ESSENTIAL DIMENSION OF CENTRAL SIMPLE ALGEBRAS

SANGHOON BAEK AND ALEXANDER S. MERKURJEV

ABSTRACT. Let p be a prime integer, $1 \leq s \leq r$ integers and F a field of characteristic different from p. We find upper and lower bounds for the essential p-dimension $\operatorname{ed}_p(\mathsf{Alg}_{p^r,p^s})$ of the class Alg_{p^r,p^s} of central simple algebras of degree p^r and exponent dividing p^s. In particular, we show that $\operatorname{ed}_2(\mathsf{Alg}_{8,2}) = 8$ and $\operatorname{ed}_p(\mathsf{Alg}_{p^2,p}) = p^2 + p$ for p odd.

1. Introduction

Let $\mathcal{F} : \mathsf{Fields}/F \to \mathsf{Sets}$ be a functor from the category Fields/F of field extensions over F to the category Sets of sets. Let $E \in \mathsf{Fields}/F$ and $K \subset E$ a subfield over F. An element $\alpha \in \mathcal{F}(E)$ is said to be *defined over* K (and K is called a *field of definition of* α) if there exists an element $\beta \in \mathcal{F}(K)$ such that α is the image of β under the map $\mathcal{F}(K) \to \mathcal{F}(E)$. The *essential dimension of* α, denoted $\operatorname{ed}^{\mathcal{F}}(\alpha)$, is the least transcendence degree $\operatorname{tr.deg}_F(K)$ over all fields of definition K of α. The *essential dimension of the functor* $\mathcal{F}$ is

$$\operatorname{ed}(\mathcal{F}) = \sup\{\operatorname{ed}^{\mathcal{F}}(\alpha)\},$$

where the supremum is taken over all fields $E \in \mathsf{Fields}/F$ and all $\alpha \in \mathcal{F}(E)$ (see [3, Def. 1.2] or [8, Sec.1]). Informally, the essential dimension of $\mathcal{F}$ is the smallest number of algebraically independent parameters required to define $\mathcal{F}$ and may be thought of as a measure of complexity of $\mathcal{F}$.

Let p be a prime integer. The *essential p-dimension of* α, denoted $\operatorname{ed}_p^{\mathcal{F}}(\alpha)$, is defined as the minimum of $\operatorname{ed}^{\mathcal{F}}(\alpha_{E'})$, where E' ranges over all field extensions of E of degree prime to p. The *essential p-dimension of* $\mathcal{F}$ is

$$\operatorname{ed}_p(\mathcal{F}) = \sup\{\operatorname{ed}_p^{\mathcal{F}}(\alpha)\},$$

where the supremum ranges over all fields $E \in \mathsf{Fields}/F$ and all $\alpha \in \mathcal{F}(E)$. By definition, $\operatorname{ed}(\mathcal{F}) \geq \operatorname{ed}_p(\mathcal{F})$ for all p.

For every integer $n \geq 1$, a divisor m of n and any field extension E/F, let $\mathsf{Alg}_{n,m}(E)$ denote the set of isomorphism classes of central simple E-algebras of degree n and exponent dividing m. Equivalently, $\mathsf{Alg}_{n,m}(E)$ is the subset of the m-torsion part $\operatorname{Br}_m(E)$ of the Brauer group of E consisting of all elements a such that $\operatorname{ind}(a)$ divides n. In particular, if $n = m$, then $\mathsf{Alg}_n(E) := \mathsf{Alg}_{n,n}(E)$

Key words and phrases. Essential dimension, Brauer group, algebraic tori *2000 Mathematical Subject Classifications: primary 16K50, secondary 14L30, 20G15* .

The work of the first author has been supported by the Beckenbach Dissertation Fellowship at the University of California at Los Angeles.

The work of the second author has been supported by the NSF grant DMS #0652316.

is the set of isomorphism classes of central simple E-algebras of degree n. We view $\mathsf{Alg}_{n,m}$ and Alg_n as functors $\mathsf{Fields}/F \to \mathsf{Sets}$.

In the present paper we give upper and lower bounds for $\operatorname{ed}_p(\mathsf{Alg}_{n,m})$ for a prime integer p. Let p^r (respectively, p^s) be the largest power of p dividing n (respectively, m). Then $\operatorname{ed}_p(\mathsf{Alg}_{n,m}) = \operatorname{ed}_p(\mathsf{Alg}_{p^r,p^s})$ and $\operatorname{ed}_p(\mathsf{Alg}_n) = \operatorname{ed}_p(\mathsf{Alg}_{p^r})$ (see Section 6). Thus, we may assume that n and m are the p-powers p^r and p^s respectively.

Using structure theorems on central simple algebras, we can compute the essential (p)-dimension of Alg_{p^r,p^s} for certain small values of r, s or p as follows. As every central simple algebra A of degree p is cyclic over a finite field extension of degree prime to p, A can be given by two parameters (see Section 2.1). In fact, $\operatorname{ed}_p(\mathsf{Alg}_p) = 2$ by [13, Lemma 8.5.7].

By Albert's theorem, every algebra in $\mathsf{Alg}_{4,2}$ is biquaternion and hence can be given by 4 parameters. In fact, $\operatorname{ed}(\mathsf{Alg}_{4,2}) = \operatorname{ed}_2(\mathsf{Alg}_{4,2}) = 4$ (see Remark 8.2).

The upper and lower bounds for $\operatorname{ed}_p(\mathsf{Alg}_{p^r})$ can be found in [12] and [10] respectively. In this paper (see Sections 6 and 7), we establish the following upper and lower bounds for $\operatorname{ed}_p(\mathsf{Alg}_{p^r,p^s})$:

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

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

Corollary. (cf. [9]) *Let p be a prime integer and F a field of characteristic different from p. Then*

$$\operatorname{ed}_p(\mathsf{Alg}_{p^2}) = p^2 + 1.$$

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

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

The corollary recovers a result in [21] that for p odd, there exists a central simple algebra of degree p^2 and exponent p which is not decomposable as a tensor product of two algebras of degree p. Indeed, if every central simple algebra of degree p^2 and exponent p is decomposable, then the essential p-dimension of $\mathsf{Alg}_{p^2,p}$ would be at most 4.

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

$$\operatorname{ed}_2(\mathsf{Alg}_{8,2}) = \operatorname{ed}(\mathsf{Alg}_{8,2}) = 8.$$

The proof is given in Section 8. The corollary recovers a result in [1] that there is a central simple algebra of degree 8 and exponent 2 which is not decomposable as a tensor product of three quaternion algebras. Indeed, if every central simple algebra of degree 8 and exponent 2 is decomposable, then the essential 2-dimension of $\mathsf{Alg}_{8,2}$ would be at most 6.

2. Character, Brauer group and algebraic tori

2.1. **Character and Brauer group.** Let F be a field, F_{sep} a separable closure of F, $\Gamma_F = \mathrm{Gal}(F_{\mathrm{sep}}/F)$. For a (discrete) Γ_F- module M, we write $H^n(F, M)$ for the Galois cohomology group $H^n(\Gamma_F, M)$.

If S is an algebraic group over F, we let $H^1(F, S)$ denote the set $H^1\big(\Gamma_F, S(F_{\mathrm{sep}})\big)$ (see [18]).

The *character group* of F is defined by

$$\mathrm{Ch}(F) := \mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, \mathbb{Q}/\mathbb{Z}) = H^1(F, \mathbb{Q}/\mathbb{Z}) \simeq H^2(F, \mathbb{Z}).$$

The *n-torsion character group* $\mathrm{Ch}_n(F)$ is identified with $H^1(F, \mathbb{Z}/n\mathbb{Z})$. For a character $\chi \in \mathrm{Ch}(F)$, set $F(\chi) = (F_{\mathrm{sep}})^{\mathrm{Ker}(\chi)}$. The field extension $F(\chi)/F$ is cyclic of degree $\mathrm{ord}(\chi)$. If $\Psi \subset \mathrm{Ch}(F)$ is a finite subgroup, we set

$$F(\Psi) := (F_{sep})^{\cap Ker(\chi)},$$

where the intersection is taken over all $\chi \in \Psi$. The Galois group $G = \mathrm{Gal}\big(F(\Psi)/F\big)$ is abelian and Ψ is canonically isomorphic to the character group $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ of G. Note that a character $\eta \in \mathrm{Ch}(F)$ is trivial over $F(\Psi)$ if and only if $\eta \in \Psi$.

We write $\mathrm{Br}(F)$ for the Brauer group $H^2(F, F_{\mathrm{sep}}^\times)$ of F. If L/F is a field extension and $\alpha \in \mathrm{Br}(F)$, we let α_L denote the image of α under the natural map $\mathrm{Br}(F) \to \mathrm{Br}(L)$. We say that L is a *splitting field* of α if $\alpha_L = 0$. The *index* $\mathrm{ind}(\alpha)$ of α is the smallest degree of a splitting field of α. The *exponent* $\exp(\alpha)$ is the order of α in $\mathrm{Br}(F)$. The integer $\exp(\alpha)$ divides $\mathrm{ind}(\alpha)$.

Let A be a central simple F-algebra. The *degree* of A in the square root of $\dim(A)$. We write $[A]$ for the class of A in $\mathrm{Br}(F)$. The index of $[A]$ divides $\deg(A)$. If $\alpha \in \mathrm{Br}(F)$ and n is a positive multiple of $\mathrm{ind}(\alpha)$, then there is a central simple F-algebra A of degree n with $[A] = \alpha$.

The cup-product

$$\mathrm{Ch}(F) \otimes F^\times = H^2(F, \mathbb{Z}) \otimes H^0(F, F_{\mathrm{sep}}^\times) \to H^2(F, F_{\mathrm{sep}}^\times) = \mathrm{Br}(F)$$

takes $\chi \otimes b$ to the class $\chi \cup (b)$ in $\mathrm{Br}(F)$ that is split by $F(\chi)$. A class $\alpha \in \mathrm{Br}(F)$ is called *n-cyclic* if $\alpha = \chi \cup (b)$ for a character χ with $n\chi = 0$. Such classes belong to $\mathrm{Br}_n(F)$. If n is prime to $\mathrm{char}(F)$, then $\mathrm{Br}_n(F) \simeq H^2(F, \mu_n)$, where μ_n is the Γ_F-module of all n-th roots of unity in F_{sep}.

Let n be prime to $\mathrm{char}(F)$ and suppose that F contains a primitive n-th root of unity ξ. For any $a \in F^\times$, let $\chi_a \in \mathrm{Ch}(F)$ be a unique character with values in $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ such that

$$\gamma(a^{1/n}) = \xi^{(n\chi_a(\gamma))} a^{1/n}$$

for all $\gamma \in \mathrm{Gal}(F_{\mathrm{sep}}/F)$. We write $(a, b)_n$ for $\chi_a \cup (b)$. The symbol $(a, b)_n$ satisfies the following properties (see [17, Chap. XIV, Prop.4]):

$(a, b)_n + (a', b)_n = (aa', b)_n$,
$(a, b)_n = -(b, a)_n$,
$(a, -a)_n = 0$.

