Algebra & Number Theory

Volume 4
2010
No. 8

A lower bound on the essential dimension of simple algebras

Alexander S. Merkurjev

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 4:8(2010)

A lower bound on the essential dimension of simple algebras

Alexander S. Merkurjev

Let p be a prime integer and F a field of characteristic different from p. We prove that the essential p-dimension $\mathrm{ed}_p\big(\mathsf{CSA}(p^r)\big)$ of the class $\mathsf{CSA}(p^r)$ of central simple algebras of degree p^r is at least $(r-1)p^r+1$. The integer $\mathrm{ed}_p\big(\mathsf{CSA}(p^r)\big)$ measures complexity of the class of central simple algebras of degree p^r over field extensions of F.

1. Introduction

The essential dimension of an *algebraic structure* is a numerical invariant that measures its complexity. Informally, the essential dimension of an algebraic structure over a field F is the smallest number of algebraically independent parameters required to define the structure over a field extension of F [Berhuy and Favi 2003; Merkurjev 2009].

Let $\mathcal{F} : \mathit{Fields}/F \to \mathit{Sets}$ be a functor (an algebraic structure) from the category Fields/F of field extensions of F and field homomorphisms over F to the category of sets. Let $K \in \mathit{Fields}/F$, $\alpha \in \mathcal{F}(K)$, and K_0 be a subfield of K over F. We say that α is *defined over* K_0 (and K_0 is called a *field of definition of* α) if there exists an element $\alpha_0 \in \mathcal{F}(K_0)$ such that the image $(\alpha_0)_K$ of α_0 under the map $\mathcal{F}(K_0) \to \mathcal{F}(K)$ coincides with α. The *essential dimension of* α, denoted $\mathrm{ed}^{\mathcal{F}}(\alpha)$, is the least transcendence degree $\mathrm{tr.deg}_F(K_0)$ over all fields of definition K_0 of α. The *essential dimension of the functor* $\mathcal{F}$ is

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

where the supremum is taken over fields $K \in \mathit{Fields}/F$ and all $\alpha \in \mathcal{F}(K)$.

Let p be a prime integer and $\alpha \in \mathcal{F}(K)$. The *essential p-dimension* $\mathrm{ed}_p^{\mathcal{F}}(\alpha)$ *of* α is the minimum of $\mathrm{ed}^{\mathcal{F}}(\alpha_{K'})$ over all finite field extensions K'/K of degree prime to p. The *essential p-dimension* $\mathrm{ed}_p(\mathcal{F})$ *of* $\mathcal{F}$ is the supremum of $\mathrm{ed}_p^{\mathcal{F}}(\alpha)$ over all

The work has been supported by the NSF grant DMS #0652316.
MSC2000: primary 16K50; secondary 14L30, 20G15.
Keywords: essential dimension, Brauer group, algebraic tori.

fields $K \in \mathit{Fields}/F$ and all $\alpha \in \mathcal{F}(K)$ [Reichstein and Youssin 2000, §6]. Clearly, $\mathrm{ed}^{\mathcal{F}}(\alpha) \geq \mathrm{ed}^{\mathcal{F}}_p(\alpha)$ and $\mathrm{ed}(\mathcal{F}) \geq \mathrm{ed}_p(\mathcal{F})$ for all p.

Let $\mathit{CSA}(n)$ be the functor taking a field extension K/F to the set of isomorphism classes $\mathit{CSA}_K(n)$ of central simple K-algebras of degree n. Let p be a prime integer and let p^r be the highest power of p dividing n. Then $\mathrm{ed}_p\big(\mathit{CSA}(n)\big) = \mathrm{ed}_p\big(\mathit{CSA}(p^r)\big)$ [Reichstein and Youssin 2000, Lemma 8.5.5]. Every central simple algebra of degree p is cyclic over a finite field extension of degree prime to p, and hence $\mathrm{ed}_p\big(\mathit{CSA}(p)\big) = 2$ [Reichstein and Youssin 2000, Lemma 8.5.7]. It was proven in [Merkurjev 2010] that $\mathrm{ed}_p\big(\mathit{CSA}(p^2)\big) = p^2 + 1$ and in general, $2p^{2r-2} - p^r + 1 \geq \mathrm{ed}_p\big(\mathit{CSA}(p^r)\big) \geq 2r$ for all $r \geq 2$ [Meyer and Reichstein 2009b, Theorem 1; Reichstein and Youssin 2000, Theorem 8.6].

We improve the lower bound for $\mathrm{ed}_p\big(\mathit{CSA}(p^r)\big)$ as follows:

Theorem 6.1. *Let F be a field and p a prime integer different from* $\mathrm{char}(F)$. *Then*

$$\mathrm{ed}_p\big(\mathit{CSA}(p^r)\big) \geq (r-1)p^r + 1.$$

Let G be an algebraic group over F. The *essential dimension* $\mathrm{ed}(G)$ (resp. *essential p-dimension* $\mathrm{ed}_p(G)$) of G is the essential dimension (resp. essential p-dimension) of the functor $G\text{-}\mathit{torsors}$ taking a field K to the set of isomorphism classes of all G-torsors (principal homogeneous G-spaces) over K.

If $G = \mathbf{PGL}(n)$ is the projective linear group over F, the functor $G\text{-}\mathit{torsors}$ is isomorphic to the functor $\mathit{CSA}(n)$. Therefore, the theorem yields the following lower bound for the essential dimension of $\mathbf{PGL}(p^r)$:

$$\mathrm{ed}\big(\mathbf{PGL}(p^r)\big) \geq \mathrm{ed}_p\big(\mathbf{PGL}(p^r)\big) \geq (r-1)p^r + 1.$$

2. Preliminaries

Characters. Let F be a field, let F_{sep} be a separable closure of F, and let

$$\Gamma = \mathrm{Gal}(F_{\mathrm{sep}}/F)$$

be the *absolute Galois group* of F. For a Γ-module M, we write $H^n(F, M)$ for the cohomology group $H^n(\Gamma, M)$.

The *character group* $\mathrm{Ch}(F)$ of F is defined as

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

For a character $\chi \in \mathrm{Ch}(F)$, set $F(\chi) = (F_{\mathrm{sep}})^{\mathrm{Ker}(\chi)}$. Then $F(\chi)/F$ is a cyclic field extension of degree $\mathrm{ord}(\chi)$. If $\Phi \subset \mathrm{Ch}(F)$ is a finite subgroup, we set

$$F(\Phi) = (F_{\mathrm{sep}})^{\cap \mathrm{Ker}(\chi)},$$

where the intersection is taken over all $\chi \in \Phi$. The Galois group $G = \mathrm{Gal}(F(\Phi)/F)$ is abelian and Φ is canonically isomorphic to the character group $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ of G.

If $F' \subset F$ is a subfield and $\chi \in \mathrm{Ch}(F')$, we write χ_F for the image of χ under the natural map $\mathrm{Ch}(F') \to \mathrm{Ch}(F)$ and $F(\chi)$ for $F(\chi_F)$. If $\Phi \subset \mathrm{Ch}(F)$ is a finite subgroup, then the character $\chi_{F(\Phi)}$ is trivial if and only if $\chi \in \Phi$.

Lemma 2.1. *Let $\Phi, \Phi' \subset \mathrm{Ch}(F)$ be two finite subgroups. Suppose that for a field extension K/F, we have $\Phi_K = \Phi'_K$ in $\mathrm{Ch}(K)$. Then there is a finite subextension K'/F in K/F such that $\Phi_{K'} = \Phi'_{K'}$ in $\mathrm{Ch}(K')$.*

Proof. Choose a set of characters $\{\chi_1, \dots, \chi_m\}$ generating Φ and a set of characters $\{\chi'_1, \dots, \chi'_m\}$ generating Φ' such that $(\chi_i)_K = (\chi'_i)_K$ for all i. Let $\eta_i = \chi_i - \chi'_i$. Since all η_i vanish over K, the finite field extension $K' := F(\eta_1, \dots, \eta_m)$ of F can be viewed as a subextension in K/F. Now $\Phi_{K'} = \Phi'_{K'}$ since $(\chi_i)_{K'} = (\chi'_i)_{K'}$. □

Brauer groups. We write $\mathrm{Br}(F)$ for the *Brauer group* $H^2(F, F_{\mathrm{sep}}^\times)$ of a field F. If $a \in \mathrm{Br}(F)$ and K/F is a field extension, then we write a_K for the image of a under the natural homomorphism $\mathrm{Br}(F) \to \mathrm{Br}(K)$. We write $\mathrm{Br}(K/F)$ for the *relative Brauer group* $\mathrm{Ker}\big(\mathrm{Br}(F) \to \mathrm{Br}(K)\big)$. We say that K is a splitting field of a if $a_K = 0$, that is, $a \in \mathrm{Br}(K/F)$. The *index* $\mathrm{ind}(a)$ of a is the smallest degree of a splitting field of a.

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 $\chi \otimes a$ to the class $\chi \cup (a)$ in $\mathrm{Br}(F)$ that is split by $F(\chi)$.

For a finite subgroup $\Phi \subset \mathrm{Ch}(F)$, write $\mathrm{Br}_{\mathrm{dec}}\big(F(\Phi)/F\big)$ 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* $\mathrm{Br}_{\mathrm{ind}}\big(F(\Phi)/F\big)$ is the factor group $\mathrm{Br}\big(F(\Phi)/F\big) / \mathrm{Br}_{\mathrm{dec}}\big(F(\Phi)/F\big)$.

