Acta Math., 209 (2012), 1–27
DOI: 10.1007/s11511-012-0080-8

Essential dimension of central simple algebras

by

Sanghoon Baek
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea

Alexander S. Merkurjev
University of California, Los Angeles
Los Angeles, CA, U.S.A.

1. Introduction

Let $\mathcal{F}\colon \mathit{Fields}/F \to \mathit{Sets}$ be a functor from the category Fields/F of field extensions over F to the category Sets of sets. Let $E \in \mathit{Fields}/F$ and $K \subset E$ be 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 by $\operatorname{ed}^{\mathcal{F}}(\alpha)$, is the least transcendence degree $\operatorname{tr\,deg}_F(K)$ over all fields of definition K of α. The *essential dimension* of $\mathcal{F}$ is

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

where the supremum is taken over all fields $E \in \mathit{Fields}/F$ and all $\alpha \in \mathcal{F}(E)$ (see [3, Definition 1.2] or [7, §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 by $\operatorname{ed}_p^{\mathcal{F}}(\alpha)$, 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 $E \in \mathit{Fields}/F$ and all $\alpha \in \mathcal{F}(E)$. By definition, $\operatorname{ed}(\mathcal{F}) \geqslant \operatorname{ed}_p(\mathcal{F})$ for all p.

For every integer $n \geqslant 1$, a divisor m of n and any field extension E/F, let $\mathit{Alg}_{n,m}(E)$ denote the set of isomorphism classes of central simple E-algebras of degree n and exponent dividing m. Equivalently, $\mathit{Alg}_{n,m}(E)$ is the subset of the m-torsion part $\operatorname{Br}_m(E)$

The first author was supported by the Beckenbach Dissertation Fellowship at the University of California, Los Angeles. The second author was supported by the NSF grant DMS #0652316.

of the Brauer group of E consisting of all elements a such that $\mathrm{ind}(a)$ divides n. In particular, if $n=m$, then $\mathsf{Alg}_n(E):=\mathsf{Alg}_{n,n}(E)$ 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 $\mathrm{ed}_p(\mathsf{Alg}_{n,m})$ for a prime integer p different from $\mathrm{char}(F)$. Let p^r (resp. p^s) be the largest power of p dividing n (resp. m). Then $\mathrm{ed}_p(\mathsf{Alg}_{n,m})=\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$ and $\mathrm{ed}_p(\mathsf{Alg}_n)=\mathrm{ed}_p(\mathsf{Alg}_{p^r})$ (see §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 and p as follows. Since every central simple algebra A of degree p is cyclic over a finite extension of fields of degree prime to p, A can be given by two parameters (see §2.1). In fact, $\mathrm{ed}_p(\mathsf{Alg}_p)=2$ by [11, Lemma 8.5.7].

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

Upper and lower bounds for $\mathrm{ed}_p(\mathsf{Alg}_{p^r})$ can be found in [14] and [9], respectively. In this paper (see §6 and §7), we establish the following upper and lower bounds for $\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$ that match the bounds in the case $r=s$ given in [14] and [9].

THEOREM 1.1. *Let F be a field and p be a prime integer different from* $\mathrm{char}(F)$. *Then, for any integers $r\geqslant 2$ and s with $1\leqslant s\leqslant r$,*

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

COROLLARY 1.2. (Cf. [8]) *Let p be a prime integer and F be a field of characteristic different from p. Then*

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

COROLLARY 1.3. *Let p be an odd prime integer and F be a field of characteristic different from p. Then*

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

The corollary recovers a result in [20] that, for p odd, there exists a central simple algebra of degree p^2 and exponent p over a field F which is not decomposable as a tensor product of two algebras of degree p over any finite extension of F of degree prime to p. Indeed, if every central simple algebra of degree p^2 and exponent p were decomposable, then the essential p-dimension of $\mathsf{Alg}_{p^2,p}$ would be at most 4.

COROLLARY 1.4. *Let F be a field of characteristic different from* 2. *Then*

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

The proof is given in §8. The corollary recovers a result in [1] that there is a central simple algebra of degree 8 and exponent 2 over a field F which is not decomposable as a tensor product of three quaternion algebras over any finite extension of F of degree prime to p. Indeed, if every central simple algebra of degree 8 and exponent 2 were decomposable, then the essential 2-dimension of $\mathit{Alg}_{8,2}$ would be at most 6.

The proof of the main theorem splits into two steps. In the first step we relate the essential p-dimensions of Alg_{p^r,p^s} and of a certain torus S^Φ by means of the iterated degeneration. In the second step, we apply [6, Theorem 1.1] to compute the essential p-dimension of S^Φ.

2. Character, Brauer group and algebraic tori

2.1. Character and Brauer group

Let F be a field, F_{sep} be a separable closure of F and $\Gamma_F=\mathrm{Gal}(F_{\mathrm{sep}}/F)$. 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 $H^1(\Gamma_F,S(F_{\mathrm{sep}}))$ (see [17]).

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

$$F(\Psi):=(F_{\mathrm{sep}})^{\bigcap_{\chi\in\Psi}\mathrm{Ker}(\chi)}.$$

The Galois group $G=\mathrm{Gal}(F(\Psi)/F)$ 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 $\eta\in\Psi$.

If K/F is a field extension, we write $K(\Psi)$ for $K(\Psi_K)$, where Ψ_K is the image of Ψ under the natural homomorphism $\mathrm{Ch}(F)\to\mathrm{Ch}(K)$.

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 is 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

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

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 nth roots of unity in F_{sep}.

Let n be prime to $\mathrm{char}(F)$ and suppose that F contains a primitive nth root of unity ξ. For any $a\in F^\times$, let $\chi_a\in\mathrm{Ch}(F)$ be the unique character with values in

$$\frac{(1/n)\mathbb{Z}}{\mathbb{Z}}\subset\frac{\mathbb{Q}}{\mathbb{Z}}$$

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 [16, Chapter XIV, Proposition 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 $\mathrm{Br}(F(\Phi)/F)_{\mathrm{dec}}$ for the *subgroup of decomposable elements* in $\mathrm{Br}(F(\Phi)/F)$ generated by the elements $\chi\cup(a)$ for all $\chi\in\Phi$ and $a\in F^\times$. The *indecomposable relative Brauer group* $\mathrm{Br}(F(\Phi)/F)_{\mathrm{ind}}$ is the factor group

$$\frac{\mathrm{Br}(F(\Phi)/F)}{\mathrm{Br}(F(\Phi)/F)_{\mathrm{dec}}}.$$

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

$$\frac{\mathrm{Br}_n(F(\Phi)/F)}{\mathrm{Br}(F(\Phi)/F)_{\mathrm{dec}}}.$$

Let E be a complete field with respect to a discrete valuation v and K be 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 $\mathrm{Ch}(E)\{p\}$.