For a finite subgroup $\Phi \subset \mathrm{Ch}(F)$ write $\mathrm{Br}\big(F(\Phi)/F\big)_{\mathrm{dec}}$ for the *subgroup of decomposable elements* in $\mathrm{Br}\big(F(\Phi)/F\big)$ generated by the elements $\chi \cup (a)$ for all $\chi \in \Phi$ and $a \in F^\times$. The *indecomposable relative Brauer group* $\mathrm{Br}\big(F(\Phi)/F\big)_{\mathrm{ind}}$ is the factor group $\mathrm{Br}\big(F(\Phi)/F\big)/\,\mathrm{Br}\big(F(\Phi)/F\big)_{\mathrm{dec}}$. Similarly, if $\Phi \subset \mathrm{Ch}_n(F)$ for some n, then $\mathrm{Br}_n(F(\Phi)/F)_{\mathrm{ind}}$ is the *indecomposable n-torsion relative Brauer group* defined as the factor group $\mathrm{Br}_n\big(F(\Phi)/F\big)/\,\mathrm{Br}\big(F(\Phi)/F\big)_{\mathrm{dec}}$.

Let E be a complete field with respect to a discrete valuation v and K its residue field. Let p be a prime integer different from $\mathrm{char}(K)$. There is a natural injective homomorphism $\mathrm{Ch}(K)\{p\} \to \mathrm{Ch}(E)\{p\}$ of the p-primary components of the character groups that identifies $\mathrm{Ch}(K)\{p\}$ with the character group of an unramified field extension of E. For a character $\chi \in \mathrm{Ch}(K)\{p\}$, we write $\widehat{\chi}$ for the corresponding character in $\mathrm{Ch}(E)\{p\}$.

By [4, §7.9], there is an exact sequence

$$0 \to \mathrm{Br}(K)\{p\} \xrightarrow{i} \mathrm{Br}(E)\{p\} \xrightarrow{\partial_v} \mathrm{Ch}(K)\{p\} \to 0.$$

If $\alpha \in \mathrm{Br}(K)\{p\}$, then we write $\widehat{\alpha}$ for the element $i(\alpha)$ in $\mathrm{Br}(E)\{p\}$. For example, if $\alpha = \chi \cup (\bar{u})$ for some $\chi \in \mathrm{Ch}(K)\{p\}$ and a unit $u \in E$, then $\widehat{\alpha} = \widehat{\chi} \cup (u)$. In the case F contains a primitive n-th root of unity, where n is a power of p, if $\alpha = (\bar{a}, \bar{b})_n$ with a and b units in E, then $\widehat{\alpha} = (a, b)_n$.

If $\beta = \widehat{\alpha} + \big(\widehat{\chi} \cup (x)\big)$ for an element $\alpha \in \mathrm{Br}(K)\{p\}$, $\chi \in \mathrm{Ch}(K)\{p\}$ and $x \in E^\times$ such that $v(x)$ is not divisible by p, we have (cf. [19, Prop. 2.4])

$$\mathrm{ind}(\beta) = \mathrm{ind}\big(\alpha_{K(\chi)}\big) \cdot \mathrm{ord}(\chi). \tag{1}$$

2.2. **Representations of algebraic tori.** Let T be an algebraic torus over a field F, L/F a finite Galois splitting field for T with Galois group G. The group G is called the *decomposition group* of T. The *character group* $T^* := \mathrm{Hom}_L(T_L, \mathbb{G}_{m,L})$ has the structure of a G-module. The torus T can be reconstructed from T^* by

$$T = \mathrm{Spec}\big(L[T^*]^G\big).$$

A torus P over F split by L is called *quasi-split* if P^* is a *permutation G-module*, i.e., if there exists a G-invariant $\mathbb{Z}$-basis X for P^*. The torus P is canonically isomorphic to the group of invertible elements of the étale F-algebra $A = \mathrm{Map}_G(X, L)$. The torus P acts linearly by multiplication on the vector space A over F making A a faithful P-space (a linear representation of P) of dimension $\dim(P)$. It follows that a homomorphism of algebraic tori $\nu : T \to P$ with P a quasi-split torus yields a linear representation of T of dimension $\dim(P)$ that is faithful if ν is injective.

Let P be a split torus over F, and P^* its character group. As above, the choice of a $\mathbb{Z}$-basis X for P^* allows us to identify P with the group of invertible elements of a split étale F-algebra A and make A a faithful P-space over F. Let $\nu : T \to P$ be a homomorphism of split tori over F. Suppose a finite group G acts on T and P by tori automorphisms so that ν is a G-equivariant homomorphism. Then the map $\nu^* : P^* \to T^*$ is a G-module homomorphism.

Suppose that there is a G-invariant $\mathbb{Z}$-basis X for P^*, i.e., P^* is permutation. Then G acts on the algebra A by F-algebra automorphisms. The torus T acts linearly on A via ν. It follows that the semidirect product $T \rtimes G$ acts linearly on A making A a $T \rtimes G$-space.

Let L be a Galois G-algebra over F (for example, L/F is a Galois field extension with Galois group G). Then $\gamma : \operatorname{Spec} L \to \operatorname{Spec} F$ is a G-torsor. Twisting the split torus T by the torsor γ, we get the torus

$$T_\gamma = (T \times \operatorname{Spec} L)/G = \operatorname{Spec}\bigl(L[T^*]^G\bigr)$$

that is split by L and T^*_γ is isomorphic to T^* as G-modules.

By [5, Prop. 28.11], the fiber of $H^1(F, T \rtimes G) \to H^1(F, G)$ over the class of γ is naturally bijective to the orbit set of the group $G_\gamma(F)$ in $H^1(F, T_\gamma)$, i.e.,

$$H^1(F, T \rtimes G) \simeq \coprod H^1(F, T_\gamma)/G_\gamma(F), \tag{2}$$

where the coproduct is taken over all $[\gamma] \in H^1(F, G)$.

2.3. **Generic torsors.** Let T be an algebraic torus split by a finite Galois field extension L/F with $G = \operatorname{Gal}(L/F)$. Let P be a quasi-split torus split by L and containing T as a subgroup. Set $S = P/T$. Then the canonical homomorphism $\gamma : P \to S$ is a T-torsor.

Proposition 2.1. *The T-torsor γ is generic, i.e., for every field extension K/F with K infinite, every T-torsor $\gamma' : E \to \operatorname{Spec} K$ and every nonempty open subset $W \subset S$, there is a morphism $s : \operatorname{Spec} K \to S$ over F with $\operatorname{Im}(s) \subset W$ such that the T-torsors γ' and $s^*(\gamma) = \gamma \times_S \operatorname{Spec} K$ over K are isomorphic.*

Proof. As P is quasi-split, the last term in the exact sequence

$$P(K) \xrightarrow{\gamma_K} S(K) \xrightarrow{\delta} H^1(K, T) \to H^1(K, P)$$

is trivial. Then there is $s \in S(K)$ with $\delta(s) = [\gamma']$. As K is infinite, the K-points of P are dense in P and we can modify s by an element in the image of γ_K so that $s \in W(K)$, i.e., $\operatorname{Im}(s) \subset W$. Then the T-torsor γ' over K with the class $\delta(s)$ satisfies the required property. □

2.4. **The algebraic tori P^Φ, S^Φ, T^Φ, U^Φ and V^Φ.** Let $1 \le s \le r$ be integers, p a prime integer, F a field with $\operatorname{char}(F) \ne p$, Φ a subgroup of $\operatorname{Ch}_p(F)$ of rank r and $L = F(\Phi)$. Let $G = \operatorname{Gal}(L/F)$. Choose a basis $\chi_1, \chi_2, \ldots, \chi_r$ for Φ. Each χ_i can be viewed as a character of G, i.e., as a homomorphism $\chi_i : G \to \mathbb{Q}/\mathbb{Z}$. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the dual basis for G, i.e.,

$$\chi_i(\sigma_j) = \begin{cases} (1/p) + \mathbb{Z}, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

Let R be the group ring $\mathbb{Z}[G]$. Consider the surjective G-modules homomorphism $\bar\varepsilon : R \to \mathbb{Z}/p^s\mathbb{Z}$, defined by $\bar\varepsilon(x) = \varepsilon(x) + p^s\mathbb{Z}$, where $\varepsilon : R \to \mathbb{Z}$ is the *augmentation homomorphism* given by $\varepsilon(\rho) = 1$ for all $\rho \in G$. Set $J := \operatorname{Ker}(\bar\varepsilon)$, thus, we have an exact sequence

$$0 \to J \to R \xrightarrow{\bar\varepsilon} \mathbb{Z}/p^s\mathbb{Z} \to 0.$$

Moreover, the G-module J is generated by I and p^s, where $I := \operatorname{Ker}(\varepsilon)$ is the *augmentation ideal* in R.

Consider the G-module homomorphism $h : R^{r+1} \to R$ taking the i-th canonical basis element e_i to $\sigma_i - 1$ for $1 \le i \le r$ and e_{r+1} to p^s. The image of h coincides with J.

Set $N := \operatorname{Ker}(h)$ and write $w_i = 1 + \sigma_i + \sigma_i^2 + \cdots + \sigma_i^{p-1} \in R$ for $1 \le i \le r$. Consider the following elements in N:

$$e_{ij} = (\sigma_i - 1)e_j - (\sigma_j - 1)e_i, \quad f_i = w_i e_i, \quad \text{and} \quad g_i = -p^s e_i + (\sigma_i - 1)e_{r+1}$$

for all $1 \le i, j \le r$.

Lemma 2.2. *The G-module N is generated by e_{ij}, f_i and g_i.*

Proof. Consider the surjective morphism $k : R^r \to I$ taking e_i to $\sigma_i - 1$ and set $N' := \operatorname{Ker}(k)$. Then we have the following commutative diagram

$$\begin{array}{ccccc}
N' & \hookrightarrow & R^r & \xrightarrow{k} & I \\
\downarrow & & \downarrow & & \downarrow \\
N & \hookrightarrow & R^{r+1} & \xrightarrow{h} & J \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle \varepsilon'} \\
I & \hookrightarrow & R & \xrightarrow{\varepsilon} & \mathbb{Z}
\end{array}$$

where $R^{r+1} \to R$ is the projection morphism to the last coordinate and $\varepsilon' : J \to \mathbb{Z}$ is given by $\varepsilon'(j) = \varepsilon(j)/p^s$.

By the exactness of the first column of the diagram, N is generated by N' and the liftings g_i of $\sigma_i - 1$ in N. The module N' is generated by e_{ij} and f_i by [10, Lemma 3.5]. This completes the proof. □

Let $\varepsilon_i : R^{r+1} \to \mathbb{Z}$ be the i-th projection followed by the augmentation map ε. It follows from Lemma 2.2 that $\varepsilon_i(N) = p\mathbb{Z}$ for every $i = 1, \dots, r$. Moreover, the G-homomorphism

$$q : N \to \mathbb{Z}^r, \quad x \mapsto \big(\varepsilon_1(x)/p, \dots, \varepsilon_r(x)/p\big)$$

is surjective. Set $M := \operatorname{Ker}(q)$ and $Q := R^{r+1}/M$.

