ESSENTIAL p-DIMENSION OF SPLIT SIMPLE GROUPS OF TYPE A_n

VLADIMIR CHERNOUSOV AND ALEXANDER MERKURJEV

1. Introduction

Let F be a field and let $\mathcal{F} : \mathsf{Fields}/F \to \mathsf{Sets}$ be a functor from the category Fields/F of field extensions over F to the category Sets of sets. Let $E \in \mathsf{Fields}/F$ and $K \subset E$ a subfield over F. We say that that K is a *field of definition of* $\alpha \in \mathcal{F}(E)$ if α belongs to the image of the map $\mathcal{F}(K) \to \mathcal{F}(E)$. The *essential dimension of* α, denoted $\mathrm{ed}^{\mathcal{F}}(\alpha)$, is the least transcendence degree $\mathrm{tr.deg}_F(K)$ over all fields of definition K 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 all fields $E \in \mathsf{Fields}/F$ and all $\alpha \in \mathcal{F}(E)$ (see [3, Def. 1.2] or [5, Sec.1]). Informally, the essential dimension of $\mathcal{F}$ is the smallest number of algebraically independent parameters required to define $\mathcal{F}$ and may be thought of as a measure of complexity of $\mathcal{F}$.

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

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

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

For every integer $n \geq 1$, a divisor m of n and any field extension E/F, let $\mathsf{Alg}_E(n,m)$ denote the set of isomorphism classes of central simple E-algebras of degree n and exponent dividing m. We can identify $\mathsf{Alg}_E(n,m)$ with the subset of the m-torsion part $\mathrm{Br}_m(E)$ of the Brauer group of E consisting of all elements a such that the index $\mathrm{ind}(a)$ of a divides n. We view $\mathsf{Alg}(n,m)$ as a functor $\mathsf{Fields}/F \to \mathsf{Sets}$. Upper and lower bounds for the essential p-dimension $\mathrm{ed}_p\big(\mathsf{Alg}(n,m)\big)$ for a prime integer p different from $\mathrm{char}(F)$ can be found in [2].

Let G be an algebraic group scheme over F. Write $\mathcal{F}_G$ for the functor taking a field extension E/F to the set $H^1(E,G)$ of isomorphism classes of principal homogeneous G-spaces (G-torsors) over E. The essential (p-)dimension of $\mathcal{F}_G$ is called the *essential (p-)dimension of* G and is denoted by $\mathrm{ed}(G)$ and $\mathrm{ed}_p(G)$.

The work of the first author has been supported in part by Canada Research Chairs Program and NSERC research grant.

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

A split simple algebraic group G of type A_{n-1} is isomorphic to $\mathbf{SL}_n/\boldsymbol{\mu}_m$ for a divisor m of n. In the present paper we compute the essential p-dimension of G in terms of the integer $\operatorname{ed}_p\big(\mathsf{Alg}(n,m)\big)$.

Theorem 1.1. *Let n be a natural number, m a divisor of n and p a prime integer. Let p^r and p^s be the largest powers of p dividing n and m respectively and let $G=\mathbf{SL}_n/\boldsymbol{\mu}_m$ be the algebraic group defined over a field F of the characteristic not p. Then*

$$ed_p(G)=\begin{cases} 0, & \text{if } s=0;\\ \operatorname{ed}_p\big(\mathsf{Alg}(p^r,p^r)\big), & \text{if } s=r;\\ \operatorname{ed}_p\big(\mathsf{Alg}(p^r,p^s)\big)+1, & \text{if } 0<s<r.\end{cases}$$

Using lower bounds for $\operatorname{ed}_p\big(\mathsf{Alg}(p^r,p^s)\big)$ obtained in [1] and [2], we get:

