ISRAEL JOURNAL OF MATHEMATICS **192** (2012), 325–346
DOI: 10.1007/s11856-012-0037-9

ESSENTIAL DIMENSION OF INVOLUTIONS AND SUBALGEBRAS

BY

Roland Lötscher

Mathematisches Institut der Ludwig-Maximilians-Universität München
Theresienstraße 39, D-80333 München, Germany
e-mail: Roland.Loetscher@mathematik.uni-muenchen.de

ABSTRACT

Essential dimension is an invariant of algebraic groups G over a field F that measures the complexity of G-torsors over field extensions of F. We use theorems of N. Karpenko about the incompressibility of Severi–Brauer varieties and quadratic Weil transfers of Severi–Brauer varieties to compute the essential dimension of some closed subgroups of $R_{K/F}(\mathbf{GL}_1(A))$, where A is a central division K-algebra of prime power degree and K/F is a separable field extension of degree ≤ 2. In particular, we determine the essential dimension of the group $\mathbf{Sim}(A,\sigma)$ of similitudes of (A,σ), where σ is an F-involution on A, and the essential dimension of the normalizer $N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$, where B is a separable subalgebra of A.

Contents

Received September 29, 2010 and in revised form March 18, 2011

1. Introduction

Essential dimension is a numerical invariant of algebraic objects measuring their complexity. Roughly, it is defined as the minimal number of independent parameters needed to define algebraic objects of a given type, e.g. degree n central simple algebras, n-dimensional quadratic forms, torsors of an algebraic group etc.

Essential dimension was introduced by J. Buhler and Z. Reichstein around 1995 when studying Tschirnhaus transformations of polynomials in one variable [BR97]. They defined the essential dimension of a finite group G (relative to a base field F) in invariant theoretic terms and showed that the essential dimension of the symmetric group $G = S_n$ can be understood as the minimal number of algebraically independent parameters in a polynomial $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ obtained by means of Tschirnhaus transformations from the generic degree n polynomial (where $a_1, \ldots, a_n$ are algebraically independent over F). Later Reichstein extended this notion to algebraic groups G and showed that this concept can be used to measure the complexity of algebraic objects like quadratic forms (when $G = \mathbf{O}_n$), central simple algebras (when $G = \mathbf{PGL}_n$), octonion algebras (when $G = \mathbf{G}_2$) etc. [Re00].

The most general definition of essential dimension, due to A. Merkurjev, assigns to each (covariant) functor $\mathcal{F}\colon \mathrm{Fields}/F \to \mathrm{Sets}$ a non-negative integer, called essential dimension of $\mathcal{F}$. We refer to [BF03] and [Me09] for its definition. Briefly, the essential dimension $\operatorname{ed}\mathcal{F}$ of the functor $\mathcal{F}$ is less than or equal to $n \in \mathbb{N}_0$ if and only if every element $a \in \mathcal{F}(L)$ (where $L \in \mathrm{Fields}/F$) can be defined over a subfield $L_0 \in \mathrm{Fields}/F$ of transcendence degree at most n.

To each functor $\mathcal{F}\colon \mathrm{Fields}/F \to \mathrm{Sets}$ we can associate its detection functor $\mathcal{D}_{\mathcal{F}}\colon \mathrm{Fields}/F \to \mathrm{Sets}$, defined by

$$\mathcal{D}_{\mathcal{F}}(L) = \begin{cases} \emptyset & \text{if } \mathcal{F}(L) = \emptyset, \\ \{L\} & \text{otherwise.} \end{cases}$$

The essential dimension of $\mathcal{D}_{\mathcal{F}}$ is called **canonical dimension** of $\mathcal{F}$, denoted $\operatorname{cdim}\mathcal{F}$. The concept of canonical dimension was introduced by G. Berhuy and Z. Reichstein [BR05]. We will mainly use [Me09] as a reference. It is easy to see that $\operatorname{cdim}\mathcal{F} \leq \operatorname{ed}\mathcal{F}$. The fields $L \in \mathrm{Fields}/F$ with $\mathcal{F}(L) \neq \emptyset$ are called splitting fields of $\mathcal{F}$. The functor $\mathcal{F}$ has canonical dimension $\leq n$ if and only if every

splitting field L of $\mathcal{F}$ contains a subfield $L_0 \in \mathrm{Fields}/F$ of transcendence degree $\leq n$ that splits $\mathcal{F}$ as well.

There is a variant of essential (and canonical) dimension relative to a prime number p, called **essential p-dimension** (resp. canonical p-dimension). Essential p-dimension measures the complexity of algebraic objects up to prime to p extensions. We refer to [Me09] for its definition.

If G is a group scheme (always assumed of finite type) over F, the essential dimension (resp. p-dimension) of G is defined as

$$\operatorname{ed} G = \operatorname{ed} H^1(-, G), \quad \text{resp. } \operatorname{ed}_p G = \operatorname{ed}_p H^1(-, G),$$

where $H^1(-, G)$ is the flat cohomology functor, which takes a field extension L/F to the set of isomorphism classes of G-torsors over L (in the finitely presented faithfully flat topology).

A variety X over F can be viewed as the functor of points

$$X \colon \mathrm{Fields}/F \to \mathrm{Sets}, \quad L \mapsto X(L) = \mathrm{Mor}(\operatorname{Spec} L, X).$$

The essential dimension and p-dimension of X are easy to compute: They are equal to the dimension of X; see [BF03, Proposition 1.17], [Me09, Proposition 1.2]. On the other hand, the canonical dimension (or p-dimension) of X is an interesting invariant of X in case that X does not have F-rational points. Interesting examples include quadrics, Severi–Brauer varieties and torsors of an algebraic group G.

A variety X is said to be p-incompressible if $\operatorname{cdim}_p X = \dim X$. In this paper we make use of the following incompressibility results due to N. Karpenko:

THEOREM 1.1 ([Ka00, Ka09]): *Let D be a central division K-algebra of degree p^r for some $r \geq 0$ and a prime p. Then $\mathrm{SB}(D)$ is p-incompressible. Moreover, if K/F is a quadratic separable field extension, $p = 2$, and the norm algebra $N_{K/F}(D)$ is split, then $R_{K/F}(\mathrm{SB}(D))$ is 2-incompressible.*

For most applications we will only use the (older) incompressibility result on $\mathrm{SB}(D)$. The (newer) incompressibility result on the Weil restriction $R_{K/F}(\mathrm{SB}(D))$ will be needed for the computation of the essential dimension of group schemes associated with unitary involutions. The reader who is only interested in group schemes associated to subalgebras and non-unitary involutions may always restrict his or her attention to the simpler case where no Weil restrictions are needed.

We will adopt and freely use the notations and conventions of [KMRT98] with just a few exceptions, that will be made explicit. Most significantly $H^1(-,G)$ (and, when G is abelian, $H^2(-,G)$) will denote flat cohomology rather than Galois cohomology. We refer to [Wa79, §17, 18] for basics on flat cohomology. The difference only shows up for non-smooth group schemes G. For example, the flat cohomology set $H^1(F,\mathbf{GO}(M_n(F),\tau))$ (where τ is transposition of matrices) stands in bijection with the set of (all) conjugacy classes of orthogonal involutions σ on $M_n(F)$, whereas the Galois cohomology set $H^1_{\mathrm{Gal}}(F,\mathbf{GO}(M_n(F),\tau))$ consists only of those classes for which σ and τ become conjugate over F_{sep}. If F_{sep} is not quadratically closed, this is a non-trivial restriction.

The rest of this paper is organized as follows: In Section 2 we describe our strategy of applying Karpenko's incompressibility results to the computation of the exact values of the essential dimension (and p-dimension) of certain subgroups G of $R_{K/F}(\mathbf{GL}_1(A))$, where K/F is a separable field extension of degree ≤ 2 and A is a division K-algebra of p-primary degree.

In Section 3 we apply this strategy to the subgroup $G=\mathbf{Sim}(A,\sigma)$ of similitudes of (A,σ), where σ is an F-involution on A. In that case G-torsors over a field extension L/F correspond to conjugacy classes of involutions on A_L of the same type (unitary, orthogonal or symplectic) as σ. In Section 4 we consider the subgroup $G=N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$, where B is a separable subalgebra of A. Here G-torsors over a field extension L/F correspond to conjugacy classes of separable subalgebras of A_L which are conjugate to B over L_{sep}. Our main results are Theorems 3.2 and 4.10, which give the precise value of the essential dimension of the groups G under consideration.