If in addition E is an extension of a field F such that v is trivial on F, then K is a field extension of F and the composition

$$\mathrm{Ch}(F)\{p\}\longrightarrow\mathrm{Ch}(K)\{p\}\longrightarrow\mathrm{Ch}(E)\{p\}$$

coincides with the canonical homomorphism for the field extension E/F.

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

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

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 nth 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 $\beta=\widehat{\alpha}+(\widehat{\chi}\cup(x))$ 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. [18, Proposition 2.4])

$$\mathrm{ind}(\beta)=\mathrm{ind}(\alpha_{K(\chi)})\,\mathrm{ord}(\chi). \tag{2.1}$$

2.2. Representations of algebraic tori

Let T be an algebraic torus over a field F and L/F be a finite Galois splitting field for T with Galois group G. The group G is called a *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

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

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 $\nu\colon T\to P$, with P being 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^* be 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 makes A into a faithful P-space over F. Let $\nu\colon T\to P$ 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 $\nu^*\colon P^*\to T^*$ is a G-module homomorphism. Suppose that there is a G-invariant $\mathbb{Z}$-basis X for P^*, i.e., P^* is a 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 into 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 $\gamma\colon \operatorname{Spec} L\to\operatorname{Spec} F$ is a G-torsor. Twisting the split torus T by the torsor γ, we get the torus

$$T_\gamma=\frac{T\times\operatorname{Spec} L}{G}=\operatorname{Spec}(L[T^*]^G),$$

which is split by L, and T_γ^* is isomorphic to T^* as G-modules.

By [5, Proposition 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.,

$$H^1(F,T\rtimes G)\simeq\coprod\frac{H^1(F,T_\gamma)}{G_\gamma(F)},\tag{2.2}$$

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 $\gamma\colon P\to S$ 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 $\gamma'\colon E\to\operatorname{Spec} K$ and every non-empty open subset $W\subset S$, there is a morphism $s\colon\operatorname{Spec} K\to S$ 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

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

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 $1\leqslant s\leqslant r$ be integers, p be a prime integer, F be a field with $\mathrm{char}(F)\neq p$, Φ be a subgroup of $\mathrm{Ch}_p(F)$ of rank r and $G=\mathrm{Gal}(F(\Phi)/F)$. Choose a basis $\chi_1,\chi_2,...,\chi_r$ for Φ. Each χ_i can be viewed as a character of G, i.e., as a homomorphism $\chi_i\colon G\to\mathbb{Q}/\mathbb{Z}$. Let $\sigma_1,\sigma_2,...,\sigma_r$ 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-module homomorphism $\bar\varepsilon\colon R\to\mathbb{Z}/p^s\mathbb{Z}$, defined by $\bar\varepsilon(x)=\varepsilon(x)+p^s\mathbb{Z}$, where $\varepsilon\colon R\to\mathbb{Z}$ is the *augmentation homomorphism* given by $\varepsilon(\varrho)=1$ for all $\varrho\in G$. Set $J:=\mathrm{Ker}(\bar\varepsilon)$. Thus, we have an exact sequence

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

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

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

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

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

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

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

Proof. Consider the surjective morphism $k\colon R^r\to I$ taking e_i to σ_i-1 for $1\leqslant i\leqslant r$ and set $N':=\mathrm{Ker}(k)$. Then we have the 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 $\varepsilon'\colon J\to\mathbb{Z}$ 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 σ_i-1 in N. The module N' is generated by e_{ij} and f_i, by [9, Lemma 3.4]. This completes the proof. □

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

$$\begin{aligned} q\colon N &\longrightarrow \mathbb{Z}^r,\\ x &\longmapsto \left(\frac{\varepsilon_1(x)}{p},\dots,\frac{\varepsilon_r(x)}{p}\right), \end{aligned}$$

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

Let P^Φ, S^Φ, T^Φ, U^Φ and V^Φ be the algebraic tori over F split by the field extension $F(\Phi)/F$ such that

$$(P^\Phi)^*=R^{r+1},\quad (S^\Phi)^*=Q,\quad (T^\Phi)^*=M,\quad (U^\Phi)^*=J\quad\text{and}\quad (V^\Phi)^*=N.$$

The diagram of homomorphisms of G-modules with exact columns and rows

$$\begin{array}{ccccc} M & = & M & & \\ \downarrow & & \downarrow & & \\ N & \hookrightarrow & R^{r+1} & \overset{h}{\twoheadrightarrow} & J \\ {\scriptstyle q}\downarrow & & \downarrow & & \| \\ \mathbb{Z}^r & \hookrightarrow & Q & \twoheadrightarrow & J \end{array} \tag{2.3}$$

yields the following diagram of homomorphisms of the tori

$$\begin{array}{ccccc} T^\Phi & = & T^\Phi & & \\ \twoheadrightarrow\uparrow & & \twoheadrightarrow\uparrow & & \\ V^\Phi & \overset{\gamma}{\twoheadleftarrow} & P^\Phi & \hookleftarrow & U^\Phi \\ {\scriptstyle\varkappa}\uparrow & & \uparrow & & \| \\ \mathbb{G}_m^r & \twoheadleftarrow & S^\Phi & \hookleftarrow & U^\Phi. \end{array} \tag{2.4}$$

The commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & R & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & J & \longrightarrow & R & \longrightarrow & \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

induces the commutative diagram of homomorphisms of algebraic groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_{p^s} & \longrightarrow & R_{F(\Phi)/F}(\mathbb{G}_{m,F(\Phi)}) & \longrightarrow & U^\Phi & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & R_{F(\Phi)/F}(\mathbb{G}_{m,F(\Phi)}) & \longrightarrow & (U')^\Phi & \longrightarrow & 1 \end{array} \tag{2.5}$$

and then the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(K,U^\Phi) & \longrightarrow & H^2(K,\mu_{p^s}) & \longrightarrow & H^2(K\otimes F(\Phi),\mathbb{G}_m) \\ & & \downarrow & & \downarrow & & \| \\ 0 & \longrightarrow & H^1(K,(U')^\Phi) & \longrightarrow & H^2(K,\mathbb{G}_m) & \longrightarrow & H^2(K\otimes F(\Phi),\mathbb{G}_m) \end{array} \tag{2.6}$$

for a field extension K/F. Note that the K-algebra $K(\Phi)$ is a direct factor of $K\otimes F(\Phi)$. Hence

$$\mathrm{Ker}(H^2(K,\mathbb{G}_m)\to H^2(K\otimes F(\Phi),\mathbb{G}_m)) = \mathrm{Ker}(H^2(K,\mathbb{G}_m)\to H^2(K(\Phi),\mathbb{G}_m)).$$

It follows that

$$H^1(K,(U')^\Phi)\simeq \mathrm{Br}(K(\Phi)/K) \quad \text{and} \quad H^1(K,U^\Phi)\simeq \mathrm{Br}_{p^s}(K(\Phi)/K). \tag{2.7}$$

LEMMA 2.3. *The map $H^1(K,U^\Phi)\to H^1(K,S^\Phi)$ induces an isomorphism*

$$H^1(K,S^\Phi)\simeq \mathrm{Br}_{p^s}(K(\Phi)/K)_{\mathrm{ind}}.$$

Proof. Consider the 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 diagram (4) in [9]. This yields a commutative diagram

