O_n

Theorem 10.3 *$\mathrm{ed}(O_n) = n$ for every $n \geq 1$.*

Proof. We proved the inequality $\mathrm{ed}(O_n) \leq n$ in Example 3.10(a) (and then again in Example 4.2); thus we only need to show $\mathrm{ed}(O_n) \geq n$. Suppose α is a non-degenerate symmetric bilinear form on $V = k^n$, so that $\mathrm{Aut}_k(V, \alpha) = O_n$. A structured space $(W = F^m, \beta)$ is of type (V, α) if and only if β is a non-degenerate symmetric bilinear form on W. Thus in view of Theorem 8.8 it suffices to construct a field extension F/k and a symmetric bilinear form β on $W = F^n$ such that $\tau(W, \beta) \geq n$.

We now proceed to construct F and β. Let $a_1, \ldots, a_n$ be algebraically independent indeterminates over k, $F = k(a_1, \ldots, a_n)$, $W = F^n$, $e_1, \ldots, e_n$ be a basis of W and $\beta = a_1(e_1^*)^2 + \ldots + a_n(e_n^*)^2$ be a symmetric bilinear form on W. We claim that $\tau(W, \beta) \geq n$ (or, equivalently, $= n$, since $\mathrm{trdeg}_k(F) = n$). Indeed, extend β to a symmetric bilinear form $\Lambda(\beta)$ to $\Lambda(V)$. Recall that by Remark 10.2

$$< 1 > \oplus \Lambda(\beta)(x, x) =<< a_1, \ldots, a_n >> ;$$

hence, $< 1 > \oplus \Lambda(\beta)(x, x)$ is an anisotropic quadratic form over F; see Lemma 10.1. On the other hand, suppose $\beta = \beta_0 \otimes_{F_0} F$ where β_0 is a symmetric bilinear form on $W_0 = (F_0)^n$ and $\mathrm{trdeg}_k(F_0) = n - 1$. By the Tsen-Lang theorem the quadratic form $< 1 > \oplus \Lambda(\beta_0)(x, x)$ defined on the 2^n-dimensional space $F_0 \oplus \Lambda(W_0)$ is isotropic; see e.g., [Pf, Sect. 5.1]. Since, $\Lambda(\beta) = \Lambda(\beta_0) \otimes_{F_0} F$, we conclude that the quadratic form $< 1 > \oplus \Lambda(\beta)(x, x)$ is isotropic as well, a contradiction. □

10.3 The essential dimension of SO_n

Theorem 10.4 $\mathrm{ed}(SO_n) = \begin{cases} 0 \text{ if } n = 2 \\ n-1, \text{ if } n \neq 2 \end{cases}$

Note that Theorem 10.4 says, in particular, that $\mathrm{ed}(SO_n) \neq 1$ for any n. This is consistent with Corollary 5.7(b).

Proof. Recall that we proved the inequality

$$\mathrm{ed}(SO_n) \leq n-1 \tag{13}$$

for every $n \geq 1$ in Example 3.10(b) (and then again in Example 4.2). If n is odd then $O_n \simeq SO_n \times \mathbb{Z}/2\mathbb{Z}$ and thus $\mathrm{ed}(O_n) \leq \mathrm{ed}(SO_n) + \mathrm{ed}(\mathbb{Z}/2\mathbb{Z})$. Since $\mathrm{ed}(O_n) = n$ (see Theorem 10.3) and $\mathrm{ed}(\mathbb{Z}/2\mathbb{Z}) = 1$, this means $n-1 \leq \mathrm{ed}(SO_n)$. Combining this inequality with (13), we conclude that $\mathrm{ed}(SO_n) = n-1$ for every odd integer $n \geq 1$.

We now assume that n is even. If $n=2$ then SO_2 is isomorphic to the 1-dimensional torus k^* and thus $\mathrm{ed}(SO_2) = 0$; see Example 3.9(a).

It remains to show that $\mathrm{ed}(SO_n) \geq n-1$ for $n = 2m$, where $m \geq 2$. Let $V = k^n$, let $e_1, \dots, e_n$ be a k-basis of V, $\alpha_1 = e_1^* \wedge \dots \wedge e_n^*$, $\alpha_2 = (e_1^*)^2 + \dots + (e_n^*)^2$, and $\alpha = \alpha_1 + \alpha_2$, as in Example 8.4(b). Recall that $\mathrm{Aut}_k(V, \alpha) = SO_n$; see Example 6.3(e). By Theorem 8.8 it is enough to construct a structured space $(W = F^n, \beta)$ of type (V, α) such that $\tau(W, \beta) \geq n-1$.

We now proceed to construct F, W, and β. Let $F = k(a_1, \dots, a_{n-1})$, where $a_1, \dots, a_{n-1}$ are independent indeterminates over k, $W = V \otimes_k F$ and $\beta = \beta_1 + \beta_2$, where $\beta_1 = e_1^* \wedge \dots \wedge e_n^* = \alpha_1 \otimes_k F \in \Lambda^n(W^*)$ and

$$\beta_2 = a_1(e_1^*)^2 + \dots + a_{n-1}(e_{n-1}^*)^2 + (a_1 \dots a_{n-1})^{-1}(e_n^*)^2 \in S^2(W^*) \,.$$

Since $\det(\beta_2) = 1$, (W, β) is a structured space of type (V, α); see Example 8.4(b).

It is enough to show that bilinear form β_2 cannot be defined over a field F_0 with $\mathrm{trdeg}_k(F_0) < n-1$. Indeed, this will immediately imply that β cannot be defined over F_0, thus proving $\tau(W, \beta) \geq n-1$. Note that β_2 is equivalent to the bilinear form

$$\gamma = a_1(e_1^*)^2 + \dots + a_{n-1}(e_{n-1}^*)^2 + (a_1 \dots a_{n-1})(e_n^*)^2 \in S^2(V^*) \,;$$

thus it is enough to show that γ cannot be defined over any field F_0 with $\mathrm{trdeg}_k(F_0) < n-1$.

We now argue as in the proof of Theorem 10.3. Let $\Lambda^i(\gamma)$ be the symmetric bilinear form on $\Lambda^i(W)$ defined in Remark 10.2. An easy computation shows that

$$\begin{aligned}\Lambda^i(\gamma)(x,x) = \oplus_{1 \leq j_1 < \dots < j_i \leq n-1} &< a_{j_1}, \dots, a_{j_i} > \\ &\oplus_{1 \leq h_1 < \dots < h_{n-1-i} \leq n-1} < a_{h_1}, \dots, a_{h_{n-1-i}} > \,.\end{aligned} \tag{14}$$

Consider the form $\lambda(\gamma) = \Lambda^1(\gamma) \oplus \dots \Lambda^{m-1}(\gamma)$ on $\Lambda^1(W) \oplus \dots \Lambda^{m-1}(W)$. (Recall that we are assuming $n = 2m$ and $m \geq 2$.) Adding up the forms (14), we see that

$< 1 > \oplus\lambda(\gamma)(x,x)$ is equivalent to $<< a_1, \ldots, a_{n-1} >>$ and therefore, is anisotropic over F; see Lemma 10.1.