Most work on essential dimension has been done for split[1] algebraic groups; see, e.g., [Ba10, BM10, BR97, Du10, GR09, KM08, Le04, Ma10, Me10, MR09, MR10, Re00, Ru11, RY00]. The essential dimension of non-split algebraic tori and twisted p-groups were recently studied in [LMMR10]. For these groups the essential dimension had already previously been known in the split case. For the groups $G=N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$ that we consider in this paper, much less is known in the split case (where A and B are split algebras). In fact the computation of the essential dimension in the split case would reveal (among other things) the exact value of the (absolute and p-relative) essential dimension of the

[1] We call a (not necessarily connected) algebraic group G over F **split** if the identity component G^0 is a reductive split group in the usual sense (i.e., containing a split maximal torus over F) and G/G^0 is a constant (finite) group.

projective linear groups $\mathbf{PGL}_{p^n}$ and the symmetric groups S_{p^n} (for all prime primes p and $n \geq 1$); see Remarks 4.8 and 4.12. At the present time determining these values for large n seems far out of reach. To my best knowledge the algebraic groups studied here provide the first examples of groups G, where the precise value of $\operatorname{ed} G$ is determined while the problem of determining $\operatorname{ed} G_{\mathrm{alg}}$ remains largely open.

2. A general strategy

Let E/F be an étale F-algebra and A be an Azumaya E-algebra. We have an exact sequence

$$1 \to R_{E/F}(\mathbf{G}_m) \to R_{E/F}(\mathbf{GL}_1(A)) \xrightarrow{\mathrm{Int}} \mathbf{Aut}_E(A) \to 1$$

of group schemes over F, where Int takes an element a of $(A \otimes_F L)^\times$ (for a field extension L/F) to the $E \otimes_F L$-algebra automorphism of $A_L := A \otimes_F L$ sending x to axa^{-1}. Let H be an arbitrary (closed) subgroup of $\mathbf{Aut}_E(A)$ and set $G = \mathrm{Int}^{-1}(H)$. Then we have a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & R_{E/F}(\mathbf{G}_m) & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & R_{E/F}(\mathbf{G}_m) & \longrightarrow & R_{E/F}(\mathbf{GL}_1(A)) & \xrightarrow{\mathrm{Int}} & \mathbf{Aut}_E(A) & \longrightarrow & 1
\end{array}$$

of group schemes over F with exact rows, where the vertical arrows are closed embeddings.

Let L/F be a field extension. The set $H^1(L, \mathbf{Aut}_E(A))$ stands in natural bijection with the set of isomorphism classes of Azumaya $L \otimes_F E$-algebras A' which become isomorphic to A_L over a seperable closure L_{sep}. Its distinguished element is the class of A_L. The group $H^2(L, R_{E/F}(\mathbf{G}_m))$ is naturally isomorphic to the Brauer group of $L \otimes_F E$. The connection map

$$\delta^1 \colon H^1(L, \mathbf{Aut}_E(A)) \to H^2(L, R_{E/F}(\mathbf{G}_m)) = \mathrm{Br}(L \otimes_F E)$$

takes the isomorphism class of an Azumaya algebra A' to the Brauer class of $A' \otimes_{L \otimes_F E} A_L^{\mathrm{op}} = A' \otimes_E A^{\mathrm{op}}$.

Take an H-torsor T over some field extension L of F. Let A' be an Azumaya $L \otimes_F E$-algebra representing the image of T in $H^1(L, \mathbf{Aut}_E(A))$. Consider the L-variety

$$X = R_{L \otimes_F E/L}(\mathrm{SB}(A' \otimes_E A^{\mathrm{op}})).$$

The splitting fields of X are precisely those $M \in \mathrm{Fields}/L$ for which T lifts to an H-torsor. They coincide with the splitting fields of the quotient stack $[T/G]$ of T by its natural G_L-action. For the definition of the quotient stack $[T/G]$ and its essential and canonical dimension, see [BRV08].

The following result will be our main tool for computing essential and canonical dimensions of algebraic groups.

PROPOSITION 2.1: *Suppose that X is p-incompressible. Then*

$$\mathrm{ed}_p G = \mathrm{ed}\, G = \dim_F A - \dim G.$$

Moreover, if $E = F$ then every subgroup S of G with $\mathrm{Int}(S) = H$ which intersects the center $\mathbf{G}_m$ of $\mathbf{GL}_1(A)$ exactly in μ_{p^n} for some $n \geq 1$ satisfies

$$\mathrm{ed}_p S = \mathrm{ed}\, S = \dim_F A - \dim S.$$

Proof. First observe that G and S embed in the group scheme $R_{E/F}(\mathbf{GL}_1(A))$ of dimension $\dim_F A$. By Hilbert's Theorem 90 and Shapiro's lemma (see [KMRT98, Theorem 29.2, Lemma 29.6]) the group scheme $R_{E/F}(\mathbf{GL}_1(A))$ has essential dimension 0. Hence application of [Me09, Corollary 4.3] yields the inequalities $\mathrm{ed}_p G \leq \mathrm{ed}\, G \leq \dim_F A - \dim G$ and $\mathrm{ed}_p S \leq \mathrm{ed}\, S \leq \dim_F A - \dim S$.

It remains to show $\mathrm{ed}_p G \geq \dim_F A - \dim G$ and $\mathrm{ed}_p S \geq \dim_F A - \dim S$. By [Me09, Theorem 4.8] (see also [BRV08, Corollary 3.3]) $\mathrm{ed}_p G \geq \mathrm{ed}_p[T/G] - \dim H$, hence $\mathrm{ed}_p G \geq \mathrm{cdim}_p[T/G] - \dim H$. By construction, the splitting fields of $[T/G]$ coincide with the splitting fields of the variety X, which is p-incompressible. Thus $\mathrm{cdim}_p[T/G] = \dim X$. It follows that $\mathrm{ed}_p G \geq \dim X - \dim H = \dim_F A - \dim G$.

Similarly we have $\mathrm{ed}_p S \geq \mathrm{ed}_p[T/S] - \dim H$. Since $[T/S]$ is a gerbe banded by μ_{p^n} we have $\mathrm{ed}_p[T/S] = \mathrm{cdim}_p[T/S] + 1$ by [Me09, Example 3.6] (see also [BRV08, Theorem 4.1]). The splitting fields of $[T/S]$ also coincide with the splitting fields of X. Therefore $\mathrm{ed}_p[T/S] \geq \dim X + 1 = \dim_F A - \dim S$. This concludes the proof. ∎

Interesting subgroups of $\mathbf{Aut}_E(A)$ are actually easy to find: Just endow A with some additional structure (an involution, a quadratic pair, a separable subalgebra in our examples) and take the subgroup of $\mathbf{Aut}_E(A)$ consisting of E-algebra automorphisms preserving that additional structure.

Our goal now is to find interesting examples where

$$X = R_{L\otimes E/L}(\mathrm{SB}(A' \otimes_E A^{\mathrm{op}}))$$

is in fact p-incompressible. We will do this in case that E/F is either a separable quadratic field extension (and $p = 2$) or $E = F$ (and p is arbitrary). We assume that $\deg A$ is a power of p. Note that in these cases, in view of Theorem 1.1 all we need for p-incompressibility of X is that $D := A' \otimes_E A^{\mathrm{op}}$ is a division algebra and that $N_{L\otimes_F E/L}(D)$ splits when $[E : F] = 2$.

We fix a prime p and use the following notation (which slightly differs from the notation used in [KMRT98]):

Definition 2.2: Let L be a field.

CASE $\operatorname{char} L \neq p$ AND L CONTAINS A PRIMITIVE pTH ROOT OF UNITY ζ: Let $a, b \in L^\times$. We denote by $(a, b)_L$ the cyclic L-algebra generated by symbols u and v with relations $u^p = a, v^p = b$ and $vu = \zeta uv$.

CASE $\operatorname{char} L = p$: Let $a, b \in L$ with b invertible. We denote by $(a, b)_L$ the cyclic L-algebra generated by symbols u and v with relations $u^p - u = a, v^p = b$ and $vu = uv + u$.

Note that the definition of $(a, b)_L$ in the first case depends on the choice of ζ. For us this choice will not matter, hence we do not include it in the notation. Different choices of ζ for different algebras $(a, b)_L$ will be fine for us, too.