Let P^Φ, S^Φ, T^Φ, U^Φ and V^Φ be the algebraic tori over F with the character G-modules R^{r+1}, Q, M, J and N, respectively. The diagram of homomorphisms of G-modules with the exact columns and rows

$$\begin{array}{ccccc}
M & = & M & & \\
\downarrow & & \downarrow & & \\
N & \hookrightarrow & R^{r+1} & \xrightarrow{h} & J \\
{\scriptstyle q}\downarrow & & \downarrow & & \| \\
\mathbb{Z}^r & \hookrightarrow & Q & \longrightarrow & J
\end{array} \tag{3}$$

yields the following diagram of homomorphisms of the tori

$$\begin{array}{ccccc} T^{\Phi} & = & T^{\Phi} & & \\ \uparrow & & \uparrow & & \\ V^{\Phi} & \overset{\gamma}{\twoheadleftarrow} & P^{\Phi} & \hookleftarrow & U^{\Phi} \\ \uparrow & & \uparrow & & \| \\ \mathbb{G}_m^r & \twoheadleftarrow & S^{\Phi} & \hookleftarrow & U^{\Phi} \end{array} \tag{4}$$

Let K/F be a field extension and set $KL := K \otimes_F L$. The commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & R & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & J & \longrightarrow & R & \longrightarrow & \mathbb{Z}/p^s\mathbb{Z} & \longrightarrow & 0 \end{array}$$

induces the commutative diagram of homomorphisms of algebraic groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_{p^s} & \longrightarrow & R_{L/F}(\mathbb{G}_{m,L}) & \longrightarrow & U^{\Phi} & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & R_{L/F}(\mathbb{G}_{m,L}) & \longrightarrow & U'^{\Phi} & \longrightarrow & 1 \end{array} \tag{5}$$

and then the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(K, U^{\Phi}) & \longrightarrow & H^2(K, \mu_{p^s}) & \longrightarrow & H^2(KL, \mathbb{G}_m) \\ & & \downarrow & & \downarrow & & \| \\ 0 & \longrightarrow & H^1(K, U'^{\Phi}) & \longrightarrow & H^2(K, \mathbb{G}_m) & \longrightarrow & H^2(KL, \mathbb{G}_m). \end{array} \tag{6}$$

Hence

$$H^1(K, U^{\Phi}) \simeq \mathrm{Br}_{p^s}(KL/K) \quad \text{and} \quad H^1(K, U'^{\Phi}) \simeq \mathrm{Br}(KL/K). \tag{7}$$

Lemma 2.3. *The map $H^1(K, U^{\Phi}) \to H^1(K, S^{\Phi})$ induces an isomorphism $H^1(K, S^{\Phi}) \simeq \mathrm{Br}_{p^s}(KL/K)_{\mathrm{ind}}$.*

Proof. Consider the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U^{\Phi} & \longrightarrow & S^{\Phi} & \longrightarrow & \mathbb{G}_m^r & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & U'^{\Phi} & \longrightarrow & S'^{\Phi} & \longrightarrow & \mathbb{G}_m^r & \longrightarrow & 1, \end{array}$$

where the bottom row is induced by the bottom row of the diagram (4) in [10]. This yields a commutative diagram

$$\begin{array}{ccccccc} (K^{\times})^r & \longrightarrow & H^1(K, U^{\Phi}) & \longrightarrow & H^1(K, S^{\Phi}) & \longrightarrow & 0 \\ \| & & \downarrow & & \downarrow & & \\ (K^{\times})^r & \overset{\lambda}{\longrightarrow} & H^1(K, U'^{\Phi}) & \longrightarrow & H^1(K, S'^{\Phi}) & \longrightarrow & 0 \end{array}$$

with the exact rows. The homomorphism λ takes $(x_1,\dots,x_r)$ to $\sum_{i=1}^r\big((\chi_i)_K\cup (x_i)\big)$ by [10, Lemma 3.6], whence the result. $\square$

3. Essential dimension of algebraic tori

Let S be an algebraic group over F. The *essential dimension* $\operatorname{ed}(S)$ (respectively, *essential p-dimension* $\operatorname{ed}_p(S)$) of S is defined to be the essential (p-)dimension of the functor taking a field extension K/F to the set of isomorphism classes $S\text{-}\mathit{torsors}(K)$ of S-torsors over K. Note that the functor $S\text{-}\mathit{torsors}$ is isomorphic to the functor taking K to the set $H^1(K,S)$.

Let S be an algebraic torus over F split by L with $G=\operatorname{Gal}(L/F)$. We assume that G is a group of order p^r, where p is a prime integer and $r\geq 2$. Let X be the G-module of characters of S. Define the group $\overline{X}:=X/(pX+IX)$, where I is the augmentation ideal in $R=\mathbb{Z}[G]$. For any subgroup $H\subset G$, consider the composition $X^H\hookrightarrow X\to\overline{X}$. For every k, let V_k denote the subgroup generated by images of the homomorphisms $X^H\to\overline{X}$ over all subgroups H with $[G:H]\leq p^k$. We have the sequence of subgroups

$$0=V_{-1}\subset V_0\subset\cdots\subset V_r=\overline{X}.$$

A *p-presentation* of X is a G-homomorphism $P\to X$ with P a permutation G-module and finite cokernel of order prime to p. A p-presentation with the smallest $\operatorname{rank}(P)$ is called *minimal*. The essential p-dimension of algebraic tori was determined in [7, Th. 1.4] in terms of a minimal p-presentation $P\to X$:

$$\operatorname{ed}_p(S)=\operatorname{rank}(P)-\dim(S). \tag{8}$$

We have the following explicit formula for the essential (p-)dimension of S (cf. [10, Th. 4.3]):

Theorem 3.1. *Let S be a torus over a field F and p a prime integer different from* $\operatorname{char}(F)$. *If the decomposition group G of S is a p-group, then*

$$\operatorname{ed}(S)=\operatorname{ed}_p(S)=\sum_{k=0}^{r}(\operatorname{rank}V_k-\operatorname{rank}V_{k-1})p^k-\dim(S).$$

Proof. The second equality was proven in [10, Th. 4.3]. Let $\nu:P\to X$ be a minimal p-presentation. By definition, the index $[X:\operatorname{Im}(\nu)]$ is prime to p. Let T and U be algebraic groups of multiplicative type split by L with the character G-modules $\operatorname{Im}(\nu)$ and $X/\operatorname{Im}(\nu)$, respectively, hence we have an exact sequence

$$1\to U\to S\to T\to 1.$$

Let K/F be a field extension. By assumption, the group $U(KL)=\operatorname{Hom}(X/\operatorname{Im}(\nu),KL^\times)$ has order prime to p. We have an exact sequence

$$H^1\big(G,U(KL)\big)\to H^1\big(G,S(KL)\big)\to H^1\big(G,T(KL)\big)\to H^2\big(G,U(KL)\big).$$

As the order of $U(KL)$ is prime to p and G is a p-group, the groups $H^i\big(G,U(KL)\big)$ are trivial for $i\geq 1$, hence the homomorphism $S\to T$ induces an isomorphism of functors S-*torsors* $\xrightarrow{\sim}$ T-*torsors*. It follows that $\mathrm{ed}(S) = \mathrm{ed}(T)$. The surjection $P \to \mathrm{Im}(\nu)$ yields a generically free representation of T by [11, Lemma 3.3]. Hence, by [3, Prop. 4.11] and (8), we have

$$\mathrm{ed}_p(S) \le \mathrm{ed}(S) = \mathrm{ed}(T) \le \mathrm{rank}(P) - \dim(T) = \mathrm{rank}(P) - \dim(S) = \mathrm{ed}_p(S),$$

therefore, $\mathrm{ed}(S) = \mathrm{ed}_p(S)$. □

Let F be a field, Φ a subgroup of $\mathrm{Ch}_p(F)$ of rank $r \ge 2$, $L = F(\Phi)$ and $G = \mathrm{Gal}(L/F)$. In this section we compute the essential (p-)dimension of the algebraic tori U^Φ and S^Φ defined by (4). For any subgroup H of G, we write $n_H := \sum_{\tau \in H} \tau$ in $R = \mathbb{Z}[G]$. An element $x \in R$ is *decomposable* if $x = yz$ with $y, z \in R$, and $\varepsilon(y), \varepsilon(z) \in p\mathbb{Z}$.

Lemma 3.2. *Let $H \subset G$ be a nontrivial subgroup and $x \in R$ such that $\varepsilon(n_H x) \in p^2\mathbb{Z}$. Then $n_H x$ is decomposable.*

Proof. If $|H| = p$, then $\varepsilon(x) \in p\mathbb{Z}$ and hence $n_H x$ is decomposable. Otherwise $H = H' \times H''$ for nontrivial subgroups H' and H''. As $n_H = n_{H'} \cdot n_{H''}$, the element n_H and therefore, $n_H x$ is decomposable. □

Lemma 3.3. *If $x \in R$ is decomposable, then $x \equiv \varepsilon(x)$ modulo $pI + I^2$.*

Proof. Let $y = \varepsilon(y) + u$ and $z = \varepsilon(z) + v$ for some $u, v \in I$. Then we have $yz - \varepsilon(yz) = \big(\varepsilon(y)v + \varepsilon(z)u\big) + uv \in pI + I^2$. □

Lemma 3.4. *The group V_k is generated by*

1. *the elements $\overline{n_H x}$ such that $|H| \ge p^{r-k}$ and $\varepsilon(n_H x) \in p^s\mathbb{Z}$ if $r - k < s$,*
2. *the elements $\overline{n}_H$ such that $|H| \ge p^{r-k}$ if $r - k \ge s$.*

Proof. The statement follows from the equality $J^H = R^H \cap J = n_H R \cap J$. □

Lemma 3.5. *If $k < r - s$, then $V_k = 0$.*

Proof. By Lemma 3.4(2), V_k is generated by $\overline{n}_H$ with $|H| \ge p^{r-k}$. As n_H is decomposable and $|H| > p^s$, in view of Lemma 3.3, we have $\overline{n}_H = \overline{\varepsilon(n_H)} = \overline{|H|} = 0$ as $|H| \in pJ$. □

Lemma 3.6. *If $s \ge 2$ and $r - s \le k \le r - 1$, then* $\dim(V_k) = 1$.

Proof. By Lemma 3.4, V_k is generated by $\overline{n_H x}$ with H nontrivial and $\varepsilon(n_H x) \in p^s\mathbb{Z}$. As $s \ge 2$, the element $n_H x$ is decomposable by Lemma 3.2. In view of Lemma 3.3, $\overline{n_H x} = \overline{\varepsilon(n_H x)}$, hence V_k is generated by $\overline{p^s}$. □

Lemma 3.7. *If $s = 1$ and p is odd, then* $\dim(V_{r-1}) = 1$.

Proof. We claim that V_{r-1} is generated by $\overline{p}$. By Lemma 3.4(2), V_{r-1} is generated by $\overline{n}_H$ with $|H| \ge p$. If $|H| \ge p^2$, then by Lemma 3.2, $\overline{n}_H$ is decomposable and in view of Lemma 3.3, $\overline{n}_H = \overline{\varepsilon(n_H)} = 0$.