On the other hand, suppose $\gamma = \delta \otimes_{F_0} F$, where δ is a symmetric bilinear form on $(F_0)^n$ and $\mathrm{trdeg}_k(F_0) < n-1$. Then $\lambda(\gamma) = \lambda(\delta) \otimes_{F_0} F$, where

$$\lambda(\delta) = \Lambda^1(\delta) \oplus \ldots \Lambda^{m-1}(\delta) \; .$$

The quadratic form $< 1 > \oplus\lambda(\delta)(x,x)$ is then defined on $F_0 \oplus \Lambda^1(W_0) \oplus \ldots \oplus \Lambda^{m-1}(W_0) \simeq F_0^{2^{n-1}}$. Thus the Tsen-Lang theorem says that this form is isotropic over F_0; see [Pf, Sect. 5.1]. Hence, so is $< 1 > \oplus\lambda(\gamma)(x,x)$, a contradiction. This completes the proof of the theorem. □

11 Some exceptional groups

11.1 Octonion algebras

Let F be a field. Recall that for any $0 \neq a, b, c \in F$, the octonion (or Cayley-Dickson) algebra $\mathbf{O}_F(a,b,c)$ is defined as follows. Let

$$Q = (a,b)_2 = F\{i,j\}/(i^2 = a, j^2 = b, ji = -ij)$$

be a 4-dimensional (associative) quaternion algebra over F. This algebra is equipped with an involution $x \to \overline{x}$ given by

$$\overline{x_0 + x_1 i + x_2 j + x_3 ij} = x_0 - x_1 i - x_2 j - x_3 ij \; . \tag{15}$$

(Here $x_0, \ldots, x_3 \in F$.) Now $\mathbf{O}_F(a,b,c) \stackrel{\mathrm{def}}{=} Q + Ql$ is an 8-dimensional F-algebra with (non-associative) multiplication given by $(x+yl)(z+wl) = (xz + c\overline{w}y) + (wx + y\overline{z})l$. The involution (15) extends from Q to $\mathbf{O}_F(a,b,c)$ via $\overline{x+yl} = \overline{x} - yl$. The algebra $\mathbf{O}_F(a,b,c)$ is also equipped with F-valued trace and norm functions given by $t(x) = x + \overline{x}$ and $n(x) = x\overline{x} = \overline{x}x$; moreover, $x^2 - \mathrm{tr}(x)x + n(x) = 0$ for any $x \in \mathbf{O}_F(a,b,c)$. Using this identity, it is easy to show that every automorphism of $\mathbf{O}_F(a,b,c)$ preserves the trace and the norm. For a more detailed description of octonion algebras we refer the reader to [J, I.5], [Sc, III.4] or [SSSZ, 2.2].

If $F = k$, we shall write $\mathbf{O}$ for $\mathbf{O}_F(1,1,1)$.

11.2 The essential dimension of G_2

Recall that $\mathrm{Aut}_k(\mathbf{O})$ is the 14-dimensional exceptional group G_2.

Lemma 11.1 *Suppose F is a field containing k. Then for any $0 \neq a, b, c \in F$, we have*

$$\mathbf{O}_F(a,b,c) \otimes_F E = \mathbf{O} \otimes_k E \; ,$$

where $E = F(\sqrt{a}, \sqrt{b}, \sqrt{c})$. In particular, $\mathbf{O}_F(a,b,c)$ is an algebra of type $\mathbf{O}$.

Proof. The E-linear map $\mathbf{O}_F(a,b,c)\otimes_k E \longrightarrow \mathbf{O}\otimes_F E$ given by

$$\begin{aligned} i &\mapsto \sqrt{a}\, i \\ j &\mapsto \sqrt{b}\, j \\ l &\mapsto \sqrt{c}\, l \end{aligned}$$

is an isomorphism of E-algebras. $\square$

Theorem 11.2 $\mathrm{ed}(G_2) = 3$.

Proof. We first prove that $\mathrm{ed}(G_2) \geq 3$. Let $F = k(a_1, a_2, a_3)$, where a_1, a_2 and a_3 are algebraically independent indeterminates over k. In view of Lemma 11.1 and Theorem 8.8(b) it is sufficient to show that $\tau(\mathbf{O}_F(a_1,a_2,a_3)) \geq 3$.

Expressing the trace form $\mathrm{tr}(x^2)$ in the basis $\{(i^{\epsilon_1}j^{\epsilon_2})l^{\epsilon_3} \mid \epsilon_1,\epsilon_2,\epsilon_3 = 0,1\}$, we see that this form is equivalent to the 3-fold Pfister form $<< a_1, a_2, a_3 >>$ and thus is anisotropic over F; see Lemma 10.1. Thus by the Tsen-Lang theorem the form $\mathrm{tr}(x^2)$ (and, hence, the F-algebra $\mathbf{O}_F(a_1,a_2,a_3)$) cannot be defined over a field F_0 with $\mathrm{trdeg}_k(F_0) \leq 2$. This proves that $\tau(\mathbf{O}_F(a_1,a_2,a_3))$ and therefore $\mathrm{ed}(G_2) \geq 3$.

Our proof of the opposite inequality will rely on an argument analogous to the one we used in Example 3.10. Let $V = k^8$ be the underlying vector space of the split octonion algebra $\mathbf{O}$. Since $\mathbf{O}$ is generated by three elements, the natural linear representation of G_2 on $V^3 = k^{24}$ is generically free. Let

$$Y = \{(x_1,x_2,x_3) \mid \mathrm{tr}(x_r) = \mathrm{tr}(x_r x_s) = \mathrm{tr}((x_1x_2)x_3) = 0,\ \mathrm{tr}(x_r^2) \neq 0,\ 1 \leq r < s \leq 3\}\,.$$

Then Y is a (locally closed) G_2-invariant subvariety of V^3. Moreover, Y irreducible and $\dim(Y) = 17$; this can be proved by considering the projection $Y \longrightarrow V^2$ to the first two components. Since Y contains a triple of generators of $\mathbf{O}$ (e.g., (i,j,l)), the action of G_2 on Y is generically free.

Now let $f : V \dashrightarrow Y$ be the G_2-equivariant rational map given by $f(x_1,x_2,x_3) = (y_1,y_2,y_3)$, where

$$\begin{aligned} y_1 &= P(x_1; 1) \\ y_2 &= P(x_2; 1, y_1) \\ y_3 &= P(x_3; 1, y_1, y_2, y_1y_2)\,; \end{aligned}$$

here $P(v; v_1, \ldots, v_m)$ is defined by equation (4) of Example 3.10 with $q(x,y) = \mathrm{tr}(xy)$. Since $f_{|Y} = id_{|Y}$, f is a compression. Thus $\mathrm{ed}(G_2) \leq \dim(Y) - \dim(G_2) = 17 - 14 = 3$, as claimed. $\square$

Remark 11.3 (a) By [Se$_3$, Sect 8.2] G_2 is 2-special; see Definition 5.5. In view of Proposition 5.6(b) this gives an alternative proof of the inequality $\mathrm{ed}(G_2) \geq 3$. Moreover, by Proposition 5.6(a), $\mathrm{ed}(X, G_2) = 0$ or 3 for every primitive (or, equivalently, irreducible) generically free G_2-variety X.

