ESSENTIAL $p$-DIMENSION OF $\text{PGL}(p^2)$

ALEXANDER S. MERKURJEV

1. INTRODUCTION

Informally, the essential dimension of an “algebraic structure” over a field $F$ is the smallest number of parameters required to define this structure over a field extension of $F$ (see [1] or [11]). Thus, the essential dimension measures the complexity of the structure.

Let $p$ be a prime integer. The essential $p$-dimension of an “algebraic structure” measures the complexity of the structure modulo the “effects of degree prime to $p$” (see [12]). In practice, the essential $p$-dimension is easier to compute than the essential dimension.

The formal definition of the essential ($p$-)dimension is as follows. Let $p$ denote either a prime integer or 0. An integer $k$ is said to be prime to $p$ if $k$ is prime to $p$ when $p > 0$ and $k = 1$ when $p = 0$. Let $F$ be a field. Consider the category $\text{Fields}/F$ of field extensions of $F$ and field homomorphisms over $F$. Let $\mathcal{F}: \text{Fields}/F \to \text{Sets}$ be a functor (an “algebraic structure”) and $K, E \in \text{Fields}/F$. An element $\alpha \in \mathcal{F}(E)$ is said to be $p$-defined over $K$ (and $K$ is called a field of $p$-definition of $\alpha$) if there exist a finite field extension $E'/E$ of degree prime to $p$ (so $E' = E$ if $p = 0$), a field homomorphism $K \to E'$ over $F$ and an element $\beta \in \mathcal{F}(K)$ such that the image of $\alpha$ under the map $\mathcal{F}(E) \to \mathcal{F}(E')$ coincides with the image of $\beta$ under the map $\mathcal{F}(K) \to \mathcal{F}(E')$. The essential $p$-dimension of $\alpha$, denoted $\text{ed}_p(\mathcal{F})(\alpha)$, is the least transcendence degree $\text{tr. deg}_p(K)$ over all fields of $p$-definition $K$ of $\alpha$. The essential $p$-dimension of the functor $\mathcal{F}$ is

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

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

We write $\text{ed}(\mathcal{F})$ for $\text{ed}_0(\mathcal{F})$ and simply call $\text{ed}(\mathcal{F})$ the essential dimension of $\mathcal{F}$. Clearly, $\text{ed}(\mathcal{F}) \geq \text{ed}_p(\mathcal{F})$ for all $p$.

Let $G$ be an algebraic group over $F$. The essential $p$-dimension of $G$ is the essential $p$-dimension of the functor $\mathcal{F}_G: \text{Fields}/F \to \text{Sets}$ taking a field $E$ to the set of isomorphism classes of all $G$-torsors (principal homogeneous $G$-spaces) over $\text{Spec}(E)$.

If $G = \text{PGL}_n$ over $F$, the functor $\mathcal{F}_G$ is isomorphic to the functor taking a field $E$ to the set of isomorphism classes of central simple $E$-algebras of degree $n$. Let $p$ be a prime integer and let $p'$ be the highest power of $p$ dividing $n$. Then $\text{ed}_p(\text{PGL}_F(n)) = \text{ed}_p(\text{PGL}_F(p'))$ [12 Lemma 8.5.5]. Every central simple
Let \( p \) be a prime integer and \( F \) a field of characteristic different from \( p \). Then
\[
ed_p(\text{PGL}_F(p^2)) = p^2 + 1.
\]

**Corollary 1.2** (Rost). If \( F \) is a field of characteristic different from 2, then
\[
ed(\text{PGL}_F(4)) = 2 \geq 5.
\]

**Proof.** By Theorem 1.1 we have \( \ed(\text{PGL}_F(4)) \geq 5 \). On the other hand, \( \ed(\text{PGL}_F(4)) \leq 5 \) by [9]. \( \square \)