Suppose $|H| = p$ and let $\sigma \in H$ be a generator. We have $n_H - p = (\sigma - 1)m$, where $m = \sum_{i=0}^{p-2} (p - 1 - i)\sigma^i$, so $\varepsilon(m) = p(p-1)/2$. As p is odd, $\varepsilon(m) \in p\mathbb{Z}$. Hence, $m \in pR + I$, therefore, $n_H - p \in pI + I^2$ and $\overline{n}_H = \overline{p}$ in $\overline{J}$. □

Lemma 3.8. *If $s = 1$ and $p = 2$, then $V_{r-1} = \overline{J}$.*

Proof. By Lemma 3.4(2), V_{r-1} is generated by $\overline{n}_H$ with $|H| \geq 2$. Take non-trivial elements $\sigma \neq \tau$ in G. Then $\overline{2} = \overline{(1+\sigma\tau)} - \sigma\overline{(1+\tau)} + \overline{(1+\sigma)} \in V_{r-1}$. Also, for any $\sigma \in G$, $\overline{\sigma - 1} = \overline{1+\sigma} - \overline{2} \in V_{r-1}$. The group $\overline{J}$ is generated by $\overline{2}$ and $\overline{\sigma - 1}$ over all $\sigma \in G$. □

Proposition 3.9. *We have*

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

Proof. Note that $V_r = \overline{J}$, $\mathrm{rank}(\overline{J}) = \mathrm{rank}(V_r) = r + 1$ and $\dim(U^\Phi) = p^r$.

Case 1: p is odd or $p = 2$ and $s \geq 2$. By Lemmas 3.5, 3.6 and 3.7, we have

$$\mathrm{rank}\, V_k = \begin{cases} r+1 & \text{if } k = r, \\ 1 & \text{if } r - s \leq k < r, \\ 0 & \text{if } 0 \leq k < r - s. \end{cases}$$

Since the decomposition group G of U^Φ is a p-group, by Theorem 3.1,

$$\mathrm{ed}(U^\Phi) = \mathrm{ed}_p(U^\Phi) = rp^r + p^{r-s} - \dim(U^\Phi) = rp^r + p^{r-s} - p^r = (r-1)p^r + p^{r-s}.$$

Case 2: $p = 2$ and $s = 1$. By Lemmas 3.5 and 3.8, we have

$$\mathrm{rank}\, V_k = \begin{cases} r+1 & \text{if } k = r-1 \text{ or } k = r, \\ 0 & \text{if } 0 \leq k \leq r - 2. \end{cases}$$

Again by Theorem 3.1,

$$\mathrm{ed}(U^\Phi) = \mathrm{ed}_2(U^\Phi) = (r+1)2^{r-1} - \dim(U^\Phi) = (r-1)2^{r-1}.$$ □

Remark 3.10. One can construct a surjective minimal p-presentation $\nu : P' \to J$ as follows.

Case 1: p is odd or $p = 2$ and $s \geq 2$. Let H be a subgroup of G of order p^s and $P' := R^r \oplus \mathbb{Z}[G/H]$. We define ν by

$$\nu(x_1, \ldots, x_n, y) = \sum_{i=1}^{r} (\sigma_i - 1)x_i + n_H y.$$

The image of ν contains I and n_H. As $n_H \equiv p^s$ modulo I, we have $p^s \in \mathrm{Im}(\nu)$, hence ν is surjective. Note that $e_{ij} = (\sigma_i - 1)e_j - (\sigma_j - 1)e_i \in \mathrm{Ker}(\nu)$. As $\sigma_i e_{ij} \neq e_{ij}$ for every $j \neq i$, the group G acts faithfully on $\mathrm{Ker}(\nu)$.

Case 2: $p = 2$ and $s = 1$. Let H_i be the subgroup of G generated by σ_i and $H = \langle \sigma_1\sigma_2 \rangle$. Set $P' = \coprod_{i=1}^{r} \mathbb{Z}[G/H_i] \oplus \mathbb{Z}[G/H]$. We define ν by

$$\nu(x_1, \ldots, x_n, y) = \sum_{i=1}^{r} (\sigma_i + 1)x_i + (\sigma_1\sigma_2 + 1)y.$$

The image of ν contains $\sigma_i + 1$ and $2 = (\sigma_1\sigma_2 + 1) - \sigma_1(\sigma_2 + 1) + (\sigma_1 + 1)$, hence ν is surjective. Note that $h_{ij} := (\sigma_i + 1)e_j - (\sigma_j + 1)e_i \in \mathrm{Ker}(\nu)$. As $\sigma_k h_{ij} \neq h_{ij}$

for distinct i, j and k, the group G acts faithfully on $\mathrm{Ker}(\nu)$ if $r \geq 3$. In fact, G acts trivially on $\mathrm{Ker}(\nu)$ if $r = 2$.

Corollary 3.11. *We have*

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

Proof. By (8) and Proposition 3.9, there is a minimal p-presentation $\nu : P \to J$ such that

$$\mathrm{rank}(P) = \begin{cases} (r+1)2^{r-1} & \text{if } p = 2 \text{ and } s = 1, \\ rp^r + p^{r-s} & \text{otherwise.} \end{cases} \tag{9}$$

The exact sequence

$$0 \to \mathbb{Z}^r \to Q \to J \to 0$$

in the bottom row of (3) yields an exact sequence

$$\mathrm{Hom}_G(P, Q) \to \mathrm{Hom}_G(P, J) \to \mathrm{Ext}^1_G(P, \mathbb{Z}^r).$$

As P and $\mathbb{Z}^r$ are permutation G-modules, $\mathrm{Ext}^1_G(P, \mathbb{Z}^r) = 0$, hence the homomorphism ν factors through a morphism $\nu' : P \to Q$.

Recall that we write $\overline{X} = X/(pX + IX)$ for a G-module X. As $\overline{\mathbb{Z}^r} \simeq (\mathbb{Z}/p\mathbb{Z})^r \to \overline{Q}$ is zero map, the natural homomorphism $\overline{Q} \to \overline{J}$ is an isomorphism, hence ν' is a minimal p-presentation of Q. Note that G is the decomposition group of S^Φ and $\dim(S^\Phi) = p^r + r$. By Theorem 3.1, $\mathrm{ed}(S^\Phi) = \mathrm{ed}_p(S^\Phi) = \mathrm{rank}(P) - \dim(S^\Phi)$, hence the result follows by (9). □

4. Degeneration

In this section we relate the essential p-dimensions of Alg_{p^r,p^s} and of the torus S^Φ by means of the iterated degeneration (Proposition 4.1). The latter is a method of comparison of the essential p-dimension of an object (a central simple algebra in our case) over a complete discrete valued field and of its specialization over the residue field.

4.1. **A simple degeneration.** Let F be a field, p a prime integer different from $\mathrm{char}(F)$ and $\Phi \subset \mathrm{Ch}_p(F)$ a finite subgroup. For integers $k \geq 0$, $s \geq 1$ and a field extension K/F, let

$$\mathcal{B}^\Phi_{k,s}(K) = \{\alpha \in \mathrm{Br}(K)\{p\} \quad | \quad \mathrm{ind}(\alpha_{K(\Phi)}) \leq p^k, \exp(\alpha) \leq p^s\}. \tag{10}$$

We say that two elements α and α' in $\mathcal{B}^\Phi_{k,s}(K)$ are *equivalent* if $\alpha - \alpha' \in \mathrm{Br}\big(K(\Phi)/K\big)_{\mathrm{dec}}$. Write $\widetilde{\mathcal{B}}^\Phi_{k,s}(K)$ for the set of equivalence classes in $\mathcal{B}^\Phi_{k,s}(K)$. To simplify notation, we shall write α for the equivalence class of an element $\alpha \in \mathcal{B}^\Phi_{k,s}(K)$ in $\widetilde{\mathcal{B}}^\Phi_{k,s}(K)$. We view $\mathcal{B}^\Phi_{k,s}$ and $\widetilde{\mathcal{B}}^\Phi_{k,s}$ as functors from Fields/F to Sets.

In particular, if $k=0$, then $\mathcal{B}^{\Phi}_{0,s}(K)$ and $\widetilde{\mathcal{B}}^{\Phi}_{0,s}(K)$ are bijective to $\mathrm{Br}_{p^s}(K(\Phi)/K)$ and $\mathrm{Br}_{p^s}(K(\Phi)/K)_{\mathrm{ind}}$, respectively. Hence, by (7) and Lemma 2.3,

$$\mathcal{B}^{\Phi}_{0,s} \simeq U^{\Phi}\text{-}\mathit{torsors} \quad \text{and} \quad \widetilde{\mathcal{B}}^{\Phi}_{0,s} \simeq S^{\Phi}\text{-}\mathit{torsors}\,. \tag{11}$$

Moreover, if $\Phi = 0$, then

$$\mathcal{B}^{\Phi}_{k,s} = \widetilde{\mathcal{B}}^{\Phi}_{k,s} \simeq \mathit{Alg}_{p^k,p^s}. \tag{12}$$

Let $\Phi' \subset \Phi$ be a subgroup of index p and $\eta \in \Phi \setminus \Phi'$, hence $\Phi = \langle \Phi', \eta\rangle$. Let E/F be a field extension such that $\eta_E \notin \Phi'_E$ in $\mathrm{Ch}(E)$. Choose an element $a \in \mathcal{B}^{\Phi}_{k,s}(E)$, i.e., $\alpha \in \mathrm{Br}(E)\{p\}$ such that $\mathrm{ind}(\alpha_{E(\Phi)}) \le p^k$ and $\exp(\alpha) \le p^s$.

Let E' be a field extension of F that is complete with respect to a discrete valuation v' over F with residue field E and set

$$\alpha' := \widehat{\alpha} + \big(\widehat{\eta}_E \cup (x)\big) \in \mathrm{Br}(E'), \tag{13}$$

for some $x \in E'^{\times}$ such that $v'(x)$ is prime to p. As $\eta_{E(\Phi')} \neq 0$, it follows from (1) that

$$\mathrm{ind}(\alpha'_{E'(\Phi')}) = p \cdot \mathrm{ind}(\alpha_{E(\Phi)}) \le p^{k+1} \quad \text{and} \quad \exp(\alpha') = \mathrm{lcm}\big(\exp(\alpha), p\big) \le p^s,$$

hence $\alpha' \in \mathcal{B}^{\Phi'}_{k+1,s}(E')$.

In the case the condition $\exp(\alpha) \le p^s$ in (10) is dropped, the following proposition was proved in [10, Prop. 5.2]:

Proposition 4.1. *Suppose that for any finite field extension N/E of degree prime to p and any character $\rho \in \mathrm{Ch}(N)$ of order p^2 such that $p\rho \in \Phi_N \setminus \Phi'_N$, we have $\mathrm{ind}\big(\alpha_{N(\Phi',\rho)}\big) \ge p^k$. Then*

$$\mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi'}_{k+1,s}}(\alpha') \ge \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi}_{k,s}}(\alpha) + 1.$$

Proof. The proof of [10, Prop. 5.2] still works with the following modification.