Remark 11.4 The converse of Lemma 11.1 is also true, namely

$(W = F^8, \beta)$ is structured space of type $\mathbf{O}$ *if and only if* $(W, \beta) = \mathbf{O}_F(a, b, c)$ *for some* $a, b, c \in F$*. This gives an alternative proof of the inequality* $\mathrm{ed}(G_2) \leq 3$*.*

The first assertion is a consequence of a theorem of Zorn [Sc, III.3.17] (see also [SSSZ, 7.3] for a more general result of Kleinfeld). To prove the second assertion, note that $\mathbf{O}_F(a, b, c)$ is defined over the field $k(a, b, c)$, which has transcendence degree ≤ 3 over k. Thus $\tau(\mathbf{O}_F(a, b, c)) \leq 3$ for every F and every $a, b, c \in F^*$. By Theorem 8.8(b) this implies $\mathrm{ed}(G_2) \leq 3$. □

11.3 The Albert algebra

Recall that the (split) Albert algebra $\mathbf{A} = H_3(\mathbf{O})$ is the Jordan algebra of 3×3 hermitian matrices over the octonion algebra $\mathbf{O}$. Elements of $\mathbf{A}$ are of the form

$$X = \begin{pmatrix} a & x & y \\ \overline{x} & b & z \\ \overline{y} & \overline{z} & c \end{pmatrix} , \qquad (16)$$

where $a, b, c \in k$ and $x, y, z \in \mathbf{O}$, and multiplication is given by $X \cdot Y = 1/2(XY + YX)$, where XY is the usual matrix product of X and Y. Every element of X of $\mathbf{A}$ satisfies a "Cayley-Hamilton identity" of the form

$$X^3 - \mathrm{tr}(X)X^2 + \frac{\mathrm{tr}(X)^2 - \mathrm{tr}(X^2)}{2} X - n(X) = 0 ,$$

where $\mathrm{tr}(X) = a + b + c \in k$ is the trace of X and $n(X)$ is the cubic norm of X; see [J, p. 233]. Both the trace and the norm are preserved under automorphisms of $\mathbf{A}$.

Let $e_{\alpha\beta}$ be the (α, β) matrix unit in $\mathrm{M}_3(k)$. We shall denote the element $xe_{\alpha\beta} + \overline{x}e_{\alpha\beta}$ by $[x]_{\alpha\beta}$. Then the 27 elements e_{11}, e_{22}, e_{33} and $[(i^{\epsilon_1} j^{\epsilon_2}) l^{\epsilon_3}]_{\alpha\beta}$ form a k-basis of $\mathbf{A}$; here ϵ_1, ϵ_2, $\epsilon_3 = 0, 1$ and $1 \leq \alpha < \beta \leq 3$.

11.4 The essential dimension of F_4

Recall that $\mathrm{Aut}_k(\mathbf{A})$ is the exceptional group F_4.

Theorem 11.5 $\mathrm{ed}(F_4) \geq 5$.

Proof. By Theorem 8.8 it is sufficient to construct a field F containing k and an F-algebra B of type $\mathbf{A}$ with $\tau(B) \geq 5$. We now proceed to construct such an algebra. Let s_1, s_2, s_3, t_1, t_2 be five independent variables over k,

$$t_3 \stackrel{\mathrm{def}}{=} t_1^{-1} t_2^{-1} , \qquad (17)$$

$S_\alpha = s_\alpha^2$ and $T_\alpha = t_\alpha^2$ for $\alpha = 1, 2, 3$. Let E and F be the fields given by $F = k(S_1, S_2, S_3, T_1, T_2)$ and $E = k(s_1, s_2, s_3, t_1, t_2)$, and let B be the F-subspace of $\mathbf{A} \otimes_k E$ spanned by the 27 elements

$$e_{11}, e_{22}, e_{33}, \text{ and } b_\alpha^{\epsilon_1,\epsilon_2,\epsilon_3} = t_\alpha {s_1}^{\epsilon_1} {s_2}^{\epsilon_2} {s_3}^{\epsilon_3} [(i^{\epsilon_1} j^{\epsilon_2}) l^{\epsilon_3}]_{\beta\gamma} \,, \tag{18}$$

where $\epsilon_1, \epsilon_2, \epsilon_3 = 0, 1$, $\{\alpha, \beta, \gamma\} = \{1, 2, 3\}$ and $\beta < \gamma$. We claim that B is an F-subalgebra of of $\mathbf{A} \otimes_k E$. Since the elements (18) form an E-basis of $\mathbf{A} \otimes_k E$, it is sufficient to check that all structure constants of $\mathbf{A} \otimes_k E$ in this basis lie in F. Indeed,

$$\begin{array}{l}
e_{\alpha\alpha} \cdot e_{\alpha\alpha} = e_{\alpha\alpha} \\
e_{\alpha\alpha} \cdot e_{\beta\beta} = 0 \\
e_{\alpha\alpha} \cdot b_\alpha^{\epsilon_1,\epsilon_2,\epsilon_3} = 0 \\
e_{\alpha\alpha} \cdot b_\alpha^{\epsilon_1,\epsilon_2,\epsilon_3} = \frac{1}{2} b_\beta^{\epsilon_1,\epsilon_2,\epsilon_3} \\
b_\alpha^{\epsilon_1,\epsilon_2,\epsilon_3} \cdot b_\alpha^{\delta_1,\delta_2,\delta_3} = \left\{ \begin{array}{l} \pm T_\alpha S_1^{\epsilon_1} S_2^{\epsilon_2} S_3^{\epsilon_3} (e_{\beta\beta} + e_{\gamma\gamma}) \text{ if } (\epsilon_1, \epsilon_2, \epsilon_3) = (\delta_1, \delta_2, \delta_3) \\ 0 \text{ otherwise .} \end{array} \right. \\
b_\alpha^{\epsilon_1,\epsilon_2,\epsilon_3} \cdot b_\beta^{\delta_1,\delta_2,\delta_3} = \pm T_\gamma^{-1} S_1^{\epsilon_1\delta_1} S_2^{\epsilon_2\delta_2} S_3^{\epsilon_3\delta_3} b_\gamma^{\epsilon_1+\delta_1,\epsilon_2+\delta_2,\epsilon_3+\delta_3} \,.
\end{array}$$

(cf. [Sc, p. 105]). Here we always assume that $\{\alpha, \beta, \gamma\} = \{1, 2, 3\}$; in the last formula the subscripts ϵ_n and δ_n are added and multiplied modulo 2. All structure constants appearing in this table are, indeed, elements of F. We have therefore verified that B is a 27-dimensional F-algebra. Since the elements (18) form an E-basis of $\mathbf{A} \otimes_k E$, we have $B \otimes_F E \simeq \mathbf{A} \otimes_k E$. Thus B is an algebra of type A.

It remains to prove that $\tau(B) \geq 5$ (or, equivalently, $= 5$, since $\mathrm{trdeg}_k(F) = 5$). We shall do so by examining the trace form of B and showing that it cannot be defined over a field F_0 with $\mathrm{trdeg}_k(F_0) \leq 4$ (and, consequently, B cannot be defined over such a field).