We use the following notation:
- \( F \) is a field, and \( \Gamma = \text{Gal}(F_{sep}/F) \) is the absolute Galois group of \( F \).
- \( X(F) \) is the character group of \( \Gamma \).
- \( \text{Br}(F) \) is the Brauer group of \( F \). For a field extension \( L/F \), we write \( \text{Br}(L/F) \) for the relative Brauer group \( \text{Ker}(\text{Br}(F) \to \text{Br}(L)) \).
- \( \mathbb{G}_m \) denotes the multiplicative algebraic group \( \text{Spec} F[t, t^{-1}] \) over \( F \).
- For a finite separable field extension \( L/F \), we write \( R_{L/F} \) for the corestriction operation (see [8, §20.5]). In particular, \( R_{L/F}(\mathbb{G}_{m,L}) \) is the multiplicative group of \( L \) considered as an algebraic group (torus) over \( F \). We write \( R_{L/F}(\mathbb{G}_{m,L}) \) for the torus of norm 1 elements in \( L \).
- If \( A \) is a central simple algebra over \( F \), then \( \text{SB}(A) \) denotes the Severi-Brauer variety of \( A \) of reduced rank 1 right ideals in \( A \) [8, §1.C].

If \( p \) is a prime integer and \( B \) is a torsion abelian group, we write \( B(p) \) for the \( p \)-primary component of \( B \) and \( p^nB \) for the subgroup of elements of exponent \( p^n \) in \( B \).

In the present paper, the word “scheme” over a field \( F \) means a separated scheme of finite type over \( F \) and a “variety” over \( F \) is an integral scheme over \( F \). If \( X \) is a scheme over \( F \) and \( E/F \) is a field extension, then \( X(E) = \text{Mor}_F(\text{Spec}(E), X) \) is the set of points of \( X \) over \( E \). We write \( X_E \) for the scheme \( X \times_F \text{Spec}(E) \).

### 2. Algebraic Tori

#### 2.1. R-equivalence of algebraic tori
Let \( T \) be an algebraic torus over a field \( F \). As usual, we write \( T^* \) for the character group of \( T \) over a separable closure \( F_{sep} \) of \( F \). The group \( T^* \) is a \( \Gamma \)-lattice.

A torus \( P \) is **quasi-trivial** if \( P^* \) is a permutation lattice, i.e., if there is a \( \Gamma \)-invariant \( \mathbb{Z} \)-basis of \( P^* \).

Let \( E/F \) be a field extension. Recall that the group of R-equivalence classes \( T(E)/R \) is the factor group of \( T(E) \) modulo the subgroup \( RT(E) \) of all elements that are R-equivalent to 1 (see [3, §5] and [15, Ch. 6]). If \( P \) is a quasi-trivial torus, then \( P(E)/R = 1 \).

**Example 2.1** ([3, Prop. 15]). Let \( L/F \) be a finite Galois field extension and \( T = R_{L/F}(\mathbb{G}_{m,L}) \) the torus of norm 1 elements in \( L \). Then the subgroup \( RT(F) \) is generated by elements of the form \( \sigma(u)/u \) over all \( \sigma \in \text{Gal}(L/F) \) and \( u \in L^\times \).
Example 2.2. The torus $T = R_{L/F}^{(1)}(\mathbb{G}_{m,L})$ is not rational if $L/F$ is a bicyclic field extension of degree $p^2$ by [15] §4.8. Moreover, $T$ is not $R$-trivial generically; i.e., there is a field extension $E/F$ such that $T(E)/R \neq 1$. In fact, the image of the generic point of $T$ in $T(F(T))/R$ is not trivial.

2.2. Characters, cyclic algebras and tori. For a field $F$, the character group $X(F)$ of $\Gamma$ is equal to

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

For a character $\chi \in X(F)$, set $F(\chi) = (F_{\text{sep}})^{\text{Ker}(\chi)}$. Then $F(\chi)/F$ is a cyclic field extension of degree $\text{ord}(\chi)$. The Galois group $\text{Gal}(F(\chi)/F)$ has a canonical generator $\sigma$ such that $\chi(\sigma) = \text{ord}(\chi)^{-1} + \mathbb{Z}$ for any lifting $\tilde{\sigma}$ of $\sigma$ to $\Gamma$.