Corollary 1.2. *If p is a prime integer then*

(1) $p^{2r-2}+p^{r-s}+1\geq \operatorname{ed}_p(\mathbf{SL}_{p^r}/\boldsymbol{\mu}_{p^s})\geq (r-1)p^r+p^{r-s}+1$ *if* $0<s<r$ *and p is odd in the case $s=1$,*
(2) $2^{2r-4}+2^{r-1}+1\geq \operatorname{ed}_2(\mathbf{SL}_{2^r}/\boldsymbol{\mu}_2)\geq (r-1)2^{r-1}+1$ *if* $r\geq 3$.
(3) $\operatorname{ed}_p(\mathbf{SL}_{p^2}/\boldsymbol{\mu}_p)=p^2+p+1$ *if p is odd,*
(4) $\operatorname{ed}_2(\mathbf{SL}_4/\boldsymbol{\mu}_2)=5$,
(5) $\operatorname{ed}_2(\mathbf{SL}_8/\boldsymbol{\mu}_2)=9$,
(6) $\operatorname{ed}_2(\mathbf{SL}_8/\boldsymbol{\mu}_4)=19$,
(7) $\operatorname{ed}_2(\mathbf{SL}_{16}/\boldsymbol{\mu}_2)=25$.

2. Unramified torsors

Let R be a commutative ring and let G be a group scheme defined over R. There is a bijection between the set of isomorphism classes of G-torsors over R and the pointed set $H^1(R,G)$ of the first cohomology of G for the flat topology (see [4, Exp. XXIV]). If G is smooth, one can use the étale topology instead of flat topology.

Let K be a discrete valued field with valuation ring $R\subset K$ and residue field $\overline{K}$. We write $H^1(K,G)_{nr}$ for the image of the map

$$H^1(R,G)\to H^1(K,G).$$

Let $\alpha\in H^1(K,G)$. If $\alpha\in H^1(K,G)_{nr}$ we say that α is *unramified*. Otherwise α is *ramified*.

If K is complete and G is smooth, the canonical map $H^1(R,G)\to H^1(\overline{K},G)$ is a bijection [4, Exp. XXIV, Prop. 8.1], hence $H^1(K,G)_{nr}\simeq H^1(\overline{K},G)$.

If G is commutative, then $H^1(K,G)_{nr}$ is a subgroup of $H^1(K,G)$. We write $H^1(K,G)_{ram}$ for the factor group.

Example 2.1. We have $H^1(K,\boldsymbol{\mu}_k)=K^\times/K^{\times k}$, $H^1(K,\boldsymbol{\mu}_k)_{nr}=R^\times/R^{\times k}$ and $H^1(K,\boldsymbol{\mu}_k)_{ram}=\mathbb{Z}/k\mathbb{Z}$.

Suppose that K is complete. Let T' be a torus over R. We write T for $T'\otimes_R K$ and $\overline{T}$ for $T'\otimes_R\overline{K}$. Clearly, T and $\overline{T}$ are tori over K and $\overline{K}$ respectively. The character group $\overline{T}^*$ of $\overline{T}$ is a module over the absolute Galois group $\Gamma_{\overline{K}}$.

The character group T^* coincides with $\overline{T}^*$, and Γ_K acts on T^* via the canonical surjective homomorphism $\Gamma_K \to \Gamma_{\overline{K}}$.

We have the split exact sequence of Galois $\Gamma_{\overline{K}}$-modules

$$1 \to R_{nr}^\times \to K_{nr}^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

where R_{nr} and K_{nr} are maximal unramified extensions of R and K respectively. Tensoring this sequence with the $\Gamma_{\overline{K}}$-module of co-characters $\overline{T}_*$, the dual of $\overline{T}^*$, and taking cohomology groups yields exact sequences

$$1 \to T(R) \to T(K) \to \overline{T}_*(\overline{K}) \to 0,$$

$$0 \to H^1_{et}(R, T) \to H^1(K, T) \xrightarrow{v_*} H^1(\overline{K}, \overline{T}_*) \to 0.$$

In particular, the group $H^1(K, T)_{ram}$ is canonically isomorphic to $H^1(\overline{K}, \overline{T}_*)$.