Let M/E' be a finite field extension of degree prime to p, $M_0 \subset M$ a subfield over F and $\alpha'_0 \in \mathcal{B}^{\Phi'}_{k+1,s}(M_0)$ such that $(\alpha'_0)_M = \alpha'_M$ in $\widetilde{\mathcal{B}}^{\Phi'}_{k+1,s}$ and $\mathrm{tr.deg}_F(M_0) = \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi'}_{k+1,s}}(\alpha')$. We extend the discrete valuation v' on E' to a (unique) discrete valuation v on M and let N be its residue field. Let n_0 be the residue field of the restriction of v on M_0. It was shown in the proof of [10, Prop. 5.2] that there exist $\alpha_0 \in \mathrm{Br}(N_0)\{p\}$ with $\mathrm{ind}(\alpha_0)_{N_0(\Phi)} \le p^k$, a prime element π_0 in M_0, and $\eta_0 \in \mathrm{Ch}_p(N_0)$ such that

$$(\alpha'_0)_{\widehat{M}_0} = \widehat{\alpha}_0 + \big(\widehat{\eta}_0 \cup (\pi_0)\big) \text{ in } \mathrm{Br}(\widehat{M}_0) \tag{14}$$

and

$$\alpha_N - (\alpha_0)_N \in \mathrm{Br}\big(N(\Phi)/N\big)_{\mathrm{dec}}. \tag{15}$$

By (14), we have

$$\exp(\alpha_0) = \exp(\widehat{\alpha}_0) \le \mathrm{lcm}\big(\exp(\alpha'_0)_{\widehat{M}_0}, p\big) \le \mathrm{lcm}\big(\exp(\alpha'_0), p\big) \le p^s,$$

hence $\alpha_0 \in \mathcal{B}^{\Phi}_{k,s}(N_0)$. Therefore, the class of α_N in $\widetilde{\mathcal{B}}^{\Phi}_{k,s}(N)$ is defined over N_0 by (15). It follows that

$$\mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi'}_{k+1,s}}(\alpha') = \mathrm{tr.deg}_F(M_0) \geq \mathrm{tr.deg}_F(N_0) + 1 \geq \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi}_{k,s}}(\alpha) + 1. \qquad \square$$

4.2. **A technical lemma.** In this subsection we prove Lemma 4.2 that will allow us to apply Proposition 4.1.

Until the end of this subsection we assume that the base field F contains a primitive p^2-th root of unity.

Let $\chi_1, \chi_2, \dots, \chi_r$ with $r \geq 2$ be linearly independent characters in $\mathrm{Ch}_p(F)$ and $\Phi = \langle \chi_1, \chi_2, \dots, \chi_r \rangle$. Let E/F be a field extension such that $\mathrm{rank}(\Phi_E) = r$ and let $\alpha \in \mathrm{Br}(E)\{p\}$ be an element that is split by $E(\Phi)$ and $\exp(\alpha) \leq p^s$.

Let $E_0 = E$, $E_1, \dots, E_r$ be field extensions of F such that for any $k = 1, 2, \dots, r$, the field E_k is complete with respect to a discrete valuation v_k over F and E_{k-1} is its residue field. For any $k = 1, 2, \dots, r$, choose elements $x_k \in E_k^\times$ such that $v_k(x_k)$ is prime to p and define the elements $\alpha_k \in \mathrm{Br}(E_k)\{p\}$ inductively by $\alpha_0 := \alpha$ and

$$\alpha_k := \widehat{\alpha_{k-1}} + \big(\widehat{(\chi_k)}_{E_{k-1}} \cup (x_k)\big).$$

Let Φ_k be the subgroup of Φ generated by $\chi_{k+1}, \dots, \chi_r$. Thus, $\Phi_0 = \Phi$, $\Phi_r = 0$ and $\mathrm{rank}(\Phi_k) = r - k$. Note that the character $(\chi_k)_{E_{k-1}(\Phi_k)}$ is not trivial. It follows from (1) that

$$\mathrm{ind}(\alpha_k)_{E_k(\Phi_k)} = p \cdot \mathrm{ind}(\alpha_{k-1})_{E_{k-1}(\Phi_{k-1})}$$

for any $k = 1, \dots, r$. As $\mathrm{ind}\, \alpha_{E(\Phi)} = 1$, we have $\mathrm{ind}(\alpha_k)_{E_k(\Phi_k)} = p^k$ for all $k = 0, 1, \dots, r$. Moreover, as $\exp(\alpha) \leq p^s$, we have $\exp(\alpha_k) = \mathrm{lcm}(\exp(\alpha_{k-1}), p) \leq p^s$. Therefore, $\alpha_k \in \mathcal{B}^{\Phi_k}_{k,s}(E_k)$.

The followings lemma assures that under a certain restriction on the element α, the conditions of Proposition 4.1 are satisfied for the fields E_k, the groups of characters Φ_k and the elements α_k. This lemma is similar to [10, Lemma 5.4].

Lemma 4.2. *Suppose that for any subgroup $\Psi \subset \Phi$ with $[\Phi : \Psi] = p^2$ and any field extension $L/E(\Psi)$ of degree prime to p, the element α_L is not p^2-cyclic . Then for every $k = 0, 1, \dots, r-1$, and any finite field extension N/E_k of degree prime to p and any character $\rho \in \mathrm{Ch}(N)$ of order p^2 such that $p\rho \in (\Phi_k)_N \setminus (\Phi_{k+1})_N$, we have*

$$\mathrm{ind}(\alpha_k)_{N(\Phi_{k+1}, \rho)} \geq p^k. \tag{16}$$

Proof. Let k, N and ρ satisfy the conditions of the lemma. We construct a new sequence of fields $\tilde{E}_0, \tilde{E}_1, \dots, \tilde{E}_r$ such that each $\tilde{E}_i$ is a finite extension of E_i of degree prime to p as follows. We set $\tilde{E}_k = N$. The fields $\tilde{E}_j$ with $j < k$ are constructed by descending induction on j. If we have constructed $\tilde{E}_j$ as a finite extension of E_j of degree prime to p, then we extend the valuation v_j to $\tilde{E}_j$ and let $\tilde{E}_{j-1}$ to be its residue field. The fields $\tilde{E}_m$ with $m > k$ are constructed by ascending induction on m. If we have constructed $\tilde{E}_m$ as a finite extension of E_m of degree prime to p, then let $\tilde{E}_{m+1}$ be an extension of E_{m+1} of degree $[\tilde{E}_m : E_m]$ with residue field $\tilde{E}_m$. Replacing E_i by $\tilde{E}_i$ and α_i by $(\alpha_i)_{\tilde{E}_i}$, we may assume that $N = E_k$.

We proceed by induction on r. The case $r = 1$ is obvious.

$(r-1) \Rightarrow r$: First suppose that $k < r-1$. Consider the fields $F' = F(\chi_r)$, $E' = E(\chi_r)$, $E'_i = E_i(\chi_r)$, the sequence of characters $\chi'_i = (\chi_i)_{F'}$, and the sequence of elements $\alpha'_i := (\alpha_i)_{E'_i} \in \operatorname{Br}(E'_i)$ for $i = 0, 1, \dots, r-1$. Let $\Phi' = \langle \chi'_1, \chi'_2, \dots, \chi'_{r-1} \rangle \subset \operatorname{Ch}(F')$, let Φ'_i be the subgroup of Φ' generated by $\chi'_{i+1}, \dots, \chi'_{r-1}$ and $\rho' = \rho_{E'_k}$.

We check the conditions of the lemma for the new datum. Let Ψ' be a subgroup of Φ' of index p^2. Then the pre-image Ψ of Ψ' under the map $\operatorname{Ch}(F) \to \operatorname{Ch}(F')$ is a subgroup of Φ of index p^2 and $E'(\Psi') = E(\Psi)$. Let $L'/E'(\Psi')$ be a field extension of degree prime to p. By assumption, the element $\alpha'_{L'} = \alpha_{L'}$ is not p^2-cyclic. We also have $p\rho' = p\rho_{E'_k} \in \big(\Phi_k\big)_{E'_k} = \big(\Phi'_k\big)_{E'_k}$. Suppose that $p\rho' \in \big(\Phi'_{k+1}\big)_{E'_k}$, i.e., $p\rho_{E'_k} = p\rho' = \eta_{E'_k}$ for some $\eta \in \big(\Phi_{k+1}\big)_{E_k}$. It follows that $p\rho - \eta \in \operatorname{Ker}\big(\operatorname{Ch}(E_k) \to \operatorname{Ch}(E'_k)\big) = \langle (\chi_r)_{E_k} \rangle$ and therefore, $p\rho \in \big(\Phi_{k+1}\big)_{E_k}$, a contradiction, hence $p\rho' \in \big(\Phi'_k\big)_{E'_k} \setminus \big(\Phi'_{k+1}\big)_{E'_k}$.

By the induction hypothesis, the inequality (16) holds for α'_k, i.e,

$$\operatorname{ind}(\alpha'_k)_{E'_k(\Phi'_{k+1}, \rho')} \geq p^k.$$

As

$$(\alpha'_k)_{E'_k(\Phi'_{k+1}, \rho')} = (\alpha_k)_{E_k(\Phi_{k+1}, \rho)},$$

the inequality (16) holds for α_k. Therefore, it remains to show the inequality (16) in the case $k = r-1$. Note that is this case $p\rho$ is a nonzero multiple of $(\chi_r)_{E_{r-1}}$ and $\Phi_{k+1} = \Phi_r = 0$.

Case 1: The character ρ is unramified with respect to v_{r-1}, i.e., $\rho = \widehat{\mu}$ for a character $\mu \in \operatorname{Ch}(E_{r-2})$ of order p^2. Note that $p\mu$ is a nonzero multiple of $(\chi_r)_{E_{r-2}}$.

By (1),

$$\operatorname{ind}(\alpha_{r-2})_{E_{r-2}(\chi_{r-1}, \mu)} = \operatorname{ind}(\alpha_{r-1})_{E_{r-1}(\rho)}/p. \tag{17}$$

Consider the fields $F' = F(\chi_{r-1})$, $E' = E(\chi_{r-1})$, $E'_i = E_i(\chi_{r-1})$, the new sequence of characters $\chi'_1 = (\chi_1)_{F'}, \dots, \chi'_{r-2} = (\chi_{r-2})_{F'}, \chi'_{r-1} = (\chi_r)_{F'}$, the group of characters $\Phi' = \langle \chi'_1, \chi'_2, \dots, \chi'_{r-1} \rangle$ and the elements $\alpha'_i \in \operatorname{Br}(E'_i)$ for $i = 0, 1, \dots, r-1$ defined by $\alpha'_i = (\alpha_i)_{E'_i}$ for $i \leq r-2$ and $\alpha'_{r-1} = \widehat{\alpha}_{r-2} + \big(\widehat{\chi}_r \cup (x_{r-1})\big)$ over E'_{r-1}, and the character μ. The new datum satisfy the conditions of the lemma. By the induction hypothesis, the inequality (16) holds for α'_{r-2}, i.e,

$$\operatorname{ind}(\alpha'_{r-2})_{E'_{r-2}(\mu)} \geq p^{r-2}.$$

As

$$(\alpha'_{r-2})_{E'_{r-2}(\mu)} = (\alpha_{r-2})_{E_{r-2}(\chi_{r-1}, \mu)},$$

the inequality (16) holds for α_{r-1} in view of the equality (17).

Case 2: The character ρ is ramified. Assume that inequality (16) does not hold for α_{r-1}, i.e., we have

$$\operatorname{ind}(\alpha_{r-1})_{E_{r-1}(\rho)} \leq p^{r-2}.$$

By [10, Lemma 2.3(2)], there exists a unit $u \in E_{r-1}$ such that $E_{r-2}(\chi_r) = E_{r-2}(\bar{u}^{1/p})$ and

$$\operatorname{ind}\big(\alpha_{r-2} - (\chi_{r-1} \cup (\bar{u}^{1/p}))\big)_{E_{r-2}(\chi_r)} = \operatorname{ind}(\alpha_{r-1})_{E_{r-1}(\rho)} \leq p^{r-2}.$$

By descending induction on $j = 0, 1, \dots, r-2$ we show that there exist an element u_j in $E_j^\times$ and a subgroup $\Psi_j \subset \Phi$ of rank $r-j-2$ such that $\langle \chi_1, \dots, \chi_j, \chi_{r-1}, \chi_r \rangle \cap \Psi_j = 0$, $E_j(\chi_r) = E_j(u_j^{1/p})$ and

$$\operatorname{ind}\big(\alpha_j - (\chi_{r-1} \cup (u_j^{1/p}))\big)_{E_j(\Theta_j)} \leq p^j, \tag{18}$$

where $\Theta_j := \langle \Psi_j, \chi_r \rangle$. We set $\Psi_{r-2} = 0$ and $u_{r-2} = \bar{u}$.

