ESSENTIAL DIMENSION OF SIMPLE ALGEBRAS

ALEXANDER S. MERKURJEV

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 (see [1] or [10]).

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 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 $\operatorname{ed}^{\mathcal{F}}(\alpha)$, is the least transcendence degree $\operatorname{tr.deg}_F(K_0)$ over all fields of definition K_0 of α. The *essential dimension of the functor* $\mathcal{F}$ is

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

where the supremum is taken over 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* $\operatorname{ed}_p^{\mathcal{F}}(\alpha)$ *of* α is the minimum of $\operatorname{ed}^{\mathcal{F}}(\alpha_{K'})$ over all finite field extensions K'/K of degree prime to p. The *essential p-dimension* $\operatorname{ed}_p(\mathcal{F})$ *of* $\mathcal{F}$ is the supremum of $\operatorname{ed}_p^{\mathcal{F}}(\alpha)$ over all fields $K \in \mathit{Fields}/F$ and all $\alpha \in \mathcal{F}(K)$ (see [14, §6]). Clearly, $\operatorname{ed}(\mathcal{F}) \geq \operatorname{ed}_p(\mathcal{F})$ for all p.

Let G be an algebraic group over F. The *essential dimension* $\operatorname{ed}(G)$ (resp. *essential p-dimension* $\operatorname{ed}_p(G)$) 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 $G = \mathbf{PGL}_n$ over F, the functor $G\text{-}\mathit{torsors}$ is isomorphic to the functor $\mathit{Alg}_F(n)$ taking a field K to the set of isomorphism classes 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 $\operatorname{ed}_p\big(\mathit{Alg}_F(n)\big) = \operatorname{ed}_p\big(\mathit{Alg}_F(p^r)\big)$ [14, Lemma 8.5.5]. Every central simple E-algebra of degree p is cyclic over a finite field extension of degree prime to p, hence $\operatorname{ed}_p\big(\mathit{Alg}_F(p)\big) = 2$ [14, Lemma 8.5.7]. It was proven in [11] that $\operatorname{ed}_p\big(\mathit{Alg}_F(p^2)\big) = p^2 + 1$ and in general, $\operatorname{ed}_p\big(\mathit{Alg}_F(p^r)\big) \geq 2r$ for all r in [14, Th. 8.6].

We prove the following:

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

$$\operatorname{ed}_p\big(\mathsf{Alg}_F(p^r)\big) \geq (r-1)p^r + 1.$$

In other words, we have the following lower bound for the essential dimension of $\mathbf{PGL}_F(p^r)$:

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

2. Preliminaries

2.1. **Characters.** Let F be a field, F_{sep} a separable closure of F and $\Gamma = \operatorname{Gal}(F_{\mathrm{sep}}/F)$ 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* $\operatorname{Ch}(F)$ of F is defined as

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

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

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

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

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

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

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 $\eta_i = \chi_i - \chi'_i$. As 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. As $(\chi_i)_{K'} = (\chi'_i)_{K'}$, we have $\Phi_{K'} = \Phi'_{K'}$. □

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

The cup-product

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

takes $\chi \otimes a$ to the class $\chi \cup (a)$ in $\operatorname{Br}(F)$ 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 $\mathrm{Br}\big(F(\Phi)/F\big)/\,\mathrm{Br}_{\mathrm{dec}}\big(F(\Phi)/F\big)$.

2.3. **Complete fields.** Let E be a complete field with respect to a discrete valuation v and K its residue field.

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

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

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

If $a \in \mathrm{Br}(K)\{p\}$, then we write $\widehat{a}$ 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 $\widehat{a} = \widehat{\chi} \cup (u)$.

The following proposition was proved in [6, Th. 5.15(a)], [16, Prop. 2.4]) and [4, Prop. 8.2].

Proposition 2.2. *Let E be a complete field with respect to a discrete valuation v and K its residue field of characteristic different from p. Then*

1. $\mathrm{ind}(\widehat{a}) = \mathrm{ind}(a)$ *for any* $a \in \mathrm{Br}(K)\{p\}$.
2. *Let* $b = \widehat{a} + \big(\chi \cup (x)\big)$ *for an element* $a \in \mathrm{Br}(K)\{p\}$, $\chi \in \mathrm{Ch}(K)\{p\}$ *and* $x \in E^\times$ *such that* $v(x)$ *is not divisible by* p. *Then*
$$\mathrm{ind}(b) = \mathrm{ind}\big(a_{K(\chi)}\big) \cdot \mathrm{ord}(\chi).$$
3. *Let* E'/E *be a finite field extension and* v' *the discrete valuation on* E' *extending* v *with residue field* K'. *Then for any* $b \in \mathrm{Br}(E)\{p\}$, *one has*
$$\partial_{v'}(b_{E'}) = e \cdot \partial_v(b)_{K'},$$
where e *is the ramification index of* E'/E.