The following lemma will help us to produce examples where $D = A' \otimes_E A^{\mathrm{op}}$ is a division algebra:

LEMMA 2.3: *Let $a_1, b_1, \dots, a_r, b_r$ be algebraically independent variables over F and let $L = F'(a_1, b_1, \dots, a_r, b_r)$, where F' is F adjoined a primitive pth root of unity if* $\operatorname{char} F \neq p$ *resp. $F' = F$ if* $\operatorname{char} F = p$. *Let*

$$A'_0 = (a_1, b_1)_L \otimes_L (a_2, b_2)_L \otimes_L \cdots \otimes_L (a_r, b_r)_L.$$

Let E/F be a (finite) separable field extension which is linearly disjoint from F' and let A be a central simple E-algebra of p-power degree. Set $M = L \otimes_F E = (F' \otimes_F E)(a_1, b_1, \dots, a_r, b_r)$. Then $A'_0 \otimes_F A^{\mathrm{op}}$ is a central simple M-algebra with

$$\operatorname{ind} A'_0 \otimes_F A^{\mathrm{op}} = p^r \operatorname{ind} A.$$

Proof. First of all note that $\operatorname{ind} A \otimes_F F' = \operatorname{ind} A$ since F'/F has degree prime to p. Hence we may replace F' by F, A by $A \otimes_F F'$ and E by the field $E \otimes_F F'$ and hence assume $F' = F$. Using induction on $r \geq 0$ one easily reduces to the case $r = 1$. The claim then follows from the index formula given in [Me10, (11) §4.1] (cf. [JW90, Prop. 1.15(a)] and [Ti78, Prop. 2.4]). ∎

We summarize this section in a corollary, which will later be invoked for various choices of group schemes H.

COROLLARY 2.4: *Let either $E = F$ or E/F be a separable quadratic field extension and let A be a division E-algebra of degree p^r. If $[E : F] = 2$ assume that $p = 2$ and that $N_{E/F}(A)$ splits. Let L/F and A'_0 be as in Lemma 2.3 and set $A' = A'_0 \otimes_F E$.*

Assume that the class of A' lies in the image of $H^1(L, H) \to H^1(L, \mathbf{Aut}_E(A))$ for a subgroup H of $\mathbf{Aut}_E(A)$. Let G be the inverse image of H under the homomorphism $\mathrm{Int}\colon R_{E/F}(\mathbf{GL}_1(A)) \to \mathbf{Aut}_E(A)$. *Then*

$$\operatorname{ed} G = \operatorname{ed}_p G = \dim_F A - \dim G.$$

Moreover, if $E = F$ then every subgroup S of G with $\mathrm{Int}(S) = H$ which intersects the center $\mathbf{G}_m$ of $\mathbf{GL}_1(A)$ exactly in μ_{p^n} for some $n \geq 1$ satisfies

$$\operatorname{ed} S = \operatorname{ed}_p S = \dim_F A - \dim S.$$

Proof. Lemma 2.3 implies that $A' \otimes_E A^{\mathrm{op}} = A'_0 \otimes_F A^{\mathrm{op}}$ is a division algebra. In case $[E : F] = 2$, note that $N_{L\otimes_F E/L}(A' \otimes_E A^{\mathrm{op}})$ splits since $N_{E/F}(A)$ and $N_{L\otimes_F E/L}(A')$ split. Theorem 1.1 shows that $X = R_{L\otimes_F E/L}(\mathrm{SB}(A' \otimes_E A^{\mathrm{op}}))$ is p-incompressible. Hence the claim follows from Proposition 2.1. ∎

3. Involutions

Let A be a central simple E-algebra admitting an involution σ. Let $F = E^\sigma \subseteq E$ be the field of central elements fixed under σ. We call (A, σ) a central simple F-algebra with involution. For unitary involutions we include the case $E = F \times F$ in this definition by allowing A to be a direct product $A = A_1 \times A_2$ with A_1 and A_2 central simple F-algebras of the same degree.

Two involutions σ' and σ on A are said to be **conjugate** if there exists $a \in A$ such that $\sigma' = \mathrm{Int}(a) \circ \sigma \circ \mathrm{Int}(a)^{-1}$. Equivalently, (A, σ) and (A, σ') are isomorphic as F-algebras with involution.

Conjugate involutions are necessarily of the same type (unitary, orthogonal or symplectic). When F is algebraically closed there are precisely 3 conjugacy classes of involutions on $A = M_n(E)$, one for each type.

For the case of characteristic 2 we will also use the notion of **quadratic pair** which extends the distinction between quadratic forms and symmetric bilinear forms to non-split central simple algebras. A quadratic pair on a central simple

F-algebra A is given by a pair (σ, f), where σ is a symplectic involution (we assume $\operatorname{char} F = 2$) and $f\colon \operatorname{Sym}(A,\sigma) \to F$ is an F-linear map subject to the condition $f(x + \sigma(x)) = \operatorname{Trd}_A(x)$ for all $x \in A$.

We want to compute the essential dimension of the group schemes $\mathbf{Sim}(A,\sigma)$ of similitudes of a central simple F-algebra with involution (A,σ), and of some subgroup schemes like the group scheme $\mathbf{Iso}(A,\sigma)$ of isometries of (A,σ). The computation of the essential dimension of $\mathbf{Sim}(A,\sigma)$ is of particular interest, since its torsors can be seen as conjugacy classes of certain involutions: For a field extension L/F the set $H^1(L, \mathbf{Sim}(A,\sigma))$ stands in natural one-to-one correspondence with the set of conjugacy classes of involutions on A_L of the same type as σ; see [KMRT98, §29.D].

Example 3.1: Let $Q = (a,b)_F$ be a quaternion algebra and denote by γ the canonical involution on Q. Let L/F be a field extension. The only symplectic involution on Q_L is γ_L. Hence $\operatorname{ed} \mathbf{Sim}(Q,\gamma) = 0$.

Every orthogonal involution σ on Q_L is of the form $\sigma = \operatorname{Int}(s) \circ \gamma_L$ for some $s \in \operatorname{Skew}(Q_L,\gamma_L) \setminus L$. The conjugacy class of σ is determined uniquely by the discriminant of σ [KMRT98, Example 7.4], given by $\operatorname{disc}\sigma = s^2 \cdot (L^\times)^2 \in L^\times/(L^\times)^2$. When Q is split every element of $L^\times$ is the square of some $s \in \operatorname{Skew}(Q_L,\gamma_L) \setminus L$, hence $H^1(-, \mathbf{Sim}(Q,\sigma))$ is isomorphic to the functor $H^1(-,\mu_2)\colon L \mapsto L^\times/(L^\times)^2$. This implies that $\operatorname{ed}_2 \mathbf{Sim}(Q,\sigma) = \operatorname{ed} \mathbf{Sim}(Q,\sigma) = 1$ for a split quaternion algebra Q. We will see that if Q is non-split then $\operatorname{ed}_2 \mathbf{Sim}(Q,\sigma) = \operatorname{ed} \mathbf{Sim}(Q,\sigma) = 2$.

THEOREM 3.2: *Let $n = 2^r$ for some $r \geq 1$. Let (A,σ) be a central simple F-algebra with involution, where A is a division algebra and $\deg A = n$. Then*

$$\begin{aligned}\operatorname{ed} \mathbf{Sim}(A,\sigma) = \operatorname{ed}_2 \mathbf{Sim}(A,\sigma) &= \dim_F A - \dim \mathbf{Sim}(A,\sigma)\\ &= \begin{cases} n^2 - 1 & \text{if } \sigma \text{ is unitary,}\\ \frac{n(n+1)}{2} - 1 & \text{if } \sigma \text{ is orthogonal,}\\ \frac{n(n-1)}{2} - 1 & \text{if } \sigma \text{ is symplectic.}\end{cases}\\ \operatorname{ed} \mathbf{Iso}(A,\sigma) = \operatorname{ed}_2 \mathbf{Iso}(A,\sigma) &= \dim_F A - \dim \mathbf{Iso}(A,\sigma)\\ &= \begin{cases} \frac{n(n+1)}{2} & \text{if } \sigma \text{ is orthogonal,}\\ \frac{n(n-1)}{2} & \text{if } \sigma \text{ is symplectic.}\end{cases}\end{aligned}$$