Our multiplicaton table shows that the 27 basis elements (18) are mutually orthogonal with respect to the trace form. Moreover, taking the trace of the square of each element and remembering that (i) $\sqrt{2}, \sqrt{-1} \in k \subset F$ by our assumption on k and (ii) $T_3 = T_1^{-1} T_2^{-1}$ by (17), we obtain

$$\mathrm{tr}(x^2) \simeq \,< 1, 1 > \oplus\, \phi \,, \tag{19}$$

where

$$\phi = < 1 > \oplus\, T_1 << S_1, S_2, S_3 >> \oplus\, T_2 << S_1, S_2, S_3 >> \oplus\, T_1 T_2 << S_1, S_2, S_3 >> .$$

Note that

$$\phi \oplus < S_1, S_2, S_3, S_1 S_2, S_1 S_3, S_2 S_3, S_1 S_2 S_3 > \simeq << S_1, S_2, S_3, T_1, T_2 >> \,. \tag{20}$$

Since the Pfister form $<< S_1, S_2, S_3, T_1, T_2 >>$ is anisotropic over F (see Lemma 10.1), so is ϕ. Thus (19) gives the Witt decomposition of the quadratic form $\mathrm{tr}(x^2)$ over $F = k(S_1, S_2, S_3, T_1, T_2)$; the anisotropic part of this form equals ϕ and has dimension

25. On the other hand, if B were defined over a field F_0 with $\operatorname{trdeg}_k(F_0) \leq 4$ then $\operatorname{tr}(x^2)$ would also be defined over F_0 and, consequently, by the Tsen-Lang theorem, its anisotropic part would have dimension $\leq 2^4 = 16$. This contradiction proves that $\tau(B) \geq 5$ and thus $\operatorname{ed}(F_4) \geq 5$, as claimed. □

11.5 The essential dimension of E_6

Recall that the simply connected exceptional group E_6 is isomorphic to $\operatorname{Aut}_k(V, \alpha)$, where $V = k^{27}$ is the underlying vector space of the Albert algebra $\mathbf{A}$ and $\alpha \in S^3(V^*)$ is the symmetric trilinear form associated to the cubic norm in $\mathbf{A}$.

Proposition 11.6 $\operatorname{ed}(E_6) \geq 3$.

Proof. Let $F = k(a, b, c)$. By a theorem of Albert there exists an exceptional Jordan division F-algebra B; see [J, IX.12 Thm. 21]. Let $W = F^{27}$ be the underlying vector space of B and let $\beta \in S^3(V^*)$ be the symmetric trilinear form associated to the cubic norm in B. Since B is an algebra of type $\mathbf{A}$, (W, β) is a structured space of type (V, α). (Here $V = k^{27}$ and $\alpha \in S^3(V^*)$ are as above.)

By Theorem 8.8 it suffices to show that $\tau(W, \beta) \geq 3$. Assume the contrary: (W, β) is defined over a field F_0 with $\operatorname{trdeg}_k(F_0) \leq 2$. Then the cubic norm $n_B(x) = \beta(x, x, x)$ on B can also be defined over F_0. Note that n_B is a cubic form in 27 variables; thus by the Tsen-Lang theorem n_B is isotropic, i.e. $n_B(x) = 0$ for some $0 \neq x \in B$. This contradicts our assumption that B is a division algebra; see [J, VI.3 Cor. 3]. We therefore conclude that $\tau(W, \beta) \geq 3$, as claimed. □

Proposition 11.7 $\operatorname{ed}(E_6) \leq \operatorname{ed}(F_4) + 1$.

Proof. E_6 is by definition a subgroup of $\mathrm{GL}_{27} = \mathrm{GL}(\mathbf{A})$; thus its linear representation on $V = \mathbf{A}^{27}$ is generically free. (Using [J, VI.7 Thm. 7], one can prove that the action of E_6 on $\mathbf{A}^n$ is generically free for every $n \geq 4$; however, we will not need this fact here.)

Let $S = \{(x_1, \ldots, x_{27}) \mid x_1 \in k1_{\mathbf{A}}\} \subset V$. Then the proof of [I, Thm. 1] shows that S is an (E_6, H)-section of V (see Definition 2.9), where $H \simeq F_4 \times \mathbb{Z}_3$ is the subgroup of E_6 generated by F_4 and multiplication by cube roots of 1. Note that S is a linear generically free H-variety. Thus by Lemma 4.1, $\operatorname{ed}(E_6) = \operatorname{ed}(V, E_6) \leq \operatorname{ed}(S, H) = \operatorname{ed}(H)$ and by Lemma 3.8, $\operatorname{ed}(H) = \operatorname{ed}(F_4 \times \mathbb{Z}_3) \leq \operatorname{ed}(F_4) + \operatorname{ed}(\mathbb{Z}_3) = \operatorname{ed}(F_4) + 1$, as claimed. □

12 Cohomological invariants

In this section we discuss the relationship between the essential dimension of an algebraic group G and cohomological invariants associated to G. This material is based entirely on results communicated to us by J.-P. Serre.

12.1 Preliminaries

We begin by recalling several definitions and results related to Galois cohomology and cohomological invariants. For details we refer the reader to [Se$_4$], [KMRT] and [B].

Let $H^i(F) = H^i(\Gamma_F, \mathbb{Z}/2Z)$, where $\Gamma_F = \mathrm{Gal}(\overline{F}/F)$, $\overline{F}$ is the algebraic closure of F, and $\mathbb{Z}/2\mathbb{Z}$ is viewed as a trivial Γ_F-module.

By Kummer theory the first cohomology group $H^1(F)$ is canonically isomorphic to $F^*/(F^*)^2$; as usual, we will denote the class of $a \in F^*$ modulo $(F^*)^2$ by (a).

Lemma 12.1 *(see e.g., [BR$_2$, Lemma 8.2]) Let $a_1, \ldots, a_n$ be independent variables over k and let $F = k(a_1, \ldots, a_n)$. Then the cup product $(a_1)\ldots(a_n)$ is non-zero in $H^n(F)$.* □

Suppose F is a field, $0 \neq a_1, \ldots, a_n \in F$ and $\phi =< a_1, \ldots, a_n >$ is a quadratic form. Then r-th Stiefel-Whitney class $w_r(\phi) \in H^r(F)$ is given by

$$w_r(\phi) = \sum_{1 \le i_1 < \ldots < i_r \le n} (a_{i_1})(a_{i_2})\ldots(a_{i_r})\,. \tag{21}$$

By a theorem of Delzant $w_r(\phi)$ depends only on the equivalence class of ϕ and not on the specific presentation of ϕ as a sum of squares; see [De].

We shall now consider the following categories:

$Fields$ - category of finitely generated field extensions of k,

$Sets'$ - category of pointed sets, i.e., sets with a marked element,

$AGrps$ - category of abelian groups,

and the following covariant functors:

$H^i(\,\cdot\,)$, from $Fields$ to $AGrps$.

$H^1(\,\cdot\,, G)$, from $Fields$ to $Sets'$. Here G is a (fixed) algebraic group.