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

with exact rows. The homomorphism λ takes $(x_1,...,x_r)$ to

$$\sum_{i=1}^r((\chi_i)_K\cup(x_i))$$

by [9, Lemma 3.6], whence the result. □

3. Essential dimension of algebraic tori

Let S be an algebraic group over F and p be a prime integer different from $\mathrm{char}(F)$. The *essential dimension* $\mathrm{ed}(S)$ (resp. *essential p-dimension* $\mathrm{ed}_p(S)$) 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 $G{=}\mathrm{Gal}(L/F)$. We assume that G is a group of order p^r, where $r{\geqslant}2$. 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 $[G{:}H]{\leqslant}p^k$. We have the sequence of subgroups

$$0=V_{-1}\subset V_0\subset\ldots\subset V_r=\overline{X}. \tag{3.1}$$

A *p-presentation* of X is a G-homomorphism $P{\to}X$, with P being a permutation G-module, having a finite cokernel of order prime to p. A p-presentation with the smallest $\mathrm{rank}(P)$ is called *minimal*. The essential p-dimension of algebraic tori was determined in [6, Theorem 1.1] in terms of a minimal p-presentation $P{\to}X$:

$$\mathrm{ed}_p(S)=\mathrm{rank}(P)-\dim(S). \tag{3.2}$$

We have the following explicit formula for the essential (p-)dimension of S (cf. [9, Theorem 4.3]).

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

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

Proof. The second equality was proven in [9, Theorem 4.3]. Let $\nu{:}\,P{\to}X$ be a minimal p-presentation. By definition, the index $m{:=}[X{:}\mathrm{Im}(\nu)]$ is prime to p. Let T be the torus split by L with the character G-module $\mathrm{Im}(\nu)$. The inclusion of $\mathrm{Im}(\nu)$ into X yields a homomorphism $\alpha{:}\,S{\to}T$. As $mX{\subset}\mathrm{Im}(\nu)$, there is a homomorphism $\beta{:}\,T{\to}S$ such that the compositions $\alpha{\circ}\beta$ and $\beta{\circ}\alpha$ are the mth power endomorphisms of T and S, respectively. It follows that for any field extension K/F, the kernel and cokernel of the induced homomorphism

$$\alpha_*{:}\,H^1(K,S)\longrightarrow H^1(K,T)$$

are m-periodic. But both groups are p-groups, since S and T are split by a p-extension. Therefore, α_* is an isomorphism.

Thus, the homomorphism $\alpha\colon S\to T$ induces an isomorphism of functors

$$S\text{-}\mathit{torsors} \xrightarrow{\sim} T\text{-}\mathit{torsors}.$$

It follows that $\mathrm{ed}(S)=\mathrm{ed}(T)$. The surjection $P\to\mathrm{Im}(\nu)$ yields a generically free representation of T by [10, Lemma 3.3]. Hence, by [3, Proposition 4.11] and (3.2), we have

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

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

Let F be a field, Φ be a subgroup of $\mathrm{Ch}_p(F)$ of rank $r\geqslant 2$, $L=F(\Phi)$ 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 (2.4). 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 non-trivial subgroup and $x\in R$ be such that*

$$\varepsilon(n_Hx)\in p^2\mathbb{Z}.$$

Then n_Hx is decomposable.

Proof. If $|H|=p$, then $\varepsilon(x)\in p\mathbb{Z}$ and hence n_Hx is decomposable. Otherwise we have $H=H'\times H''$ for non-trivial subgroups H' and H''. As $n_H=n_{H'}n_{H''}$, the element n_H, and therefore n_Hx, 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

$$yz-\varepsilon(yz)=(\varepsilon(y)v+\varepsilon(z)u)+uv\in pI+I^2.$$ □

Consider the sequence of subgroups $V_k\subset\bar{J}$ as in (3.1) with respect to the algebraic torus U^Φ. If $x\in J$, we write $\bar{x}$ for the class of x in $\bar{J}$. The classes $\overline{\sigma_i-1}$ and $\overline{p^s}$ form a basis for $\bar{J}$. Hence, $\mathrm{rank}(\bar{J})=r+1$.

LEMMA 3.4. *The group V_k is generated by*

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

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

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

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

LEMMA 3.6. *If $s\geqslant 2$ and $r-s\leqslant k\leqslant r-1$, then* $\dim(V_k)=1$.

Proof. By Lemma 3.4, V_k is generated by $\overline{n_H x}$ with H non-trivial and $\varepsilon(n_H x)\in p^s\mathbb{Z}$. As $s\geqslant 2$, 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 $\bar{p}$. By Lemma 3.4 (2), V_{r-1} is generated by $\bar{n}_H$ with $|H|\geqslant p$. If $|H|\geqslant p^2$ then, by Lemma 3.2, n_H is decomposable and, in view of Lemma 3.3, $\bar{n}_H=\overline{\varepsilon(n_H)}=0$.

Suppose that $|H|=p$ 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 $\varepsilon(m)=\frac{1}{2}p(p-1)$. As p is odd, $\varepsilon(m)\in p\mathbb{Z}$. Hence, $m\in pR+I$, and therefore $n_H-p\in pI+I^2$ and $\bar{n}_H=\bar{p}$ in $\bar{J}$. □

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

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

PROPOSITION 3.9. *We have*

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

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

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

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

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

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

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

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

Again by Theorem 3.1,

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

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

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

$$\nu(x_1,\dots,x_r,\bar{y})=\sum_{i=1}^{r}(\sigma_i-1)x_i+n_Hy.$$

Note that the element n_Hy is independent of the choice of the representative $y\in\mathbb{Z}[G]$ of $\bar{y}$. The image of ϱ contains I and n_H. Since $n_H\equiv p^s$ modulo I, we have $p^s\in\mathrm{Im}(\varrho)$, and hence ϱ is surjective. Note that $e_{ij}=(\sigma_i-1)e_j-(\sigma_j-1)e_i\in\mathrm{Ker}(\varrho)$. As $\sigma e_{ij}\neq e_{ij}$ for $j\neq i$ and every $\sigma\in G\setminus\{1\}$, the group G acts faithfully on $\mathrm{Ker}(\varrho)$.