$j \Rightarrow (j-1)$: The field $E_j(u_j^{1/p}) = E_j(\chi_r)$ is unramified over E_j, hence $v_j(u_j)$ is divisible by p. Modifying u_j by a p^2-th power, we may assume that $u_j = v x_j^{mp}$ for a unit $v \in E_j$, $x_j \in E_j^\times$ and an integer m. Then

$$\big(\alpha_j - (\chi_{r-1} \cup (u_j^{1/p}))\big)_{E_j(\Theta_j)} = \widehat{\beta} + \big(\widehat{\eta} \cup (x_j)\big)_{E_j(\Theta_j)},$$

where $\eta = \chi_j - m\chi_{r-1}$ and $\beta = \big(\alpha_{j-1} - (\chi_{r-1} \cup (u_{j-1}^{1/p}))\big)_{E_{j-1}(\Theta_j)}$, where $u_{j-1} = \bar{v}$. As η is not contained in Θ_j, the character $\eta_{E_{j-1}(\Theta_j)}$ is not trivial. Set $\Psi_{j-1} = \langle \Psi_j, \eta \rangle$. It follows from (1) and the induction hypothesis that

$$\operatorname{ind}(\beta_{E_{j-1}(\Theta_{j-1})}) = \operatorname{ind}\big(\alpha_j - (\chi_{r-1} \cup (u_j^{1/p}))\big)_{E_j(\Theta_j)}/p \leq p^{j-1}.$$

Applying the inequality (18) in the case $j = 0$, we have

$$\alpha_{E(\Theta_0)} = \big(\chi_{r-1} \cup (w^{1/p})\big)_{E(\Theta_0)}$$

for an element $w \in E^\times$ such that $E(w^{1/p}) = E(\chi_r)$. Hence

$$\alpha_{E(\Psi_0)(w^{1/p^2})} = (\alpha_{E(\Theta_0)})_{E(\Theta_0)(w^{1/p^2})} = 0 \text{ in } \operatorname{Br}(E(\Psi_0)(w^{1/p^2})).$$

Since $\alpha_{E(\Psi_0)}$ is split by a cyclic extension $E(\Psi_0)(w^{1/p^2})/E(\Psi_0)$ of degree p^2, $\alpha_{E(\Psi_0)}$ is p^2-cyclic. As $[\Phi : \Psi_0] = p^2$, this contradicts the assumption. Hence, the inequality (16) holds for α_{r-1}. □

5. Non-cyclicity of the generic element

The aim of this section is the technical Lemma 5.4 that will allow us to apply later Lemma 4.2 and Proposition 4.1.

In this section we assume that the base field F contains a primitive p^3-th root of unity. The choice of a primitive p^2-th root of unity ξ allows us to define the symbol $(a, b)_{p^2}$ as in Section 2.1. As -1 is a p^2-th power in $F^\times$, we have $(a, -1)_{p^2} = 0$, hence $(a, a)_{p^2} = 0$ for all $a \in F^\times$. We shall write $(a, b)_p$ for $p(a, b)_{p^2} = (a^p, b)_{p^2}$.

Lemma 5.1. *Let E be a field extension of F that is complete with respect to a discrete valuation v with residue field K and $\alpha \in \mathrm{Br}(K)$. Set $\beta = \widehat{\alpha} + (a, x)_p$ for a unit $a \in E$ and $x \in E^\times$ such that $\bar{a} \notin K^{\times p}$ and $v(x)$ is prime to p. If β is p^2-cyclic, then $\alpha = (\bar{a}, z)_{p^2}$ in $\mathrm{Br}(K)$ for some $z \in K^\times$.*

Proof. Suppose that $\beta = (u\pi^i, w\pi^j)_{p^2}$ and write $x = t\pi^k$ for a prime element π, integers $i, j, k = v(x)$ and units u, w, t in E. Then we have

$$\widehat{\alpha} + (a^p, w\pi^k)_{p^2} = \beta = (u\pi^i, v\pi^j)_{p^2} = (u, v)_{p^2} + (u^j/v^i, \pi)_{p^2}.$$

Applying the residue map ∂_v, we get $\bar{a}^{pk} = \bar{u}^j/\bar{v}^i$ in $K^\times/K^{\times p^2}$ and

$$\alpha = (\bar{u}, \bar{v})_{p^2} - (\bar{a}, \bar{w}^p)_{p^2}.$$

Suppose that i/j is a p-integer (the other case is similar). As k is not divisible by p and $\bar{a}$ is not a p-th power in $K^\times$, j is not divisible by p^2. It follows that $\bar{u} \in \langle \bar{a}, \bar{v} \rangle$ in $K^\times/K^{\times p^2}$ and then $\bar{u} \in \bar{a}^r \bar{v}^s K^{\times p^2}$ for some r and s. Hence $\alpha = (\bar{a}, \bar{v}^r/\bar{w}^p)_{p^2}$. □

Corollary 5.2. *Let x,y be independent variables over F and $a, b \in F^\times$. If $(a, b)_p \neq 0$ in $\mathrm{Br}(F)$, then for any field extension $M/F(x, y)$ of degree prime to p, the element $(a, x)_p + (b, y)_p$ in $\mathrm{Br}(M)$ is not p^2-cyclic.*

Proof. Let $M/F(x, y)$ be a field extension of degree prime to p and $\beta = (a, x)_p + (b, y)_p$ over M. As the degree of $M/F(x, y)$ is prime to p, by [8, Lemma 6.1], there exists a field extension E of the fields $F(\!(y)\!)(\!(x)\!)$ and M over F such that the degree of $E/F(\!(y)\!)(\!(x)\!)$ is finite and prime to p. The discrete valuation v_x on the complete field $F(\!(y)\!)(\!(x)\!)$ extends uniquely to a discrete valuation v of E. The ramification index of $E/F(\!(y)\!)(\!(x)\!)$ is prime to p, hence $v(x)$ is prime to p. The residue field K of v is an extension of $F(\!(y)\!)$ of degree prime to p.

Let v' be the valuation on K extending the discrete valuation v_y on $F(\!(y)\!)$. The ramification index e' of $K/F(\!(y)\!)$ is prime to p. The residue field N of v' is a finite extension of F of degree prime to p.

Let $\alpha = (b, y)_p$ over K, so $\beta_E = \widehat{\alpha} + (a, x)_p$. Suppose that β is p^2-cyclic over M. Then β_E is also p^2-cyclic. By Lemma 5.1, applied to β_E over E, we have $\alpha = (a, z)_{p^2}$ for some $z \in K^\times$, hence $(b^p, y)_{p^2} = (a, z)_{p^2}$. Taking the cup product with $(a)_{p^2} \in K^\times/K^{\times p^2}$, we get

$$(a)_{p^2} \cup (b^p, y)_{p^2} = (a)_{p^2} \cup (a, z)_{p^2} = (a, a)_{p^2} \cup (z)_{p^2} = 0.$$

Applying the residue map $\partial_{v'}$, we find that $e'(a, b)_p = e'(a, b^p)_{p^2} = 0$ over N, hence $(a, b)_p = 0$ in $\mathrm{Br}(N)$. Taking the corestriction map $\mathrm{Br}(N) \to \mathrm{Br}(F)$, we see that $(a, b)_p = 0$ in $\mathrm{Br}(F)$, a contradiction. □

Lemma 5.3. *For any integer $r \geq 2$, there exist a field extension F'/F and a subgroup $\Phi \subset \mathrm{Ch}_p(F')$ of rank r such that for any subgroup $\Psi \subset \Phi$ of index p^2, there is an element $\beta \in \mathrm{Br}_p\big(F'(\Phi)/F'\big)$ with the property that any field extension $M/F'(\Psi)$ of degree prime to p, the element β_M is not p^2-cyclic.*

Proof. Let $a_1, a_2, \dots, a_r, x, y$ be independent variables over F and set $F' := F(a_1, a_2, \dots, a_r, x, y)$. For every $i = 1, \dots, r$, let $\chi_i \in \mathrm{Ch}_p(F')$ be a character such that $F'(\chi_i) = F'(a_i^{1/p})$ and set $\Phi := \langle \chi_1, \chi_2, \dots, \chi_r \rangle$. Let Ψ be a subgroup of Φ of index p^2. Choose a basis $\eta_1, \eta_2, \dots, \eta_r$ for Φ such that $\Psi = \langle \eta_1, \eta_2, \dots, \eta_{r-2} \rangle$ and the elements $b_1, b_2, \dots, b_r$ in F' such that $F(\eta_i) = F(b_i^{1/p})$ for all $i = 1, \dots, r$ and $F(b_1, b_2, \dots, b_r) = F(a_1, a_2, \dots, a_r)$. Clearly, $b_1, b_2, \dots, b_r$ are algebraically independent over F and $F'(\Psi) = L(x, y)$, where $L := F(b_1^{1/p}, \dots, b_{r-2}^{1/p}, b_{r-1}, b_r)$ with the generators algebraically independent over F.

Let $\beta = (b_{r-1}, x)_p + (b_r, y)_p$ in $\mathrm{Br}_p\big(F'(\Phi)/F'\big)$ and $M/F'(\Psi)$ a field extension of degree prime to p. As $\partial_v\big((b_{r-1}, b_r)_p\big) = \bar{b}_{r-1}$, where v is the discrete valuation on L associated with b_r, is nontrivial, we have $(b_{r-1}, b_r)_p \neq 0$ in $\mathrm{Br}(L)$. The result follows from Corollary 5.2. □

Let F'/F be the field extension and $\Phi \subset \mathrm{Ch}_p(F')$ the subgroup of rank r as in Lemma 5.3. Consider the algebraic tori P^Φ, S^Φ, T^Φ, U^Φ and V^Φ over F' defined in Section 2.4. The morphism $\gamma : P^\Phi \to V^\Phi$ in the diagram (4) is a U^Φ-torsor. Denote by δ the image of the class of γ under the composition

$$H^1_{\acute{e}t}(V^\Phi, U^\Phi) \to H^1_{\acute{e}t}(V^\Phi, U'^\Phi) \to H^2_{\acute{e}t}(V^\Phi, \mathbb{G}_m),$$

induced by the diagram (5). We write δ_{gen} for the image of δ under the homomorphism

$$H^2_{\acute{e}t}(V^\Phi, \mathbb{G}_m) \to H^2\big(F(V^\Phi), \mathbb{G}_m\big) = \mathrm{Br}\big(F'(V^\Phi)\big)$$

induced by the generic point morphism $\mathrm{Spec}\big(F'(V^\Phi)\big) \to V^\Phi$. It follows from (6) that $\delta_{gen} \in \mathrm{Br}_{p^s}\big(F'(V^\Phi)\big)$.