$G - Var(\,\cdot\,)$, from $Fields$ to $Sets'$. Here again, G is a fixed algebraic group. If $F \in Fields$ then $G - Var(F)$ is the set of birational equivalence classes of generically free primitive G-varieties X such that $k(X/G) \simeq F$ (as field extensions of k). Note that for each $F \in Fields$ the marked element in $G - Var(F)$ is the G-variety $X_0 \times G$; here the variety X_0 is chosen so that $k(X_0) = F$. An inclusion $F \hookrightarrow F'$ of fields induces the map $G - Var(F) \longrightarrow G - Var(F')$ of pointed sets given by $X \mapsto X_0' \times_{X/G} X$, where $k(X_0') = F'$.

$Spaces_{(V,\alpha)}$, from $Fields$ to $Sets'$. Here $(V = k^n, \alpha)$ is a (fixed) structured space. If $F \in Fields$ then $Spaces_{(V,\alpha)}(F)$ is defined as the set of all structured spaces $(W = F^n, \beta)$ of type (V, α); see Definition 8.1. The marked element in this set is $(V, \alpha) \otimes_k F$. An inclusion $F \hookrightarrow F'$ of fields induces a morphism $Spaces_{(V,\alpha)}(F) \longrightarrow Spaces_{(V,\alpha)}(F')$ given by $(W, \beta) \mapsto (W, \beta) \otimes_F F'$.

Definition 12.2 *([Se$_3$, 6.1], [B, 4.1], [KMRT, 31.B]) Let G be an algebraic group. A cohomological invariant of dimension n associated to G is a morphism of functors $f : H^1(\,\cdot\,, G) \longrightarrow H^n(\,\cdot\,)$.*

12.2 Cohomological invariants and essential dimension

Lemma 12.3 *(a) The functors $H^1(\,\cdot\,, G)$ and $G - Var(\,\cdot\,)$ are isomorphic.*

(b) If (V, α) is a structured space and $G = \mathrm{Aut}_k(V, \alpha)$ then the functors $H^1(\,\cdot\,, G)$, $G - Var(\,\cdot\,)$ and $Spaces_{(V,\alpha)}$ are isomorphic.

Proof. Part (a) is proved in [Se$_4$, I.5.2]; see also [Po, 1.3] and Remark 2.17. To prove part (b), define

$$f_F : G - Var(\,\cdot\,)(F) \longrightarrow Spaces_{(V,\alpha)}(F)$$

by $f_F : X \mapsto (RMaps_G(X, V), \alpha_G^X)$ for every $F \in Fields$. Now Lemma 7.6(c) shows that f_F is a map of pointed sets for each F, Lemma 7.6(a) shows that the maps f_F collectively define a morphism of functors f from $G - Var(\,\cdot\,)$ to $Spaces_{(V,\alpha)}$, and Proposition 8.6 shows that f is an isomorphism. $\square$

In view of the above lemma we can view a cohomological invariant of degree n associated to G as a morphism of functors $G - Var(\,\cdot\,, G) \longrightarrow H^n(\,\cdot\,)$ or, if G is of the form $\mathrm{Aut}(V, \alpha)$, as a morphism of functors $Spaces_{(V,\alpha)} \longrightarrow H^n(\,\cdot\,)$.

Proposition 12.4 *Let $f : G - Var \longrightarrow H^n(\,\cdot\,)$ be a cohomological invariant associated to G and let X be a primitive generically free G-variety such that $f_F(X) \neq 0$. (Here $F = k(X)^G$.) Then*

(a) $\mathrm{ed}(X, G) \geq n$.

(b) Let V be a generically free linear representation of G and let $K = k(V)^G$. Then $f_K(V) \neq 0$.

Proof. (a) Assume the contrary. Then there exists a G-compressions $X \dashrightarrow Y$ such that $\dim(Y/G) \leq n - 1$, i.e.,

$$\mathrm{trdeg}_k(L) \leq n - 1\,, \text{ where } L = k(Y/G)^G = k(Y)^G\,. \tag{22}$$

Since X is birationally isomorphic to $X/G \times_{Y/G} Y$ (see Lemma 2.16(b)) and f is a morphism of functors, we conclude that $f_L(Y) \xrightarrow{res} f_F(X)$ where res is the restriction map $H^n(L, C) \longrightarrow H^n(F, C)$. However, in view of (22), the cohomological dimension of L is $\leq n - 1$ (see [Se$_4$, II.4.2]) and thus $f_L(Y) \in H^n(L, C) = (0)$. Consequently, $f_F(X) = (0)$ in $H^n(F, C)$, a contradiction.

(b) By Corollary 2.20, there exists a compression $X \times k^d \dashrightarrow V$, where $d = \dim(V)$. Then $f_{F'}(X \times k^d)$ is a homomorphic image of $f_K(V)$; here $F' = k(X \times k^d)^G$; hence it is enough to show that $f_{F'}(X \times k^d) \neq 0$. Note that $f_{F'}(X \times k^d)$ is the image of $f_F(X)$ under the restriction map $H^n(F) \longrightarrow H^n(F')$. Since F' is a purely transcendental extension of F, this restriction map is injective; see [Se$_4$, Remark 1, p. 85]. Thus $f_{F'}(X \times k^d) \neq 0$, as claimed. $\square$

Note that we can associate a trivial cohomological invariant to any group G by setting f_F to be the zero map for every $F \in Fields$. We shall denote this invariant by $f = 0$ and refer to it as the zero invariant.

Corollary 12.5 *If there exists a non-zero cohomological invariant of dimension n associated to G then* $\mathrm{ed}(G) \geq n$.

Proof. Immediate from Proposition 12.4; see Definition 3.5. $\square$

12.3 Examples

We now apply Corollary 12.5 to give alternative proofs of several lower bounds on $\mathrm{ed}(G)$, which we previously established by other methods. Every group G we shall consider in Examples 12.6-12.10 is of the form $G = \mathrm{Aut}_k(V, \alpha)$; thus we will interpret a cohomological invariant of degree n associated to G as a morphism of functors $f : Spaces_{(V,\alpha)}(\,\cdot\,) \longrightarrow H^n(\,\cdot\,)$; see Lemma 12.3.

Example 12.6 $G = O_n$. Let $V = k^n$ and α be a non-degenerate symmetric bilinear form on V so that $\mathrm{Aut}_k(V, \alpha) = O_n$. Recall that for any $F \in Fields$, $(W = F^n, \beta)$ is of type F if and only if β is a non-degenerate symmetric bilinear form on W. For each $i \geq 1$ we can now define a cohomological invariant $f_i : Spaces_{(V,\alpha)}(\,\cdot\,) \longrightarrow H^i(\,\cdot\,)$ of degree i associated to O_n by $(f_i)_F(W, \beta) = w_i(\overline{\beta})$, where $\overline{\beta}$ is the quadratic form such that $\overline{\beta}(x) = \beta(x, x)$ and $w_i(\overline{\beta})$ is the Stiefel-Whitney class of $\overline{\beta}$.

It is easy to see that $f_i = 0$ for all $i \geq n + 1$. We claim that $f_i \neq 0$ for any $i = 1, \dots, n$. Indeed, suppose $F = k(a_1, \dots, a_i)$ and $\overline{\beta} =< a_1, \dots, a_i, 1, \dots, 1 >$, where $a_1, \dots, a_i$ are independent variables over k. Then $w_i(\overline{\beta}) = (a_1) \cdot \ldots \cdot (a_i) \neq 0$ in $H^i(F)$; see Lemma 12.1. Applying Proposition 12.4 to f_n, we obtain an alternative proof the inequality $\mathrm{ed}(O_n) \geq n$ (cf. Theorem 10.3).