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

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

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

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

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

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 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, i.e., $p \cdot \eta = \widehat{\nu}$ 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 $b = \widehat{a} + \big(\widehat{\chi} \cup (x)\big) \in \mathrm{Br}(E)$, where $x \in E^\times$ is an element such that $v(x)$ is not divisible by p. Then:*

1. *If η is unramified, , i.e., $\eta = \widehat{\mu}$ for some $\mu \in \mathrm{Ch}(K)$ of order p^2, then $\mathrm{ind}(b_{E(\eta)}) = p \cdot \mathrm{ind}(a_{K(\mu,\chi)})$.*
2. *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. (1) If $\eta = \widehat{\mu}$ for some $\mu \in \mathrm{Ch}(K)$, then $K(\mu)$ is the residue field of $E(\eta)$ and we have

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

As χ and ν are linearly independent, the character $\chi_{K(\mu)}$ is nontrivial. The first statement follows from Proposition 2.2(2).

(2) Since $p \cdot \eta$ is unramified, the ramification index of $E(\eta)/E$ is equal to p, 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 $E(\eta)$. As $u^{1/p}x$ is a p-th power in $E(\eta)$, the class

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

is unramified. It follows from Proposition 2.2(1) 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. $\square$

3. Brauer group and algebraic tori

3.1. **Torsors.** Let G be an algebraic groups 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 $H^1(K, G)$ (see [15]).

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 $G = \mathbf{PGL}_{n,F}$.

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*, i.e., there is a non-empty open subset $W' \subset W$ and a G-torsor $\beta : W' \to X$ for a variety X over F. The torsor β is *versal*, i.e., 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 $F(X)$ (see [4] and [13]).

Example 3.3. Let S be an algebraic torus over F. We embed S into the quasi-trivial torus $P = R_{L/F}(\mathbb{G}_{m,L})$, where L is an étale F-algebra (see [3]). 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.

3.2. **The tori P^Φ, S^Φ, T^Φ, U^Φ and V^Φ.** Let F be a field, Φ a subgroup of ${}_p\mathrm{Ch}(F)$ of rank r and $L = F(\Phi)$. Let $G = \mathrm{Gal}(L/F)$. Choose a basis $\chi_1, \chi_2, \dots, \chi_r$ for Φ. We can view each χ_i as a character of G, i.e., 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, 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 homomorphism of G-modules $k : R^r \to R$ taking the i-th basis element e_i of R^r to $\sigma_i - 1$. The image of k is the *augmentation ideal* $I = \mathrm{Ker}(\varepsilon)$ 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 $N := \mathrm{Ker}(k)$. 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 i-th basis element $\bar{e}_i$ to $t_i - 1$ (see [9, Th. 43]) implies that $\mathrm{Ker}(\bar{k})$ 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 $x := \sum x_i e_i \in \mathrm{Ker}(k)$. 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 $\bar{k}(\bar{x}) \in J$, 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 $\overline{N}_i\bar{e}_i$, hence x is a linear combination of e_{ij} and f_i. $\square$

Let $\varepsilon_i : R^r \to \mathbb{Z}$ be the i-th 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

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

is surjective. Set $M = \operatorname{Ker}(l)$ 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 $(\sigma_j - 1)f_i = N_i e_{ij} \in M'$, hence $If_i \subset M'$.

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 $x_i \in R$. As $l(m) = 0$, we have $\varepsilon(x_i) = 0$, i.e., $x_i \in I$ for all i, hence $m \in \sum I f_i \subset M'$. $\square$

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

(4)
$$\begin{array}{ccccc}
M & = & M & & \\
\downarrow & & \downarrow & & \\
N & \hookrightarrow & R^r & \xrightarrow{k} & I \\
{\scriptstyle l}\downarrow & & \downarrow & & \| \\
\mathbb{Z}^r & \hookrightarrow & Q & \twoheadrightarrow & I
\end{array}$$

yields the following diagram of homomorphisms of the tori

(5)
$$\begin{array}{ccccc}
U^\Phi & \hookrightarrow & S^\Phi & \twoheadrightarrow & \mathbb{G}_m^r \\
\| & & \downarrow & & \downarrow \\
U^\Phi & \hookrightarrow & P^\Phi & \twoheadrightarrow & V^\Phi \\
 & & \downarrow & & \downarrow \\
 & & T^\Phi & = & T^\Phi
\end{array}$$

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

(6)
$$0 \to I \to R \to \mathbb{Z} \to 0$$

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

$$H^1(K,U^\Phi)\simeq \mathrm{Br}(KL/K). \tag{7}$$

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* (5) *takes* $(x_1,\dots,x_r)$ *to* $\sum_{i=1}^r\big((\chi_i)_K\cup(x_i)\big)$.

