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 \( \mathcal{F} : \text{Fields}/F \to \text{Sets} \) be a functor from the category \( \text{Fields}/F \) of field extensions over \( F \) to the category \( \text{Sets} \) of sets. Let \( E \in \text{Fields}/F \) and \( K \subset E \) a subfield over \( F \). We say that \( K \) is a field of definition of \( \alpha \in \mathcal{F}(E) \) if \( \alpha \) belongs to the image of the map \( \mathcal{F}(K) \to \mathcal{F}(E) \).

The essential dimension of \( \alpha \), denoted \( ed^{\mathcal{F}}(\alpha) \), is the least transcendence degree \( tr.\deg_{E}(K) \) over all fields of definition \( K \) of \( \alpha \). The essential dimension of the functor \( \mathcal{F} \) is

\[
\text{ed}(\mathcal{F}) = \sup \{ \text{ed}^{\mathcal{F}}(\alpha) \},
\]

where the supremum is taken over all fields \( E \in \text{Fields}/F \) and all \( \alpha \in \mathcal{F}(E) \) (see [3, Def. 1.2] or [1, 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 \( \alpha \), denoted \( ed_{p}^{\mathcal{F}}(\alpha) \), is defined as the minimum of \( \text{ed}^{\mathcal{F}}(\alpha_{E'}) \), where \( E' \) ranges over all finite field extensions of \( E \) of degree prime to \( p \). The essential \( p \)-dimension of \( \mathcal{F} \) is

\[
\text{ed}_{p}(\mathcal{F}) = \sup \{ \text{ed}^{\mathcal{F}}_{p}(\alpha) \},
\]

where the supremum ranges over all fields \( E \in \text{Fields}/F \) and all \( \alpha \in \mathcal{F}(E) \).

By definition, \( \text{ed}(\mathcal{F}) \geq \text{ed}_{p}(\mathcal{F}) \) for all \( p \).

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

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

\text{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 $\text{SL}_n/\mu_m$ for a divisor $m$ of $n$. In the present paper we compute the essential $p$-dimension of $G$ in terms of the integer $\text{ed}_p(\text{Alg}(n, m))$.

**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 $G = \text{SL}_n/\mu_m$ be the algebraic group defined over a field $F$ of the characteristic not $p$. Then

\[
\text{ed}_p(G) = \begin{cases} 
0, & \text{if } s = 0; \\
\text{ed}_p(\text{Alg}(p^r, p^s)), & \text{if } s = r; \\
\text{ed}_p(\text{Alg}(p^r, p^s)) + 1, & \text{if } 0 < s < r.
\end{cases}
\]

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

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

1. $p^{2r-2} + p^{s-r} + 1 \geq \text{ed}_p(\text{SL}_{p^r}/\mu_{p^s}) \geq (r-1)p^r + p^{s-r} + 1$ if $0 < s < r$ and $p$ is odd in the case $s = 1$.
2. $2^{2r-4} + 2^{r-1} + 1 \geq \text{ed}_2(\text{SL}_{2^r}/\mu_2) \geq (r-1)2^{r-1} + 1$ if $r \geq 3$.
3. $\text{ed}_p(\text{SL}_{p^2}/\mu_p) = p^2 + p + 1$ if $p$ is odd,
4. $\text{ed}_2(\text{SL}_4/\mu_2) = 5$,
5. $\text{ed}_2(\text{SL}_8/\mu_2) = 9$,
6. $\text{ed}_2(\text{SL}_8/\mu_4) = 19$,
7. $\text{ed}_2(\text{SL}_{16}/\mu_2) = 25$.

## 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 [1, 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 $\alpha$ is unramified. Otherwise $\alpha$ 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 [1, 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 $H^1(K, \mu_k) = K^\times/K^{\times k}$, $H^1(K, \mu_k)_{nr} = R^\times/R^{\times k}$ and $H^1(K, \mu_k)_{ram} = \mathbb{Z}/k\mathbb{Z}$.

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 $\Gamma_{\overline{K}}$. 
Let $\Gamma_K$ acts on $T^*$ via the canonical surjective homomorphism $\Gamma_K \to \Gamma_T$.

We have the split exact sequence of Galois $\Gamma_T$-modules

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

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

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

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

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

3. Azumaya algebras and torsors

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

$$(1) \quad 1 \to \mu_k \to G \to \text{PGL}_n \to 1.$$

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

$$H^1(R, G) \to H^1(R, \text{PGL}_n) \xrightarrow{\text{Br}} H^2(R, \mu_k).$$

Moreover, the group $H^1(R, \mu_k) = R^\times / R^{\times k}$ acts on the set $H^1(R, G)$ transitively in the fibers of the map $\alpha$. 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 $\xi$.

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

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

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

$$1 \to \mu_k \to G' \to \text{PGL}_1(A') \to 1.$$

The connecting homomorphism

$$A^\times / R^\times = \text{PGL}_1(A)(R) \to H^1(R, \mu_k) = R^\times / R^{\times k}$$

takes the class $aR^\times$ to Nrd$(a)R^{\times k}$, where 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 $A \in \text{Alg}_R(n, m)$. Then the factor group $R^\times / (R^{\times k} \cdot \text{Nrd}(A))$ acts simply transitively on the fiber of the surjective maps $H^1(R, G) \to \text{Alg}_R(n, m)$ over $A$. 