Example 12.7 $G = SO_n$. Let $V = k^n$ and let $\alpha = \alpha_1 + \alpha_2$, where α_1 is a volume form and α_2 is a non-degenerate symmetric bilinear form on V, as in the beginning of Section 10.3. Recall that $\mathrm{Aut}_k(V, \alpha) = SO_n$ (see Example 6.3(e)) and that for any $F \in Fields$, $Spaces_{(V,\alpha)}(F)$ can be identified with the set of isomorphism classes of symmetric bilinear forms on F^n of determinant 1 (see Example 8.4(b)). For every $i \geq 1$ we can define a cohomological invariant $f_i : Spaces_{(V,\alpha)}(\,\cdot\,) \longrightarrow H^i(\,\cdot\,)$ of degree i associated to SO_n by $(f_i)_F(\beta_2) = w_i(\overline{\beta_2})$, where w_i is the ith Stiefel-Whitney class, β_2 is a symmetric bilinear form of determinant 1 on F^n, and $\overline{\beta_2}(x) = \beta_2(x, x)$. Note that

$$\overline{\beta_2} \simeq < a_1, \dots, a_{n-1}, (a_1 \dots a_{n-1})^{-1} > \simeq < a_1, \dots, a_{n-1}, a_1 \dots a_{n-1} >$$

for some $a_1, \dots, a_n \in F$. It is easy to see that $f_i = 0$ for all $i \geq n$. If n is odd then $w_{n-1}(\overline{\beta}) = (a_1) \dots (a_{n-1})$, which is non-zero if $a_1, \dots, a_n$ are independent variables over k and $F = k(a_1, \dots, a_n)$; see Lemma 12.1. This gives an alternative proof of the inequality $\mathrm{ed}(SO_n) \geq n - 1$ for n odd; cf. Theorem 10.4.

If n is even then $f_{n-1} = 0$. Taking $a_1, \dots, a_{n-2}$ to be independent variables over k and $a_{n-1} = 1$ and applying Lemma 12.1, we see that $f_{n-2} \neq 0$. This proves the inequality $\mathrm{ed}(SO_n) \geq n - 2$ for n even. To recover the stronger inequality

$$\mathrm{ed}(SO_n) \geq n - 1 \qquad (23)$$

of Theorem 10.4 for even integers $n \geq 4$, we consider the cohomological invariant

$$g_{n-1} : Spaces_{(V,\alpha)}(\,\cdot\,) \longrightarrow H^{n-1}(\,\cdot\,)$$

given by $(a_1)(a_2)\ldots(a_{n-1})$; see [Se$_4$, Remark 2, p. 188]. Here $a_1, \ldots, a_{n-1}$ are the coefficients of $\overline{\beta_2}$, as above. Taking $a_1, \ldots, a_{n-1}$ to be independent variables over k and applying Lemma 12.1 once again, we conclude that $g_{n-1} \neq 0$. This gives an alternative proof of the inequality (23).

Note that this argument is not as different from the proof of Theorem 10.4 as it may seem. The key step here is proving that g_{n-1} is well-defined. One way of doing it involves passing to a Pfister form on $\oplus_{i=1}^{n/2-1} \Lambda^i(k^n)$, in a manner similar to the argument we used in Section 10.3.

Example 12.8 $G = S_n$. Let A be the (split) etale k-algebra $k \oplus \ldots \oplus k$, so that $\mathrm{Aut}_k(A) = S_n$; see Example 6.3(f). Recall that $(W = F^n, \beta)$ is a structured space of type A if and only if β defines the structure of an n-dimensional etale F-algebra on W; see Example 8.4(c). Thus a cohomological invariant associated to S_n is a cohomological invariant of etale algebras. These invariants were completely described by Serre; see [B, Section 4]. In particular, for each $i = 1, \ldots, n$, one can define a cohomological invariant $f_i : Spaces_A(\,\cdot\,) \longrightarrow H^i(\,\cdot\,)$ by $(f_i)_F(B) = w_i(\mathrm{tr}_B(x^2))$, where B is an n-dimensional etale F-algebra, $\mathrm{tr}_B(x^2)$ is the trace form on B, and w_i is the i-th Stiefel-Whitney class. Then $f_i = 0$ for any $i > [n/2]$ (see [B, 4.6]) but $f_i \neq 0$ for $i = [n/2]$ (see [BR$_2$, Theorem 8.4]). Consequently, by Proposition 12.4, $\mathrm{ed}(S_n) \geq [n/2]$; cf. [BR$_1$, Thm. 6.5].

Example 12.9 $G = G_2$. A non-zero cohomological invariant f_3 of dimension 3 associated to G_2 is constructed in [Se$_3$, Sect. 8]. By Proposition 12.4 this construction gives an alternative proof of the inequality $\mathrm{ed}(G_2) \geq 3$; cf. Theorem 11.2 and Remark 11.3.

For the reader's convenience, we briefly recall the definition of f_3. Recall that $G_2 = \mathrm{Aut}_k(\mathbf{O})$, where $\mathbf{O}$ is the split octonion algebra over k. Moreover, for $F \in Fields$ the structured space $(W = F^n, \beta)$ is of type $\mathbf{O}$ if and only if $(W, \beta) = \mathbf{O}_F(a, b, c)$ for some $a, b, c \in F$; see Remark 11.4. The trace form of $\mathbf{O}_F(a, b, c)$ is isomorphic to a 3-fold Pfister form $<< a, b, c >>$. We now define f_3 as the Arason invariant of this form, i.e., $f_F : Spaces_{\mathbf{O}}(F) \longrightarrow H^3(F)$ is given by $\mathbf{O}_F(a, b, c) \longrightarrow (a)(b)(c)$. This invariant is non-zero because $(a)(b)(c) \neq 0$ in $H^3(F)$ if a, b, c are algebraically independent over k and $F = k(a, b, c)$; see Lemma 12.1.

Example 12.10 $G = F_4$. Non-zero cohomological invariants f_3 and f_5, of dimension, respectively 3 and 5, associated to F_4 are constructed in [Se$_3$]; we briefly recall their definition below. The existence of f_5 gives an alternative proof of the inequality $\mathrm{ed}(F_4) \geq 5$; cf. Theorem 11.5.