3. Azumaya algebras and torsors

Let $n = km$ and $G = \mathbf{SL}_n / \boldsymbol{\mu}_m$ over a field F, so we have an exact sequence

$$1 \to \boldsymbol{\mu}_k \to G \to \mathbf{PGL}_n \to 1. \tag{1}$$

Let R be a commutative local F-algebra. The exact sequence (1) yields an exact sequence of pointed sets

$$H^1(R, G) \xrightarrow{\alpha} H^1(R, \mathbf{PGL}_n) \xrightarrow{\partial} H^2(R, \boldsymbol{\mu}_k).$$

Moreover, the group $H^1(R, \boldsymbol{\mu}_k) = R^\times / R^{\times k}$ acts on the set $H^1(R, G)$ transitively in the fibers of the map α. For an element $r \in R^\times$ and $\xi \in H^1(R, G)$ we write $r\xi$ for the result of the action of $rR^{\times k}$ on ξ.

Recall that there is a canonical bijection between $H^1(R, \mathbf{PGL}_n)$ and the set of isomorphism classes $\mathsf{Alg}_R(n)$ of Azumaya R-algebras of degree n, so we have the map $H^1(R, G) \to \mathsf{Alg}_R(n)$ [6, Ch. IV].

The group $H^2(R, \boldsymbol{\mu}_k)$ is identified with the subgroup $\mathrm{Br}_k(R)$ of the Brauer group $\mathrm{Br}(R) = H^2(R, \mathbf{G}_\mathrm{m})$ of R and the map ∂ takes an algebra A to the class of $A^{\otimes m}$ in $\mathrm{Br}(R)$. Therefore, the image of an element $\xi \in H^1(R, G)$ in $H^1(R, \mathbf{PGL}_n)$ yields a class A_ξ in $\mathsf{Alg}_R(n, m) \subset \mathsf{Alg}_R(n)$ of algebras of exponent dividing m. Moreover, every class $A \in \mathsf{Alg}_R(n, m)$ is of the form $A = A_\xi$ for some $\xi \in H^1(R, G)$.

Twisting (1) by the class of an algebra $A \in \mathsf{Alg}_R(n)$ yields an exact sequence

$$1 \to \boldsymbol{\mu}_k \to G' \to \mathbf{PGL}_1(A) \to 1.$$

The connecting homomorphism

$$A^\times / R^\times = \mathbf{PGL}_1(A)(R) \to H^1(R, \boldsymbol{\mu}_k) = R^\times / R^{\times k}$$

takes the class $aR^\times$ to $\mathrm{Nrd}(a) R^{\times k}$, where $\mathrm{Nrd} : A^\times \to R^\times$ is the reduced norm homomorphism. This yields:

Lemma 3.1. *Let R be a commutative local F-algebra and $A \in \mathsf{Alg}_R(n, m)$. Then the factor group $R^\times / \big(R^{\times k} \cdot \mathrm{Nrd}(A)\big)$ acts simply transitively on the fiber of the surjective map $H^1(R, G) \to \mathsf{Alg}_R(n, m)$ over A.*

Let K/F be a field extension with a discrete valuation v over F and a prime element π.

Lemma 3.2. *Let $\xi \in H^1(K,G)$ be an unramified element such that $A_\xi \neq 0$ in $\operatorname{Br}(K)$. If $\pi\xi$ is unramified then k and $\operatorname{ind}(A_\xi)$ are relatively prime.*

Proof. Let $R \subset K$ be the valuation ring. By assumption, there are $\zeta, \zeta' \in H^1(R,G)$ such that $\xi = \zeta_K$ and $\pi\xi = \zeta'_K$. We have $(A_\zeta)_K = A_\xi = A_{\pi\xi} = (A_{\zeta'})_K$. As the map $\operatorname{Br}(R) \to \operatorname{Br}(K)$ is injective by [6, Ch. IV, Cor. 2.6], we have $A_\zeta = A_{\zeta'}$. It follows from Lemma 3.1 that $\zeta' = \lambda\zeta$ for some $\lambda \in R^\times$. Then $\pi\xi = \zeta'_K = \lambda\zeta_K = \lambda\xi$, therefore by Lemma 3.1 again, $\pi \in \lambda(K^{\times k} \cdot \operatorname{Nrd}(A_\xi))$. Therefore, $1 = v(\pi) \in k\mathbb{Z} + \operatorname{ind}(A_\xi)\mathbb{Z}$ as $v(\operatorname{Nrd}(A_\xi)) \subset \operatorname{ind}(A_\xi)\mathbb{Z}$ by [7, Ch. XII, §2]. □