For a quadratic pair (σ, f) on A (where $\operatorname{char} F = 2$) we have

$$\begin{aligned}\operatorname{ed}\mathbf{GO}(A,\sigma,f) &= \operatorname{ed}_2\mathbf{GO}(A,\sigma,f) = \dim_F A - \dim\mathbf{GO}(A,\sigma,f)\\ &= \frac{n(n+1)}{2} - 1,\\ \operatorname{ed}\mathbf{O}(A,\sigma,f) &= \operatorname{ed}_2\mathbf{O}(A,\sigma,f) = \dim_F A - \dim\mathbf{O}(A,\sigma,f)\\ &= \frac{n(n+1)}{2}.\end{aligned}$$

Moreover, in case, $r \geq 2$:

$$\begin{aligned}\operatorname{ed}\mathbf{GO}^+(A,\sigma,f) &= \operatorname{ed}_2\mathbf{GO}^+(A,\sigma,f) = \dim_F A - \dim\mathbf{GO}^+(A,\sigma,f)\\ &= \frac{n(n+1)}{2} - 1,\\ \operatorname{ed}\mathbf{O}^+(A,\sigma,f) &= \operatorname{ed}_2\mathbf{O}^+(A,\sigma,f) = \dim_F A - \dim\mathbf{O}^+(A,\sigma,f)\\ &= \frac{n(n+1)}{2}.\end{aligned}$$

REMARK 3.3: The assumption $r \geq 2$ in the statements about $\mathbf{GO}^+(A,\sigma,f)$ and $\mathbf{O}^+(A,\sigma,f)$ is needed. When $r = 1$ the algebra A is a quaternion division algebra, $A = (a,b)_F$, σ its canonical involution, and I claim that $\operatorname{ed}\mathbf{GO}^+(A,\sigma,f) = 0 < 2$ and $\operatorname{ed}\mathbf{O}^+(A,\sigma,f) = 1 < 3$. In fact $\mathbf{GO}^+(A,\sigma,f) = R_{F(u)/F}(\mathbf{G}_m)$ and $\mathbf{O}^+(A,\sigma,f) = R^{(1)}_{F(u)/F}(\mathbf{G}_m)$ are tori. Their essential dimension and 2-dimension were computed in [LMMR10] (cf. [BF03, Theorem 2.5]).

Proof of Theorem 3.2. It is routine to compute the dimension of the algebraic groups G under consideration. Thus it remains to show that for all these groups the equalities $\operatorname{ed} G = \operatorname{ed}_2 G = \dim_F A - \dim G$ hold true, for which we have to verify the assumptions of Corollary 2.4. Let K be the center of A, which is either F (when σ is symplectic or orthogonal) or a separable quadratic extension of F (when σ is unitary). First note that in the case $[K : F] = 2$ the norm algebra $N_{K/F}(A)$ is split, since A has a unitary involution σ.

The groups $\mathbf{Sim}(A,\sigma)$, $\mathbf{GO}(A,\sigma,f)$ and $\mathbf{GO}^+(A,\sigma,f)$ are the inverse images of the groups $\mathbf{Aut}_K(A,\sigma)$, $\mathbf{Aut}_K(A,\sigma,f)$ and $\mathbf{PGO}^+(A,\sigma,f)$, respectively, under $\mathrm{Int}\colon R_{K/F}(\mathbf{GL}_1(A)) \to \mathbf{Aut}_K(A)$. Moreover, they have the same image under Int as their subgroups $\mathbf{Iso}(A,\sigma)$, $\mathbf{O}(A,\sigma,f)$ and $\mathbf{O}^+(A,\sigma,f)$, respectively. The intersection of $\mathbf{Iso}(A,\sigma)$, $\mathbf{O}(A,\sigma,f)$ and $\mathbf{O}^+(A,\sigma,f)$ with the center $\mathbf{G}_m$ of $\mathbf{GL}_1(A)$ is μ_2 in every case (note that σ is orthogonal or symplectic here).

All that remains is to show that the isomorphism class of the algebra $A' = (a_1, b_1)_L \otimes_L \cdots \otimes_L (a_r, b_r)_L \otimes_F K$ from Corollary 2.4 lies in the image of the maps $H^1(L, H) \to H^1(L, \mathbf{Aut}_K(A))$, where H is one of the groups $\mathbf{Aut}_K(A, \sigma)$, $\mathbf{Aut}_K(A, \sigma, f)$ and $\mathbf{PGO}^+(A, \sigma, f)$.

The image of $H^1(L, \mathbf{Aut}_K(A, \sigma)) \to H^1(L, \mathbf{Aut}_K(A))$ consists of those isomorphism classes of Azumaya $L \otimes_F K$-algebras which admit an L-involution of the same type as σ. Since $A' \otimes_F A'$ splits when $K = F$ and $N_{K/F}(A')$ splits when $[K : F] = 2$, and since $r \geq 1$, the algebra A' does admit an L-involution of the respective type. Similarly, the image of the map

$$H^1(L, \mathbf{Aut}_F(A, \sigma, f)) \to H^1(L, \mathbf{Aut}_F(A))$$

consists of those isomorphism classes of central simple L-algebras that admit a quadratic pair, hence it contains the isomorphism class of A'.

The map $H^1(L, \mathbf{PGO}^+(A, \sigma, f)) \to H^1(L, \mathbf{Aut}_F(A))$ consists of the classes of central simple L-algebras A' of degree $\deg A' = \deg A$ which admit a quadratic pair (σ', f') such that $\operatorname{disc}(\sigma_L, f_L) = \operatorname{disc}(\sigma', f')$. By [Be05, Theorem 2] (note that $\operatorname{char} L = 2$) every central simple L-algebra A' which is not a quaternion division algebra, and which has a symplectic involution, admits quadratic pairs of arbitrary discriminant. In particular, since $r \geq 2$, the algebra A' admits quadratic pairs of arbitrary discriminant. This concludes the proof. ∎

As $H^1(-, \mathbf{Sim}(A, \sigma))$ classifies conjugacy classes of involutions, Theorem 3.2 has the following interpretation:

COROLLARY 3.4: *Let (A, σ) and $n = \deg A$ be as in Theorem 3.2, where σ is unitary (resp. orthogonal, resp. symplectic). The integer $e = n^2 - 1$ (resp. $\frac{n(n-1)}{2} + 1$, resp. $\frac{n(n-1)}{2} - 1$) is the smallest integer with the following property: For every field extension L/F and unitary (resp. orthogonal, resp. symplectic) involution σ' on A_L there exists a sub-extension L_0/F of L/F with $\operatorname{tdeg}_F L_0 \leq e$ and an involution σ_0 on A_{L_0} such that σ' is conjugate to $(\sigma_0) \otimes_{L_0} L$.*

REMARK 3.5: For unitary involutions σ on a division algebra A of degree $n = 2^r$ we only know $n^2 - 1 \leq \operatorname{ed}_2 \mathbf{Iso}(A, \sigma) \leq \operatorname{ed} \mathbf{Iso}(A, \sigma) \leq n^2$. These bounds follow from Theorem 3.2 and the following lemma, which relates the essential dimension of $\mathbf{Sim}(A, \sigma)$ and $\mathbf{Iso}(A, \sigma)$. Suppose the equality $\operatorname{ed}_2 \chi = \operatorname{cdim}_2 \chi + 1$ holds for every quadratic separable extension K/F and every gerbe χ banded by $R^{(1)}_{K/F}(\mathbf{G}_m)$ (for the notion of gerbes and their essential dimension see [BRV08]).

Then one can show that $\operatorname{ed}\mathbf{Iso}(A,\sigma) = \operatorname{ed}_2\mathbf{Iso}(A,\sigma) = n^2$ with similar arguments as above.