Complete fields. Let E be a complete field with respect to a discrete valuation v, and let 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 $\hat{\chi}$ for the corresponding character in $\mathrm{Ch}(E)\{p\}$.

By [Garibaldi et al. 2003, §7.9], there is an exact sequence

$$0 \to \mathrm{Br}(K)\{p\} \xrightarrow{i} \mathrm{Br}(E)\{p\} \xrightarrow{\partial_v} \mathrm{Ch}(K)\{p\} \to 0. \tag{2-1}$$

If $a \in \mathrm{Br}(K)\{p\}$, we write $\hat{a}$ for the element $i(a)$ in $\mathrm{Br}(E)\{p\}$. For example, if $a = \chi \cup (\bar{u})$ for some $\chi \in \mathrm{Ch}(K)\{p\}$ and a unit $u \in E$, then $\hat{a} = \hat{\chi} \cup (u)$.

Proposition 2.2 [Tignol 1978, Proposition 2.4; Jacob and Wadsworth 1990, Theorem 5.15(a); Garibaldi et al. 2003, Proposition 8.2]. *Let E be a complete field with respect to a discrete valuation v, and let K be its residue field of characteristic different from p. Then*:

(i) $\mathrm{ind}(\hat{a}) = \mathrm{ind}(a)$ *for any* $a \in \mathrm{Br}(K)\{p\}$.

(ii) *Let* $b = \hat{a} + \big(\hat{\chi} \cup (x)\big)$ *for an element* $a \in \mathrm{Br}(K)\{p\}$, $\chi \in \mathrm{Ch}(K)\{p\}$ *and* $x \in E^\times$. *Then* $\partial_v(b) = v(x)\chi$. *Also, if $v(x)$ is not divisible by p, we have*

$$\mathrm{ind}(b) = \mathrm{ind}(a_{K(\chi)}) \cdot \mathrm{ord}(\chi).$$

(iii) *Let E'/E be a finite field extension and v' the discrete valuation on E' extending v with residue field K'. Then for any* $b \in \mathrm{Br}(E)\{p\}$, *we have*

$$\partial_{v'}(b_{E'}) = e \cdot \partial_v(b)_{K'},$$

where e is the ramification index of E'/E.

The choice of a prime element π in E provides us with a splitting of the sequence (2-1) by sending a character χ to the class $\hat{\chi} \cup (\pi)$ in $\mathrm{Br}(E)\{p\}$. Thus, any $b \in \mathrm{Br}(E)\{p\}$ can be written in the form

$$b = \hat{a} + \big(\hat{\chi} \cup (\pi)\big), \tag{2-2}$$

for $\chi = \partial_v(b)$ and a unique $a \in \mathrm{Br}(K)\{p\}$.

The homomorphism

$$s_\pi : \mathrm{Br}(E)\{p\} \to \mathrm{Br}(K)\{p\},$$

defined by $s_\pi(b) = a$, where a is given by (2-2), is called a *specialization* map. For example, $s_\pi(\hat{a}) = a$ for any $a \in \mathrm{Br}(K)\{p\}$ and $s_\pi\big(\hat{\chi} \cup (x)\big) = \chi \cup (\bar{u})$, where $\chi \in \mathrm{Ch}(K)\{p\}$, $x \in E^\times$ and u is the unit in E such that $x = u\pi^{v(x)}$.

If v is trivial on a subfield $F \subset E$ and $\Phi \subset \mathrm{Ch}(F)\{p\}$ a finite subgroup, then

$$s_\pi\big(\mathrm{Br}_{\mathrm{dec}}(E(\Phi)/E)\big) \subset \mathrm{Br}_{\mathrm{dec}}\big(K(\Phi)/K\big). \tag{2-3}$$

We shall need the following technical lemma. For an abelian group A we write ${}_pA$ for the subgroup of all elements in A of exponent dividing p.

Lemma 2.3. *Let (E, v) be a complete discrete valued field with the residue field K of characteristic different from p containing a primitive p^2-th root of unity. Let $\eta \in \mathrm{Ch}(E)$ be a character of order p^2 such that $p \cdot \eta$ is unramified, that is, $p \cdot \eta = \hat{\nu}$ for some $\nu \in \mathrm{Ch}(K)$ of order p. Let $\chi \in {}_p\mathrm{Ch}(K)$ be a character linearly independent from ν. Let $a \in \mathrm{Br}(K)$ and set $b = \hat{a} + \big(\hat{\chi} \cup (x)\big) \in \mathrm{Br}(E)$, where $x \in E^\times$ is an element such that $v(x)$ is not divisible by p. Then*:

(i) *If η is unramified, that is, $\eta = \hat{\mu}$ for some $\mu \in \mathrm{Ch}(K)$ of order p^2, then* $\mathrm{ind}(b_{E(\eta)}) = p \cdot \mathrm{ind}(a_{K(\mu,\chi)})$.

(ii) *If η is ramified, then there exists a unit $u \in E^\times$ such that $K(\nu) = K(\bar{u}^{1/p})$ and* $\mathrm{ind}(b_{E(\eta)}) = \mathrm{ind}\big(a - (\chi \cup (\bar{u}^{1/p}))\big)_{K(\nu)}$.

Proof. (i) If $\eta = \hat{\mu}$ for some $\mu \in \mathrm{Ch}(K)$, then $K(\mu)$ is the residue field of $E(\eta)$ and we have

$$b_{E(\eta)} = \hat{a}_{K(\mu)} + \big(\hat{\chi}_{K(\mu)} \cup (x)\big).$$

Since χ and ν are linearly independent, the character $\chi_{K(\mu)}$ is nontrivial. The first statement follows from Proposition 2.2(ii).

(ii) Since $p \cdot \eta$ is unramified, the ramification index of $E(\eta)/E$ is equal to p, and hence $E(\eta) = E\big((ux^p)^{1/p^2}\big)$ for some unit $u \in E$. Note that $K(\nu) = K(\bar{u}^{1/p})$ is the residue field of $E(\eta)$. Since $u^{1/p}x$ is a pth power in $E(\eta)$, the class

$$b_{E(\eta)} = \hat{a}_{K(\nu)} - \big(\hat{\chi}_{K(\nu)} \cup (u^{1/p})\big) = \hat{a}_{K(\nu)} - \big(\widehat{\chi_{K(\nu)} \cup (\bar{u}^{1/p})}\big)$$

is unramified. It follows from Proposition 2.2(i) that the elements $b_{E(\eta)}$ in $\mathrm{Br}\big(E(\eta)\big)$ and $a_{K(\nu)} - \big(\chi_{K(\nu)} \cup (\bar{u}^{1/p})\big)$ in $\mathrm{Br}\big(K(\nu)\big)$ have the same indices. □

3. Brauer group and algebraic tori

Torsors. Let G be an algebraic group over F and let K/F be a field extension. The set of isomorphism classes of G-torsors (principal homogeneous spaces) over K is bijective to $H^1(K, G)$ [Serre 1997].

Example 3.1. Let A be a central simple F-algebra of degree n and $G = \mathbf{Aut}(A)$. Then $H^1(K, G)$ is the set of isomorphism classes of central simple K-algebras of degree n, or equivalently, the set of elements in $\mathrm{Br}(K)$ of index dividing n. If $A = M_n(F)$ is the split algebra, then $G = \mathbf{PGL}(n)$.

Example 3.2. Let L be an étale F-algebra of dimension n. Consider the algebraic torus $U = R_{L/F}(\mathbb{G}_{m,L})/\,\mathbb{G}_m$ over F. The exact sequence

$$1 \to \mathbb{G}_m \to R_{L/F}(\mathbb{G}_{m,L}) \to U \to 1$$

and Hilbert Theorem 90 yield an isomorphism $\theta : H^1(F, U) \xrightarrow{\sim} \mathrm{Br}(L/F)$. Note that if L is a subalgebra of a central simple F-algebra A of degree n, then U is a maximal torus in the group $\mathbf{Aut}(A)$.

Let $\alpha : G \to \mathbf{GL}(W)$ be a finite dimensional representation over F. Suppose that α is *generically free*, that is, there is a nonempty open subset $W' \subset W$ and a G-torsor $\beta : W' \to X$ for a variety X over F. The torsor β is *versal*, that is, every G-torsor over a field extension K/F is the pull-back of β with respect to a K-point of X. The generic fiber of β is called a *generic* G-torsor. It is a torsor over the function field $F(X)$ [Garibaldi et al. 2003; Reichstein 2000].

Example 3.3. Let S be an algebraic torus over F. We embed S into the quasitrivial torus $P = R_{L/F}(\mathbb{G}_{m,L})$, where L is an étale F-algebra [Colliot-Thélène and Sansuc 1977]. Then S acts on the vector space L by multiplication, so that the action on the open subset P is regular. If T is the factor torus P/S, then the S-torsor $P \to T$ is versal.