4. Tori

Let L/F be a separable field extension of degree $n = p^r$, where p is a prime integer and $m = p^s$ a divisor of n. Consider the torus of norm one elements $R^{(1)}_{L/F}\big(\mathbf{G}_{\mathrm{m},L}\big)$ for the extension L/F, the factor torus $T = R^{(1)}_{L/F}\big(\mathbf{G}_{\mathrm{m},L}\big)/\boldsymbol{\mu}_m$ and $S = R_{L/F}\big(\mathbf{G}_{\mathrm{m},L}\big)/\,\mathbf{G}_{\mathrm{m}}$. Then T and S can be viewed as maximal tori of G and $\mathbf{PGL}_n$ respectively and we have an exact sequence

$$1 \to \boldsymbol{\mu}_k \to T \to S \to 1. \tag{2}$$

Let R be a commutative local F-algebra. The group $H^1(R,S)$ is identified with the relative Brauer group $\operatorname{Br}(LR/R) := \operatorname{Ker}\big(\operatorname{Br}(R) \to \operatorname{Br}(LR)\big)$, where we write LR for $L \otimes_F R$. The composition $H^1(R,S) \to H^1(R,\mathbf{PGL}_n) \hookrightarrow \operatorname{Br}(R)$ is identified with the inclusion of $\operatorname{Br}(LR/R)$ into $\operatorname{Br}(R)$. Comparing the exact sequences (1) and (2) we have:

Lemma 4.1. *The image of $H^1(R,T) \to H^1(R,G)$ coincides with the set of all ξ such that $A_\xi \in \operatorname{Br}_m(LR/R)$.*

Let Γ be the Galois group of a normal closure L'/F of L/F, so Γ is the decomposition group of the tori T and S. Let X be the Γ-set of all F-homomorphisms $L \to L'$. We have $|X| = n$ and $R_{L/K}\big(\mathbf{G}_{\mathrm{m},L}\big)^* = \mathbb{Z}[X]$.

Choose a point $x_0 \in X$ and let Γ_0 be the stabilizer of x_0 in Γ. As Γ acts transitively on X, we have, $X \simeq \Gamma/\Gamma_0$ and $[\Gamma : \Gamma_0] = n$.

Let I be the augmentation ideal in $\mathbb{Z}[\Gamma]$. Write I_X for the kernel of the augmentation map $\varepsilon : \mathbb{Z}[X] \to \mathbb{Z}$. We have $I_X = I \cdot \mathbb{Z}[X]$.

Write $N_X = \sum_{x\in X} x \in \mathbb{Z}[X]$, so $\varepsilon(N_X) = n$.

Let $V = R_{L/K}\big(\mathbf{G}_{\mathrm{m},L}\big)/\boldsymbol{\mu}_m$. The character group J_X of V is identified with the subgroup of elements $w \in \mathbb{Z}[X]$ with $\varepsilon(w) \in m\mathbb{Z}$. Note that $I_X \subset J_X$.

Lemma 4.2. *Suppose that $r > s$. Then $N_X \in pJ_X + I \cdot J_X$.*

Proof. The map

$$\Gamma \to I/I^2, \quad \gamma \mapsto (\gamma - 1) + I^2$$

is a group homomorphism. It follows that if γ belongs to the commutator subgroup $[\Gamma,\Gamma]$ of Γ, then

$$\gamma - 1 \in I^2. \tag{3}$$

Set $\Delta := [\Gamma,\Gamma]\Gamma_0$. Suppose first that Δ contains Γ_0 properly. Consider the sum u in $\mathbb{Z}[\Gamma]$ of all representatives of the set of left cosets Δ/Γ_0 chosen in $[\Gamma,\Gamma]$. It follows from (3) that u is congruent to $[\Delta : \Gamma_0]$ modulo I^2.