Proof. Consider the composition

$$h:\mathrm{Hom}_G(\mathbb{Z}^r,\mathbb{Z})\to \mathrm{Ext}^1_G(I,\mathbb{Z})\to \mathrm{Ext}^2_G(\mathbb{Z},\mathbb{Z})=H^2(G,\mathbb{Z})=\mathrm{Ch}(G), \tag{8}$$

where the first homomorphism is induced by the bottom row of the diagram (4) and the second one - by the exact sequence (6).

We claim that for any k, the image of the k-th projection $p_k:\mathbb{Z}^r\to\mathbb{Z}$ under the composition (8) 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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}^r & \longrightarrow & Q & \longrightarrow & I & \longrightarrow & 0\\ & & \downarrow{\scriptstyle p_k} & & \downarrow & & \downarrow{\scriptstyle f_k} & & \\ 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array} \tag{9}$$

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 (9) 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 (8). Hence $h(p_k)$ is also the image of the class β of the sequence (6) 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 (9) yields a commutative diagram

$$\begin{array}{ccc} H^1(G,I) & \xrightarrow{\partial} & H^2(G,\mathbb{Z}^r)\\ \downarrow{\scriptstyle f_k^*} & & \downarrow{\scriptstyle p_k^*}\\ H^1(G,\mathbb{Q}/\mathbb{Z}) & = & H^2(G,\mathbb{Z}) \end{array}$$

As we have shown, $p_k^*(\partial(\beta))=h(p_k)$. 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

$$\begin{array}{ccccc} (K^\times)^r=\mathrm{Hom}_G(\mathbb{Z}^r,\mathbb{Z})\otimes K^\times & \longrightarrow & \mathrm{Ext}^1_G(I,\mathbb{Z})\otimes K^\times & \longrightarrow & \mathrm{Ext}^2_G(\mathbb{Z},\mathbb{Z})\otimes K^\times\\ \| & & \downarrow & & \downarrow\\ (K^\times)^r=\mathrm{Hom}_G(\mathbb{Z}^r,KL^\times) & \longrightarrow & \mathrm{Ext}^1_G(I,KL^\times) & \longrightarrow & \mathrm{Ext}^2_G(\mathbb{Z},KL^\times), \end{array}$$

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

Corollary 3.7. *The map $H^1(K, U^\Phi) \to H^1(K, S^\Phi)$ induces an isomorphism $H^1(K, S^\Phi) \simeq \operatorname{Br}_{\text{ind}}(KL/K)$.*

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

$$
\begin{array}{ccccc}
V(K) & \longrightarrow & H^1(K, U^\Phi) & = & \operatorname{Br}(KL/K) \\
\downarrow & & \downarrow & & \downarrow \\
T(K) & \longrightarrow & H^1(K, S^\Phi) & = & \operatorname{Br}_{\text{ind}}(KL/K)
\end{array} \tag{10}
$$

with surjective homomorphisms.

3.3. **The element** a**.** Let a' be the image of the generic point of V over $K = F(V)$ in $\operatorname{Br}\big(L(V)/F(V)\big)$ in the diagram (10). Choose also an element $a \in \operatorname{Br}\big(L(T)/F(T)\big)$ corresponding to the generic point of T over $F(T)$. The field $F(T)$ is a subfield of $F(V)$ and the classes $a_{F(V)}$ and a' are equal in $\operatorname{Br}_{\text{ind}}\big(L(V)/F(V)\big)$. It follows that $pa_{F(V)} = pa'$ in $\operatorname{Br} F(V)$.