Let \( K/F \) be a field extension with a discrete valuation \( v \) over \( F \) and a prime element \( \pi \).

**Lemma 3.2.** Let \( \xi \in H^1(K, G) \) be an unramified element such that \( A_\xi \neq 0 \) in \( \text{Br}(K) \). If \( \pi \xi \) is unramified then \( k \) and \( \text{ind}(A_\xi) \) 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 \( (A_\zeta)_K = A_\zeta = A_{\pi \xi} = (A_{\zeta'})_K \). As the map \( \text{Br}(R) \to \text{Br}(K) \) is injective by [3, 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 3.2 again, \( \pi \in \lambda(K^\times k \cdot \text{Nrd}(A_\xi)) \). Therefore, \( 1 = v(\pi) \in k\mathbb{Z} + \text{ind}(A_\xi)\mathbb{Z} \) as \( v(\text{Nrd}(A_\xi)) \subset \text{ind}(A_\xi)\mathbb{Z} \) by [3, Ch. XII, §2]. \( \square \)

4. TORI

Let \( L/F \) be a separable field extension of degree \( n = p^e \), where \( p \) is a prime integer and \( m = p^f \) a divisor of \( n \). Consider the torus of norm one elements \( R_{L/F}^{(1)}(G_{m, L}) \) for the extension \( L/F \), the factor torus \( T = R_{L/F}^{(1)}(G_{m, L})/\mu_m \) and \( S = R_{L/F}^{(1)}(G_{m, L})/G_m \). Then \( T \) and \( S \) can be viewed as maximal tori of \( G \) and \( \text{PGL}_n \) respectively and we have an exact sequence

\[
1 \to \mu_k \to T \to S \to 1.
\]

Let \( R \) be a commutative local \( F \)-algebra. The group \( H^1(R, S) \) is identified with the relative Brauer group \( \text{Br}(LR/R) := \text{Ker}(\text{Br}(R) \to \text{Br}(LR)) \), where we write \( LR \) for \( L \otimes_F R \). The composition \( H^1(R, S) \to H^1(R, \text{PGL}_n) \to \text{Br}(R) \) is identified with the inclusion of \( \text{Br}(LR/R) \) into \( \text{Br}(R) \). 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 \( \xi \) such that \( A_\xi \in \text{Br}_m(LR/R) \).

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

Choose a point \( x_0 \in X \) and let \( \Gamma_0 \) be the stabilizer of \( x_0 \) in \( \Gamma \). As \( \Gamma \) acts transitively on \( X \), we have, \( X = \Gamma/\Gamma_0 \) 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 \( V = R_{L/K}(G_{m, L})/\mu_m \). 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 $\gamma$ belongs to the commutator subgroup $[\Gamma, \Gamma]$ of $\Gamma$, then

\[(3) \quad \gamma - 1 \in I^2.\]

Set $\Delta := [\Gamma, \Gamma]/\Gamma_0$. Suppose first that $\Delta$ contains $\Gamma_0$ properly. Consider the sum $u$ in $\mathbb{Z}[\Gamma]$ of all representatives of the set of left cosets $\Delta/\Gamma_0$ 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 $N_X \in pJ_X + I \cdot J_X \subset pJ_X + I \cdot J_X$.

Now suppose that $\Delta = \Gamma_0$, i.e., $\Gamma_0$ is normal in $\Gamma$. It follows that $\Gamma_0 = 1$ and $\Gamma$ is an abelian $p$-group of order $n$. Let $\Gamma'$ be a subgroup of $\Gamma$ 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

\[1 \to T \to V \to G_m \to 1\]

yields an exact sequence of $\Gamma$-modules of co-characters

\[(4) \quad 0 \to T_* \to V_* \to \mathbb{Z} \to 0.\]

Write $\theta_T$ 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 $\theta_T$ is not divisible by $p$ in $H^1(F, T_*)$.

**Proof.** Consider the exact sequence of $\Gamma$-modules

\[(5) \quad 0 \to \mathbb{Z} \overset{f}{\to} J_X \to T^* \to 0\]
dual to (3). The image $\nu$ of $\theta_T$ under the canonical isomorphisms

\[H^1(F, T_*) \simeq \text{Ext}^1_{\Gamma}(\mathbb{Z}, T_*) \simeq \text{Ext}^1_{\Gamma}(T^*, \mathbb{Z})\]

is the class of the sequence (5).