The element N_X is divisible by u, i.e., there is $M \in \mathbb{Z}[X]$ such that $N_X = uM$. It follows that N_X is congruent to $[\Delta : \Gamma_0]M$ modulo $I \cdot I_X$. As $[\Delta : \Gamma_0]$ is divisible by p, we have $[\Delta : \Gamma_0]M = pR$ for some $R \in \mathbb{Z}[X]$ with $\varepsilon(R) = n/p$. Since $r > s$, n/p is divisible by m, hence we have $R \in J_X$. Overall $N_X \in pJ_X + I \cdot I_X \subset pJ_X + I \cdot J_X$.

Now suppose that $\Delta = \Gamma_0$, i.e., Γ_0 is normal in Γ. It follows that $\Gamma_0 = 1$ and Γ is an abelian p-group of order n. Let Γ' be a subgroup of Γ of order p and $v = \sum_{\gamma\in\Gamma'} \gamma$ in $\mathbb{Z}[\Gamma]$. Then N_X is divisible by v, i.e., there is $M' \in \mathbb{Z}[X]$ such that $N_X = vM'$. Since $\varepsilon(M') = n/p$, we have $M' \in J_X$. As v is congruent to p modulo I, N_X is congruent to pM' modulo $I \cdot J_X$, hence $N_X \in pJ_X + I \cdot J_X$. □

The exact sequence of tori

$$1 \to T \to V \to \mathbf{G}_{\mathrm{m}} \to 1$$

yields an exact sequence of Γ-modules of co-characters

$$0 \to T_* \to V_* \to \mathbb{Z} \to 0. \tag{4}$$

Write θ_T for the image of 1 under the connecting homomorphism $\mathbb{Z} \to H^1(\Gamma, T_*) = H^1(F, T_*)$.

Proposition 4.3. *Suppose that $r > s$. Then θ_T is not divisible by p in $H^1(F, T_*)$.*

Proof. Consider the exact sequence of Γ-modules

$$0 \to \mathbb{Z} \xrightarrow{f} J_X \to T^* \to 0 \tag{5}$$

dual to (4). The image ν of θ_T under the canonical isomorphisms

$$H^1(F, T_*) \simeq \mathrm{Ext}^1_\Gamma(\mathbb{Z}, T_*) \simeq \mathrm{Ext}^1_\Gamma(T^*, \mathbb{Z})$$

is the class of the sequence (5).

Suppose that ν is divisible by p. Then the image of ν under the map $\mathrm{Ext}^1_\Gamma(T^*, \mathbb{Z}) \to \mathrm{Ext}^1_\Gamma(T^*, \mathbb{Z}/p\mathbb{Z})$ is trivial, i.e, the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ factors as $\mathbb{Z} \xrightarrow{f} J_X \xrightarrow{h} \mathbb{Z}/p\mathbb{Z}$ for a Γ-homomorphism h. Note that $f(1) = N_X$, hence $h(N_X) = 1 + p\mathbb{Z}$.

The map h vanishes on $pJ_X + I \cdot J_X$, hence by Lemma 4.2, $h(N_X) = 0$, a contradiction. □

5. The key proposition

Let K/F be a complete field with discrete valuation v over F and residue field $\overline{K}$. Let $\xi \in H^1(K,G)$ be an element and L/K an unramified (separable) field extension of degree n splitting A_ξ. Let $T = R^{(1)}_{L/K}\big(\mathbf{G}_{\mathrm{m},L}\big)/\boldsymbol{\mu}_m$ be the torus as defined in Section 4. Note that T is actually defined over the valuation ring, so the residue torus $\overline{T}$ is defined over $\overline{K}$. As $A_\xi \in \mathrm{Br}_m(L/K)$, the element ξ has a lifting to $H^1(K,T)$ by Lemma 4.1.