The exact sequence of G-modules

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

induces an exact sequence

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

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

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

Then (4) and (6) 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. (cf., [11, Lemma 2.4]) *We have $\varphi(\xi) = -a' + \operatorname{Br}(F)$.*

Proof. Consider the following diagram

$$\begin{array}{ccccc}
 & & & & \operatorname{Hom}_G(\mathbb{Z},\mathbb{Z}) \\
 & & & & \downarrow \\
 & & \operatorname{Hom}_G(I,I) & \longrightarrow & \operatorname{Ext}^1_G(\mathbb{Z},I) \\
 & & \downarrow & & \downarrow \\
\operatorname{Hom}_G(N,N) & \longrightarrow & \operatorname{Ext}^1_G(I,N) & \longrightarrow & \operatorname{Ext}^2_G(\mathbb{Z},N) \\
\downarrow & & \downarrow{\scriptstyle l} & & \downarrow \\
\operatorname{Hom}_G\big(N,L(V)^\times\big) & \longrightarrow & \operatorname{Ext}^1_G\big(I,L(V)^\times\big) & \longrightarrow & \operatorname{Ext}^2_G\big(\mathbb{Z},L(V)^\times\big)
\end{array}$$

By [2, Ch. XIV], the images of $1_{\mathbb{Z}}$ and -1_I agree in $\operatorname{Ext}^1_G(\mathbb{Z},I)$ and the images of 1_N and -1_I agree in $\operatorname{Ext}^1_G(I,N)$. It follows from [2, Ch. V, Prop. 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 $a' + \operatorname{Br}(F)$ in the right bottom corner. □

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

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

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 $\operatorname{rank}(P)$ is called *minimal.*

Essential p-dimension of algebraic tori was determined in [8, Th. 1.4]:

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

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

Proof. As explained in Example 3.3, a surjective G-homomorphism f yields a generically free representation of S of dimension $\operatorname{rank}(P)$. By [13, §3],

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

In this section we derive from 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 $[G : H] \leq p^k$. We have the sequence of subgroups

$$0 = V_{-1} \subset V_0 \subset \cdots \subset V_r = \overline{X}. \tag{11}$$

Theorem 4.3. *We have the following explicit formula for the essential p-dimension of S:*

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

Proof. Set$b_k = \operatorname{rank}(V_k)$. By Theorem 4.1, it suffices to prove that the smallest rank of the G-module P is 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. As 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 $|A_j| \leq p^k$. 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 we have

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

Set $c'_k = b_r - c_k$, so that $b_k \geq c'_k$ 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

$$\operatorname{rank}(P) = \sum_{k=0}^{r} (c_{k-1} - c_k) p^k = \sum_{k=0}^{r} (c'_k - c'_{k-1}) p^k =$$
$$c'_r p^r + \sum_{k=0}^{r-1} c'_k (p^k - p^{k+1}) \geq b_r p^r + \sum_{k=0}^{r-1} b_k (p^k - p^{k+1}) = \sum_{k=0}^{r} (b_k - b_{k-1}) p^k.$$

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 pre-image 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. As 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 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

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

4.1. **Examples.** Let F be a field, Φ a subgroup of ${}_p\operatorname{Ch}(F)$ of rank r, $L = F(\Phi)$ and $G = \operatorname{Gal}(L/F)$. Consider the torus U^Φ with the character group the augmentation ideal I defined in 3.2.

The middle row of (4) yields an exact sequence

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

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

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 $N_H x$ for all $x \in I$, where $N_H = \sum_{h \in H} h \in R$. Since $\overline{I}$ is of period p with the trivial G-action, the classes of the elements $N_H x$ in $\overline{I}$ are trivial if H is a nontrivial subgroup of G. It follows that the maps $I^H \to \overline{I}$ are trivial for all $H \neq 1$. In the notation of (11), $V_0 = \cdots = V_{r-1} = 0$ and $V_r = \overline{I}$. 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,

$$\operatorname{ed}(U^\Phi) = \operatorname{ed}_p(U^\Phi) = (r-1)p^r + 1. \tag{12}$$

Let S^Φ be the torus with the character group Q defined in 3.2. As in (4), the homomorphism k factors through a surjective map $R^r \to Q$ that is then necessarily a minimal p-presentation of Q. According to Theorem 4.3 and Corollary 4.2,

$$\operatorname{ed}(S^\Phi) = \operatorname{ed}_p(S^\Phi) = rp^r - \dim(S^\Phi) = (r-1)p^r - r + 1. \tag{13}$$

5. Degeneration

In this section we study the behavior of the essential p-dimension under degeneration, i.e. 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.

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

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

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. (1) If Φ is the zero subgroup, then $\mathcal{F}_k^{\Phi} = \mathcal{B}_k^{\Phi} \simeq \mathsf{Alg}(p^r) \simeq \mathbf{PGL}(p^r)$- $\mathsf{torsors}$.

(2) 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 3.2, thus, $\mathcal{F}_0^{\Phi} \simeq S^{\Phi}$- $\mathsf{torsors}$.