Case 2. $p=2$ and $s=1$. Let H_i be the subgroup of G generated by σ_i and let $H=\langle\sigma_1\sigma_2\rangle$. Set

$$P'=\coprod_{i=1}^{r}\mathbb{Z}[G/H_i]\oplus\mathbb{Z}[G/H].$$

We define ϱ by

$$\varrho(\bar{x}_1,\dots,\bar{x}_r,\bar{y})=\sum_{i=1}^{r}(\sigma_i+1)x_i+(\sigma_1\sigma_2+1)y.$$

The image of ϱ contains σ_i+1 and $2=(\sigma_1\sigma_2+1)-\sigma_1(\sigma_2+1)+(\sigma_1+1)$. Hence, ϱ is surjective. Note that we have $h_{ij}:=(\sigma_i+1)e_j-(\sigma_j+1)e_i\in\mathrm{Ker}(\varrho)$. Since $\sigma h_{ij}\neq h_{ij}$ for $i\neq j$ and $\sigma\in G\setminus\langle\sigma_i,\sigma_j\rangle$, the group G acts faithfully on $\mathrm{Ker}(\varrho)$ if $r\geqslant 3$. In fact, G acts trivially on $\mathrm{Ker}(\varrho)$ 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 (3.2) and Proposition 3.9, there is a minimal p-presentation $\nu\colon P\to J$ such that

$$\mathrm{rank}(P)=\begin{cases}(r+1)2^{r-1}, & \text{if } p=2 \text{ and } s=1,\\ rp^r+p^{r-s}, & \text{otherwise.}\end{cases} \tag{3.3}$$

The exact sequence

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

in the bottom row of (2.3) yields an exact sequence

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

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 $\nu'\colon P\to Q$.

Recall that we write $\overline{X}=X/(pX+IX)$ for a G-module X. Since $\overline{\mathbb{Z}^r}\simeq(\mathbb{Z}/p\mathbb{Z})^r\to\overline{Q}$ is the zero map, the natural homomorphism $\overline{Q}\to\bar{J}$ is an isomorphism, and hence ν' is a minimal p-presentation of Q. Note that G is a decomposition group of S^Φ and we have $\dim(S^\Phi)=p^r+r$. By Theorem 3.1, $\mathrm{ed}(S^\Phi)=\mathrm{ed}_p(S^\Phi)=\mathrm{rank}(P)-\dim(S^\Phi)$. Hence, the result follows by (3.3). □

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 be a prime integer different from $\mathrm{char}(F)$ and $\Phi\subset\mathrm{Ch}_p(F)$ be a finite subgroup. For integers $k\geqslant 0$, $s\geqslant 1$ and a field extension K/F, let

$$\mathcal{B}^\Phi_{k,s}(K)=\{\alpha\in\mathrm{Br}(K)\{p\}:\mathrm{ind}(\alpha_{K(\Phi)})\leqslant p^k \text{ and } \exp(\alpha)\leqslant p^s\}. \tag{4.1}$$

We say that two elements α and α' in $\mathcal{B}^\Phi_{k,s}(K)$ are *equivalent* if $\alpha-\alpha'\in\mathrm{Br}(K(\Phi)/K)_{\mathrm{dec}}$. 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 (2.7) and Lemma 2.3,

$$\mathcal{B}^\Phi_{0,s}\simeq U^\Phi\text{-}\mathit{torsors} \quad\text{and}\quad \widetilde{\mathcal{B}}^\Phi_{0,s}\simeq S^\Phi\text{-}\mathit{torsors}. \tag{4.2}$$

Moreover, if $\Phi=0$, then

$$\mathcal{B}^\Phi_{k,s}=\widetilde{\mathcal{B}}^\Phi_{k,s}\simeq \mathit{Alg}_{p^k,p^s}. \tag{4.3}$$

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 $\alpha\in\mathcal{B}^\Phi_{k,s}(E)$, i.e., $\alpha\in\mathrm{Br}(E)\{p\}$ such that $\mathrm{ind}(\alpha_{E(\Phi)})\leqslant p^k$ and $\exp(\alpha)\leqslant p^s$.

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

$$\alpha' := \widehat{\alpha} + (\hat{\eta}_E \cup (x)) \in \mathrm{Br}(E')\{p\}, \tag{4.4}$$

for some $x \in (E')^\times$ such that $v'(x)$ is prime to p. Since $\eta_{E(\Phi')} \neq 0$, it follows from (2.1) applied to the element $\alpha'_{E'(\Phi')}$ over the complete field $E'(\Phi')$ with residue field $E(\Phi')$ that

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

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

In the case the condition $\exp(\alpha) \leqslant p^s$ in (4.1) is dropped, the following result was proved in [9, Proposition 5.2].

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

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

Proof. The proof of [9, Proposition 5.2] still works with the following modification.

Let M/E' be a finite extension of fields of degree prime to p, $M_0 \subset M$ be a subfield over F and $\alpha'_0 \in \mathcal{B}^{\Phi'}_{k+1,s}(M_0)$ be 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 to M_0. It was shown in the proof of [9, Proposition 5.2] that there exist $\alpha_0 \in \mathrm{Br}(N_0)\{p\}$ with $\mathrm{ind}(\alpha_0)_{N_0(\Phi)} \leqslant p^k$, a prime element π_0 in M_0 and $\eta_0 \in \mathrm{Ch}_p(N_0)$ such that

$$(\alpha'_0)_{\widehat{M}_0} = \widehat{\alpha}_0 + (\hat{\eta}_0 \cup (\pi_0)) \quad \text{in } \mathrm{Br}(\widehat{M}_0), \tag{4.5}$$

where $\widehat{M}_0$ is the completion of the field M_0 with respect to the restriction of v on M_0, and

$$\alpha_N - (\alpha_0)_N \in \mathrm{Br}(N(\Phi)/N)_{\mathrm{dec}}. \tag{4.6}$$

By (4.5), we have

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

and 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 (4.6). It follows that

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

4.2. A technical lemma

In this subsection we prove Lemma 4.2, which 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 $\chi_1, \chi_2, ..., \chi_r$, with $r \geqslant 2$, be linearly independent characters in $\mathrm{Ch}_p(F)$ and let $\Phi = \langle \chi_1, \chi_2, ..., \chi_r \rangle$. Let E/F be a field extension such that $\mathrm{rank}(\Phi_E) = r$ and $\alpha \in \mathrm{Br}(E)\{p\}$ be an element that is split by $E(\Phi)$ and is such that $\exp(\alpha) \leqslant p^s$.

Let $E = E_0, E_1, ..., E_r$ be field extensions of F such that, for any $k = 1, 2, ..., r$, 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 $k = 1, 2, ..., r$, 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

$$\alpha_k := \widehat{\alpha}_{k-1} + ((\widehat{\chi}_k)_{E_{k-1}} \cup (x_k)).$$

Let Φ_k be the subgroup of Φ generated by $\chi_{k+1}, ..., \chi_r$. 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 (2.1) applied to the element $(\alpha_k)_{E_k(\Phi_k)}$ over the complete field $E_k(\Phi_k)$ with residue field $E_{k-1}(\Phi_k)$ that

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

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

The following 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 [9, Lemma 5.3].