Lemma 5.1. *The image of the class $xK^{\times k}$ under the composition*

$$K^\times/K^{\times k} = H^1(K,\boldsymbol{\mu}_k) \to H^1(K,T) \xrightarrow{v_*} H^1(\overline{K},\overline{T}_*)$$

is equal to $v(x)\theta_{\overline{T}}$.

Proof. The commutativity of the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \boldsymbol{\mu}_k & \longrightarrow & \mathbf{G}_\mathrm{m} & \xrightarrow{k} & \mathbf{G}_\mathrm{m} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & T & \longrightarrow & V & \longrightarrow & \mathbf{G}_\mathrm{m} & \longrightarrow & 1 \end{array}$$

shows that the image of $xK^{\times k}$ in $H^1(K,T)$ coincides with the image of $xK^{\times k}$ under the connecting homomorphism induced by the bottom sequence in the diagram.

The result follows from the commutativity of the diagram

$$\begin{array}{ccc} K^\times & \longrightarrow & H^1(K,T) \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle v_*} \\ \mathbb{Z} & \longrightarrow & H^1(\overline{K},\overline{T}_*), \end{array}$$

where the bottom map in the connecting homomorphism for the exact sequence (4). □

Lemma 5.2. *Suppose that ξ is unramified and* $\mathrm{ind}(A_\xi) \in k\mathbb{Z}$. *Then every $\rho \in H^1(K,T)$ over ξ is unramified.*

Proof. By assumption, the class $A_\xi \in \mathsf{Alg}_K(n,m)$ is unramified. By Lemma 4.1, there is an unramified element $\eta \in H^1(K,T)$ over ξ. In view of Lemma 3.1, $\rho = x\eta$ for some $x \in K^\times$. It follows that $\xi = x\xi$.

By Lemma 3.1, $x \in \mathrm{Nrd}(A_\xi)K^{\times k}$. As $v\big(\mathrm{Nrd}(A_\xi)\big) \subset \mathrm{ind}(A)\mathbb{Z}$, by assumption, $v(x) \in k\mathbb{Z}$. Multiplying x by a kth power in $K^\times$ we may assume that x is a unit. Therefore, ρ is unramified. □

Let M be a field extension of K and let w be an extension on M of the discrete valuation v. We assume that M is complete. Write e for the ramification index of M/K and $\overline{M}$ for the residue field of M.

Lemma 5.3. *Suppose that* $\mathrm{ind}((A_\xi)_M) \in k\mathbb{Z}$ *and $\xi_M = x\xi'$, where $x \in M^\times$ and ξ' is an unramified element in $H^1(M,G)$. Then the element $w(x)\theta_{\overline{T}}$ in $H^1(\overline{M},\overline{T}_*)$ is divisible by e.*

Proof. Choose an element $\rho \in H^1(K,T)$ over ξ. The image of $\rho' := x^{-1}\rho_M$ in $H^1(M,G)$ is equal to ξ' and hence is unramified. By Lemma 5.2, applied to the field M, ρ' is unramified.

Consider the following commutative diagram:

$$\begin{array}{ccc} H^1(K,T) & \xrightarrow{v_*} & H^1(\overline{K},\overline{T}_*) \\ \big\downarrow & & \big\downarrow{\scriptstyle e} \\ H^1(M,T) & \xrightarrow{w_*} & H^1(\overline{M},\overline{T}_*) \end{array}$$

where the right vertical map is e times the canonical map. Hence the image of ρ in $H^1(\overline{M},\overline{T}_*)$ is divisible by e. On the other hand, $\rho_M = x\rho'$ and ρ' is unramified. Hence by Lemma 5.1, the image of ρ in $H^1(\overline{M},\overline{T}_*)$ coincides with $w(x)\theta_{\overline{T}}$. □

Proposition 5.4. *Let M/K be an extension of complete fields with discrete valuations, let $\xi \in H^1(K,G)$ be such that* $\operatorname{ind}\big((A_\xi)_M\big) = n = p^r$. *Suppose that $\xi_M = \pi\xi'$ for a prime element $\pi \in M$ and an unramified element $\xi' \in H^1(M,G)$. If $s < r$ then the ramification index of the extension M/K is not divisible by p.*