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 $a \in \mathcal{B}_k^{\Phi}(E)$, i.e., $a \in \mathrm{Br}(E)\{p\}$ 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

$$a' = \widehat{a} + \big(\widehat{\eta}_E \cup (x)\big) \in \mathrm{Br}(E'), \tag{14}$$

for some $x \in E'^{\times}$ such that $v'(x)$ is not divisible by p. By Proposition 2.2(2), $\operatorname{ind}(a_{E'(\Phi')}) = p \cdot \operatorname{ind}(a_{E(\Phi)}) \leq p^{k+1}$, hence $a' \in \mathcal{B}_{k+1}^{\Phi'}(E')$.

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 $\operatorname{ind} a_{N(\Phi',\rho)} > p^{k-1}$. Then*

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

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

$$a'_M - (a'_0)_M \in \mathrm{Br}_{\mathrm{dec}}\big(M(\Phi')/M\big). \tag{15}$$

It follows from (14) that

$$a'_M = \widehat{a}_N + \big(\widehat{\eta}_N \cup (x)\big) \tag{16}$$

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(3),

$$\partial_v(a'_M) = e' \cdot \partial_{v'}(a') = e'q \cdot \eta_E. \tag{17}$$

Let v_0 be the restriction of v to M_0 and N_0 its residue field. It follows from (15) that

$$\partial_v(a'_M) - \partial_v((a'_0)_M) \in \Phi'_N. \tag{18}$$

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

$$\eta_N \notin \Phi'_N. \tag{19}$$

By (17), (18) and (19), $\partial_v\big((a'_0)_M\big) \neq 0$, i.e., $(a'_0)_M$ is ramified and therefore v_0 is nontrivial, i.e., 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(3),

$$\partial_v((a'_0)_M) = e \cdot (\eta_0)_N, \tag{20}$$

where e is the ramification index of M/M_0, hence $(\eta_0)_N \neq 0$. It follows from (17),(18) and (20) that

$$e'q \cdot \eta_N - e \cdot (\eta_0)_N \in \Phi'_N. \tag{21}$$

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

$$\eta_N \in \langle \Phi'_N, (\eta_0)_N \rangle \quad \text{in} \quad \mathrm{Ch}(N). \tag{22}$$

Let p^t $(t \geq 1)$ be the order of $(\eta_0)_N$. It follows from (19) and (21) that $v_p(e) = t - 1$ and

$$p^{t-1} \cdot (\eta_0)_N \in \Phi_N \setminus \Phi'_N. \tag{23}$$

Choose a prime element π_0 in M_0 and write

$$(a'_0)_{\widehat{M}_0} = \widehat{a}_0 + \big(\widehat{\eta}_0 \cup (\pi_0)\big) \tag{24}$$

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 (15), (16) and (24), using (3) and (22), we get

$$a_N - (a_0)_N \in \mathrm{Br}_{\mathrm{dec}}\big(N(\Phi', \eta_0)/N\big). \tag{25}$$

It follows from (25) that

$$a_{N(\Phi',\eta_0)} = (a_0)_{N(\Phi',\eta_0)} \tag{26}$$

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

By (24),

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

As no nontrivial multiple of $(\eta_0)_N$ belongs to Φ'_N by (23), the order of the character $(\eta_0)_{N_0(\Phi')}$ is at least p^t. It follow from Proposition 2.2(2) that

$$\operatorname{ind}(a_0)_{N_0(\Phi',\eta_0)} = \operatorname{ind}(a'_0)_{\widehat{M_0}(\Phi')}/\operatorname{ord}(\eta_0)_{N_0(\Phi')} \le p^{k+1}/p^t = p^{k-t+1}. \tag{27}$$

By (26) and (27),

$$\operatorname{ind}(a_{N(\Phi',\eta_0)}) \le p^{k-t+1}. \tag{28}$$

Suppose that $t \ge 2$ and consider the character $\rho = p^{t-2}\cdot(\eta_0)_N$ of order p^2 in $\operatorname{Ch}(N)$. We have $p\cdot\rho = p^{t-1}(\eta_0)_N \in \Phi_N \setminus \Phi'_N$ by (23). Moreover, the degree of the field extension $N(\Phi',\eta_0)/N(\Phi',\rho)$ is equal to p^{t-2}. Hence by (28),

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

This contradicts the assumption. Therefore, $t = 1$, i.e., $\operatorname{ord}(\eta_0)_N = p$. Then $(e,p) = 1$ and it follows from (21) that $(\eta_0)_N \in \langle \Phi'_N, \eta_N\rangle$. Moreover,

$$\langle \Phi', \eta_0\rangle_N = \langle \Phi', \eta\rangle_N = \Phi_N. \tag{29}$$

By Lemma 2.1, there is a finite subextension N_1/N_0 of N/N_0 such that $\langle \Phi', \eta_0\rangle_{N_1} = \Phi_{N_1}$. 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 $\operatorname{Ch}(N_0)$.