LEMMA 3.6: *Let (A,σ) be a central simple algebra with involution. Then $\operatorname{ed}\mathbf{Iso}(A,\sigma)$ is either equal to $\operatorname{ed}\mathbf{Sim}(A,\sigma)$ or $\operatorname{ed}\mathbf{Sim}(A,\sigma)+1$. The same holds for essential p-dimension for every prime p.*

Proof. The inequality $\operatorname{ed}\mathbf{Iso}(A,\sigma) \leq \operatorname{ed}\mathbf{Sim}(A,\sigma) + 1$ follows from [Me09, Corollary 4.3]. Note that we have an exact sequence

$$1 \to \mathbf{Iso}(A,\sigma) \to \mathbf{Sim}(A,\sigma) \to \mathbf{G}_m \to 1$$

of group schemes over F. By Hilbert's Theorem 90 we get a surjection of functors

$$H^1(-,\mathbf{Iso}(A,\sigma)) \twoheadrightarrow H^1(-,\mathbf{Sim}(A,\sigma)).$$

Hence $\operatorname{ed}\mathbf{Sim}(A,\sigma) \leq \operatorname{ed}\mathbf{Iso}(A,\sigma)$ by [BF03, Lemma 1.9] and similarly $\operatorname{ed}_p\mathbf{Sim}(A,\sigma) \leq \operatorname{ed}_p\mathbf{Iso}(A,\sigma)$. ∎

REMARK 3.7: The (unique) split forms G_s and S_s of the (connected reductive) groups $G = \mathbf{Sim}(A,\sigma)$ and $S = \mathbf{Iso}(A,\sigma)$ from Theorem 3.2 have much lower essential dimension. Assume $\operatorname{char} F \neq 2$ and let $n = \deg A > 1$ be a power of 2.

(a) If σ is orthogonal then $S_s = \mathbf{O}_n$ has essential dimension n [Re00, Theorem 10.3]. Therefore by Lemma 3.6, $G_s = \mathbf{GO}_n$ has either essential dimension $n-1$ or n. Since every non-degenerate n-dimensional symmetric bilinear form is similar to a diagonal form $\langle a_1,\dots,a_n\rangle$ with $a_1 = 1$, the true value of $\operatorname{ed}\mathbf{GO}_n$ is thus $n-1$. The lower bound $n-1$ was also proven in [GR09] by different means.

(b) If σ is symplectic then $S_s = \mathbf{Sp}_n$ has essential dimension 0 [Re00, Example 8.9b)]. Hence $\mathbf{G}_s = \mathbf{GSp}_n$ has essential dimension 0 as well.

(c) If σ is unitary then $G_s \simeq \mathbf{GL}_n \times \mathbf{G}_m$ and $S_s \simeq \mathbf{GL}_n$ have essential dimension 0 by Hilbert's Theorem 90.

For unitary involutions, the case when K/F is a non-trivial quadratic étale extension is more interesting. Let A be the split central simple K-algebra $A = \operatorname{End}_K(V)$, where V is a n-dimensional K-vector space. Every unitary involution on A is adjoint to a hermitian form h on V, i.e. of the form σ_h. The group $\mathbf{Sim}(\operatorname{End}_K(V),\sigma_h)$ is denoted by $\mathbf{GU}(V,h)$ and $\mathbf{Iso}(\operatorname{End}_K(V),\sigma_h))$ by $\mathbf{U}(V,h)$. The values $\operatorname{ed}\mathbf{GU}(V,h)$ and $\operatorname{ed}\mathbf{U}(V,h)$ seem to be unknown in general.

Since $H^1(L, \mathbf{U}(V,h))$ (for a field extension L/F) classifies non-degenerate hermitian forms of rank n with respect to the quadratic étale extension $K \otimes_F L/L$ and every hermitian form is diagonalizable (with first entry equal to 1 up to similarity), it is only clear that $\operatorname{ed} \mathbf{U}(V,h) \leq n$ and $\operatorname{ed} \mathbf{GU}(V,h) \leq n-1$, which is (for large n) still much smaller than the value $\operatorname{ed} \mathbf{GU}(A,\sigma) = n^2 - 1$ from Theorem 3.2.

4. Subalgebras

An algebra B over a field K is called **separable**, if it is semisimple and remains semisimple over every field extension of K. A finite-dimensional K-algebra is separable if and only if it is a direct product of finite-dimensional simple K-algebras whose centers are finite separable field extensions of K.

Let A be a central simple F-algebra and B a separable subalgebra of A. We call (A,B) a pair of F-algebras. If (A',B') is another pair of F-algebras, we say that (A,B) and (A',B') are isomorphic if there exists an isomorphism $\varphi\colon A \xrightarrow{\sim} A'$ of F-algebras which restricts to an isomorphism $B \xrightarrow{\sim} B'$. We call two subalgebras B and B' of A **conjugate** if (A,B) and (A,B') are isomorphic. Equivalently, there exists $a \in A^\times$ such that $B' = aBa^{-1}$.

In this section we consider the group $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$, the normalizer of $\mathbf{GL}_1(B)$ in $\mathbf{GL}_1(A)$. It is the inverse image of $H = \mathbf{Aut}_F(A,B)$ under $\operatorname{Int}\colon \mathbf{GL}_1(A) \to \mathbf{Aut}_F(A)$. We will compute the essential dimension of G in some cases. First we introduce the **type** of B, which allows us to classify separable subalgebras of A up to conjugacy after scalar extension to F_{sep}.

Let $e_1, \ldots, e_m$ be the primitive central idempotents of $B_{\mathrm{sep}} := B_{F_{\mathrm{sep}}}$. They are unique up to permutation. Let $B_i = B_{\mathrm{sep}} e_i$ for $i = 1, \ldots, m$. Then B_i is a matrix algebra over F_{sep} and the B_i are the simple ideals of B_{sep}. The algebra $A_i := e_i A_{\mathrm{sep}} e_i$ is central simple and contains B_i as a (central) simple subalgebra. Let C_i be the centralizer of B_i in A_i. For $i = 1, \ldots, m$ define $d_i := \deg B_i$ and $r_i := \deg C_i$. The double centralizer theorem implies $d_i r_i = \deg A_i$.

The multiset $t_E := [(d_1, r_1), \ldots, (d_m, r_m)]$ is uniquely determined by B as subalgebra and is invariant under conjugation and scalar extension. We call it the **type** of the subalgebra B.

REMARK 4.1: Separable subalgebras include central simple subalgebras and étale subalgebras. These are precisely those separable subalgebras whose type is of the form $[(d,r)]$ and $[(1,r_1),\dots,(1,r_m)]$, respectively. For étale subalgebras the notion of type has been introduced in [Kr10] by D. Krashen and is equivalent to ours.

LEMMA 4.2: *Let B be a separable subalgebra of a central simple algebra A.*

(a) *The type $t_B = [(d_1,r_1),\dots,(r_m,d_m)]$ satisfies the relations:*

$$\sum_{i=1}^{m} d_i^2 = \dim B \quad \text{and} \quad \sum_{i=1}^{m} d_i r_i = \deg A.$$

(b) *Case $A = M_n(F)$: For every choice of positive integers $d_1, r_1, \dots, d_m, r_m$ satisfying $\sum_{i=1}^m d_i r_i = \deg A$ there exists a separable subalgebra B of A with type $t_B = [(d_1,r_1),\dots,(d_m,r_m)]$.*

(c) *Case A is division: The type of every separable subalgebra of A is constant, i.e., of the form $[(d,r),\dots,(d,r)]$ where $dr \mid \deg A$ and (d,r) appears $\frac{\deg A}{dr}$ times in this multiset. Moreover, if A decomposes as a tensor product of degree p algebras (where p is a fixed prime) then all types of this form appear.*

(d) *Two separable subalgebras of a central simple algebra A have the same type if and only if they are conjugate over F_{sep}.*

Proof. (a) Since $B_{\mathrm{sep}} \simeq B_1 \times \cdots \times B_m$ we have $\dim B = \sum_{i=1}^m \dim B_i = \sum_{i=1}^m d_i^2$. The tensor product $A_{\mathrm{sep}} \otimes_{F_{\mathrm{sep}}} (e_i A_{\mathrm{sep}} e_i)^{\mathrm{op}}$ is canonically isomorphic to the algebra of F_{sep}-linear endomorphisms on $A_{\mathrm{sep}} e_i$. Comparing dimensions yields the equality $d_i r_i \deg A = \dim A_{\mathrm{sep}} e_i$ for every i. Since $A_{\mathrm{sep}} = \bigoplus_{i=1}^m A_{\mathrm{sep}} e_i$ we get $\sum_{i=1}^m d_i r_i = \deg A$.

(b) There exist embeddings $\varphi_i \colon M_{d_i}(F) \hookrightarrow M_{d_i r_i}(F)$ of F-algebras. Set

$$\varphi = \varphi_1 \times \cdots \times \varphi_m \colon M_{d_1}(F) \times \cdots \times M_{d_m}(F) \hookrightarrow M_{d_1 r_1}(F) \times \cdots \times M_{d_m r_m}(F) \subseteq M_n(F).$$

The subalgebra $E = \operatorname{Im}\varphi$ of $A = M_n(F)$ has the desired properties.