Lemma 5.4. *Let $K = F'(V^\Phi)$ and $\Psi \subset \Phi$ a subgroup with $[\Phi : \Psi] = p^2$. Then for any field extension $M/K(\Psi)$ of degree prime to p, the element $(\delta_{gen})_M$ is not p^2-cyclic.*

Proof. Suppose that there exist a subgroup $\Psi \subset \Phi$ with $[\Phi : \Psi] = p^2$ and a field $M/K(\Psi)$ of degree prime to p such that $(\delta_{gen})_M = \chi \cup (a)$ for some $\chi \in H^2(M, \mathbb{Z}) = \mathrm{Ch}(M)$ with $p^2\chi = 0$ and $a \in H^0(M, \mathbb{G}_m) = M^\times$. Choose an integral scheme X over F' such that $F'(X) = M$ together with a dominant F'-morphism

$$f : X \to V^\Phi(\Psi) := (V^\Phi)_{F'(\Psi)}$$

of degree prime to p that induces the embedding of the function field $K(\Psi)$ into M. Let $h : X \to V^\Phi$ be the composition of f with the natural morphism $g : V^\Phi(\Psi) \to V^\Phi$. Replacing X by a nonempty open set, we may assume that $h^*(\delta) = \chi_0 \cup (a_0)$ for some $\chi_0 \in H^2_{\acute{e}t}(X, \mathbb{Z})$ with $p^2\chi_0 = 0$ and $a_0 \in H^0_{\acute{e}t}(X, \mathbb{G}_m)$.

By [8, Lemma 6.2], there is a nonempty open set $W' \subset V^\Phi(\Psi)$ such that for every $x' \in W'$ there exists a point $x \in X$ with $f(x) = x'$ and the degree $[F'(x) : F'(x')]$ prime to p. Let $Z = V^\Phi(\Psi) \setminus W'$. As g is finite, $g(Z) \neq V^\Phi$, hence the open set $W := V^\Phi \setminus g(Z)$ is not empty. We have $g^{-1}(W) \subset W'$.

Consider the element $\beta \in \mathrm{Br}_p\big(F'(\Phi)/F'\big)$ constructed in Lemma 5.3. Let $\gamma' \in H^1(F', U^\Phi)$ be the corresponding class of U^Φ-torsors over F' under the isomorphism $H^1(F', U^\Phi) \simeq \mathrm{Br}_{p^s}\big(F'(\Phi)/F'\big)$ by (7). As γ is a generic U^Φ-torsor, there exists an F'-morphism $v : \mathrm{Spec}\, F' \to V^\Phi$ such that $v^*(\gamma) = \gamma'$ and $\mathrm{Im}(v) \subset W$ (see Section 2.3). From the commutativity of the diagram

$$\begin{array}{ccc} H^1_{\acute{e}t}(V^\Phi, U^\Phi) & \xrightarrow{v^*} & H^1(F', U^\Phi) \\ \big\downarrow & & \big\downarrow \\ H^2_{\acute{e}t}(V^\Phi, \mathbb{G}_m) & \xrightarrow{v^*} & H^2(F', \mathbb{G}_m) \end{array}$$

we find that $v^*(\delta) = \beta$.

Let $v' : \mathrm{Spec}\, F'(\Psi) \to V^\Phi(\Psi)$ be the morphism $v_{F'(\Psi)}$. Note that $\mathrm{Im}(v') \subset g^{-1}(W) \subset W'$.

By the definition of W', there is a point $x \in X$ such that the degree of the field extension $F'(x)$ over the residue field of (the only) point in $\mathrm{Im}(v')$ is prime to p. By [8, Lemma 6.1], there exist a field extension $M/F'(\Psi)$ of degree prime to p and a morphism $w : \mathrm{Spec}(M) \to X$ such that the diagram

$$\begin{array}{ccccc} \mathrm{Spec}(M) & \longrightarrow & \mathrm{Spec}\big(F'(\Psi)\big) & \longrightarrow & \mathrm{Spec}(F') \\ {\scriptstyle w}\big\downarrow & & {\scriptstyle v'}\big\downarrow & & {\scriptstyle v}\big\downarrow \\ X & \xrightarrow{f} & V^\Phi(\Psi) & \xrightarrow{g} & V^\Phi \end{array}$$

is commutative. It follows that

$$\beta_M = v^*(\delta)_M = w^* h^*(\delta) = w^*\big(\chi_0 \cup (a_0)\big) = w^*(\chi_0) \cup w^*(a_0),$$

i.e., β_M is p^2-cyclic. This contradicts Lemma 5.3. □

6. A lower bound for $\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$

Let $n \geq 1$ be an integer, m a divisor of n and p a prime integer. Let p^r (respectively, p^s) be the largest power of p dividing n (respectively, m). If $A \in \mathsf{Alg}_{n,m}(K)$ for some field extension K/F, then there is a finite field extension E/K of degree prime to p such that $\mathrm{ind}(A_E)$ is a p-power. Hence $\mathrm{ind}(A_E)$ divides p^r and $\exp(A_E)$ divides p^s as it divides m and $\mathrm{ind}(A_E)$, i.e., $A_E \in \mathsf{Alg}_{p^r,p^s}(E)$. It follows that the embedding functor $\mathsf{Alg}_{p^r,p^s} \to \mathsf{Alg}_{n,m}$ is p-surjective and hence $\mathrm{ed}_p(\mathsf{Alg}_{n,m}) \leq \mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$ by [8, Sec. 1.3]. Conversely, if $A \in \mathsf{Alg}_{n,m}(K)$, then the p-primary component A_p of A satisfies $A_p \in \mathsf{Alg}_{p^r,p^s}(K)$, hence the morphism of functors $\mathsf{Alg}_{n,m} \to \mathsf{Alg}_{p^r,p^s}$, taking A to A_p is surjective and therefore, $\mathrm{ed}_p(\mathsf{Alg}_{n,m}) \geq \mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$. We proved that

$$\mathrm{ed}_p(\mathsf{Alg}_{n,m}) = \mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s}).$$

Theorem 6.1. *Let F be a field and p a prime integer different from* $\mathrm{char}(F)$. *Then, for any integers r and s with $1 \le s \le r$,*

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

Proof. By [8, Prop.1.5], we can replace the base field by any field extension. Hence we may assume that F contains a primitive p^3-th root of unity. Moreover, we can replace F by the field F' in Lemma 5.3. Let V^Φ be the algebraic torus constructed in Section 2.4. Set $E = F(V^\Phi)$ and let $\alpha := \delta_{gen} \in \mathrm{Br}_{p^s}(E(\Phi)/E)$ be the element defined in Section 5. Let E_k be the fields and $\alpha_k \in \mathcal{B}^{\Phi_k}_{k,s}(E_k)$ the elements constructed in Section 4.2, so that $E_0 = E$ and $\alpha_0 = \alpha$. By Lemma 5.4, α_M is not p^2-cyclic for any subgroup $\Psi \subset \Phi$ with $[\Phi : \Psi] = p^2$ and any field extension $M/E(\Psi)$ of degree prime to p, hence α satisfies the condition of Lemma 4.2. It follows that we can apply Proposition 4.1. By the iterated application of this proposition, we have

$$\begin{aligned} (19) \quad \mathrm{ed}_p^{\mathsf{Alg}_{p^r,p^s}}(\alpha_r) &= \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi_r}_{r,s}}(\alpha_r) \ge \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi_{r-1}}_{r-1,s}}(\alpha_{r-1}) + 1 \ge \dots \\ &\ge \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi_1}_{1,s}}(\alpha_1) + (r-1) \ge \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi_0}_{0,s}}(\alpha_0) + r = \mathrm{ed}_p^{\widetilde{\mathcal{B}}^{\Phi}_{0,s}}(\alpha) + r. \end{aligned}$$

Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U^\Phi & \longrightarrow & P^\Phi & \xrightarrow{\gamma} & V^\Phi & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & S^\Phi & \longrightarrow & P^\Phi \times \mathbb{G}_m^r & \xrightarrow{\gamma'} & V^\Phi & \longrightarrow & 1, \end{array}$$

where $P^\Phi \to P^\Phi \times \mathbb{G}_m^r$ takes x to $(x, 1)$ and $S^\Phi \hookrightarrow P^\Phi \times \mathbb{G}_m^r$ is the product of $S^\Phi \hookrightarrow P^\Phi$ and $S^\Phi \twoheadrightarrow \mathbb{G}_m^r$.

The element α considered in $\mathcal{B}^\Phi_{0,s}(E)$ corresponds to the generic fiber of the U^Φ-torsor γ under the bijection $\mathcal{B}^\Phi_{0,s}(E) \simeq U^\Phi\text{-}\mathsf{torsors}(E)$ in (11). Hence, by the diagram, the class of α in $\widetilde{\mathcal{B}}^\Phi_{0,s}(E)$ corresponds to the generic fiber γ'_{gen} of the S^Φ-torsor γ' under the bijection $\widetilde{\mathcal{B}}^\Phi_{0,s}(E) \simeq S^\Phi\text{-}\mathsf{torsors}(E)$. As $P^\Phi \times \mathbb{G}_m^r$ is a quasi-split torus, γ' is a generic S^Φ-torsor by Proposition 2.1, hence

$$(20) \qquad \mathrm{ed}_p^{\widetilde{\mathcal{B}}^\Phi_{0,s}}(\alpha) = \mathrm{ed}_p^{S^\Phi\text{-}\mathsf{torsors}}(\gamma'_{gen}) = \mathrm{ed}_p(S^\Phi)$$

by [8, Th. 2.9]. The essential p-dimension of S^Φ was calculated in Corollary 3.11. From (19),(20) and this corollary, we have

$$\mathrm{ed}_p\big(\mathsf{Alg}_{p^r,p^s}\big) \ge \mathrm{ed}_p^{\mathsf{Alg}_{p^r,p^s}}(\alpha_r) \ge \mathrm{ed}_p(S^\Phi) + r = \begin{cases} (r-1)2^{r-1} & \text{if } p=2 \text{ and } s=1, \\ (r-1)p^r + p^{r-s} & \text{otherwise.} \end{cases}$$

This concludes the proof. □

7. An upper bound for $\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$

Lemma 7.1. *Let F be a field and p a prime. Then, for any integers r and s with $1 \le s \le r$,*
$$\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s}) \le \mathrm{ed}_p(\mathsf{Alg}_{p^r}) + p^{r-s} - 1.$$

Proof. Let $A \in \mathsf{Alg}_{p^r,p^s}(K) \subset \mathsf{Alg}_{p^r}(K)$ for a field extension K/F. There exist a field extension K'/K of degree prime to p, a subfield $K_0 \subset K'$ over F and $B \in \mathsf{Alg}_{p^r}(K_0)$ such that $\mathrm{tr.deg}_F(K_0) \le \mathrm{ed}_p(\mathsf{Alg}_{p^r})$ and $A \otimes_K K' \simeq B \otimes_{K_0} K'$.