Suppose that $\nu$ is divisible by $p$. Then the image of $\nu$ under the map $\text{Ext}^1_{\Gamma}(T^*, \mathbb{Z}) \to \text{Ext}^1_{\Gamma}(T^*, \mathbb{Z}/p\mathbb{Z})$ is trivial, i.e, the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ factors as $\mathbb{Z} \overset{f}{\to} J_X \overset{h}{\to} \mathbb{Z}/p\mathbb{Z}$ for a $\Gamma$-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. $\square$
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 $A_\xi$. Let $T = R^{(1)}_{L/K}(G_m, L)/\mu_m$ be the torus as defined in Section \[. Note that $T$ is actually defined over the valuation ring, so the residue torus $\overline{T}$ is defined over $\overline{K}$. As $A_\xi \in \text{Br}_m(L/K)$, the element $\xi$ has a lifting to $H^1(K, T)$ by Lemma \[.

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

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

is equal to $v(x)\theta_T$.

Proof. The commutativity of the diagram

$$
\begin{array}{ccccccc}
1 & \longrightarrow & \mu_k & \longrightarrow & G_m & \xrightarrow{k} & G_m & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \| & & \| & & \\
1 & \longrightarrow & T & \longrightarrow & V & \longrightarrow & G_m & \longrightarrow & 1 \\
\end{array}
$$

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

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

where the bottom map in the connecting homomorphism for the exact sequence (\[).

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

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

By Lemma 4.1, $x \in \text{Nrd}(A_\xi)K^{\times k}$. As $v(\text{Nrd}(A_\xi)) \subset \text{ind}(A)\mathbb{Z}$, by assumption, $v(x) \in k\mathbb{Z}$. Multiplying $x$ by a $k$th power in $K^{\times}$ we may assume that $x$ is a unit. Therefore, $\rho$ 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 $\text{ind}(A_\xi)_M \in k\mathbb{Z}$ and $\xi_M = x\xi'$, where $x \in M^{\times}$ and $\xi'$ is an unramified element in $H^1(M, G)$. Then the element $w(x)\theta_T$ in $H^1(\overline{M}, \overline{T})$ is divisible by $e$. 


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

Consider the following commutative diagram:

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

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

**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 $\text{ind}(A_\xi, M) = n = p^r$. 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 splitting field for $A_\xi$ of degree $n$ and let $T$ be the torus as above. By Lemma 5.3, $\theta_T$ in $H^1(M, \overline{T}_*)$ is divisible by the ramification index $e$ and by Proposition 4.3 applied to the torus $T_M$ over $M$, $\theta_T$ is not divisible by $p$ in $H^1(M, \overline{T}_*)$. Hence, $p$ does not divide $e$. □

### 6. PROOF OF THE THEOREM

We prove Theorem 4.4. Write $n = p^r n'$, $m = p^m m'$ and $k = n'/m'$. Consider the groups $H = \text{SL}_{np} / \mu_{p^r}$ and $G' = \text{SL}_{n'} / \mu_{m'}$. We have a natural group homomorphism $H \times G' \rightarrow G$. For a field extension $E/F$ take algebras $B \in \text{Alg}_E(p^r, p^s)$, $A' \in \text{Alg}_E(n', m')$ and $A := B \otimes A' \in \text{Alg}_E(n, m)$. By Lemma 4.4, the fiber of the natural surjection $H^1(F, H) \rightarrow \text{Alg}_R(p^r, p^s)$ over $B$ is a principal homogeneous space under $C := E^x/(E^{x, p^{r-s}} \cdot \text{Nrd}(B))$. Similarly, the fibers of the natural surjections $H^1(E, G') \rightarrow \text{Alg}_E(n', m')$ and $H^1(E, G) \rightarrow \text{Alg}_E(n, m)$ over $A'$ and $A$ are principal homogeneous spaces under $D' := E^x/(E^{x, k'} \cdot \text{Nrd}(A'))$ and $D := E^x/(E^{x, k} \cdot \text{Nrd}(A))$ respectively.

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

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

is a bijection.

This bijection yields a surjection $\mathcal{F}_G \rightarrow \mathcal{F}_H$ and a $p$-surjective map $\mathcal{F}_H \rightarrow \mathcal{F}_G$. By [3, Sec. 1.3], $\text{ed}_p(G) = \text{ed}_p(H)$.

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

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

$$\text{ed}_p(G) \leq \text{ed}_p(\text{Alg}(p^r, p^s)) + 1.$$  

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

$$\text{ed}_p(\text{Alg}(p^r, p^s)) = \text{ed}_p(A).$$

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 $\text{tr. deg}_F(K) = \text{ed}_p(t\xi')$ and there is an element $\xi \in H^1(K, G)$ with $K = t\xi M$.

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 $\xi_M$ is ramified by Lemma 3.2, hence the restriction on $K$ of the discrete valuation of $M$ is nontrivial. We have $\text{tr. deg}_F(K) \geq \text{tr. deg}_F(\overline{K}) + 1$, therefore,

$$\text{ed}_p(t\xi') \geq \text{tr. deg}_F(\overline{K}) + 1.$$  

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 3.1, the ramification index $e$ of $M/\hat{K}$ is not divisible by $p$.

As char$(F)$ is not equal to $p$, there is the residue homomorphism [1, Ch. XII]

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

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

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

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

$$\text{tr. deg}_F(\overline{K}) = \text{tr. deg}_F(\overline{K}(\overline{\chi})) \geq \text{ed}_p(A).$$

We have by (8), (7) and (5):

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


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