(c) Let B be a separable subalgebra of the central division algebra A and $e_1,\dots,e_r$ the primitive central idempotents of B_{sep}. The absolute Galois group $\mathrm{Gal}(F_{\mathrm{sep}}/F)$ permutes the e_i transitively, since A does not contain non-trivial idempotents. It follows that all simple ideals $B_{\mathrm{sep}} e_i$

of B_{sep} have the same dimension and all algebras $e_i A_{\mathrm{sep}} e_i$ have the same dimension. Hence d_i is constant and r_i is constant as well.

Now assume further $A \simeq D_1 \otimes \cdots \otimes D_n$ where $D_1, \ldots, D_n$ are central simple (division) algebras of degree p. Write $d = p^a$, $r = p^b$ with $0 \leq a + b \leq n$. Choose p-dimensional étale subalgebras L_i of D_{i+a} for $i = 1, \ldots, n - (a + b)$. Set

$$B = D_1 \otimes_F \cdots \otimes_F D_a \otimes_F L_1 \otimes_F \cdots \otimes_F L_{n-(a+b)} \otimes_F F \otimes_F \cdots \otimes_F F.$$

This is a subalgebra of type $[(d, r), \ldots, (d, r)]$ as required.

(d) We may assume that F is separably closed and $A = M_n(F)$. Clearly, if two separable subalgebras are conjugate they have the same type. Conversely, let B and B' be separable subalgebras of A of type $[(d_1, r_1) \ldots, (d_m, r_m)]$ and let $e_1, \ldots, e_m$ and $e'_1, \ldots, e'_m$ be the primitive central idempotents of B and B', respectively, such that $\dim Be_i = d_i^2 = \dim B'e'_i$ and $\dim e_i A e_i = (r_i d_i)^2 = \dim e'_i A e'_i$. Since the e_i (resp. e'_i) can be diagonalized simultaneously and the number of ones on the diagonal is given by $r_i d_i$, we may assume that $e_i = e'_i$ for each i. Then $Be_i \simeq M_{d_i}(F)$ and $B'e'_i = B'e_i \simeq M_{d_i}(F)$ are isomorphic simple subalgebras of the central simple algebra $e_i A e_i$. By the Skolem–Noether theorem there exists $a_i \in (e_i A e_i)^\times$ such that $a_i (Be_i) a_i^{-1} = B'e'_i$. Set $a = \sum_{i=1}^m a_i \in A^\times$. Then $aBa^{-1} = B'$, hence B and B' are conjugate. ∎

LEMMA 4.3: *Let A be a central simple algebra, B a separable subalgebra of A and φ an automorphism of B. Then φ is the restriction of an inner automorphism of A if and only if* $\deg \varphi(e) A \varphi(e) = \deg eAe$ *for all primitive central idempotents of B.*

Proof. The "only if" part is clear. Let us prove the "if" part. Let I denote the set of primitive central idempotents of B and assume $\deg \varphi(e) A \varphi(e) = \deg eAe$ for all $e \in I$. Write $A = \mathrm{End}_D(V)$ for a central division algebra D and a finite-dimensional D-right-module V. For $e \in I$ let V_e denote the eigenspace of e with eigenvalue 1, which is a D-submodule of V. Then $V = \bigoplus_{e \in I} V_e$ and $eAe \simeq \mathrm{End}_D(V_e)$ for $e \in I$. The isomorphism φ induces a permutation of I and $\mathrm{rdim}_D V_{\varphi(e)} = \deg \varphi(e) A \varphi(e) / \deg D = \deg eAe / \deg D = \mathrm{rdim}_D V_e$ for every $e \in I$. For each $e \in I$ choose a D-basis $v_j^{(e)}$, $j = 1, \ldots, \mathrm{rdim}_D V_e$ of V_e. Define $a \in A = \mathrm{End}_D(V)$ by $a v_j^{(e)} = v_j^{(\varphi(e))}$ for all $e \in I$ and all j. The element a is

invertible and $aea^{-1} = \varphi(e)$ for all $e \in I$. Then $\mathrm{Int}(a^{-1}) \circ \varphi$ preserves eAe for every e. Since Be is a simple subalgebra of the central simple subalgebra eAe we can choose $b_e \in (eAe)^\times$ such that $b_e x_e b_e^{-1} = a^{-1}\varphi(x_e)a$ for all $x_e \in Be$. Set $b = \sum_{e \in I} b_e$. Then $b \in A^\times$ and $\varphi = \mathrm{Int}(ab)$. This proves the claim. ∎

Definition 4.4: Let t be a multiset of the form $t = [(d_1, r_1), \ldots, (d_r, r_m)]$. We say that t is **well-behaved** if

$$\forall i, j \in \{1, \ldots, m\}\ (d_i = d_j \Rightarrow r_i = r_j).$$

We say that t is **constant** if $d_1 = d_2 = \cdots = d_m$ and $r_1 = r_2 = \cdots = r_m$. Clearly every constant t is well-behaved.

COROLLARY 4.5: *Let B be a separable subalgebra of a central simple F-algebra. Assume that t_B is well-behaved. Then the morphism*

$$N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B)) \to \mathbf{Aut}_F(B)$$

of group schemes over F, which takes $a \in G(R) \subseteq (A \otimes_F R)^\times$ to $\mathrm{Int}(a)\,|_{B_R}$ for every commutative F-algebra R, is surjective.

Proof. Since $\mathbf{Aut}_F(B)$ is smooth we may check surjectivity on F_{alg}-rational points. Hence the claim follows from Lemma 4.3. ∎

The functor $H^1(-, G)$ has the following interpretation:

LEMMA 4.6: *Let A be a central simple F-algebra, B a separable subalgebra of A, $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$ and L/F be a field extension.*

The set $H^1(L, G)$ stands in natural (in L/F) one-to-one correspondence with the set of conjugacy classes of separable L-subalgebras B' of A_L such that B' has the same type as B.

Moroever, if the type of B is well-behaved then we can replace "conjugacy classes" by "isomorphism classes" in the statement above.

Proof. By [KMRT98, §29.C] the set $H^1(L, \mathbf{Aut}_F(A, B))$ is in natural one-to-one correspondence with the set of F-isomorphism classes of pairs of L-algebras (A', B') such that $(A', B')_{\mathrm{sep}} \simeq (A_L, B_L)_{\mathrm{sep}}$.

We have an exact sequence $1 \to \mathbf{G}_m \to G \to \mathbf{Aut}_F(A, B) \to 1$. The map $H^1(L, G) \to H^1(L, \mathbf{Aut}_F(A, B))$ is injective, since $H^1(L, \mathbf{G}_m)$ is trivial and $\mathbf{G}_m$ lies in the center of G. Hence $H^1(L, G)$ is naturally (in L/F) bijective to the kernel of the connecting map $H^1(L, \mathbf{Aut}_F(A, B)) \to H^2(L, \mathbf{G}_m) = \mathrm{Br}(L)$,

which takes a pair (A', B') to the Brauer class of $A' \otimes_F A^{\mathrm{op}}$. Thus $H^1(L, G)$ is the set of isomorphism classes of pairs of L-algebras (A', B') such that $A' \simeq A_L$ and $(A', B')_{\mathrm{sep}} \simeq (A_L, B_L)_{\mathrm{sep}}$. Associate to a L-subalgebra B' of A_L of the same type as B the pair (A_L, B'). By Lemma 4.2 two such subalgebras B' and B'' have the same type if and only if $(A_L, B')_{\mathrm{sep}} \simeq (A_L, B'')_{\mathrm{sep}}$. Hence we get a (well-defined and in L/F natural) bijection between the set of conjugacy classes of L-subalgebras B' of A_L such that B' and B have the same type and the set $H^1(L, G)$.