Since by (27),

$$\operatorname{ind}(a_0)_{N_0(\Phi)} = \operatorname{ind}(a_0)_{N_0(\Phi',\eta_0)} \le p^k,$$

we have $a_0 \in \mathcal{B}^{\Phi}_k(N_0)$.

It follows from (25) that

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

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

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

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

Let Φ be a subgroup in ${}_p\operatorname{Ch}(F)$ of rank r. Choose a basis $\chi_1, \chi_2, \dots, \chi_r$ of Φ. Let E/F be a field extension such that $\operatorname{rank}(\Phi_E) = r$ and let $a \in \operatorname{Br}(E)\{p\}$ 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 $a_k \in \operatorname{Br}(E_k)\{p\}$ 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(2) that

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

for any $k = 1, \dots, r$. As $\operatorname{ind} a_{E(\Phi)} = 1$, 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 followings 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 $p^{r-1}a \notin \operatorname{Im}\bigl(\operatorname{Br}(F) \to \operatorname{Br}(E)\bigr)$. 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 $\rho \in \operatorname{Ch}(N)$ of order p^2 such that $p \cdot \rho \in \bigl(\Phi_k)_N \setminus (\Phi_{k+1}\bigr)_N$, we have*

$$\operatorname{ind}(a_k)_{N(\Phi_{k+1},\rho)} > p^{k-1}. \tag{30}$$

Proof. Induction on r. The case $r = 1$ is obvious. Suppose that the inequality (30) does not hold for some $k = 1, \dots, r-1$, a finite field extension N/E_k and a character $\rho \in \operatorname{Ch}(N)$. Suppose first that $k < r-1$. Consider the fields $F' = F(\Phi_{k+1})$, $E' = E(\Phi_{k+1})$, $E'_i = E_i(\Phi_{k+1})$, $N' = N(\Phi_{k+1})$, the sequence of characters $(\chi_i)_{F'}$ and the sequence of elements $a'_i := (a_i)_{E'_i} \in \operatorname{Br}(E_i)$ for $i = 0, 1, \dots, k+1$. As $(a'_k)_{N'(\rho)} = (a_k)_{N(\Phi_{k+1},\rho)}$, the inequality (30) does not hold for the term a'_k of the new sequence, the field extension N'/E'_k and the character $\rho_{N'}$.

Note that $p^k a_{E'} \notin \operatorname{Im}\bigl(\operatorname{Br}(F') \to \operatorname{Br}(E')\bigr)$, because otherwise, taking the norm map for the extension F'/F of degree p^{r-k-1}, we would get $p^{r-1}a \in \operatorname{Im}\bigl(\operatorname{Br}(F) \to \operatorname{Br}(E)\bigr)$. By induction, the inequality (30) holds for all the terms of the new sequence, in particular for a'_k, a contradiction.

Thus we can assume that $k = r-1$. 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 $\tilde{E}_{r-1} = N$ and let $\tilde{E}_r$ be an unramified extension of E_r with the residue field $\tilde{E}_{r-1}$. The fields $\tilde{E}_j$ with $j < r-1$ are constructed by descending induction on j. If we have constructed $\tilde{E}_j$ as a finite extension of E_j of degree prime to p, then we extend the valuation v_j to $\tilde{E}_j$ and let $\tilde{E}_{j-1}$ to be its residue field. Replacing E_i by $\tilde{E}_i$ and a_i by $(a_i)_{\tilde{E}_i}$, we may assume that $N = E_{r-1}$.

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

$$\operatorname{ind}(a_{r-2})_{E_{r-2}(\chi_{r-1},\mu)} = \operatorname{ind}(a_{r-1})_{E_{r-1}(\rho)}/p = \operatorname{ind}(a_{r-1})_{E_{r-1}(\Phi_r,\rho)}/p \le p^{r-3}. \tag{31}$$

Consider the fields $F' = F(\chi_{r-1})$, $E' = E(\chi_{r-1})$, $E'_i = E_i(\chi_{r-1})$, $N' = N(\chi_{r-1})$, the sequence of characters $\chi_1, \dots, \chi_{r-2}, \chi_r$ and the elements $a'_i \in \operatorname{Br}(E'_i)$ for $i = 0, 1, \dots, r-1$ defined by $a'_i = (a_i)_{E'_i}$ for $i \le r-2$ and $a'_{r-1} = \widehat{a}_{r-2} + \bigl(\widehat{\chi}_r \cup (x_{r-1})\bigr)$ over E'_{r-1}. As $(a'_{r-2})_{N'(\mu)} = (a_{r-2})_{N(\chi_{r-1},\rho)}$, the inequality (31) shows that (30) does not hold for the term a'_{r-2} of the new sequence, the field extension N'/E'_{r-2} and the character $\mu_{N'}$.