Proof. Let L/K be an unramified spitting field for A_ξ of degree n and let T be the torus as above. By Lemma 5.3, $\theta_{\overline{T}}$ in $H^1(\overline{M},\overline{T}_*)$ is divisible by the ramification index e and by Proposition 4.3 applied to the torus T_M over M, $\theta_{\overline{T}}$ is not divisible by p in $H^1(\overline{M},\overline{T}_*)$. Hence, p does not divide e. □

6. Proof of the theorem

We prove Theorem 1.1. Write $n = p^r n'$, $m = p^s m'$ and $k' = n'/m'$. Consider the groups $H = \mathbf{SL}_{p^r}/\boldsymbol{\mu}_{p^s}$ and $G' = \mathbf{SL}_{n'}/\boldsymbol{\mu}_{m'}$. We have a natural group homomorphism $H \times G' \to G$. For a field extension E/F take algebras $B \in \mathsf{Alg}_E(p^r,p^s)$, $A' \in \mathsf{Alg}_E(n',m')$ and $A := B \otimes A' \in \mathsf{Alg}_E(n,m)$. By Lemma 3.1, the fiber of the natural surjection $H^1(F,H) \to \mathsf{Alg}_R(p^r,p^s)$ over B is a principal homogeneous space under $C := E^\times/\big(E^{\times p^{r-s}} \cdot \operatorname{Nrd}(B)\big)$. Similarly, the fibers of the natural surjections $H^1(E,G') \to \mathsf{Alg}_E(n',m')$ and $H^1(E,G) \to \mathsf{Alg}_E(n,m)$ over A' and A are principal homogeneous spaces under $D' := E^\times/\big(E^{\times k'} \cdot \operatorname{Nrd}(A')\big)$ and $D := E^\times/\big(E^{\times k} \cdot \operatorname{Nrd}(A)\big)$ respectively.

The tensor product yields a bijection $\mathsf{Alg}_R(p^r,p^s)\times\mathsf{Alg}_R(n',m') \to \mathsf{Alg}_R(n,m)$. There is a natural isomorphism $C \times D' \to D$. It follows that the natural map

$$H^1(E,H) \times H^1(E,G') \to H^1(E,G)$$

is a bijection.

This bijection yields a surjection $\mathcal{F}_G \to \mathcal{F}_H$ and a p-surjective map $\mathcal{F}_H \to \mathcal{F}_G$. By [5, Sec. 1.3], $\operatorname{ed}_p(G) = \operatorname{ed}_p(H)$.

Replacing G by H we may assume that $n = p^r$ and $m = p^s$. If $s = 0$ then $G = \mathbf{SL}_n$ and $\operatorname{ed}_p(G) = 0$ as G is special, i.e., all G-torsors over fields are trivial. If $s = r$, $G = \mathbf{PGL}_n$ and $\mathcal{F}_G = \mathsf{Alg}(p^r,p^r)$, hence $\operatorname{ed}_p(G) = \operatorname{ed}_p\big(\mathsf{Alg}(p^r,p^r)\big)$.

We may assume that $0 < s < r$. By Lemma 3.1, for any field E, the natural map $H^1(E,G) \to \mathit{Alg}(p^r,p^s)(E)$ is surjective and the fibers are homogeneous sets under $E^\times$. It follows that

$$\operatorname{ed}_p(G) \le \operatorname{ed}_p\big(\mathit{Alg}(p^r,p^s)\big) + 1.$$

To prove the opposite inequality choose a field E/F and a (generic) algebra A in $\mathit{Alg}(p^r,p^s)(E)$ such that

$$\operatorname{ed}_p\big(\mathit{Alg}(p^r,p^s)\big) = \operatorname{ed}_p(A). \tag{6}$$

Note that as $s > 0$, the index of A is equal to p^r. Choose an element $\eta \in H^1(E,G)$ with $A_\eta = A$.