Now assume that the type of B is well-behaved. We must prove that a separable subalgebra B' of A_L of type $t_{B'} = t_B$ isomorphic to B (as L-algebra) is already conjugate to B. Let C be the centralizer of B in A, which is another separable subalgebra of A. Then $\mathbf{GL}_1(C)$ is the centralizer of $\mathbf{GL}_1(B)$ in $\mathbf{GL}_1(A)$, hence the kernel of the surjective morphism $G \to \mathbf{Aut}_F(B)$ of group schemes over F from Corollary 4.5. Therefore, we see that the sequence $1 \to \mathbf{GL}_1(C) \to G \to \mathbf{Aut}_F(B) \to 1$ is exact. By Lemma 4.2, B and B' are conjugate over L_{sep}. The conjugacy class of B' viewed as element of $H^1(L, G)$ lies in the kernel of the map $H^1(L, G) \to H^1(L, \mathbf{Aut}_F(B))$, hence in the image of the map $H^1(L, \mathbf{GL}_1(C)) \to H^1(L, G)$. Since C is separable, Hilbert's Theorem 90 (see [KMRT98, Theorem 29.2]) implies that the pointed set $H^1(L, \mathbf{GL}_1(C))$ is trivial. Hence B and B' are conjugate. This concludes the proof. ∎

Remark 4.7: Let A be a central simple algebra, B a separable subalgebra of A and $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$. Lemma 4.6 shows that the functor $H^1(-, G)$ depends (up to isomorphism) only on the type $t_B = [(d_1, r_1), \ldots, (d_m, r_m)]$ of B (for fixed base field F). Moreover, replacing B by its centralizer in A, which is a separable subalgebra of type $[(r_1, d_1), \ldots, (r_m, d_m)]$, does neither change G nor its essential dimension.

Remark 4.8: Let A be a central simple algebra of degree n and let B be a separable subalgebra of constant type $t = [(d, r), \ldots, (d, r)]$ (where dr divides n). Assume that r is divisible by $d \operatorname{ind}(A)$. Then $H^1(-, G)$ is the functor that takes a field $L \in \mathrm{Fields}/F$ to the set of isomorphism classes of L-forms of B. In fact every L-form B' of B embeds in $\mathrm{End}_L(B') \simeq M_{nd/r}(L)$ with constant type, therefore in A_L with type t. In particular, this implies:

(a) If B is étale, $m = \dim B$, with n divisible by $m \operatorname{ind} A$ (this condition is vacuous if A is split), then $H^1(-, G)$ is isomorphic to the functor $\mathbf{Ét}_m$,

taking L/F to the set of isomorphism classes of m-dimensional étale L-algebras.

(b) If B is central simple, $d = \deg B$, with n divisible by $d^2 \operatorname{ind} A$, then $H^1(-, G)$ is isomorphic to the functor $\mathbf{CSA}_d$, taking a field $L \in \mathrm{Fields}/F$ to the set of isomorphism classes of central simple L-algebras of degree d.

LEMMA 4.9: *Let B be a separable subalgebra of a central simple algebra and let $[(d_1, r_1), \dots, (d_m, r_m)]$ be the type of B. Then $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$ has dimension equal to $\sum_{i=1}^m (r_i^2 + d_i^2 - 1)$.*

Proof. Consider the morphism of group schemes $G \to \mathbf{Aut}_F(Z(B))$, which takes $g \in G(R)$ to $\mathrm{Int}(g)\ |_{Z(B_R)}$ for every F-algebra R. Its kernel becomes isomorphic to $\prod_{i=1}^m (\mathbf{GL}_{d_i} \times \mathbf{GL}_{r_i})/\mathbf{G}_m$ over F_{sep}. Since $\mathbf{Aut}_F(Z(B))$ is finite the claim follows. ∎

For the computation of the essential dimension of $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$ we must assume that A is a division algebra. As noticed in Lemma 4.2 every separable subalgebra of A has constant type.

THEOREM 4.10: *Let p be a prime, a, b, n non-negative integers with $a + b \le n$, and let A be a division F-algebra of degree p^n. Let B be a separable subalgebra of A of type $[(p^a, p^b), \dots, (p^a, p^b)]$ (the multiset with p^{n-a-b} identical elements) and let $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$. Then*

$$\operatorname{ed} G = \operatorname{ed}_p G = \dim_F A - \dim G = p^{2n} - p^{n+a-b} - p^{n-a+b} + p^{n-a-b}.$$

Proof. The last equality follows from Lemma 4.9.

The image of $H^1(L, \mathbf{Aut}_F(A, B)) \to H^1(L, \mathbf{Aut}_F(A))$ consists of those isomorphism classes of central simple L-algebras that admit a separable subalgebra of type t_B. In view of Corollary 2.4 it suffices to show that the division F-algebra $A' = (a_1, b_1)_L \otimes_L \cdots \otimes_L (a_r, b_r)_L$ from Corollary 2.4 admits a separable subalgebra of type t_B. This follows from Lemma 4.2(c). ∎

In view of Lemma 4.6 the result of Theorem 4.10 has the following interpretation:

COROLLARY 4.11: *Let p, a, b, n and A be as in Theorem 4.10. Assume that A admits a subalgebra of type $t = [(p^a, p^b), \dots, (p^a, p^b)]$. Then the integer $e = p^{2n} - p^{n+a-b} - p^{n-a+b} + p^{n-a-b}$ is the smallest integer with the following*

property: For every field extension L/F and every separable subalgebra B' of A_L with $t_{B'} = t$ there exists a subextension L_0/F of L/F with $\operatorname{tdeg}_F L_0 \leq e$ and a separable subalgebra B'_0 of A_{L_0} with $(B'_0)_L$ conjugate to B.

Note that Theorem 4.10 covers the extreme case when A is a division algebra. In the final remark below we consider the other extreme, where A is split. As pointed out in the introduction, the latter case is surprisingly much harder with respect to computing $\operatorname{ed} G$ than the former.

REMARK 4.12: Let $n = p^r$ for some $r \geq 1$ and $A \simeq M_n(F)$ the split algebra. Let B be a separable subalgebra of A with $t_B = [(d, r), \dots, (d, r)]$ constant, where (d, r) appears $m := n/dr$ times. Note that d, r and m are powers of p. Let $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$. If $r < d$ we replace B by its centralizer in A without changing G. Therefore, we can reduce the computation of $\operatorname{ed} G$ and $\operatorname{ed}_p G$ to the case $d \mid r$, which we will assume in the sequel. By Remark 4.8, $H^1(-, G)$ is isomorphic to the functor $\mathrm{Fields}/F \to \mathrm{Sets}$, which takes a field extension L/F to the set of L-forms of B, i.e., separable L-algebras of dimension $\dim B$ and of constant rank whose center is an m-dimensional étale field extension of L.

(a) Case $d = 1$: Then $H^1(-, G) \simeq H^1(-, S_m)$ classifies m-dimensional étale algebras. The value $\operatorname{ed} G = \operatorname{ed} S_m$ is unknown for $m \geq 8$. In that case the best lower bound on $\operatorname{ed} S_m$ is currently $\lfloor \frac{m+1}{2} \rfloor$ in characteristic 0, $\lfloor \frac{m}{2} \rfloor$ in odd characteristic and $\lfloor \frac{m}{3} \rfloor$ in characteristic 2 [Du10, BR97, BF03]. The best upper bound on $\operatorname{ed} S_m$ is $m - 3$ (valid for $m \geq 5$, in arbitrary characteristic) [BF03, BR97].

However, the essential p-dimension of G is known in $\operatorname{char} F \neq p$, namely $\operatorname{ed}_p G = \operatorname{ed}_p S_m = \left\lfloor \frac{m}{p} \right\rfloor$. The second equality was established by J.-P. Serre; see [MR09, Corollary 4.2]. It is valid for arbitrary $m \in \mathbb{N}$.

(b) Case $m = 1$: Then $H^1(-, G) \simeq H^1(-, \mathbf{PGL}_d)$ classifies central simple algebras of degree d. The value of $\operatorname{ed} G$ is only known for $d = 2$ and $d = 3$, where $\operatorname{ed} G = 2$, and for $d = 4$ in $\operatorname{char} F \neq 2$, where $\operatorname{ed} G = 5$. The essential p-dimension of G is known for $d = p$, where $\operatorname{ed}_p G = 2$, for $d = p^2$ in $\operatorname{char} F \neq p$, where $\operatorname{ed}_p G = p^2 + 1$, and for $d = 2^3$ in $\operatorname{char} F \neq 2$, where $\operatorname{ed}_p G = 17$. Write $d = p^a$. The best lower bounds on $\operatorname{ed} G = \operatorname{ed} \mathbf{PGL}_{p^a}$ in the other cases with $\operatorname{char} F \neq p$ are due to recent results of A. Merkurjev [Me11]:

$$(a - 1)p^a + 1 \leq \operatorname{ed}_p G \leq \operatorname{ed} G.$$

The best upper bound on $\operatorname{ed}_p G = \operatorname{ed}_p \mathbf{PGL}_d$ is

$$\operatorname{ed}_p G \leq p^{2a-2} + 1$$

in $\operatorname{char} F \neq p$ [Ru11]. For $\operatorname{ed} G$, slightly weaker upper bounds have been established in [LRRS03, Le04, FF08]. For more information on the essential dimension and essential p-dimension of $\mathbf{PGL}_d$ we refer the reader to [ABGV11, §6].