The tori P^Φ, S^Φ, T^Φ, U^Φ and V^Φ. Let F be a field, Φ be a subgroup of ${}_p\operatorname{Ch}(F)$ of rank r, and $L = F(\Phi)$. Let $G = \operatorname{Gal}(L/F)$. Choose a basis $\chi_1, \chi_2, \dots, \chi_r$ for Φ. We can view each χ_i as a character of G, that is, as a homomorphism $\chi_i : G \to \mathbb{Q}/\mathbb{Z}$. Let $\sigma_1, \sigma_2, \dots, \sigma_r$ be the dual basis for G, that is,

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

Let R be the group ring $\mathbb{Z}[G]$. Consider the surjective homomorphism of G-modules $k : R^r \to R$ taking the ith basis element e_i of R^r to $\sigma_i - 1$. The image of k is the *augmentation ideal* $I = \operatorname{Ker}(\varepsilon)$ in R, where $\varepsilon : R \to \mathbb{Z}$ is defined by $\varepsilon(\rho) = 1$ for all $\rho \in G$.

Write $N_i = 1 + \sigma_i + \sigma_i^2 + \dots + \sigma_i^{p-1} \in R$.

Set $N := \operatorname{Ker}(k)$. Consider the following elements in N:

$$e_{ij} := (\sigma_i - 1)e_j - (\sigma_j - 1)e_i \quad \text{and} \quad f_i = N_i e_i, \quad i, j = 1, \dots r.$$

Lemma 3.4. *The G-module N is generated by e_{ij} and f_i.*

Proof. Let $\overline{R} = \mathbb{Z}[t_1, \dots, t_r]$ be the polynomial ring. Acyclicity of the Koszul complex for the homomorphism $\bar{k} : (\overline{R})^r \to \overline{R}$, taking the ith basis element $\bar{e}_i$ to $t_i - 1$ [Matsumura 1980, Theorem 43] implies that $\operatorname{Ker}(\bar{k})$ is generated by $\bar{e}_{ij} := (t_i - 1)\bar{e}_j - (t_j - 1)\bar{e}_i$.

The kernel J of the surjective homomorphism $\overline{R} \to R$, taking t_i to σ_i, is generated by $t_i^p - 1$.

Let $x := \sum x_i e_i \in \operatorname{Ker}(k)$. Lift every x_i to a polynomial $\bar{x}_i \in \overline{R}$ and consider $\bar{x} := \sum \bar{x}_i \bar{e}_i \in (\overline{R})^r$. We have $\bar{k}(\bar{x}) \in J$, and hence

$$\bar{k}(\bar{x}) = \sum (t_i - 1)\bar{x}_i = \sum (t_i^p - 1)h_i = \sum (t_i - 1)\overline{N}_i h_i,$$

for some polynomials $h_i \in \overline{R}$, where $\overline{N}_i = 1 + t_i + t_i^2 + \dots + t_i^{p-1} \in R$. Hence the element $\sum (\bar{x}_i - h_i \overline{N}_i)\bar{e}_i$ belongs to the kernel of $\bar{k}$ and therefore is a linear combination of $\bar{e}_{ij}$. It follows that $\bar{x}$ is a linear combination of $\bar{e}_{ij}$ and $\overline{N}_i \bar{e}_i$, and hence x is a linear combination of e_{ij} and f_i. □

Let $\varepsilon_i : R^r \to \mathbb{Z}$ be the ith projection followed by the augmentation map ε. It follows from Lemma 3.4 that $\varepsilon_i(N) = p\mathbb{Z}$ for every i. Moreover, the G-homomorphism

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

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

Lemma 3.5. *The G-module M is generated by e_{ij}.*

Proof. Let M' be the submodule of N generated by e_{ij}. Clearly, $M' \subset M$. Note also that $(\sigma_j - 1) f_i = N_i e_{ij} \in M'$, and hence $I f_i \subset M'$.

Suppose that $m \in M$. By Lemma 3.4, modifying m by an element in M', we can assume that $m = \sum_{i=1}^r x_i f_i$ for some $x_i \in R$. Since $l(m) = 0$, we have $\varepsilon(x_i) = 0$, that is, $x_i \in I$ for all i, and hence $m \in \sum I f_i \subset M'$. □

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, Q, M, I and N, respectively. The diagram of homomorphisms of G-modules with exact columns and rows

$$\begin{tikzcd} M \arrow[r, equal] \arrow[d, hook] & M \arrow[d, hook] & \\ N \arrow[r, hook] \arrow[d, two heads, "l"'] & R^r \arrow[r, two heads, "k"] \arrow[d, two heads] & I \arrow[d, equal] \\ \mathbb{Z}^r \arrow[r, hook] & Q \arrow[r, two heads] & I \end{tikzcd} \tag{3-1}$$

yields the following diagram of homomorphisms of the tori:

$$\begin{tikzcd} U^\Phi \arrow[r, hook] \arrow[d, equal] & S^\Phi \arrow[r, two heads] \arrow[d, hook] & \mathbb{G}_m^r \arrow[d, hook] \\ U^\Phi \arrow[r, hook] & P^\Phi \arrow[r, two heads] \arrow[d, two heads] & V^\Phi \arrow[d, two heads] \\ & T^\Phi \arrow[r, equal] & T^\Phi \end{tikzcd} \tag{3-2}$$

Let K/F be a field extension. Set $KL := K \otimes_F L$. The exact sequence of G-modules

$$0 \to I \to R \to \mathbb{Z} \to 0 \tag{3-3}$$

gives an exact sequence of the tori

$$1 \to \mathbb{G}_m \to R_{L/F}(\mathbb{G}_{m,L}) \to U \to 1,$$

and then an exact sequence

$$0 \to H^1(K, U^\Phi) \to H^2(K, \mathbb{G}_m) \to H^2(KL, \mathbb{G}_m).$$

Hence

$$H^1(K, U^\Phi) \simeq \mathrm{Br}(KL/K). \tag{3-4}$$

Lemma 3.6. *The homomorphism $(K^\times)^r \to H^1(K, U^\Phi) \simeq \mathrm{Br}(KL/K)$ induced by the first row of the diagram (3-2) takes $(x_1, \dots, x_r)$ to $\sum_{i=1}^r \big((\chi_i)_K \cup (x_i)\big)$.*

Proof. Consider the composition

$$h : \mathrm{Hom}_G(\mathbb{Z}^r, \mathbb{Z}) \to \mathrm{Ext}^1_G(I, \mathbb{Z}) \to \mathrm{Ext}^2_G(\mathbb{Z}, \mathbb{Z}) = H^2(G, \mathbb{Z}) = \mathrm{Ch}(G), \tag{3-5}$$

where the first homomorphism is induced by the bottom row of the diagram (3-1), and the second one by the exact sequence (3-3).

We claim that for any k, the image of the kth projection $p_k : \mathbb{Z}^r \to \mathbb{Z}$ under the composition (3-5) coincides with χ_k. Consider the G-homomorphism $R^r \to \mathbb{Q}$, taking e_k to $1/p$ and e_i to 0 for all $i \neq k$. By Lemma 3.5, this homomorphism vanishes on M, and hence it factors through a map $Q \to \mathbb{Q}$. Thus, we have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}^r \arrow[r] \arrow[d, "p_k"'] & Q \arrow[r] \arrow[d] & I \arrow[r] \arrow[d, "f_k"'] & 0 \\ 0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Q} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \end{tikzcd} \tag{3-6}$$

for the map f_k defined by $f_k(\sigma_k - 1) = 1/p + \mathbb{Z}$ and $f_k(\sigma_i - 1) = 0$ for all $i \neq k$.

Let α be the image of the class of the top row of (3-6) under the map $p_k^* : \mathrm{Ext}^1_G(I, \mathbb{Z}^r) \to \mathrm{Ext}^1_G(I, \mathbb{Z})$. Then $h(p_k)$ is the image of α under the second map in the composition (3-5). Hence $h(p_k)$ is also the image of the class β of the sequence (3-3) under the connecting map

$$H^1(G, I) = \mathrm{Ext}^1_G(\mathbb{Z}, I) \to \mathrm{Ext}^2_G(\mathbb{Z}, \mathbb{Z}) = H^2(G, \mathbb{Z})$$

induced by the exact sequence representing the class α.

The diagram (3-6) yields a commutative diagram

$$\begin{tikzcd} H^1(G, I) \arrow[r, "\partial"] \arrow[d, "f_k^*"'] & H^2(G, \mathbb{Z}^r) \arrow[d, "p_k^*"'] \\ H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r, equal] & H^2(G, \mathbb{Z}) \end{tikzcd}$$

As we have shown, $p_k^*\big(\partial(\beta)\big) = h(p_k)$. Therefore, it suffices to prove that $f_k^*(\beta) = \chi_k$. The cocycle β satisfies $\beta(\sigma_i) = \sigma_i - 1$. It follows that $f_k^*(\beta)(\sigma_k) = f_k(\sigma_k - 1) = 1/p + \mathbb{Z}$ and $f_k^*(\beta)(\sigma_i) = 0$ for all $i \neq k$. This proves the claim.