Recall that $F_4 = \mathrm{Aut}_k(\mathbf{A})$, where $\mathbf{A}$ is the split Albert algebra over k and that structured spaces of type $\mathbf{A}$ are precisely 27-dimensional exceptional simple Jordan algebras; see Example 8.4(d). If B is a F-algebra of type **A** than the trace form of B satisfies the identity

$$\mathrm{tr}_B(x^2) \oplus << a_1, a_2, a_3 >> \simeq < 1, 1, 1 > \oplus << a_1, a_2, a_3, b_1, b_2 >>$$

for some $a_1, a_2, a_3, b_1, b_2 \in F$, where the Pfister forms $<< a_1, a_2, a_3 >>$ and $<< a_1, a_2, a_3, b_1, b_2 >>$ are uniquely defined by B; see [Se$_3$, Theorem 10]. (The proof of this assertion for reduced Jordan Algebras is, in fact, similar to our computation in Section 11.4.) Then $(f_3)_F(B) \stackrel{\text{def}}{=} (a_1)(a_2)(a_3) \in H^3(F)$ and $(f_5)_F(B) \stackrel{\text{def}}{=} (a_1)(a_2)(a_3)(b_1)(b_2) \in H^5(F)$. To see that these invariants are non-zero, let $F = k(S_1, S_2, S_3, T_1, T_2)$ and B be as in the proof of Theorem 11.5. Then in view of (19) and (20), we have $(f_3)_F = (S_1)(S_2)(S_3) \neq 0$ in $H^3(F)$ and $(f_5)_F = (S_1)(S_2)(S_3)(T_1)(T_2) \neq 0$ in $H^5(F)$; see Lemma 12.1. Thus $f_3, f_5 \neq 0$, as claimed.

12.4 The Rost invariant and simply connected semisimple groups

The Rost invariant $H^1(\,\cdot\,, G) \longrightarrow H^3(\,\cdot\,)$ is defined in [KMRT, 31B]. This invariant is non-zero for every simply connected exceptional group G; see [KMRT, (31.40) and (31.47)]. For $G = G_2$ and F_4, this invariant is the invariant f_3 of (respectively) Examples 12.9 and 12.10. In the case $G = E_6$, the non-vanishing of the Rost invariant gives an alternative proof of the inequality $\mathrm{ed}(E_6) \geq 3$; cf. Proposition 11.6. For $G = E_7$ and E_8, we obtain the following result.

Proposition 12.11 *(a)* $\mathrm{ed}(E_7) \geq 3$*, (b)* $\mathrm{ed}(E_8) \geq 3$*.* □

The next theorem may be viewed as a weak form of Serre's Conjecture II [Se$_4$, III.3, p. 139]. The conjecture says (in the case of function fields over k) that every simply connected semisimple group G is 2-special; cf. Definition 5.5 and Remark 5.9. This is equivalent to the assertion that $\mathrm{ed}(X, G) = 0$ or ≥ 3 for every irreducible generically free G-variety X; cf. Proposition 5.6. On the other hand, Theorem 12.12 below says that $\mathrm{ed}(V, G) = 0$ or ≥ 3, where V is a vector space with a generically free linear action of G.

Theorem 12.12 *Let G be a simply connected semisimple group. Then either G is special (and thus* $\mathrm{ed}(G) = 0$*) or* $\mathrm{ed}(G) \geq 3$*.*

Proof. We may assume without loss of generality that G is simple and simply connected. Indeed, if $\mathrm{ed}(G_i) = 0$ for every simple factor G_i of G then $\mathrm{ed}(G) = 0$ (see Lemma 3.8) and if $\mathrm{ed}(G_i) \geq 3$ for one of the factors G_i then $\mathrm{ed}(G) \geq 3$ (see Lemma 3.7).

If $G = G_2$, $G = F_4$ or G is of classical type then G is known to be 2-special (see Definition 5.5 and Remark 5.9) and thus the desired conclusion follows from Proposition 5.6. If $G = E_6$ then $\mathrm{ed}(G) \geq 3$ by Proposition 11.6. If $G = E_7$ or E_8 then $\mathrm{ed}(G) \geq 3$ by Proposition 12.11. □

12.5 Mod p invariants

Definition 12.2 and Proposition 12.4 remain valid if $H^i(\,\cdot\,)$ is interpreted as $H^i(\,\cdot\,, C)$, where C is a cyclic group of prime order (not necessarily $\mathbb{Z}/2\mathbb{Z}$). Moreover, Proposition 12.4(b) can be strengthened as follows.

Proposition 12.13 *Suppose there exists a non-zero cohomological invariant $f : G-Var(\,\cdot\,) \longrightarrow H^n(\,\cdot\,, C)$. Let V be a generically free linear representation of G, X be a primitive generically free G-variety, and $X \dashrightarrow V$ be a G-compression which is generically $m : 1$. (In other words, $[k(X)^G : k(V)^G] = m$.) If m is relatively prime to the order of C then* $\mathrm{ed}(X, G) \geq n$.

Proof. Since $m = [k(X)^G : k(V)^G]$ is relatively prime to $|C|$, the restriction map $H^n(k(V)^G, C) \longrightarrow H^n(k(X)^G, C)$ is injective; see [Se$_4$, Sect. 2.4]. The desired conclusion now follows from Proposition 12.4(b). □

Example 12.14 Applying Proposition 12.13 to the cohomological invariants we discussed above (all defined with $C = \mathbb{Z}/2\mathbb{Z}$), we arrive at the following result.

Suppose V is a generically free linear representation of G and, $X \dashrightarrow V$ is an $m : 1$-compression, where m is an odd integer. Then

(a) $\mathrm{ed}(X, G) = n$, *if $G = O_n$,*

(b) $\mathrm{ed}(X, G) = n - 1$, *if $G = SO_n$ with $n \geq 3$,*

(c) $\mathrm{ed}(X, G) \geq [n/2]$ *if $G = S_n$ (cf. [BR$_2$, Thm. 7.1]),*

(d) $\mathrm{ed}(X, G) = 3$ *if $G = G_2$,*

(e) $\mathrm{ed}(X, G) \geq 5$ *if $G = F_4$, and*

(f) $\mathrm{ed}(X, G) \geq 3$ *if $G = E_6$, E_7 or E_8.*

Example 12.15 *Let V be a generically free linear representation of the exceptional group F_4, X be a generically free F_4-variety, and $X \dashrightarrow V$ be an F_4-compression, which is generically $m : 1$, where m is not divisible by 3. Then* $\mathrm{ed}(X, F_4) \geq 3$.

This follows from the non-vanishing of the Serre-Rost invariant

$$H^1(\,\cdot\,, F_4) \simeq Spaces_{\mathbf{A}}(\,\cdot\,) \longrightarrow H^3(\,\cdot\,, \mathbb{Z}/3\mathbb{Z})\,;$$

see [Se$_3$, Sect. 9.3] and [Rost$_1$]. (Here $\mathbf{A}$ is the Albert algebra and $Spaces_{\mathbf{A}}(F)$ is the set of 27-dimensional exceptional Jordan algebras over F, as in Examples 8.4(d) and 12.10.) □

Remark 12.16 We do not know whether the inequality $\mathrm{ed}(PGL_{n^r}) \geq 2r$ of Theorem 9.3 can be proved by the methods of this section. However, if $n = p$ is a prime then the above bound is "stable under prime to p-extensions" in the following sense. Let V be a generically free linear representation of PGL_{p^r} and X be a generically free irreducible PGL_{p^r}-variety. If X admits an $m : 1$-compression $X \dashrightarrow V$, with m relatively prime to p, then $\mathrm{ed}(X, \mathrm{PGL}_{p^r}) \geq 2r$. Equivalently, if D is a prime-to-p extension of a universal division algebra $\mathrm{UD}(m, p^r)$ then $\tau(D) \geq 2r$; see [Re, Theorem 16.1(b)].