Note that $p^{r-2}a_{E'} \notin \operatorname{Im}\bigl(\operatorname{Br}(F') \to \operatorname{Br}(E')\bigr)$, as otherwise, taking the norm map for the extension F'/F of degree p, we get $p^{r-1}a \in \operatorname{Im}\bigl(\operatorname{Br}(F) \to \operatorname{Br}(E)\bigr)$.

By induction, the inequality (30) holds for all the terms of the new sequence, in particular for a'_{r-2}, a contradiction.

Case 2: The character ρ is ramified. Note that $p\cdot\rho$ is a nonzero multiple of $(\chi_r)_{E_{r-1}}$. As the inequality (30) fails for a_{r-1}, we have

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

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

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

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 $\langle \chi_1, \dots, \chi_j, \chi_{r-1}\rangle \cap \Theta_j = 0$, $E_j(\chi_r) = E_j(\bar{u}_j^{1/p})$ and

$$\operatorname{ind}\big(a_j - (\chi_{r-1} \cup (\bar{u}_j^{1/p}))\big)_{E_j(\Theta_j)} \le p^j. \tag{32}$$

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

($j \Rightarrow j-1$): The field $E_j(\bar{u}_j^{1/p}) = E_j(\chi_r)$ is unramified over E_j, 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

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

where $\eta = \chi_j - m\chi_{r-1}$ and $b = \big(a_{j-1} - (\chi_{r-1} \cup (\bar{u}_{j-1}^{1/p}))\big)_{E_{j-1}(\Theta_j)}$. As 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(2) that

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

Applying the inequality (32) in the case $j = 0$, we get

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

for an element $w \in E^\times$ such that $E(w^{1/p}) = E(\chi_r)$. The degree of the extension $E(\Theta_0)/E$ is equal to p^{r-1} and $E(w^{1/p}) \subset E(\Theta_0)$. Taking the norm for the extension $E(\Theta_0)/E$, we get that $p^{r-1}a$ is a multiple of $\chi_{r-1} \cup (w)$. As the character χ_r is defined over F, we may assume that $w \in F^\times$, hence $p^{r-1}a \in \operatorname{Im}\big(\operatorname{Br}(F) \to \operatorname{Br}(E)\big)$, a contradiction. Thus, we have shown that the inequality (30) holds. □

By Example 5.1(2), we can view a as an S^Φ-torsor over E.

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

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

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

$$\begin{aligned}\operatorname{ed}_p^{\mathsf{Alg}(p^r)}(a_r) = \operatorname{ed}_p^{\mathcal{F}_r^{\Phi_r}}(a_r) \geq \operatorname{ed}_p^{\mathcal{F}_{r-1}^{\Phi_{r-1}}}(a_{r-1}) + 1 \geq \dots \\ \geq \operatorname{ed}_p^{\mathcal{F}_1^{\Phi_1}}(a_1) + (r-1) \geq \operatorname{ed}_p^{\mathcal{F}_0^{\Phi_0}}(a_0) + r = \operatorname{ed}_p^{S^\Phi\text{-}\mathsf{torsors}}(a) + r.\end{aligned}$$

□

6. Proof of the main theorem

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

$$\operatorname{ed}_p\big(\mathsf{Alg}_F(p^r)\big) \geq (r-1)p^r + 1.$$

Proof. As $\operatorname{ed}_p\big(\mathsf{Alg}_F(p^r)\big) \geq \operatorname{ed}_p\big(\mathsf{Alg}_{F'}(p^r)\big)$ for any field extension F'/F by [10, Prop. 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 there is a subgroup Φ of ${}_p\operatorname{Ch}(F)$ of rank r. Let T^Φ be the algebraic torus constructed in Section 3 for the field extension $L = F(\Phi)$ of F. Set $E = F(T^\Phi)$ and let $a \in \operatorname{Br}(EL/E)$ be the element defined in 3.3. Let $a_r \in \operatorname{Br}(E_r)$ be the element of index p^r constructed in 5.2. By Corollary 3.9, the class $p^{r-1}a$ in $\operatorname{Br}(E)$ does not belong to the image of $\operatorname{Br}(F) \to \operatorname{Br}(E)$. It follows from Corollary 5.4 that

$$\operatorname{ed}_p^{\mathsf{Alg}(p^r)}(a_r) \geq \operatorname{ed}_p^{S^\Phi\text{-}\mathsf{torsors}}(a) + r. \tag{33}$$