(c) General case: The case where B is neither étale nor central simple has not been investigated in the literature. We would like to point out that

$$\operatorname{ed}(\underbrace{\mathbf{PGL}_d \times \cdots \times \mathbf{PGL}_d}_{m \text{ copies}}) \leq \operatorname{ed} G \leq m \cdot \operatorname{ed} \mathbf{PGL}_d \quad \text{for } d > 1.$$

This is proved as follows: We may assume that B is split as well, i.e., isomorphic to a direct product of m copies of $M_d(F)$ as an F-algebra. Let $T = \{(t, t^{-1}) \in \mathbf{G}_m^2\} \subseteq \mathbf{G}_m^2 = Z(\mathbf{GL}_d \times \mathbf{GL}_r)$. An easy computation reveals that $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$ is isomorphic to the semi-direct product

$$(\underbrace{(\mathbf{GL}_d \times \mathbf{GL}_r)/T \times \cdots \times (\mathbf{GL}_d \times \mathbf{GL}_r)/T}_{m \text{ copies}}) \rtimes S_m,$$

where the symmetric group S_m acts by permuting the m factors. Note that $H^1(-, (\mathbf{GL}_d \times \mathbf{GL}_r)/T)$ and $H^1(-, \mathbf{PGL}_d)$ are isomorphic. Hence

$$\operatorname{ed}(\mathbf{PGL}_d \times \cdots \times \mathbf{PGL}_d) = \operatorname{ed} G^0 \leq \operatorname{ed} G.$$

The inequality $\operatorname{ed} G \leq m \cdot \operatorname{ed}((\mathbf{GL}_d \times \mathbf{GL}_r)/T) = m \cdot \operatorname{ed} \mathbf{PGL}_d$ follows from Lemma 4.13 below.

LEMMA 4.13: *Let H be a group scheme with $\operatorname{ed} H > 0$. Then*

$$\operatorname{ed} H^m \rtimes S_m \leq m \operatorname{ed} H.$$

Proof. Let V be a generically free H-space. It is known that $\operatorname{ed} H$ coincides with the least value of $\dim X - \dim H$, where the minimum is taken over all generically free H-varieties admitting a dominant H-equivariant rational map $\varphi\colon V \dashrightarrow X$; see, e.g., [Lö10, Lemma 1.2]. Take such a H-variety X with $\operatorname{ed} H = \dim X - \dim H$. Let $G = H^m \rtimes S_m$. Then $V^{\oplus m}$ affords a natural G-space structure and X^m admits a natural G-variety structure. Since $\dim X > \dim H$ both G-actions are generically free. Moreover, $\varphi^m\colon V^{\oplus m} \dashrightarrow X^m$ is dominant

and G-equivariant. Hence $\operatorname{ed} G \leq \dim X^m - \dim G = m \cdot (\dim X - \dim H) = m \cdot \operatorname{ed} H$. ∎

Acknowledgments. I am grateful to Z. Reichstein for helpful comments. Moreover, I would like to thank the referee for his careful reading and for his valuable suggestions to improve the exposition of the paper.

References

[ABGV11] A. Auel, E. Brussel, S. Garibaldi and U. Vishne, *Open problems on central simple algebras*, Transformation Groups **16** (2011), 219–264.

[Ba10] S. Baek, *Essential dimension of simple algebras with involutions*, in *Linear Algebraic Groups and Related Structures* (preprint server) **401** (2010, Oct 9), 10 pages.

[Be05] G. Berhuy, *Erratum to: "On the set of discriminants of quadratic pairs" [JPAA* **188** *(2004) 33–44]*, Journal of Pure and Applied Algebra **195** (2005), 125–126.

[BF03] G. Berhuy and G. Favi, *Essential dimension: A functorial point of view (after A. Merkurjev)*, Documenta Mathematica **8** (2003), 279–330 (electronic).

[BM10] S. Baek and A. Merkurjev, *Essential dimension of central simple algebras*, Acta Mathematica, 2010, to appear.

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica **106** (1997), 159–179.

[BR05] G. Berhuy and Z. Reichstein, *On the notion of canonical dimension of algebraic groups*, Advances in Mathematics **198** (2005), 128–171.

[BRV08] P. Brosnan, Z. Reichstein and A. Vistoli, *Essential dimension of moduli of curves and other algebraic stacks*, Journal of the European Mathematical Society **13** (2011), 1079–1112. With an appendix by N. Fakhruddin.

[Du10] A. Duncan, *Essential dimensions of A_7 and S_7*, Mathematical Research Letters **17** (2010), 263–266.

[FF08] G. Favi and M. Florence, *Tori and essential dimension*, Journal of Algebra **319** (2008), 3885–3900.

[GR09] P. Gille and Z. Reichstein, *A lower bound on the essential dimension of a connected linear group*, Commentarii Mathematici Helvetici **84** (2009), 189–212.

[JW90] B. Jacob and A. Wadsworth, *Division algebras over Henselian fields*, Journal of Algebra **128** (1990), 126–179.

[Ka00] N. A. Karpenko, *On anisotropy of orthogonal involutions*, Journal of the Ramanujan Mathematical Society **15** (2000), 1–22.

[Ka09] N. A. Karpenko, *Incompressibility of quadratic Weil transfer of generalized Severi-Brauer varieties*, in *Linear Algebraic Groups and Related Structures* (preprint server) **362** (2009), 12 pp.

[KM08] N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite p-groups*, Inventiones Mathematicae **172** (2008), 491–508.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The Book of Involutions*, American Mathematical Society, Providence, RI, 1998, with a preface in French by J. Tits.

[Kr10] D. Krashen, *Zero cycles on homogeneous varieties*, Advances in Mathematics **223** (2010), 2022–2048.

[Le04] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transformation Groups **9** (2004), 337–379.

[Lö10] R. Lötscher, *Contributions to the essential dimension of finite and algebraic groups*, PhD thesis, University of Basel (2010), `http://edoc.unibas.ch/1147/`.

[LMMR10] R. Lötscher, M. MacDonald, A. Meyer and Z. Reichstein, *Essential dimension of algebraic tori*, in *Linear Algebraic Groups and Related Structures* (preprint server) **399** (2010, Aug 17), 12 pp.

[LRRS03] M. Lorenz, Z. Reichstein, L. H. Rowen and D. J. Saltman, *Fields of definition for division algebras*, Journal of the London Mathematical Society, Second Series **68** (2003), 651–670.

[Ma10] M. L. MacDonald, *Cohomological invariants of Jordan algebras with frames*, Journal of Algebra **323** (2010), 1665–1677.

[Me09] A. S. Merkurjev, *Essential dimension*, in *Quadratic Forms – Algebra, Arithmetic, and Geometry (R. Baeza, W.K. Chan, D. W. Hoffmann and R. Schulze-Pillot, eds.)*, Contemporary Mathematics **493**, 2009, pp. 299–326.

[Me10] A. S. Merkurjev, *Essential dimension of* $\mathbf{PGL}(p^2)$, Journal of the American Mathematical Society **23** (2010), 693–712.

[Me11] A. S. Merkurjev, *A lower bound on the essential dimension of simple algebras*, Algebra & Number Theory **4** (2010), 1055–1076.

[MR09] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra & Number Theory **3** (2009), 467–487.

[MR10] A. Meyer and Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, Journal of Algebra **329** (2011), 213–221. Special Issue celebrating the 60th birthday of Corrado De Concini.

[Re00] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformation Groups **5** (2000), 265–304.

[Ru11] A. Ruozzi, *Essential p-dimension of* $\mathbf{PGL}_n$, Journal of Algebra **328** (2011), 488–494.

[RY00] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, with an appendix by J. Kollár and E. Szabó, Canadian Journal of Mathematics **52** (2000), 1018–1056.

[Ti78] J.-P. Tignol, *Sur les classes de similitude de corps à involution de degrée* 8, Comptes Rendus Mathématique. Académie des Sciences. Paris **286** (1978), A875–A876.

[Wa79] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Springer, New York 1979.