Consider the commutative diagram

$$\begin{tikzcd} (K^\times)^r = \mathrm{Hom}_G(\mathbb{Z}^r, \mathbb{Z}) \otimes K^\times \arrow[r] \arrow[d, equal] & \mathrm{Ext}^1_G(I, \mathbb{Z}) \otimes K^\times \arrow[r] \arrow[d] & \mathrm{Ext}^2_G(\mathbb{Z}, \mathbb{Z}) \otimes K^\times \arrow[d] \\ (K^\times)^r = \mathrm{Hom}_G(\mathbb{Z}^r, KL^\times) \arrow[r] & \mathrm{Ext}^1_G(I, KL^\times) \arrow[r] & \mathrm{Ext}^2_G(\mathbb{Z}, KL^\times), \end{tikzcd}$$

where the vertical homomorphisms are given by the cup products. By the claim, the image of the tuple $(x_1, \dots, x_r)$ under the diagonal composition is equal to

$\sum_{i=1}^{r}\big((\chi_i)_K \cup (x_i)\big)$. On the other hand, the bottom composition coincides with

$$(K^\times)^r \to H^1(K, U^\Phi) \simeq \mathrm{Br}(KL/K). \qquad \square$$

Corollary 3.7. *The map $H^1(K, U^\Phi) \to H^1(K, S^\Phi)$ induces an isomorphism*

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

It follows from Corollary 3.7 and the triviality of the group $H^1(K, P^\Phi)$ that we have a commutative diagram

$$\begin{tikzcd} V^\Phi(K) \arrow[r] \arrow[d] & H^1(K, U^\Phi) \arrow[r, equal] \arrow[d] & \mathrm{Br}(KL/K) \arrow[d] \\ T^\Phi(K) \arrow[r] & H^1(K, S^\Phi) \arrow[r, equal] & \mathrm{Br}_{\mathrm{ind}}(KL/K) \end{tikzcd} \tag{3-7}$$

with surjective homomorphisms.

3.1. ***The element a.*** Let a' be the image of the generic point of V^Φ over $K = F(V^\Phi)$ in $\mathrm{Br}\big(L(V^\Phi)/F(V^\Phi)\big)$ in the diagram (3-7). Choose also an element $a \in \mathrm{Br}\big(L(T^\Phi)/F(T^\Phi)\big)$ corresponding to the generic point of T^Φ over $F(T^\Phi)$. The field $F(T^\Phi)$ is a subfield of $F(V^\Phi)$ and the classes $a_{F(V^\Phi)}$ and a' are equal in $\mathrm{Br}_{\mathrm{ind}}\big(L(V^\Phi)/F(V^\Phi)\big)$. It follows that $pa_{F(V^\Phi)} = pa'$ in $\mathrm{Br}\, F(V^\Phi)$.

The exact sequence of G-modules

$$0 \to L^\times \oplus N \to L(V^\Phi)^\times \to \mathrm{Div}(V_L^\Phi) \to 0$$

induces an exact sequence

$$H^1\big(G, \mathrm{Div}(V_L^\Phi)\big) \to H^2(G, L^\times) \oplus H^2(G, N) \to H^2\big(G, L(V^\Phi)^\times\big).$$

Since $\mathrm{Div}(V_L^\Phi)$ is a permutation G-module, the first term in the sequence is trivial. Therefore, we get an injective homomorphism

$$\varphi : H^2(G, N) \to \mathrm{Br}\, F(V^\Phi)/\,\mathrm{Br}(F).$$

Then (3-1) and (3-3) yield

$$H^2(G, N) \simeq H^1(G, I) \simeq \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/p^r\mathbb{Z};$$

thus, $H^2(G, N)$ has a canonical generator ξ of order p^r.

Lemma 3.8 [Merkurjev 2010, Lemma 2.4]. *We have $\varphi(\xi) = -a' + \mathrm{Br}(F)$.*

Proof. Consider the diagram

$$\begin{tikzcd}
 & & \mathrm{Hom}_G(\mathbb{Z},\mathbb{Z}) \arrow[d] \\
 & \mathrm{Hom}_G(I,I) \arrow[r] \arrow[d] & \mathrm{Ext}^1_G(\mathbb{Z},I) \arrow[d] \\
\mathrm{Hom}_G(N,N) \arrow[r] \arrow[d] & \mathrm{Ext}^1_G(I,N) \arrow[r] \arrow[d, "l"'] & \mathrm{Ext}^2_G(\mathbb{Z},N) \arrow[d] \\
\mathrm{Hom}_G\big(N, L(V^\Phi)^\times\big) \arrow[r] & \mathrm{Ext}^1_G\big(I, L(V^\Phi)^\times\big) \arrow[r] & \mathrm{Ext}^2_G\big(\mathbb{Z}, L(V^\Phi)^\times\big)
\end{tikzcd}$$

By [Cartan and Eilenberg 1999, Chapter XIV], the images of $1_{\mathbb{Z}}$ and -1_I agree in $\mathrm{Ext}^1_G(\mathbb{Z}, I)$, and the images of 1_N and -1_I agree in $\mathrm{Ext}^1_G(I, N)$. It follows from [Cartan and Eilenberg 1999, Chapter V, Proposition 4.1] that the upper square is anticommutative. The image of $1_{\mathbb{Z}}$ is equal to $\varphi(\xi)$, and the image of 1_N is equal to $a' + \mathrm{Br}(F)$ in the right bottom corner. $\square$

Corollary 3.9. *If $r \geq 2$, then the class $p^{r-1}a$ in $\mathrm{Br}\, F(T^\Phi)$ does not belong to the image of $\mathrm{Br}(F) \to \mathrm{Br}\, F(T^\Phi)$.*

Proof. The image of $p^{r-1}a$ in $\mathrm{Br}\, F(V^\Phi)$ coincides with $p^{r-1}a'$. Modulo the image of the map $\mathrm{Br}(F) \to \mathrm{Br}\, F(V^\Phi)$, the class $p^{r-1}a'$ is equal to $-\varphi(p^{r-1}\xi)$ and is therefore nonzero, since φ is injective. $\square$

4. Essential dimension of algebraic tori

Let S be an algebraic torus over F with the splitting group G. We assume that G is a p-group of order p^r. Let X be the G-module of characters of S. A *p-presentation* of X is a G-homomorphism $f : P \to X$ with P a permutation G-module and finite cokernel of order prime to p. A p-presentation with the smallest $\mathrm{rank}(P)$ is called *minimal*.

Essential p-dimension of algebraic tori was determined in [Lötscher et al. 2009, Theorem 1.4]:

Theorem 4.1. *Let S be an algebraic torus over F with the (finite) splitting group G, X the G-module of characters of S, and $f : P \to X$ a minimal p-presentation of X. Then $\mathrm{ed}_p(S) = \mathrm{rank}\big(\mathrm{Ker}(f)\big)$.*

Corollary 4.2. *Suppose that X admits a surjective minimal p-presentation $f : P \to X$. Then $\mathrm{ed}(S) = \mathrm{ed}_p(S) = \mathrm{rank}\big(\mathrm{Ker}(f)\big)$.*

Proof. As explained in Example 3.3, a surjective G-homomorphism f yields a generically free representation of S of dimension $\mathrm{rank}(P)$. In view of Section 3 of

[Reichstein 2000], we have

$$\mathrm{ed}_p(S) \le \mathrm{ed}(S) \le \mathrm{rank}(P) - \dim(S) = \mathrm{rank}\big(\mathrm{Ker}(f)\big). \qquad \square$$

In this section we derive from Theorem 4.1 an explicit formula for the essential p-dimension of algebraic tori.

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 image of the homomorphism

$$\coprod_{H \subset G} X^H \to \overline{X},$$

where the coproduct is taken over all subgroups H with $[G:H] \le p^k$. We have the sequence of subgroups

$$0 = V_{-1} \subset V_0 \subset \cdots \subset V_r = \overline{X}. \tag{4-1}$$

Theorem 4.3. *The essential p-dimension of S is given by the explicit formula*

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

Proof. Set $b_k = \mathrm{rank}(V_k)$. By Theorem 4.1, it suffices to prove that the smallest rank of the G-module P in a p-presentation of X is equal to $\sum_{k=0}^{r}(b_k - b_{k-1})p^k$.

Let $f : P \to X$ be a p-presentation of X and A a G-invariant basis of P. The set A is the disjoint union of the G-orbits A_j, so that P is the direct sum of the permutation G-modules $\mathbb{Z}[A_j]$.

The composition $\bar{f} : P \to X \to \overline{X}$ is surjective. Since G acts trivially on $\overline{X}$, the rank of the group $\bar{f}(\mathbb{Z}[A_j])$ is at most 1 for all j and $\bar{f}(\mathbb{Z}[A_j]) \subset V_k$ if $|A_j| \le p^k$. It follows that the group $\overline{X}/V_k$ is generated by the images under the composition

$$P \xrightarrow{\bar{f}} \overline{X} \to \overline{X}/V_k$$

of all $\mathbb{Z}[A_j]$ with $|A_j| > p^k$. Denote by c_k the number of such orbits A_j, so that

$$c_k \ge \mathrm{rank}(\overline{X}/V_k) = b_r - b_k.$$

Set $c'_k = b_r - c_k$, so that $b_k \ge c'_k$ for all k and $b_r = c'_r$.