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 $k = 0, 1, ..., r-1$, any finite extension of fields N/E_k of degree prime to p and any character $\varrho \in \mathrm{Ch}(N)$ of order p^2 such that $p\varrho \in (\Phi_k)_N \setminus (\Phi_{k+1})_N$, we have*

$$\mathrm{ind}(\alpha_k)_{N(\Phi_{k+1}, \varrho)} \geqslant p^k. \tag{4.7}$$

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

constructed $\widetilde{E}_m$ as a finite extension of E_m of degree prime to p, then let $\widetilde{E}_{m+1}$ be an extension of E_{m+1} of degree $[\widetilde{E}_m{:}E_m]$ with residue field $\widetilde{E}_m$. Replacing E_i by $\widetilde{E}_i$ and α_i by $(\alpha_i)_{\widetilde{E}_i}$, 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 $F'{=}F(\chi_r)$, $E'{=}E(\chi_r)$ and $E'_i{=}E_i(\chi_r)$, the sequence of characters $\chi'_i{=}(\chi_i)_{F'}$ and the sequence of elements $\alpha'_i{:=}(\alpha_i)_{E'_i}{\in}\mathrm{Br}(E'_i)$ for $0{\leqslant}i{\leqslant}r{-}1$. Let $\Phi'{=}\langle\chi'_1,\chi'_2,...,\chi'_{r-1}\rangle{\subset}\mathrm{Ch}(F')$, let Φ'_i be the subgroup of Φ' generated by $\chi'_{i+1},...,\chi'_{r-1}$ and let $\varrho'{=}\varrho_{E'_k}$.

We check the conditions of the lemma for the new datum. Let Ψ' be a subgroup of Φ' of index p^2. Then the preimage Ψ of Ψ' under the map $\mathrm{Ch}(F){\to}\mathrm{Ch}(F')$ 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 that $p\varrho'{=}p\varrho_{E'_k}{\in}(\Phi_k)_{E'_k}{=}(\Phi'_k)_{E'_k}$. Suppose that $p\varrho'{\in}(\Phi'_{k+1})_{E'_k}$, i.e., $p\varrho_{E'_k}{=}p\varrho'{=}\eta_{E'_k}$ for some $\eta{\in}(\Phi_{k+1})_{E_k}$. It follows that $p\varrho{-}\eta{\in}\mathrm{Ker}(\mathrm{Ch}(E_k){\to}\mathrm{Ch}(E'_k)){=}\langle(\chi_r)_{E_k}\rangle$, and therefore, $p\varrho{\in}(\Phi_{k+1})_{E_k}$, which is a contradiction. Hence $p\varrho'{\in}(\Phi'_k)_{E'_k}\setminus(\Phi'_{k+1})_{E'_k}$.

By the induction hypothesis, the inequality (4.7) holds for α'_k, i.e,

$$\mathrm{ind}(\alpha'_k)_{E'_k(\Phi'_{k+1},\varrho')}{\geqslant}p^k.$$

Since $(\alpha'_k)_{E'_k(\Phi'_{k+1},\varrho')}{=}(\alpha_k)_{E_k(\Phi_{k+1},\varrho)}$, inequality (4.7) holds for α_k. Therefore, it remains to show that inequality (4.7) holds in the case $k{=}r{-}1$. Note that in this case $p\varrho$ is a non-zero 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., $\varrho{=}\hat{\mu}$ for a character $\mu{\in}\mathrm{Ch}(E_{r-2})$ of order p^2. Note that $p\mu$ is a non-zero multiple of $(\chi_r)_{E_{r-2}}$.

By (2.1), we have

$$\mathrm{ind}(\alpha_{r-2})_{E_{r-2}(\chi_{r-1},\mu)}=\frac{\mathrm{ind}(\alpha_{r-1})_{E_{r-1}(\varrho)}}{p}. \tag{4.8}$$

Consider the fields $F'{=}F(\chi_{r-1})$, $E'{=}E(\chi_{r-1})$ and $E'_i{=}E_i(\chi_{r-1})$, the new sequence of characters $\chi'_1{=}(\chi_1)_{F'},...,\chi'_{r-2}{=}(\chi_{r-2})_{F'},\chi'_{r-1}{=}(\chi_r)_{F'}$, the group of characters

$$\Phi'=\langle\chi'_1,\chi'_2,...,\chi'_{r-1}\rangle,$$

the elements $\alpha'_i{\in}\mathrm{Br}(E'_i)$, $0{\leqslant}i{\leqslant}r{-}1$, defined by $\alpha'_i{=}(\alpha_i)_{E'_i}$ for $i{\leqslant}r{-}2$ and

$$\alpha'_{r-1}=\widehat{\alpha}_{r-2}{+}(\widehat{\chi}_r{\cup}(x_{r-1}))$$

over E'_{r-1}, and the character μ. The new datum satisfies the conditions of the lemma. By the induction hypothesis, the inequality (4.7) holds for α'_{r-2}, i.e,

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

Since $(\alpha'_{r-2})_{E'_{r-2}(\mu)}=(\alpha_{r-2})_{E_{r-2}(\chi_{r-1},\mu)}$, inequality (4.7) holds for α_{r-1} in view of equality (4.8).

Case 2. The character ϱ is ramified. Assume that inequality (4.7) does not hold for α_{r-1}, i.e., we have

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

By [9, 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

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

By descending induction on $0\leqslant j\leqslant r-2$, 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

$$\operatorname{ind}(\alpha_j-(\chi_{r-1}\cup(u_j^{1/p})))_{E_j(\Theta_j)}\leqslant p^j, \tag{4.9}$$

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, and hence $v_j(u_j)$ is divisible by p. Modifying u_j by a p^2-th power, we may assume that $u_j=vx_j^{mp}$ for a unit $v\in E_j$ and an integer m. Then

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

where $\eta=\chi_j-m\chi_{r-1}$ and $\beta=(\alpha_{j-1}-(\chi_{r-1}\cup(u_{j-1}^{1/p})))_{E_{j-1}(\Theta_j)}$, with $u_{j-1}=\bar{v}$. 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 (2.1) and the induction hypothesis that

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

This completes the induction step.

Applying inequality (4.9) in the case $j=0$, we have

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

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

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

As $\chi_r\notin\Psi_0$, the field $E(\Psi_0)(w^{1/p})=E(\Psi_0)(\chi_r)$ is a cyclic extension of $E(\Psi_0)$ of degree p. Hence $E(\Psi_0)(w^{1/p^2})/E(\Psi_0)$ is a cyclic extension of degree p^2. Since $\alpha_{E(\Psi_0)}$ is split by the extension $E(\Psi_0)(w^{1/p^2})/E(\Psi_0)$, $\alpha_{E(\Psi_0)}$ is p^2-cyclic. As $[\Phi:\Psi_0]=p^2$, this contradicts the assumption. Hence, the inequality (4.7) holds for α_{r-1}. □

5. Non-cyclicity of the generic element

The aim of this section is the technical Lemma 5.4, which will allow us to later apply 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 §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 let $\alpha\in\mathrm{Br}(K)$. 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 $\beta=(u\pi^i,t\pi^j)_{p^2}$ and write $x=w\pi^k$ for a prime element π, integers i, j and $k=v(x)$, and units u, t and w in E. Then we have