If $F' \subset F$ is a subfield and $\chi \in X(F')$, we write $\chi_F$ for the image of $\chi$ under the natural map $X(F') \to X(F)$ and write $F(\chi)$ for $F(\chi_F)$.

Let $K/F$ be a cyclic field extension. Choose a character $\chi \in X(F)$ such that $K = F(\chi)$. The cup product

$$X(F) \otimes F^\times = H^2(F, \mathbb{Z}) \otimes H^0(F, F_{\text{sep}}^\times) \to H^2(F, F_{\text{sep}}^\times) = \text{Br}(F)$$

takes $\chi \otimes a$ to the class $\chi \cup (a)$ of a cyclic algebra split by $K$. In fact, every element of $\text{Br}(K/F)$ is of the form $\chi \otimes a$ for some $a \in F^\times$.

Let $L$ be an étale $F$-algebra of dimension $n$ and $S = R_{L/F}(\mathbb{G}_{m,L})/ \mathbb{G}_m$. The exact sequence

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

and Hilbert Theorem 90 yield an isomorphism $\theta : H^1(F, S) \cong \text{Br}(L/F)$. Let $\alpha \in H^1(F, S)$ and let $S_\alpha$ be the corresponding principal homogeneous space of $S$. As $S$ is an open subscheme of the projective space $\mathbb{P}_F(L)$, the variety $S_\alpha$ is an open subset of the Severi-Brauer variety $SB(\alpha)$ of a central simple $F$-algebra $A_\alpha$ of degree $n$ such that $[A_\alpha] = \theta(\alpha)$ in $\text{Br}(L/F)$. Moreover, $S_\alpha$ is trivial if and only if $A_\alpha$ is split.

Let $\chi \in X(F)$ and $L = F(\chi)$. Then $S \simeq R_{L/F}^{(1)}(\mathbb{G}_{m,L})$ by Hilbert Theorem 90 and $[A_\alpha] = \chi \cup a$ for some $a \in F^\times$. Moreover, the principal homogeneous space $S_\alpha$ coincides with the fiber $S_\alpha$ of the norm homomorphism $R_{L/F}(\mathbb{G}_{m,L}) \to \mathbb{G}_m$ over $a$.

2.3. Bicyclic algebras and tori. Let $\chi$ and $\eta$ be two characters in $X(F)$ of order $p$. Then the fields $K = F(\chi)$ and $K' = F(\eta)$ are cyclic extensions of $F$ of degree $p$. Set $L = K \otimes_F K'$, so $L$ is a bicyclic extension of $F$ of degree $p^2$. The group $G = \text{Gal}(K/F) \times \text{Gal}(K'/F)$ acts naturally on $L$ by automorphisms and $G$ is generated by elements $\sigma$ and $\tau$ such that $L^\sigma = K'$ and $L^\tau = K$.

Let $I$ be the augmentation ideal in the group ring $\Lambda := \mathbb{Z}[G]$, i.e., $I = \text{Ker}(\varepsilon)$, where $\varepsilon : \Lambda \to \mathbb{Z}$ is defined by $\varepsilon(\rho) = 1$ for all $\rho \in G$. We have:

(1) $$\text{Br}(L/F) = H^2(G, L^\times) = \text{Ext}^2_G(\mathbb{Z}, L^\times) = \text{Ext}^1_G(I, L^\times).$$

Consider the exact sequences of $G$-modules

(2) $$0 \to M \to \Lambda^2 \overset{f}{\to} I \to 0,$$

where $f(x, y) = (\sigma - 1)x + (\tau - 1)y$ and $M = \text{Ker}(f)$ and

(3) $$0 \to \Lambda/\mathbb{Z}_G \overset{g}{\to} M \overset{h}{\to} \mathbb{Z}^2 \to 0,$$
where $N_G = \sum_{\rho \in G} \rho \in \Lambda$, $g(x + \mathbb{Z}N_G) = ((\tau - 1)x, (1 - \sigma)x)$ and $h(x, y) = (\varepsilon(x)/p, \varepsilon(y)/p)$.