By [16, Lemma 5.6], $\mathrm{ind}(B^{\otimes p^s})$ divides p^{r-s}. Choose a central simple algebra C of degree p^{r-s} over K_0 in the Brauer class of $B^{\otimes p^s}$ in $\mathrm{Br}(K_0)$ and consider the *Severi-Brauer variety* $X := \mathrm{SB}(C)$ of C. Since $\exp(A)$ divides p^s, the algebra C is split over K', hence $X(K') \ne \emptyset$. This implies that there exists $x \in X$ such that $K_0(x) \subset K'$ and $X\big(K_0(x)\big) \ne \emptyset$. Therefore, $C_{K_0(x)}$ is split, hence $\exp(B_{K_0(x)})$ divides p^s, i.e., $B_{K_0(x)} \in \mathsf{Alg}_{p^r,p^s}\big(K_0(x)\big)$. Since $\dim(X) = p^{r-s}-1$, we have
$$\mathrm{ed}_p^{\mathsf{Alg}_{p^r,p^s}}(A) \le \mathrm{tr.deg}_F(K_0(x)) = \mathrm{tr.deg}_F(K_0) + \mathrm{tr.deg}_{K_0}(K_0(x)) \le \mathrm{ed}_p(\mathsf{Alg}_{p^r}) + \dim(x) \le \mathrm{ed}_p(\mathsf{Alg}_{p^r}) + (p^{r-s} - 1). \quad \square$$

By [12, Th.1.1],
$$\mathrm{ed}_p(\mathsf{Alg}_{p^r}) \le 2p^{2r-2} - p^r + 1,$$
if $r \ge 2$, therefore, by Lemma 7.1, we have the following upper bound for $\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$:

Theorem 7.2. *Let F be a field and p a prime integer. Then, for any integers $r \ge 2$ and s with $1 \le s \le r$,*
$$\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s}) \le 2p^{2r-2} - p^r + p^{r-s}.$$

8. Essential dimension of $\mathsf{Alg}_{L/F}$, Alg_G and ALG_G.

Let G be an elementary abelian group of order p^r and K/F a field extension. Consider the subset $\mathsf{Alg}_G(K)$ of $\mathsf{Alg}_{p^r,p^s}(K)$ consisting of all classes that have a splitting Galois K-algebra E with $\mathrm{Gal}(E/K) \simeq G$.

Let L/F be a Galois field extension with $\mathrm{Gal}(L/F) \simeq G$. Consider the subset $\mathsf{Alg}_{L/F}(K)$ of $\mathsf{Alg}_G(K)$ consisting of all classes split by the field extension KL/K. We have the subfunctors of Alg_{p^r,p^s}:
$$\mathsf{Alg}_{L/F} \subset \mathsf{Alg}_G \subset \mathsf{Alg}_{p^r,p^s}.$$
We write $\mathsf{ALG}_G(K)$ for the set of pairs (A, E), where $A \in \mathsf{Alg}_G(K)$ and E is a Galois G-algebra splitting A. We have an obvious surjective morphism of functors $\mathsf{ALG}_G \to \mathsf{Alg}_G$.

Theorem 8.1. *Let F be a field, p a prime integer different from* $\mathrm{char}(F)$, *G an elementary abelian group of order p^r with $r \ge 2$, and L/F a Galois field extension with* $\mathrm{Gal}(L/F) \simeq G$. *Let an integer s satisfy $1 \le s \le r$. Suppose* *that $r \geq 3$ if $p = 2$ and $s = 1$. Let $\mathcal{F}$ be one of the three functors: $\mathsf{Alg}_{L/F}$, Alg_G or ALG_G. Then*

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

Proof. Let Φ be a subgroup of $\mathrm{Ch}_p(F)$ of rank r such that $L = F(\Phi)$. By (7), we have $\mathsf{Alg}_{L/F} \simeq U^\Phi$*- torsors*. It follows from Proposition 3.9 that

$$\mathrm{ed}_p(\mathsf{Alg}_{L/F}) = \mathrm{ed}(\mathsf{Alg}_{L/F}) = d_{p,r,s} := \begin{cases} (r-1)2^{r-1} & \text{if } p = 2 \text{ and } s = 1, \\ (r-1)p^r + p^{r-s} & \text{otherwise.} \end{cases}$$

Let $\alpha_r \in \mathrm{Br}(E_r)$ be as in the proof of Theorem 6.1. By construction, α_r is split by $E_r(\Phi)$, hence $\alpha_r \in \mathsf{Alg}_G(E_r)$. Note that $\mathrm{ed}_p^{\mathcal{B}}(\beta) \leq \mathrm{ed}_p^{\mathcal{H}}(\beta)$ for any subfunctor $\mathcal{H}$ of a functor $\mathcal{B}$ and any $\beta \in \mathcal{H}(K)$. Hence, by the proof of Theorem 6.1, we have

$$\mathrm{ed}_p(\mathsf{Alg}_G) \geq \mathrm{ed}_p^{\mathsf{Alg}_G}(\alpha_r) \geq \mathrm{ed}_p^{\mathsf{Alg}_{p^r,p^s}}(\alpha_r) \geq d_{p,r,s}.$$

Let J be the G-module defined in the Section 2.4 and $T := \operatorname{Spec} F[J]$ the split torus with the character group J. Consider the minimal surjective p-presentation $\nu : P' \to J$ as in Remark 3.10. As explained in Section 2.2, a choice of a G-invariant basis of P yields a linear $T \rtimes G$-space V with $\dim(V) = \mathrm{rank}(P')$. By Remark 3.10, G acts faithfully on $\mathrm{Ker}(\nu)$. It follows from [11, Lemma 3.3] that the action of $T \rtimes G$ on V is generically free in this case, hence, by [3, Prop. 4.11],

$$\begin{aligned} \mathrm{ed}(T \rtimes G) &\leq \dim(V) - \dim(T \rtimes G) \\ &= \mathrm{rank}(P') - \mathrm{rank}(J) \\ &= \mathrm{rank}\big(\mathrm{Ker}(\nu)\big) \\ &= d_{p,r,s}. \end{aligned}$$

Let $\gamma \in H^1(F, G)$ and let L be the corresponding Galois G-algebra over F. Since G is an abelian group, we have $G = G_\gamma$. The G-action on $R_{L/F}(\mathbb{G}_{m,L})$ restricts to the trivial action on the subgroup μ_{p^s}. As $T_\gamma = R_{L/F}(\mathbb{G}_{m,L})/\mu_{p^s}$, the connecting map

$$H^1(F, T_\gamma) \to H^2(F, \mu_{p^s}) = \mathrm{Br}_{p^s}(F)$$

is injective, hence the group $G_\gamma(F) = G$ acts trivially on $H^1(F, T_\gamma)$. By (2),

$$H^1(F, T \rtimes G) = \coprod_{\mathrm{Gal}(E/F) = G} \mathrm{Br}_{p^s}(E/F),$$

where the disjoint union is taken over all isomorphism classes of Galois G-algebras E/F. Hence we have a surjective morphism of functors $T \rtimes G$*- torsors* $\to \mathsf{ALG}_G$. As ALG_G surjects on Alg_G, we have

$$\mathrm{ed}_p(\mathsf{Alg}_G) \leq \big(\mathrm{ed}_p(\mathsf{ALG}_G) \text{ or } \mathrm{ed}(\mathsf{Alg}_G)\big) \leq \mathrm{ed}(\mathsf{ALG}_G) \leq \mathrm{ed}(T \rtimes G) \leq d_{p,r,s}. \quad \square$$

Remark 8.2. Suppose that $p = r = 2$ and $s = 1$ and F is a field of characteristic different from 2. By [15, Th.1] or [2, Sec.2.4], there exists a nontrivial cohomological invariant of degree 4 for Alg_G over $F(i)$, where i is a primitive 4-th root of unity. Hence, $\mathrm{ed}_2(\mathsf{Alg}_G) \geq \mathrm{ed}_2(\mathsf{Alg}_G)_{F(i)} \geq 4$ by [13, Lemma 6.9]. Moreover, by the structure theorem on central simple algebras split by a biquadratic field extension [20, Cor.2.8], every $(A, E) \in \mathsf{ALG}_G(K)$ is of the form $E = K(a^{1/2}, b^{1/2})$ and $[A] = (a, x)_2 + (b, y)_2$ for some $a, b, x, y \in K^\times$. Hence $\mathrm{ed}(\mathsf{ALG}_G) \leq 4$. As ALG_G surjects on Alg_G, we have

$$4 \leq \mathrm{ed}_2(\mathsf{Alg}_G) \leq \big(\mathrm{ed}_2(\mathsf{ALG}_G) \ \text{ or } \ \mathrm{ed}(\mathsf{Alg}_G)\big) \leq \mathrm{ed}(\mathsf{ALG}_G) \leq 4,$$

hence the essential (2)-dimension of Alg_G and ALG_G is equal to 4.

Corollary 8.3. *Let F be a field of characteristic $\neq 2$. Then*

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

Proof. As any central simple algebra of degree 8 and exponent 2 has a triquadratic splitting field by [14], we have $\mathsf{Alg}_{8,2} = \mathsf{Alg}_G$ for the elementary abelian group G of order 8, hence the statement follows from Theorem 8.1. Note that the inequality $\mathrm{ed}_2(\mathsf{Alg}_{8,2}) \geq 8$ is also proven in Theorem 6.1 and the opposite inequality $\mathrm{ed}(\mathsf{Alg}_{8,2}) \leq 8$ was shown in [2, Th.2.12]. □

References

[1] S. A. Amitsur, L. H. Rowen, and J.-P. Tignol, *Division algebras of degree 4 and 8 with involution*, Israel J. Math. **33** (1979), no. 2, 133–148.

[2] S. Baek and A. Merkurjev, *Invariants of simple algebras*, Manuscripta Math, Vol. 129, No. 4 (2009), 409–421.

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

[4] R. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in galois cohomology*, American Mathematical Society, Providence, RI, 2003.

[5] 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.

[6] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670.

[7] R. Lötscher, M. MacDonald, A. Meyer, and R. Reichstein, *Essential p-dimension of algebraic tori*, preprint, `http://www.math.uni-bielefeld.de/LAG/` (n. 363, 2009).

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

[9] A. S. Merkurjev, *Essential p-dimension of* $\mathrm{PGL}(p^2)$, to appear in JAMS, 2009, DOI: 10.1090/S0894-0347-10-00661-2.

[10] A. S. Merkurjev, *Essential dimension of simple algebras*, preprint, `http://www.math.uni-bielefeld.de/LAG/` (n. 370, 2009).

[11] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra and Number Theory **3** (2009), no. 4, 467–487.

[12] A. Meyer and Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, to appear in the Journal of Algebra.

[13] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, With an appendix by János Kollár and Endre Szabó.

[14] L. Rowen, *Central simple algebras*, Israel J. Math. **29** (1978), no. 2-3, 285–301.
[15] M. Rost, J.-P. Serre, J.-P. Tignol, *La forme trace d'une algèbre simple centrale de degré 4*, C. R. Acad. Sci. Paris, Ser. I 342 (2006), 83-87.
[16] D. J. Saltman, *Lectures on Division Algebras*, Amer. Math. Soc., Providence, RI, (1999).
[17] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, **67**, Springer-Verlag, (1979).
[18] J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.
[19] J.-P. Tignol, *Sur les classes de similitude de corps à involution de degré* 8, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 20, A875–A876.
[20] J.-P. Tignol, *Corps à involution neutralisés par une extension abélienne élémentaire*, The Brauer group (Sem., Les Plans-sur-Bex, 1980), pp. 1–34, Lecture Notes in Math., **844**, Springer, Berlin, (1981).
[21] J.-P. Tignol, *Algébres indecomposables d'exposant premier*, Advances in Math. **65** (1987) 205228.

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA
E-mail address: shbaek@math.ucla.edu

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA
E-mail address: merkurev@math.ucla.edu