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

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

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

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 pth power in $K^\times$, j is not divisible by p^2. It follows that $\bar{u}\in\langle\bar{a},\bar{t}\rangle$ in $K^\times/(K^\times)^{p^2}$, and then $\bar{u}\in\bar{a}^r\bar{t}^s(K^\times)^{p^2}$ for some r and s. Hence, $\alpha=(\bar{a},\bar{t}^r/\bar{w}^p)_{p^2}$. □

COROLLARY 5.2. *Let x and y be independent variables over F and $a,b\in F^\times$. If $(a,b)_p\neq0$ 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 [7, 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, and 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 $z\in K^\times$, and 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

$$\partial_{v'}\colon H^3(K,\mu_{p^2}^{\otimes 2})\longrightarrow H^2(N,\mu_{p^2})=\mathrm{Br}_{p^2}(N),$$

we find that $e'(a,b)_p=e'(a,b^p)_{p^2}=0$ over N, and 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 $r\geqslant 2$, 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 $\beta\in\mathrm{Br}_p(F'(\Phi)/F')$ 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 and y be independent variables over F and set

$$F':=F(a_1,a_2,\dots,a_r,x,y).$$

For every $1\leqslant i\leqslant r$, 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 elements $b_1,b_2,\dots,b_r$ in F' such that $F(\eta_i)=F(b_i^{1/p})$ for all $1\leqslant i\leqslant r$ 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 $\mathrm{Br}_p(F'(\Phi)/F')$ and $M/F'(\Psi)$ be a field extension of degree prime to p. Since $\partial_v((b_{r-1},b_r)_p)=\bar{b}_{r-1}$ is non-trivial, where v is the discrete valuation on L associated with b_r, 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 $\Phi\subset\mathrm{Ch}_p(F')$ be 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 §2.4. The morphism $\gamma\colon P^\Phi\to V^\Phi$ in the diagram (2.4) is a U^Φ-torsor. Denote by δ the image of the class of γ under the composition

$$H^1_{\text{ét}}(V^\Phi,U^\Phi)\longrightarrow H^1_{\text{ét}}(V^\Phi,(U')^\Phi)\longrightarrow H^2_{\text{ét}}(V^\Phi,\mathbb{G}_m)$$

induced by the diagram (2.5). We write δ_{gen} for the image of δ under the homomorphism

$$H^2_{\text{ét}}(V^\Phi,\mathbb{G}_m)\longrightarrow H^2(F'(V^\Phi),\mathbb{G}_m)=\mathrm{Br}(F'(V^\Phi))$$

induced by the generic point morphism $\mathrm{Spec}(F'(V^\Phi))\to V^\Phi$. It follows from (2.6) that $\delta_{\mathrm{gen}}\in \mathrm{Br}_{p^s}(F'(V^\Phi))$.

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

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

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

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

By [7, Lemma 6.2], there is a non-empty 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 degree $[F'(x):F'(x')]$ prime to p. Let $Z=V^\Phi(\Psi)\setminus W'$. As g is finite, $g(Z)\neq V^\Phi$, and hence the open set $W:=V^\Phi\setminus g(Z)$ is not empty. We have $g^{-1}(W)\subset W'$.

Consider the element $\beta\in\mathrm{Br}_p(F'(\Phi)/F')$ defined 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

$$H^1(F',U^\Phi)\simeq \mathrm{Br}_{p^s}(F'(\Phi)/F')$$

by (2.7). As γ is a generic U^Φ-torsor, there exists an F'-morphism $v\colon \mathrm{Spec}\,F'\to V^\Phi$ such that $v^*(\gamma)=\gamma'$ and $\mathrm{Im}(v)\subset W$ (see §2.3). From the commutativity of the diagram

$$\begin{array}{ccc} H^1_{\text{ét}}(V^\Phi,U^\Phi) & \xrightarrow{v^*} & H^1(F',U^\Phi) \\ \downarrow & & \downarrow \\ H^2_{\text{ét}}(V^\Phi,\mathbb{G}_m) & \xrightarrow{v^*} & H^2(F',\mathbb{G}_m), \end{array}$$

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

Let $v'\colon \mathrm{Spec}\,F'(\Psi)\to V^\Phi(\Psi)$ 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 z in $\mathrm{Im}(v')$ is prime to p. By

[7, Lemma 6.1], there exist a field extension $M'/F'(\Psi)$ of degree prime to p and a field homomorphism $F'(x)\to M'$ extending $F'(z)\to F'(\Psi)$. Therefore, there is a morphism $w\colon \mathrm{Spec}(M')\to X$ (with image $\{x\}$) such that the diagram

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

is commutative. It follows that

$$\beta_{M'} = v^*(\delta)_{M'} = w^*h^*(\delta) = w^*(\chi_0\cup(a_0)) = w^*(\chi_0)\cup w^*(a_0),$$

i.e., $\beta_{M'}$ is p^2-cyclic. This contradicts Lemma 5.3. □

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

Let $n\geqslant 1$ be an integer, m be a divisor of n and p be a prime integer. Let p^r (resp. p^s) be the largest power of p dividing n (resp. m). If $A\in \mathit{Alg}_{n,m}(K)$ for some field extension K/F, then there is a finite extension of fields 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, since it divides m and $\mathrm{ind}(A_E)$, i.e., $A_E\in \mathit{Alg}_{p^r,p^s}(E)$. It follows that the embedding functor $\mathit{Alg}_{p^r,p^s}\to \mathit{Alg}_{n,m}$ is p-surjective, and thus $\mathrm{ed}_p(\mathit{Alg}_{n,m})\leqslant \mathrm{ed}_p(\mathit{Alg}_{p^r,p^s})$ by [7, §1.3]. On the other hand, if $A\in \mathit{Alg}_{n,m}(K)$, then the p-primary component A_p of A satisfies $A_p\in \mathit{Alg}_{p^r,p^s}(K)$. Hence the morphism of functors $\mathit{Alg}_{n,m}\to \mathit{Alg}_{p^r,p^s}$ taking A to A_p is surjective, and therefore $\mathrm{ed}_p(\mathit{Alg}_{n,m})\geqslant \mathrm{ed}_p(\mathit{Alg}_{p^r,p^s})$. We proved that

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

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

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

Proof. By [7, Proposition 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 $\Phi\subset \mathrm{Ch}_p(F)$ be the subgroup in Lemma 5.3 and let V^Φ be the algebraic torus constructed in §2.4. Set $E=F(V^\Phi)$ and let $\alpha:=\delta_{\mathrm{gen}}\in \mathrm{Br}_{p^s}(E(\Phi)/E)$ be the element defined in §5. Let E_k be the fields

and $\alpha_k \in \mathcal{B}_{k,s}^{\Phi_k}(E_k)$ be the elements constructed in §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, and 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

$$\begin{aligned} \mathrm{ed}_p^{\mathit{Alg}_{p^r,p^s}}(\alpha_r) = \mathrm{ed}_p^{\widetilde{\mathcal{B}}_{r,s}^{\Phi_r}}(\alpha_r) &\geqslant \mathrm{ed}_p^{\widetilde{\mathcal{B}}_{r-1,s}^{\Phi_{r-1}}}(\alpha_{r-1}) + 1 \geqslant \ldots \geqslant \mathrm{ed}_p^{\widetilde{\mathcal{B}}_{1,s}^{\Phi_1}}(\alpha_1) + r - 1 \\ &\geqslant \mathrm{ed}_p^{\widetilde{\mathcal{B}}_{0,s}^{\Phi_0}}(\alpha_0) + r = \mathrm{ed}_p^{\widetilde{\mathcal{B}}_{0,s}^{\Phi}}(\alpha) + r. \end{aligned} \tag{6.1}$$

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 $(x,1)$, $S^\Phi \hookrightarrow P^\Phi \times \mathbb{G}_m^r$ is the product of $S^\Phi \hookrightarrow P^\Phi$ and $S^\Phi \twoheadrightarrow \mathbb{G}_m^r$ and $\gamma'(x,t) = \gamma(x)\varkappa(t)^{-1}$ (see diagram (2.4)).