The S^Φ-torsor a is the generic fiber of the versal S^Φ-torsor $P^\Phi \to S^\Phi$ (see Example 3.3), hence a is a generic torsor. By [14, §6] or [10, Th. 2.9]

$$\operatorname{ed}_p^{S^\Phi\text{-}\mathsf{torsors}}(a) = \operatorname{ed}_p(S^\Phi). \tag{34}$$

The essential p-dimension of S^Φ was calculated in (13):

$$\operatorname{ed}_p(S^\Phi) = (r-1)p^r - r + 1. \tag{35}$$

Finally, it follows from (33), (34) and (35) that

$$\operatorname{ed}_p\big(\mathsf{Alg}_F(p^r)\big) \geq \operatorname{ed}_p^{\mathsf{Alg}(p^r)}(a_r) \geq \operatorname{ed}_p^{S^\Phi\text{-}\mathsf{torsors}}(a) + r = (r-1)p^r + 1.$$

□

7. Remarks

Let K/F be a field extension and G an elementary abelian group of order p^r. Consider the subset $\mathsf{Alg}_K(G)$ of $\mathsf{Alg}_K(p^r)$ consisting of all classes admitting a splitting Galois K-algebra with the Galois group G. Equivalently, $\mathsf{Alg}_K(G)$ consists of all classes represented by crossed product algebras with the group G (see [5, §4.4]).

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

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

Theorem 7.1. *Let F be a field, p an 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 $\mathsf{Alg}(L/F)$, $\mathsf{Alg}(G)$ and $\mathsf{Pair}_K(G)$. Then*

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

Proof. The functor $\mathsf{Alg}(L/F)$ is isomorphic to U^Φ*-* $\mathsf{torsors}$ by (7). It follows from (12) that

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

Let a_r be the element in $\mathrm{Br}(E_r)$ in the proof of Theorem 6.1. It satisfies $\mathrm{ed}_p^{\mathsf{Alg}(p^r)}(a_r) \geq (r-1)p^r + 1$. By construction, $a_r \in \mathsf{Alg}_{E_r}(G)$. As $\mathsf{Alg}(G)$ is a subfunctor of $\mathsf{Alg}(p^r)$, we have

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

The upper bound $\mathrm{ed}\big(\mathsf{Alg}(G)\big) \leq (r-1)p^r + 1$ was proven in [7, Cor. 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 $\mathsf{Pair}_K(G)$ is isomorphic to H- $\mathsf{torsors}$.

The character group of U is G-isomorphic to the ideal I in $R = \mathbb{Z}[G]$. By [12, §3], the G-homomorphism $k : R^r \to I$ constructed in 3.2 yields a representation W of the group H of dimension rp^r. As $r \geq 2$, by Lemma 3.4, G acts faithfully on the kernel N of k. By [12, Lemma 3.3], the action of H on W is generically free, hence

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

Since $\mathsf{Pair}(G)$ surjects onto $\mathsf{Alg}(G)$, we have

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

References

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

[2] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1999, With an appendix by David A. Buchsbaum, Reprint of the 1956 original.

[3] J.-L. Colliot-Thélène and J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. (4) **10** (1977), no. 2, 175–229.

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

[5] I. N. Herstein, *Noncommutative rings*, Mathematical Association of America, Washington, DC, 1994, Reprint of the 1968 original, With an afterword by Lance W. Small.

[6] B. Jacob and A. Wadsworth, *Division algebras over Henselian fields*, J. Algebra **128** (1990), no. 1, 126–179.

[7] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670.
[8] R. Lötscher, M. MacDonald, A. Meyer, and R. Reichstein, *Essential p-dimension of algebraic tori*, preprint, 2009.
[9] H. Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.
[10] A. S. Merkurjev, *Essential dimension*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 299–325.
[11] A. S. Merkurjev, *Essential p-dimension of* $\mathrm{PGL}(p^2)$, to appear, 2009.
[12] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra and Number Theory **3** (2009), no. 4, 467–487.
[13] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.
[14] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, With an appendix by János Kollár and Endre Szabó.
[15] J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.
[16] J.-P. Tignol, *Sur les classes de similitude de corps à involution de degré* 8, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 20, A875–A876.

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