Since the number of orbits A_j with $|A_j| = p^k$ is equal to $c_{k-1} - c_k$, we have

$$\begin{aligned}\mathrm{rank}(P) &= \sum_{k=0}^{r}(c_{k-1} - c_k)p^k = \sum_{k=0}^{r}(c'_k - c'_{k-1})p^k = c'_r p^r + \sum_{k=0}^{r-1} c'_k (p^k - p^{k+1}) \\ &\ge b_r p^r + \sum_{k=0}^{r-1} b_k (p^k - p^{k+1}) = \sum_{k=0}^{r}(b_k - b_{k-1})p^k.\end{aligned}$$

It remains to construct a p-presentation with P of rank $\sum_{k=0}^{r}(b_k-b_{k-1})p^k$. For every $k\geq 0$, choose a subset X_k in X of the preimage of V_k under the canonical map $X\to\overline{X}$, with the property that for any $x\in X_k$ there is a subgroup $H_x\subset G$ with $x\in X^{H_x}$, and $[G:H_x]=p^k$ such that the composition

$$X_k\to V_k\to V_k/V_{k-1}$$

yields a bijection between X_k and a basis of V_k/V_{k-1}. In particular, $|X_k|=b_k-b_{k-1}$. Consider the G-homomorphism

$$f:P:=\coprod_{k=0}^{r}\coprod_{x\in X_k}\mathbb{Z}[G/H_x]\to X,$$

taking 1 in $\mathbb{Z}[G/H_x]$ to x in X.

By construction, the composition of f with the canonical map $X\to\overline{X}$ is surjective. Since G is a p-group, the ideal $pR_{(p)}+I$ of $R_{(p)}$ is the Jacobson radical of the ring $R_{(p)}:=R\otimes\mathbb{Z}_{(p)}$. By the Nakayama Lemma, $f_{(p)}$ is surjective. Hence the cokernel of f is finite of order prime to p. The rank of the permutation G-module P is equal to

$$\sum_{k=0}^{r}\sum_{x\in X_k}p^k=\sum_{k=0}^{r}|X_k|p^k=\sum_{k=0}^{r}(b_k-b_{k-1})p^k. \qquad \square$$

Remark 4.4. In the context of finite p-groups, Theorem 4.3 was proved in [Meyer and Reichstein 2010, Theorem 1.2].

Example 4.5. Let F be a field and Φ be a subgroup of ${}_p\operatorname{Ch}(F)$ of rank r, and let $L=F(\Phi)$ and $G=\operatorname{Gal}(L/F)$. Consider the torus U^{Φ} with the character group the augmentation ideal I defined in Section 3.

The middle row of (3-1) yields an exact sequence

$$\overline{N}\to(\overline{R})^r\to\bar{I}\to 0.$$

It follows from Lemma 3.4 that $N\subset pR^r+I^r$, and hence the first homomorphism in the sequence is trivial. The middle group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$, and hence $\operatorname{rank}(\bar{I})=r$.

For any subgroup $H\subset G$, the Tate cohomology group $\hat{H}^0(H,I)\simeq\hat{H}^{-1}(H,\mathbb{Z})$ is trivial. It follows that the group I^H is generated by N_Hx for all $x\in I$, where $N_H=\sum_{h\in H}h\in R$. Since $\bar{I}$ is of period p with trivial G-action, the classes of the elements N_Hx in $\bar{I}$ are trivial if H is a nontrivial subgroup of G. It follows that the maps $I^H\to\bar{I}$ are trivial for all $H\neq 1$. In the notation of (4-1), $V_0=\cdots=V_{r-1}=0$ and $V_r=\bar{I}$. By Theorem 4.3,

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

and the rank of the permutation module in a minimal p-presentation of I is equal to rp^r. Therefore, $k : R^r \to I$ is a minimal p-presentation of I that appears to be surjective. Therefore, by Corollary 4.2,

$$\mathrm{ed}(U^\Phi) = \mathrm{ed}_p(U^\Phi) = (r-1)p^r + 1. \tag{4-2}$$

Let S^Φ be the torus with the character group Q defined in Section 3. As in (3-1), the homomorphism k factors through a surjective map $R^r \to Q$ that is then necessarily a minimal p-presentation of Q. By Theorem 4.3 and Corollary 4.2,

$$\mathrm{ed}(S^\Phi) = \mathrm{ed}_p(S^\Phi) = rp^r - \dim(S^\Phi) = (r-1)p^r - r + 1. \tag{4-3}$$

5. Degeneration

In this section we study the behavior of the essential p-dimension under degeneration, that is, we compare the essential p-dimension of an object over a complete discrete valued field and its specialization over the residue field (Proposition 5.2). The iterated degeneration (Corollary 5.4) connects a class in the Brauer group degree p^r over some (large) field and the elements of the indecomposable relative Brauer group that are torsors for a certain torus.

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

$$\mathcal{B}_k^\Phi(K) = \{a \in \mathrm{Br}(K)\{p\} \text{ such that } \operatorname{ind} a_{K(\Phi)} \leq p^k\}.$$

Two elements a and a' in $\mathcal{B}_k^\Phi(K)$ are *equivalent* if $a - a' \in \mathrm{Br}_{\mathrm{dec}}\big(K(\Phi)/K\big)$. Write $\mathcal{F}_k^\Phi(K)$ for the set of equivalence classes in $\mathcal{B}_k^\Phi(K)$. Abusing notation, we shall write a for the equivalence class of an element $a \in \mathcal{B}_k^\Phi(K)$ in $\mathcal{F}_k^\Phi(K)$.

We view $\mathcal{B}_k^\Phi$ and $\mathcal{F}_k^\Phi$ as functors from *Fields*$/F$ to *Sets*.

Example 5.1. (i) If Φ is the zero subgroup, then $\mathcal{F}_r^\Phi = \mathcal{B}_r^\Phi \simeq \mathit{CSA}(p^r) \simeq \mathbf{PGL}(p^r)$- *torsors*.

(ii) The set $\mathcal{B}_0^\Phi(K)$ is naturally bijective to $\mathrm{Br}\big(K(\Phi)/K\big)$ and

$$\mathcal{F}_0^\Phi(K) \simeq \mathrm{Br}_{\mathrm{ind}}\big(K(\Phi)/K\big).$$

By Corollary 3.7, the latter group is naturally isomorphic to $H^1(K, S^\Phi)$, where S^Φ is the torus defined in Section 3, and thus, $\mathcal{F}_0^\Phi \simeq S^\Phi$- *torsors*.

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 $a \in \mathcal{B}_k^\Phi(E)$, that is, $a \in \mathrm{Br}(E)\{p\}$ and $\operatorname{ind}(a_{E(\Phi)}) \leq p^k$.

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

$$a' = \hat{a} + \big(\hat{\eta}_E \cup (x)\big) \in \mathrm{Br}(E') \tag{5-1}$$

for some $x \in E'^{\times}$ such that $v'(x)$ is not divisible by p. By Proposition 2.2(ii), $\mathrm{ind}(a'_{E'(\Phi')}) = p \cdot \mathrm{ind}(a_{E(\Phi)}) \leq p^{k+1}$, and hence $a' \in \mathcal{B}^{\Phi'}_{k+1}(E')$.

Proposition 5.2. *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 $p \cdot \rho \in \Phi_N \setminus \Phi'_N$, we have* $\mathrm{ind}\, a_{N(\Phi',\rho)} > p^{k-1}$. *Then*

$$\mathrm{ed}_p^{\mathcal{F}^{\Phi'}_{k+1}}(a') \geq \mathrm{ed}_p^{\mathcal{F}^{\Phi}_{k}}(a) + 1.$$

Proof. Let M/E' be a finite field extension of degree prime to p, let $M_0 \subset M$ be a subfield over F, and let $a'_0 \in \mathcal{B}^{\Phi'}_{k+1}(M_0)$ be such that $(a'_0)_M = a'_M$ in $\mathcal{F}^{\Phi'}_{k+1}$ and

$$\mathrm{tr.deg}_F(M_0) = \mathrm{ed}_p^{\mathcal{F}^{\Phi'}_{k+1}}(a').$$

We have

$$a'_M - (a'_0)_M \in \mathrm{Br}_{\mathrm{dec}}\big(M(\Phi')/M\big). \tag{5-2}$$

It follows from (5-1) that

$$a'_M = \hat{a}_N + \big(\hat{\eta}_N \cup (x)\big) \tag{5-3}$$

and $\partial_{v'}(a') = q \cdot \eta_E$, where $q = v'(x)$ is relatively prime to p. We extend the discrete valuation v' on E' to a (unique) discrete valuation v on M. The ramification index e' and inertia degree are both prime to p. Thus, the residue field N of v is a finite extension of E of degree prime to p. By Proposition 2.2(iii),

$$\partial_v(a'_M) = e' \cdot \partial_{v'}(a')_N = e'q \cdot \eta_N. \tag{5-4}$$

Let v_0 be the restriction of v to M_0 and N_0 its residue field. From (5-2), we have

$$\partial_v(a'_M) - \partial_v\big((a'_0)_M\big) \in \Phi'_N. \tag{5-5}$$

Recall that $\eta_E \notin \Phi'_E$. Since $[N : E]$ is not divisible by p, it follows that

$$\eta_N \notin \Phi'_N. \tag{5-6}$$

By (5-4), (5-5) and (5-6), $\partial_v\big((a'_0)_M\big) \neq 0$, that is, $(a'_0)_M$ is ramified and therefore v_0 is nontrivial, that is, v_0 is a discrete valuation on M_0.