The element α considered in $\mathcal{B}_{0,s}^\Phi(E)$ corresponds to the generic fiber of the U^Φ-torsor γ under the bijection $\mathcal{B}_{0,s}^\Phi(E) \simeq U^\Phi\text{-}\mathit{torsors}(E)$ in (4.2). Hence, by the diagram, the class of α in $\widetilde{\mathcal{B}}_{0,s}^\Phi(E)$ corresponds to the generic fiber γ'_{gen} of the S^Φ-torsor γ' in the diagram under the bijection $\widetilde{\mathcal{B}}_{0,s}^\Phi(E) \simeq S^\Phi\text{-}\mathit{torsors}(E)$. As $P^\Phi \times \mathbb{G}_m^r$ is a quasi-split torus, γ' is a generic S^Φ-torsor by Proposition 2.1, and hence

$$\mathrm{ed}_p^{\widetilde{\mathcal{B}}_{0,s}^\Phi}(\alpha) = \mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(\gamma'_{\mathrm{gen}}) = \mathrm{ed}_p(S^\Phi), \tag{6.2}$$

by [7, Theorem 2.9]. The essential p-dimension of S^Φ was calculated in Corollary 3.11. From (6.1), (6.2) and this corollary, we have

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

This concludes the proof. □

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

LEMMA 7.1. *Let F be a field and p be a prime. Then, for any integers r and s with $1 \leqslant s \leqslant r$,*

$$\mathrm{ed}_p(\mathit{Alg}_{p^r,p^s}) \leqslant \mathrm{ed}_p(\mathit{Alg}_{p^r}) + p^{r-s} - 1.$$

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 $\operatorname{tr}\deg_F(K_0)\leqslant \operatorname{ed}_p(\mathsf{Alg}_{p^r})$ and $A\otimes_K K'\simeq B\otimes_{K_0} K'$.

By [15, Lemma 5.6], $\operatorname{ind}(B^{\otimes p^s})$ 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 $\operatorname{Br}(K_0)$, and consider the *Severi–Brauer variety* $X:=\operatorname{SB}(C)$ of C. Since $\exp(A)$ divides p^s, the algebra C is split over K', and hence $X(K')\neq\varnothing$. This implies that there exists $x\in X$ such that $K_0(x)\subset K'$ and $X(K_0(x))\neq\varnothing$. Therefore, $C_{K_0(x)}$ is split, and hence $\exp(B_{K_0(x)})$ divides p^s, i.e., $B_{K_0(x)}\in \mathsf{Alg}_{p^r,p^s}(K_0(x))$. Since $\dim(X)=p^{r-s}-1$, we have

$$\begin{aligned}\operatorname{ed}_p^{\mathsf{Alg}_{p^r,p^s}}(A)&\leqslant \operatorname{tr}\deg_F(K_0(x))=\operatorname{tr}\deg_F(K_0)+\operatorname{tr}\deg_{K_0}(K_0(x))\\&\leqslant \operatorname{ed}_p(\mathsf{Alg}_{p^r})+\dim(x)\leqslant \operatorname{ed}_p(\mathsf{Alg}_{p^r})+p^{r-s}-1.\end{aligned}$$

□

By [14], we have

$$\operatorname{ed}_p(\mathsf{Alg}_{p^r})\leqslant p^{2r-2}+1,$$

if $r\geqslant 2$ and $\operatorname{char}(F)\neq p$. Therefore, by Lemma 7.1, we have the following upper bound for $\operatorname{ed}_p(\mathsf{Alg}_{p^r,p^s})$.

THEOREM 7.2. *Let F be a field and p be a prime integer different from* $\operatorname{char}(F)$. *Then, for any integers $r\geqslant 2$ and s with $1\leqslant s\leqslant r$,*

$$\operatorname{ed}_p(\mathsf{Alg}_{p^r,p^s})\leqslant p^{2r-2}+p^{r-s}.$$

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 be 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 $\operatorname{Gal}(E/K)\simeq G$.

Let L/F be a Galois field extension with $\operatorname{Gal}(L/F)\simeq G$. Let further $\mathsf{Alg}_{L/F}(K)$ be the subset of $\mathsf{Alg}_G(K)$ consisting of all classes split by the Galois G-algebra KL/K. We have the following 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 isomorphism classes 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 be a prime integer different from* $\mathrm{char}(F)$, *G be an elementary abelian group of order p^r with $r\geqslant 2$ and L/F be a Galois field extension with* $\mathrm{Gal}(L/F)\simeq G$. *Let s be an integer such that $1\leqslant s\leqslant r$. Suppose that $r\geqslant 3$ if $p=2$ and $s=1$. Let $\mathcal{F}$ be one of the three functors $\mathsf{Alg}_{L/F}$, Alg_G and 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 (2.7), 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 $E_r(\Phi)$, and hence $\alpha_r\in\mathsf{Alg}_G(E_r)$. Note that $\mathrm{ed}_p^{\mathcal{B}}(\beta)\leqslant\mathrm{ed}_p^{\mathcal{H}}(\beta)$ for any subfunctor $\mathcal{H}$ of a functor $\mathcal{B}$ and any $\beta\in\mathcal{H}(K)$. Thus, by the proof of Theorem 6.1, we have

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

Let J be the G-module defined in §2.4 and $T:=\mathrm{Spec}\,F[J]$ be the split torus with character group J. Consider the minimal surjective p-presentation $\nu\colon P'\to J$ as in Remark 3.10. As explained in §2.2, a choice of a G-invariant basis for 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 [10, Lemma 3.3] that the action of $T\rtimes G$ on V is generically free in this case. Hence, by [3, Proposition 4.11],

$$\mathrm{ed}(T\rtimes G)\leqslant\dim(V)-\dim(T\rtimes G)=\mathrm{rank}(P')-\mathrm{rank}(J)=\mathrm{rank}(\mathrm{Ker}(\nu))=d_{p,r,s}.$$