Appendix

Since the time that this paper was first submitted for publication, a number of new results on essential dimension have been obtained by this and other authors. We summarize some of them in the table below.

Group	Essential Dimension	Proof
PO_n	$\geq n-1$	[RY]
Spin_n	$= 4, \text{if } n = 7^{(*)}, 10$	[Rost_2]
	$= 5, \text{if } n = 8, 9, 11$	[Rost_2]
	$= 6, \text{if } n = 12, 13$	[Rost_2]
	$= 7, \text{if } n = 14$	[Rost_2]
	$\geq [n/2] + 1 \text{ if } n \equiv 0, \pm 1 \bmod 8$	[RY]
F_4	$= 5$	[Ko_2]
E_6 simply conn.	≥ 4	[RY]$^{(**)}$
	≤ 6	[Ko_2]
E_7 simply conn.	≥ 7	[RY]
	≤ 9	[Ko_2]
E_7 adjoint	≥ 8	[RY]
E_8	≥ 9	[RY]

$^{(*)}$ For $n = 2, \ldots, 6$, the group Spin_n is special and, hence, has essential dimension 0; see Proposition 5.3.

$^{(**)}$ Independent proofs of the inequality $\mathrm{ed}(E_6) \geq 4$ were communicated to us by R. S. Garibaldi and M. Rost.

References

[B] E. Bayer-Fluckiger, *Galois cohomology and the trace form*, Jahresber. Deutsch. Math.-Verein **96**(1994), no. 2, 35-55.

[BP] E. Bayer-Fluckiger, R. Parimala, *Galois cohomology of classical groups over fields of cohomological dimension* ≤ 2, Invent. Math. **122** (1995), 195-229.

[BK] F. Bogomolov, P. Katsylo, *Rationality of certain quotient varieties*, Mat. Sbornik, **126**(168) (1985), no. 4, 584-589.

[BR_1] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159-179.

[BR_2] J. Buhler, Z. Reichstein, *On Tschirnhaus transformations*, in "Number Theory", Proceedings of a conference held at Penn. State University, edited by S. Ahlgren, G. Andrews and K. Ono, Kluwer Acad. Publishers, 127-142, 1999. Preprint available at http://www.orst.edu/~reichstz/pub.html.

[De] 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.

[Do] I. V. Dolgachev, *Rationality of fields of invariants*, in Algebraic Geometry, Bowdoin 1985, Proceedings of Symposia in Pure Mathematics, vol. 46, part 2, AMS, 1987, 3-16.

[Gi] Ph. Gille, *Cohomologie galoisienne des groupes quasi-déployés sur des corps de dimension cohomologique ≤ 2*, preprint, 1998.

[G] A. Grothendieck, *Torsion homologique et sections rationnelles*, Exposé 5, Séminaire C. Chevalley, Anneaux de Chow et applications, 2nd année, IHP, 1958.

[H] J. E. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, Springer-Verlag, 1975.

[I] A. V. Iltyakov, *On rational invariants of the group E_6*, Proc. Amer. Math. Soc. **124**, vol. 124, no. 12 (1996), 3637-3640.

[J] N. Jacobson, Structure and Representations of Jordan Algebras, AMS Colloq. Publ. **39**, Amer. Math. Soc., Providence, Rhode Island, 1968.

[Ka_1] P. I. Katsylo, *Rationality of the orbit spaces of irreducible representations of the group* SL_2, Izv. Acad. Nauk SSSR Ser. Mat. **47** (1983), 26-36.
English translation: Math. USSR-Izvestya, **22** (1984), no. 1, 23-32.

[Ka_2] P. I. Katsylo, *Rationality of the module variety of mathematical instantons with* $c_2 = 5$, in Lie Groups, their discrete subgroups, and invariant theory, Advances in Soviet Math **8** (1992), American Math. Soc., Providence, RI., 65-68.

[KMRT] M.-A.Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, AMS Colloquium Publications, vol. 44.

[Ko_1] V. E. Kordonsky, *Essential dimensions of algebraic groups* (in Russian), preprint.

[Ko_2] V. E. Kordonsky, *On the essential dimension and Serre's Conjecture II for exceptional groups*, (in Russian), preprint.

[Pf] A. Pfister, *Quadratic Forms with Applications to Geometry and Topology*, Cambridge University Press, 1995.

[Pi] R. S. Pierce, *Associative Algebras*, Springer, New York, 1982.

[Po] V. L. Popov, *Sections in Invariant Theory*, Proceedings of the Sophus Lie Memorial Conference, Scandinavian University Press, 1994, 315-362.

[PV] V. L. Popov, E. B. Vinberg, *Invariant Theory*, in Encyclopedia of Math. Sciences **55**, Algebraic Geometry IV, edited by A. N. Parshin and I. R. Shafarevich, Springer-Verlag, 1994.

[Pr_1] C. Procesi, *Non-commutative affine rings*, Atti Acc. Naz. Lincei, S. VIII, v. VIII, fo. 6 (1967), 239-255.

[Pr_2] C. Procesi, *The invariant theory of $n \times n$-matrices*, Adv. Math., **19** (1976), 306-381.

[Re] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canadian J. Math., to appear. Preprint available at http://www.orst.edu/~reichstz/pub.html.

[RY] Z. Reichstein, B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, with an appendix by J. Kollár and E. Szabó, submitted for publication. Preprint available at http://www.orst.edu/~reichstz/pub.html.

[Ros_1] M. Rosenlicht, *Some basic theorems on algebraic groups*, American Journal of Math., **78** (1956), 401-443.

[Ros_2] M. Rosenlicht, *A remark on quotient spaces*, Anais da Academia Brasileira de Ciências **35** (1963), 487-489.

[$Rost_1$] M. Rost, *A (mod 3) invariant of exceptional Jordan algebras*, C. R. Acad. Sci. Paris Sér. I Math. **313**, no. 12 (1991), 823-827.

[$Rost_2$] M. Rost, *On Galois cohomology of Spin(14)*, preprint, March 1999. Available at http://www.physik.uni-regensburg.de/~rom03516.

[Row] L. H. Rowen, *Brauer factor sets and simple algebras*, Trans. Amer. Math. Soc., **282**, no. 2 (1984), 765-772.

[Sc] R. D. Schaefer, An Introduction to Non-associative Algebras, Academic Press, New York and London, 1966.

[Se_1] J.-P. Serre, *Espaces fibrés algébriques*, Exposé 5, Séminaire C. Chevalley, Anneaux de Chow et applications, 2nd année, IHP, 1958.

[Se_2] J.-P. Serre, *Local Fields*, Springer-Verlag, 1979.

[Se_3] J.-P. Serre, *Cohomologie galoisienne: progrès et problèmes*, in "Séminaire Bourbaki, Volume 1993/94, Exposés 775-789", Astérisque **227** (1995), 229-257.

[Se_4] J.-P. Serre, *Galois Cohomology*, Springer, 1997.

[St] R. Steinberg, *Regular elements of semisimple groups*, Publ. Math. I.H.E.S. **25** (1965), 281-312. Reprinted in [Se_4], pp. 155-186.

[SSSZ] I. P. Shestakov, A. I. Shirshov, A. M. Slin'ko, K. A. Zhevlakov, Rings that are Nearly Associative, Academic Press, 1982.