Let $\eta_0 := \partial_{v_0}(a'_0) \in \mathrm{Ch}(N_0)\{p\}$. By Proposition 2.2(iii),

$$\partial_v\big((a'_0)_M\big) = e \cdot (\eta_0)_N, \tag{5-7}$$

where e is the ramification index of M/M_0, and hence $(\eta_0)_N \neq 0$. It follows from (5-4), (5-5) and (5-7) that

$$e'q \cdot \eta_N - e \cdot (\eta_0)_N \in \Phi'_N. \tag{5-8}$$

Since $e'q$ is relatively prime to p,

$$\eta_N \in \langle \Phi'_N, (\eta_0)_N \rangle \quad \text{in} \quad \mathrm{Ch}(N). \tag{5-9}$$

Let p^t $(t \geq 1)$ be the order of $(\eta_0)_N$. It follows from (5-6) and (5-8) that $v_p(e) = t-1$ and

$$p^{t-1} \cdot (\eta_0)_N \in \Phi_N \setminus \Phi'_N. \tag{5-10}$$

Choose a prime element π_0 in M_0 and write

$$(a'_0)_{\widehat{M}_0} = \hat{a}_0 + \big(\hat{\eta}_0 \cup (\pi_0)\big) \tag{5-11}$$

in $\mathrm{Br}(\widehat{M}_0)$, where $a_0 \in \mathrm{Br}(N_0)\{p\}$.

Applying the specialization homomorphism $s_\pi : \mathrm{Br}(M)\{p\} \to \mathrm{Br}(N)\{p\}$ (for a prime element π in M) to (5-2), (5-3) and (5-11), using (2-3) and (5-9), we get

$$a_N - (a_0)_N \in \mathrm{Br}_{\mathrm{dec}}\big(N(\Phi', \eta_0)/N\big). \tag{5-12}$$

It follows from (5-12) that

$$a_{N(\Phi',\eta_0)} = (a_0)_{N(\Phi',\eta_0)} \tag{5-13}$$

in $\mathrm{Br}\big(N(\Phi', \eta_0)\big)$.

By (5-11),

$$(a'_0)_{\widehat{M}_0(\Phi')} = \widehat{(a_0)}_{N_0(\Phi')} + \big(\widehat{(\eta_0)}_{N_0(\Phi')} \cup (\pi_0)\big).$$

Since no nontrivial multiple of $(\eta_0)_N$ belongs to Φ'_N, by (5-10), the order of the character $(\eta_0)_{N_0(\Phi')}$ is at least p^t. It follows from Proposition 2.2(ii) that

$$\mathrm{ind}(a_0)_{N_0(\Phi',\eta_0)} = \mathrm{ind}(a'_0)_{\widehat{M}_0(\Phi')}/\operatorname{ord}(\eta_0)_{N_0(\Phi')} \leq p^{k+1}/p^t = p^{k-t+1}. \tag{5-14}$$

By (5-13) and (5-14),

$$\mathrm{ind}(a_{N(\Phi',\eta_0)}) \leq p^{k-t+1}. \tag{5-15}$$

Suppose that $t \geq 2$, and consider the character $\rho = p^{t-2} \cdot (\eta_0)_N$ of order p^2 in $\mathrm{Ch}(N)$. We have $p \cdot \rho = p^{t-1}(\eta_0)_N \in \Phi_N \setminus \Phi'_N$, by (5-10). Also, the degree of the field extension $N(\Phi', \eta_0)/N(\Phi', \rho)$ is equal to p^{t-2}. Hence, by (5-15),

$$\mathrm{ind}(a_{N(\Phi',\rho)}) \leq \mathrm{ind}(a_{N(\Phi',\eta_0)}) \cdot p^{t-2} \leq p^{k-t+1} \cdot p^{t-2} = p^{k-1}.$$

This contradicts the assumption. Therefore, $t = 1$, that is, $\operatorname{ord}(\eta_0)_N = p$. Then $(e, p) = 1$ and it follows from (5-8) that $(\eta_0)_N \in \langle \Phi'_N, \eta_N \rangle$. Moreover,

$$\langle \Phi', \eta_0 \rangle_N = \langle \Phi', \eta \rangle_N = \Phi_N. \tag{5-16}$$

There is a finite subextension N_1/N_0 of N/N_0 such that $\langle \Phi', \eta_0\rangle_{N_1} = \Phi_{N_1}$, by Lemma 2.1. Replacing N_0 by N_1 and a_0 by $(a_0)_{N_1}$, we may assume that $\langle \Phi', \eta_0\rangle_{N_0} = \Phi_{N_0}$. In particular, η_0 is of order p in $\mathrm{Ch}(N_0)$.

Since $\operatorname{ind}(a_0)_{N_0(\Phi)} = \operatorname{ind}(a_0)_{N_0(\Phi',\eta_0)} \le p^k$ by (5-14), we have $a_0 \in \mathcal{B}_k^{\Phi}(N_0)$. It follows from (5-12) that

$$a_N - (a_0)_N \in \mathrm{Br}_{\mathrm{dec}}\big(N(\Phi)/N\big).$$

Hence the classes of a_N and $(a_0)_N$ are equal in $\mathcal{F}_k^{\Phi}(N)$. The class of a_N in $\mathcal{F}_k^{\Phi}(N)$ is then defined over N_0, and therefore

$$\mathrm{ed}_p^{\mathcal{F}_{k+1}^{\Phi'}}(a') = \operatorname{tr.deg}_F(M_0) \ge \operatorname{tr.deg}_F(N_0) + 1 \ge \mathrm{ed}_p^{\mathcal{F}_k^{\Phi}}(a) + 1. \qquad \square$$

5.1. ***Multiple degeneration.*** In this section we assume that the base field F contains a primitive p^2-th root of unity.

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

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 not divisible by p, and define the elements $a_k \in \mathrm{Br}(E_k)\{p\}$ inductively by $a_0 = a$ and

$$a_k = \widehat{a_{k-1}} + \big(\widehat{(\chi_k)}_{E_{k-1}} \cup (x_k)\big).$$

Let Φ_k be the subgroup of Φ generated by $\chi_{k+1}, \dots, \chi_r$. Thus, $\Phi_0 = \Phi$, $\Phi_r = 0$ and $\operatorname{rank}(\Phi_k) = r - k$. Note that the character $(\chi_k)_{E_{k-1}(\Phi_k)}$ is not trivial. It follows from Proposition 2.2(ii) that

$$\operatorname{ind}(a_k)_{E_k(\Phi_k)} = p \cdot \operatorname{ind}(a_{k-1})_{E_{k-1}(\Phi_{k-1})}$$

for any $k = 1, \dots, r$. Since $\operatorname{ind} a_{E(\Phi)} = 1$, we have $\operatorname{ind}(a_k)_{E_k(\Phi_k)} = p^k$ for all $k = 0, 1, \dots, r$. In particular, $a_k \in \mathcal{B}_k^{\Phi_k}(E_k)$.

The following lemma assures that under a certain restriction on the element a, the conditions of Proposition 5.2 are satisfied for the fields E_k, the groups of characters Φ_k, and the elements a_k.

Lemma 5.3. *Suppose that $a_{E(\Psi)} \notin \operatorname{Im}\big(\mathrm{Br}\, F(\Psi) \to \mathrm{Br}\, E(\Psi)\big)$ for any proper subgroup $\Psi \subset \Phi$. 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 $p \cdot \rho \in (\Phi_k)_N \setminus (\Phi_{k+1})_N$, we have*

$$\operatorname{ind}(a_k)_{N(\Phi_{k+1},\rho)} > p^{k-1}. \tag{5-17}$$

Proof. Let $k=0,1,\dots,r-1$ and N/E_k be a finite field extension of degree prime to p. 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 $\tilde{E}_j = N$. 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 $\tilde{E}_{j-1}$ be its residue field. The fields $\tilde{E}_j$ with $j>k$ are constructed by induction on j. If we have constructed $\tilde{E}_j$ as a finite extension of E_j of degree prime to p, then let $\tilde{E}_{j+1}$ be an extension of E_{j+1} of degree $[\tilde{E}_j : E_j]$ with residue field $\tilde{E}_j$.

Replacing E_i by $\tilde{E}_i$ and a_i by $(a_i)_{\tilde{E}_i}$, we may assume that $N=E_k$. Let $\rho \in \mathrm{Ch}(E_k)$ be a character of order p^2. We prove the inequality (5-17) by induction on r. The case $r=1$ is obvious. Suppose first 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 $a'_i := (a_i)_{E'_i} \in \mathrm{Br}(E'_i)$ for $i=0,1,\dots,r-1$. Let $\Phi' = \langle \chi'_1, \chi'_2, \dots, \chi'_{r-1}\rangle$ and let Φ'_k be the subgroup of Φ' generated by $\chi'_{k+1},\dots,\chi'_{r-1}$.

Let $\Psi' \subset \Phi'$ be a proper subgroup. Then $\Psi := \Psi' + \langle \chi_r\rangle$ is a proper subgroup of Φ. Since $F(\Psi)=F'(\Psi')$ and $E(\Psi)=E'(\Psi')$, we have

$$a_{E'(\Psi')} \notin \mathrm{Im}\big(\mathrm{Br}\, F'(\Psi') \to \mathrm{Br}\, E'(\Psi')\big).$$

By induction, the inequality (5-17) holds for the term a'_k of the new sequence. Since

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

the inequality (5-17) holds for the term a_k.