Let γ be a G-torsor over F and let L be the corresponding Galois G-algebra over F. As 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}. Since $T_\gamma=R_{L/F}(\mathbb{G}_{m,L})/\mu_{p^s}$, the connecting G-equivariant map

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

is injective for any field extension K/F. Hence the group $G_\gamma(K)=G$ acts trivially on $H^1(K,T_\gamma)$. By (2.2),

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

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

$$\operatorname{ed}_p(\mathit{Alg}_G)\leqslant \operatorname{ed}_p(\mathit{ALG}_G)\leqslant \operatorname{ed}(\mathit{ALG}_G)\leqslant \operatorname{ed}(T\rtimes G)\leqslant d_{p,r,s},$$
$$\operatorname{ed}_p(\mathit{Alg}_G)\leqslant \operatorname{ed}(\mathit{Alg}_G)\leqslant \operatorname{ed}(\mathit{ALG}_G)\leqslant \operatorname{ed}(T\rtimes G)\leqslant d_{p,r,s}.$$ □

Remark 8.2. Suppose that $p=r=2$ and $s=1$, and let F be a field of characteristic different from 2. By [12, Theorem 1] or [2, §2.4], there exists a non-trivial cohomological invariant $\mathit{Alg}_G\to H^4(\cdot,\mathbb{Z}/2\mathbb{Z})$ over $F(i)$, where i is a primitive fourth root of unity. Hence, $\operatorname{ed}_2(\mathit{Alg}_G)\geqslant\operatorname{ed}_2(\mathit{Alg}_G)_{F(i)}\geqslant 4$ by [3, Corollary 3.6] and [11, Lemma 6.9]. Moreover, by the structure theorem on central simple algebras split by a biquadratic field extension [19, Corollary 2.8], every isomorphism class $(A,E)\in\mathit{ALG}_G(K)$ is of the form $E=K(a^{1/2},b^{1/2})$ and $A=(a,x)_2\otimes(b,y)_2$, for some $a,b,x,y\in K^\times$. Hence $\operatorname{ed}(\mathit{ALG}_G)\leqslant 4$. As ALG_G surjects on Alg_G, we have

$$4\leqslant \operatorname{ed}_2(\mathit{Alg}_G)\leqslant \operatorname{ed}_2(\mathit{ALG}_G)\leqslant \operatorname{ed}(\mathit{ALG}_G)\leqslant 4,$$
$$4\leqslant \operatorname{ed}_2(\mathit{Alg}_G)\leqslant \operatorname{ed}(\mathit{Alg}_G)\leqslant \operatorname{ed}(\mathit{ALG}_G)\leqslant 4.$$

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

Corollary 8.3. *Let F be a field of characteristic different from 2. Then*

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

Proof. As any central simple algebra of degree 8 and exponent 2 has a triquadratic splitting field by [13], we have that $\mathit{Alg}_{8,2}=\mathit{Alg}_G$ for the elementary abelian group G of order 8, and hence the statement follows from Theorem 8.1. Note that the inequality $\operatorname{ed}_2(\mathit{Alg}_{8,2})\geqslant 8$ is also proven in Theorem 6.1, while the opposite inequality $\operatorname{ed}(\mathit{Alg}_{8,2})\leqslant 8$ was shown in [2, Theorem 2.12]. □

References

[1] Amitsur, S. A., Rowen, L. H. & Tignol, J.-P., Division algebras of degree 4 and 8 with involution. *Israel J. Math.*, 33 (1979), 133–148.

[2] Baek, S. & Merkurjev, A., Invariants of simple algebras. *Manuscripta Math.*, 129 (2009), 409–421.

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

[4] Garibaldi, S., Merkurjev, A. & Serre, J.-P., *Cohomological Invariants in Galois Cohomology*. University Lecture Series, 28. Amer. Math. Soc., Providence, RI, 2003.

[5] KNUS, M. A., MERKURJEV, A., ROST, M. & TIGNOL, J.-P., *The Book of Involutions*. American Mathematical Society Colloquium Publications, 44. Amer. Math. Soc., Providence, RI, 1998.
[6] LÖTSCHER, R., MACDONALD, M., MEYER, A. & REICHSTEIN, Z., Essential dimension of algebraic tori. To appear in *J. Reine Angew. Math.*
[7] MERKURJEV, A. S., Essential dimension, in *Quadratic Forms—Algebra, Arithmetic, and Geometry*, Contemp. Math., 493, pp. 299–325. Amer. Math. Soc., Providence, RI, 2009.
[8] — Essential p-dimension of $\mathrm{PGL}(p^2)$. *J. Amer. Math. Soc.*, 23 (2010), 693–712.
[9] — A lower bound on the essential dimension of simple algebras. *Algebra Number Theory*, 4 (2010), 1055–1076.
[10] MEYER, A. & REICHSTEIN, Z., The essential dimension of the normalizer of a maximal torus in the projective linear group. *Algebra Number Theory*, 3 (2009), 467–487.
[11] REICHSTEIN, Z. & YOUSSIN, B., Essential dimensions of algebraic groups and a resolution theorem for G-varieties. *Canad. J. Math.*, 52 (2000), 1018–1056.
[12] ROST, M., SERRE, J.-P. & TIGNOL, J.-P., La forme trace d'une algèbre simple centrale de degré 4. *C. R. Math. Acad. Sci. Paris*, 342 (2006), 83–87.
[13] ROWEN, L. H., Central simple algebras. *Israel J. Math.*, 29 (1978), 285–301.
[14] RUOZZI, A., Essential p-dimension of PGL_n. *J. Algebra*, 328 (2011), 488–494.
[15] SALTMAN, D. J., *Lectures on Division Algebras*. CBMS Regional Conference Series in Mathematics, 94. Amer. Math. Soc., Providence, RI, 1999.
[16] SERRE, J.-P., *Local Fields*. Graduate Texts in Mathematics, 67. Springer, New York, 1979.
[17] — *Galois Cohomology*. Springer, Berlin–Heidelberg, 1997.
[18] TIGNOL, J.-P., Sur les classes de similitude de corps à involution de degré 8. *C. R. Acad. Sci. Paris Sér. A-B*, 286 (1978), A875–A876.
[19] — Corps à involution neutralisés par une extension abélienne élémentaire, in *The Brauer Group* (Les Plans-sur-Bex, 1980), Lecture Notes in Math., 844, pp. 1–34. Springer, Berlin–Heidelberg, 1981.
[20] — Algèbres indécomposables d'exposant premier. *Adv. in Math.*, 65 (1987), 205–228.

SANGHOON BAEK
Department of Mathematical Sciences
Korea Advanced Institute of Science and Technology
291 Daehak-ro, Yuseong-gu
Daejeon 305-701
Republic of Korea
sanghoonbaek@kaist.ac.kr

ALEXANDER S. MERKURJEV
Department of Mathematics
University of California, Los Angeles
Los Angeles, CA 90095-1555
U.S.A.
merkurev@math.ucla.edu

Received March 4, 2010
Received in revised form July 5, 2010