Consider the field of formal Laurent series $E((t))$ and set $\xi' := \eta_{E((t))} \in H^1(E((t)),G)$. We have $A_{\xi'} = A_{E((t))}$. Choose a finite field extension $M/E((t))$ of degree prime to p and a subfield $K \subset M$ over F such that $\operatorname{tr.deg}_F(K) = \operatorname{ed}_p(t\xi')$ and there is an element $\xi \in H^1(K,G)$ with $\xi_M = t\xi'_M$.

Let w be the extension of the discrete valuation of $E((t))$ on M. The ramification index of $M/E((t))$ is not divisible by p. The degree of the residue field $\overline{M}$ over E is also not divisible by p.

Note that the element ξ_M is ramified by Lemma 3.2, hence the restriction on K of the discrete valuation of M is nontrivial. We have $\operatorname{tr.deg}_F(K) \ge \operatorname{tr.deg}_F(\overline{K}) + 1$, therefore,

$$\operatorname{ed}_p(t\xi') \ge \operatorname{tr.deg}_F(\overline{K}) + 1. \tag{7}$$

Write $\hat{K}$ for the completion of K. As M is complete we may assume that $\hat{K}$ is a subfield of M. Since $0 < s < r$, by Proposition 5.4, the ramification index e of $M/\hat{K}$ is not divisible by p.

As $\operatorname{char}(F)$ is not equal to p, there is the residue homomorphism [7, Ch. XII]

$$\partial : \operatorname{Br}_n(\hat{K}) \to H^1(\overline{K}, \mathbb{Z}/n\mathbb{Z}).$$

Let $\bar{\chi} = \partial(A_\xi) \in H^1(\overline{K}, \mathbb{Z}/n\mathbb{Z})$. As $(A_\xi)_M = A_{t\xi'} = A_{\xi'} = A_M$ is unramified, we have $e \cdot \bar{\chi}_{\overline{M}} = 0$ and hence $\bar{\chi}_{\overline{M}} = 0$ as e is not divisible by p. Hence we can view the cyclic extension $\overline{K}(\bar{\chi})$ of $\overline{K}$ given by $\bar{\chi}$ as a subfield of $\overline{M}$.

Let $\chi \in H^1(\hat{K}, \mathbb{Z}/n\mathbb{Z})$ be the lift of $\bar{\chi}$. The field $\hat{K}(\chi)$ is a subfield of M. Therefore, the algebra $B := (A_\xi)_{\hat{K}(\chi)}$ is unramified and its residue $\overline{B}$ satisfies $\overline{B} \in \mathit{Alg}(p^r,p^s)\big(\overline{K}(\bar{\chi})\big)$ and $(\overline{B})_{\overline{M}} = A_{\overline{M}}$.

Thus, the algebra $A_{\overline{M}}$ is defined over $\overline{K}(\bar{\chi})$, hence

$$\operatorname{tr.deg}_F(\overline{K}) = \operatorname{tr.deg}_F\big(\overline{K}(\bar{\chi})\big) \ge \operatorname{ed}_p(A). \tag{8}$$

We have by (6), (7) and (8):

$$\operatorname{ed}_p(G) \ge \operatorname{ed}_p(t\xi') \ge \operatorname{tr.deg}_F(\overline{K}) + 1 \ge \operatorname{ed}_p(A) + 1 = \operatorname{ed}_p\big(\mathit{Alg}(p^r,p^s)\big) + 1.$$

References

[1] S. Baek, *Essential dimension of simple algebras with involutions*, Preprint.

[2] S. Baek and A. S. Merkurjev, *Essential dimension of central simple algebras*, To appear in Acta Mathematica.

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

[4] M. Demazure and A. Grothendieck, *Schémas en groupes. III: Structure des schémas en groupes réductifs*, Springer-Verlag, Berlin, 1962/1964, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 153.

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

[6] J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980.

[7] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

Department of Mathematical Sciences, University of Alberta, Edmonton, Alberta, Canada T6G 2G1

E-mail address: `chernous@math.ualberta.ca`

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA

E-mail address: `merkurev@math.ucla.edu`