Thus we can assume that $k=r-1$.

Case 1. The character ρ is unramified with respect to v_{r-1}, that is, $\rho=\hat{\mu}$ for a character $\mu \in \mathrm{Ch}(E_{r-2})$ of order p^2. By Lemma 2.3(i),

$$\mathrm{ind}(a_{r-2})_{E_{r-2}(\chi_{r-1},\mu)} = \mathrm{ind}(a_{r-1})_{E_{r-1}(\rho)}/p = \mathrm{ind}(a_{r-1})_{E_{r-1}(\Phi_r,\rho)}/p. \tag{5-18}$$

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 $\chi_1,\dots,\chi_{r-2},\chi_r$ and the elements $a'_i \in \mathrm{Br}(E'_i)$ for $i=0,1,\dots,r-1$ defined by $a'_i=(a_i)_{E'_i}$ for $i \le r-2$ and $a'_{r-1} = \hat{a}_{r-2} + \big(\hat{\chi}_r \cup (x_{r-1})\big)$ over E'_{r-1}.

Let $\Phi' = \langle \chi_1,\dots,\chi_{r-2},\chi_r\rangle$ and $\Psi' \subset \Phi'$ be a proper subgroup. Then $\Psi := \Psi' + \langle \chi_{r-1}\rangle$ is a proper subgroup of Φ. Since $F(\Psi)=F'(\Psi')$ and $E(\Psi)=E'(\Psi')$, we have $a_{E'(\Psi')} \notin \mathrm{Im}\big(\mathrm{Br}\, F'(\Psi') \to \mathrm{Br}\, E'(\Psi')\big)$. By induction, the inequality (5-17) holds for the term a'_{r-2} of the new sequence, the field $N=E'_{r-2}$, and the character μ_N. Since

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

the equality (5-18) shows that (5-17) holds for a_{r-1}.

Case 2. The character ρ is ramified. Note that $p \cdot \rho$ is a nonzero multiple of $(\chi_r)_{E_{r-1}}$. Suppose the inequality (5-17) fails for a_{r-1}, that is, we have

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

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

$$\operatorname{ind}\bigl(a_{r-2} - (\chi_{r-1} \cup (\bar{u}^{1/p}))\bigr)_{E_{r-2}(\chi_r)} = \operatorname{ind}(a_{r-1})_{E_{r-1}(\rho)} \le p^{r-2}.$$

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

$$\operatorname{ind}\bigl(a_j - (\chi_{r-1} \cup (\bar{u}_j^{1/p}))\bigr)_{E_j(\Theta_j)} \le p^j. \tag{5-19}$$

If $j = r-2$, we set $u_j = u$ and $\Theta_j = \langle \chi_r \rangle$.

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

$$\bigl(a_j - (\chi_{r-1} \cup (\bar{u}_j^{1/p}))\bigr)_{E_j(\Theta_j)} = \hat{b} + \bigl(\hat{\eta} \cup (x_j)\bigr)_{E_j(\Theta_j)},$$

where $\eta = \chi_j - m\chi_{r-1}$ and $b = \bigl(a_{j-1} - (\chi_{r-1} \cup (\bar{u}_{j-1}^{1/p}))\bigr)_{E_{j-1}(\Theta_j)}$. Since η is not contained in Θ_j, the character $\eta_{E_{j-1}(\Theta_j)}$ is not trivial. Set $\Theta_{j-1} = \langle \Theta_j, \eta \rangle$. It follows from Proposition 2.2(ii) that

$$\operatorname{ind}(b_{E_{j-1}(\Theta_{j-1})}) = \operatorname{ind}\bigl(a_j - (\chi_{r-1} \cup (\bar{u}_j^{1/p}))\bigr)_{E_j(\Theta_j)}/p \le p^{j-1}.$$

Applying the inequality (5-19) in the case $j = 0$, we get

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

for an element $w \in E^\times$ such that $E(w^{1/p}) = E(\chi_r)$. Since the character χ_r is defined over F, we may assume that $w \in F^\times$, and therefore

$$a_{E(\Theta_0)} \in \operatorname{Im}\bigl(\operatorname{Br} F(\Theta_0) \to \operatorname{Br} E(\Theta_0)\bigr).$$

The degree of the extension $E(\Theta_0)/E$ is equal to p^{r-1}, and hence Θ_0 is a proper subgroup of Φ, a contradiction. Thus, we have shown that the inequality (5-17) holds. $\square$

By Example 5.1(ii), we can view a as an S^Φ-torsor over E.

Corollary 5.4. *Suppose that $p^{r-1}a \notin \operatorname{Im}\bigl(\operatorname{Br}(F) \to \operatorname{Br}(E)\bigr)$. Then*

$$\operatorname{ed}_p^{CSA(p^r)}(a_r) \ge \operatorname{ed}_p^{S^\Phi\text{-}torsors}(a) + r.$$

Proof. By iterated application of Proposition 5.2 and Example 5.1,

$$\begin{aligned}\mathrm{ed}_p^{CSA(p^r)}(a_r) &= \mathrm{ed}_p^{\mathscr{F}_r^{\Phi_r}}(a_r) \geq \mathrm{ed}_p^{\mathscr{F}_{r-1}^{\Phi_{r-1}}}(a_{r-1}) + 1 \geq \dots \\ &\geq \mathrm{ed}_p^{\mathscr{F}_1^{\Phi_1}}(a_1) + (r-1) \geq \mathrm{ed}_p^{\mathscr{F}_0^{\Phi_0}}(a_0) + r = \mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) + r. \qquad \square\end{aligned}$$

6. Proof of the main theorem

Theorem 6.1. *Let F be a field and p a prime integer different from* $\mathrm{char}(F)$. *Then*

$$\mathrm{ed}_p\big(CSA(p^r)\big) \geq (r-1)p^r + 1.$$

Proof. Since $\mathrm{ed}_p\big(CSA(p^r)\big)$ can only go down if we replace the base field F by any field extension [Merkurjev 2009, Proposition 1.5], we can replace F by any field extension. In particular, we may assume that F contains a primitive p^2-th root of unity and that there is a subgroup Φ of ${}_p\mathrm{Ch}(F)$ of rank r (replacing F by the field of rational functions in r variables over F).

Let T^Φ be the algebraic torus constructed in Section 3 for the subgroup Φ. Set $E = F(T^\Phi)$, and let $a \in \mathrm{Br}(EL/E)$ be the element defined in Section 3.1. Let $a_r \in \mathrm{Br}(E_r)$ be the element of index p^r constructed in Section 5.1. By Corollary 3.9, the class $p^{r-1}a$ in $\mathrm{Br}(E)$ does not belong to the image of $\mathrm{Br}(F) \to \mathrm{Br}(E)$. It follows from Corollary 5.4 that

$$\mathrm{ed}_p^{CSA(p^r)}(a_r) \geq \mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) + r. \tag{6-1}$$

The S^Φ-torsor a is the generic fiber of the versal S^Φ-torsor $P^\Phi \to T^\Phi$ (see Example 3.3), and hence a is a generic torsor. By [Reichstein and Youssin 2000, §6] or [Merkurjev 2009, Theorem 2.9],

$$\mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) = \mathrm{ed}_p(S^\Phi). \tag{6-2}$$

The essential p-dimension of S^Φ was calculated in (4-3):

$$\mathrm{ed}_p(S^\Phi) = (r-1)p^r - r + 1. \tag{6-3}$$

Finally, it follows from (6-1), (6-2) and (6-3) that

$$\mathrm{ed}_p\big(CSA(p^r)\big) \geq \mathrm{ed}_p^{CSA(p^r)}(a_r) \geq \mathrm{ed}_p^{S^\Phi\text{-}\mathit{torsors}}(a) + r = (r-1)p^r + 1. \qquad \square$$

7. Remarks

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

consists of all classes represented by crossed product algebras with the group G [Herstein 1994, §4.4].

Write $\mathit{Pair}_K(G)$ for the set of isomorphism classes of pairs (a, E), where $a \in \mathit{CSA}_K(G)$ and E is a Galois G-algebra splitting a.

Finally, fix a Galois field extension L/F with $\mathrm{Gal}(L/F) \simeq G$ and consider the subset $\mathit{CSA}_K(L/F)$ of $\mathit{CSA}_K(G)$ consisting of all classes split by the extension KL/K. Thus, $\mathit{CSA}(L/F)$ is a subfunctor of $\mathit{CSA}(G)$ and there is the obvious surjective morphism of functors $\mathit{Pair}(G) \to \mathit{CSA}(G)$.

Theorem 7.1. *Let F be a field, p a prime integer different from $\mathrm{char}(F)$, G an elementary abelian group of order p^r, $r \geq 2$, and L/F a Galois field extension with $\mathrm{Gal}(L/F) \simeq G$. Let $\mathcal{F}$ be one of the three functors $\mathit{CSA}(L/F)$, $\mathit{CSA}(G)$, $\mathit{Pair}(G)$. Then*

$$\mathrm{ed}(\mathcal{F}) = \mathrm{ed}_p(\mathcal{F}) = (r-1)p^r + 1.$$

Proof. The functor $\mathit{CSA}(L/F)$ is isomorphic to $U^{\Phi}\text{-}\mathit{torsors}$ by (3-4), where Φ is a subgroup of $\mathrm{Ch}(F)$ such that $L = F(\Phi)$. It follows from (4-2) that

$$\mathrm{ed}\big(\mathit{CSA}(L/F)\big) = \mathrm{ed}_p\big(\mathit{CSA}(L/F)\big) = (r-1)p^r + 1.$$

Let a_r be the element in $\mathrm{Br}(E_r)$ in the proof of Theorem 6.1. It satisfies

$$\mathrm{ed}_p^{\mathit{CSA}(p^r)}(a_r) \geq (r-1)p^r + 1.$$

By construction, $a_r \in \mathit{CSA}_{E_r}(G)$. Since $\mathit{CSA}(G)$ is a subfunctor of $\mathit{CSA}(p^r)$, we have

$$\mathrm{ed}_p\big(\mathit{CSA}(G)\big) \geq \mathrm{ed}_p^{\mathit{CSA}(G)}(a_r) \geq \mathrm{ed}_p^{\mathit{CSA}(p^r)}(a_r) \geq (r-1)p^r + 1.$$

The upper bound $\mathrm{ed}\big(\mathit{CSA}(G)\big) \leq (r-1)p^r + 1$ was proven in [Lorenz et al. 2003, Corollary 3 10].

The split étale F-algebra $E := \mathrm{Map}(G, F)$ has the natural structure of a Galois G-algebra over F. The group G acts on the split torus $U := R_{E/F}(\mathbb{G}_{m,E})/\mathbb{G}_m$. Let A be the split F-algebra $\mathrm{End}_F(E)$. The semidirect product $H := U \rtimes G$ acts naturally on A by F-algebra automorphisms. Moreover, by the Skolem–Noether Theorem, H is precisely the automorphism group of the pair (A, E). It follows that the functor $\mathit{Pair}_K(G)$ is isomorphic to $H\text{-}\mathit{torsors}$.

The character group of U is G-isomorphic to the ideal I in $R = \mathbb{Z}[G]$. By [Meyer and Reichstein 2009a, §3], the G-homomorphism $k : R^r \to I$ constructed in Section 3 yields a representation W of the group H of dimension rp^r. Since $r \geq 2$, by Lemma 3.4, G acts faithfully on the kernel N of k. By [Meyer and Reichstein 2009a, Lemma 3.3], the action of H on W is generically free, and hence

$$\mathrm{ed}\big(\mathit{Pair}(G)\big) = \mathrm{ed}(H) \leq \dim(W) - \dim(H) = (r-1)p^r + 1.$$

Since $\mathit{Pair}(G)$ surjects onto $\mathit{CSA}(G)$, we have

$$\mathrm{ed}\big(\mathit{Pair}(G)\big) \geq \mathrm{ed}_p\big(\mathit{Pair}(G)\big) \geq \mathrm{ed}_p\big(\mathit{CSA}(G)\big) = (r-1)p^r + 1. \qquad \square$$

Remark 7.2. The generic G-crossed product algebra D constructed in [Amitsur and Saltman 1978] is a generic element for the functor $\mathit{CSA}(G)$ in the sense of [Merkurjev 2009, §2], and hence

$$\mathrm{ed}(D) = \mathrm{ed}_p(D) = (r-1)p^r + 1$$

for $r \geq 2$ by Theorem 7.1.

References

[Amitsur and Saltman 1978] S. A. Amitsur and D. Saltman, "Generic Abelian crossed products and p-algebras", *J. Algebra* **51**:1 (1978), 76–87. MR 58 #10988 Zbl 0391.13001

[Berhuy and Favi 2003] G. Berhuy and G. Favi, "Essential dimension: a functorial point of view (after A. Merkurjev)", *Doc. Math.* **8** (2003), 279–330. MR 2004m:11056 Zbl 1101.14324

[Cartan and Eilenberg 1999] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, 1999. MR 2000h:18022 Zbl 0933.18001

[Colliot-Thélène and Sansuc 1977] J.-L. Colliot-Thélène and J.-J. Sansuc, "La R-équivalence sur les tores", *Ann. Sci. École Norm. Sup.* (4) **10**:2 (1977), 175–229. MR 56 #8576 Zbl 0356.14007

[Garibaldi et al. 2003] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series **28**, American Mathematical Society, Providence, RI, 2003. MR 2004f:11034 Zbl 1159.12311

[Herstein 1994] I. N. Herstein, *Noncommutative rings*, Carus Mathematical Monographs **15**, Mathematical Association of America, Washington, DC, 1994. MR 97m:16001 Zbl 0874.16001

[Jacob and Wadsworth 1990] B. Jacob and A. Wadsworth, "Division algebras over Henselian fields", *J. Algebra* **128**:1 (1990), 126–179. MR 91d:12006 Zbl 0692.16011

[Lorenz et al. 2003] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman, "Fields of definition for division algebras", *J. London Math. Soc.* (2) **68**:3 (2003), 651–670. MR 2004j:16022 Zbl 1071.16012

[Lötscher et al. 2009] R. Lötscher, M. MacDonald, A. Meyer, and R. Reichstein, "Essential p-dimension of algebraic tori", preprint, 2009. arXiv 0910.5574v1

[Matsumura 1980] H. Matsumura, *Commutative algebra*, 2nd ed., Mathematics Lecture Note Series **56**, Benjamin/Cummings, Reading, MA, 1980. MR 82i:13003 Zbl 0441.13001

[Merkurjev 2009] A. S. Merkurjev, "Essential dimension", pp. 299–325 in *Quadratic forms: algebra, arithmetic, and geometry*, edited by R. Baeza et al., Contemp. Math. **493**, Amer. Math. Soc., Providence, RI, 2009. MR 2010i:14014 Zbl 1188.14006

[Merkurjev 2010] A. S. Merkurjev, "Essential p-dimension of $\mathrm{PGL}(p^2)$", *J. Amer. Math. Soc.* **23** (2010), 693–712. Zbl 05775681

[Meyer and Reichstein 2009a] A. Meyer and Z. Reichstein, "The essential dimension of the normalizer of a maximal torus in the projective linear group", *Algebra Number Theory* **3**:4 (2009), 467–487. MR 2010h:11065 Zbl 05588054

[Meyer and Reichstein 2009b] A. Meyer and Z. Reichstein, "An upper bound on the essential dimension of a central simple algebra", preprint, 2009, Available at www.math.ubc.ca/~reichst/meyer-reichstein3.pdf. To appear in *J. Algebra*.

[Meyer and Reichstein 2010] A. Meyer and Z. Reichstein, "Some consequences of the Karpenko–Merkurjev theorem", *Docum. Math.* extra vol. (2010), 445–457. Zbl 05827449

[Reichstein 2000] Z. Reichstein, "On the notion of essential dimension for algebraic groups", *Transform. Groups* **5**:3 (2000), 265–304. MR 2001j:20073 Zbl 0981.20033

[Reichstein and Youssin 2000] Z. Reichstein and B. Youssin, "Essential dimensions of algebraic groups and a resolution theorem for G-varieties", *Canad. J. Math.* **52**:5 (2000), 1018–1056. MR 2001k:14088 Zbl 1044.14023

[Serre 1997] J.-P. Serre, *Galois cohomology*, Springer, Berlin, 1997. MR 98g:12007 Zbl 0902.12004

[Tignol 1978] J.-P. Tignol, "Sur les classes de similitude de corps à involution de degré 8", *C. R. Acad. Sci. Paris Sér. A-B* **286**:20 (1978), A875–A876. MR 58 #16605 Zbl 0374.16006

Communicated by Raman Parimala
Received 2009-11-27 Revised 2010-03-30 Accepted 2010-05-15

merkurev@math.ucla.edu *Department of Mathematics, University of California, Los Angeles, CA 90095-1555, United States*

Algebra & Number Theory

www.jant.org

EDITORS

Managing Editor	Editorial Board Chair
Bjorn Poonen Massachusetts Institute of Technology Cambridge, USA	David Eisenbud University of California Berkeley, USA

Board of Editors

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Andrei Okounkov	Princeton University, USA
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Universität Duisburg-Essen, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Ronald Solomon	Ohio State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Ehud Hrushovski	Hebrew University, Israel	Bernd Sturmfels	University of California, Berkeley, USA
Craig Huneke	University of Kansas, USA	Richard Taylor	Harvard University, USA
Mikhail Kapranov	Yale University, USA	Ravi Vakil	Stanford University, USA
Yujiro Kawamata	University of Tokyo, Japan	Michel van den Bergh	Hasselt University, Belgium
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Hendrik W. Lenstra	Universiteit Leiden, The Netherlands	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Andrei Zelevinsky	Northeastern University, USA
Barry Mazur	Harvard University, USA	Efim Zelmanov	University of California, San Diego, USA

PRODUCTION

ant@mathscipub.org

Silvio Levy, Scientific Editor

Andrew Levy, Production Editor

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2010 is US $140/year for the electronic version, and $200/year (+$30 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFlow™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://www.mathscipub.org

A NON-PROFIT CORPORATION

Typeset in LaTeX

Copyright ©2010 by Mathematical Sciences Publishers

Algebra & Number Theory

Volume 4 No. 8 2010