Let $T$ be the torus of norm 1 elements for the extension $L/F$ and let $T'$ be the torus with the character lattice $M$. We have
\[
(4) \quad T(E) = \text{Hom}_G(\Lambda/\mathbb{Z}N_G, (EL)^\times), \quad T'(E) = \text{Hom}_G(M, (EL)^\times)
\]
for any field extension $E/F$.

The exact sequences $(2)$, $(3)$, the isomorphisms $(1)$ and $(4)$ and Hilbert Theorem 90 yield a commutative diagram for any field extension $E/F$:
\[
\begin{array}{cccccc}
\text{Hom}_G(\mathbb{Z}^2, (EL)^\times) & \xrightarrow{h^*} & T'(E) & \xrightarrow{\alpha} & \text{Br}(EL/E) & \xrightarrow{0} \\
\text{Hom}_G(\Lambda^2, (EL)^\times) & \xrightarrow{\beta} & T(E) & \xrightarrow{g^*} & & \\
& & \downarrow & & \downarrow & \\
& & 0 & & \end{array}
\]

It follows that the cokernels of $\alpha$ and $\beta$ are naturally isomorphic. The image of $\alpha : E^\times \to \text{Br}(EL/E)$ is the subgroup of decomposable elements $\text{Br}_{\text{dec}}(EL/E)$ of $\text{Br}(EL/E)$ generated by $\chi_E \cup (a)$ and $\eta_E \cup (b)$ with $a, b \in E^\times$.

The cokernel of $\beta : (EL)^\times \to T(E)$ is the group of $R$-equivalence classes $T(E)/R$ (see Example 2.4). We have proved:

**Proposition 2.3.** Let $L/F$ be a bicyclic extension and $T = R^{1(1)}_{L/F}(\mathbb{G}_{m,L})$. Then for any field extension $E/F$, there is a natural isomorphism
\[
T(E)/R \simeq \text{Br}(EL/E)/\text{Br}_{\text{dec}}(EL/E).
\]

Let $A'$ be a central simple algebra of degree $p^2$ over $F(T')$ corresponding to the generic point of $T'$. Also choose a central simple algebra $A$ of degree $p^2$ over $F(T)$ corresponding to the generic point of $T$ by Proposition 2.3. The field $F(T)$ is a subfield of $F(T')$ and the classes $[A_{F(T')}]$ and $[A']$ are congruent in $\text{Br}(L(T')/F(T'))$ modulo $\text{Br}_{\text{dec}}(L(T')/F(T'))$. It follows that $p[A_{F(T')}] = p[A']$ in $\text{Br}(F(T'))$.

The exact sequence of $G$-modules
\[
0 \to L^\times \oplus M \to L(T')^\times \to \text{Div}(T_L') \to 0
\]
induces an exact sequence
\[
H^1(G, \text{Div}(T_L')) \to H^2(G, L^\times) \oplus H^2(G, M) \to H^2(G, L(T')^\times).
\]

As $\text{Div}(T_L')$ is a permutation $G$-module, the first term in the sequence is trivial. Therefore, we get an injective homomorphism
\[
\varphi : H^2(G, M) \to \text{Br}(F(T'))/\text{Br}(F).
\]
It follows from $(2)$ that
\[
H^2(G, M) \simeq H^1(G, I) \simeq \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/p^2\mathbb{Z};
\]
thus, $H^2(G, M)$ has a canonical generator $\xi$ of order $p^2$. 

\[\text{License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use} \]
Lemma 2.4. We have $\varphi(\xi) = -[A'] + \text{Br}(F)$.

Proof. Consider the following diagram:

$$
\begin{array}{ccc}
\text{Hom}_G(\mathbb{Z}, \mathbb{Z}) & \to & \text{Ext}_G^1(\mathbb{Z}, I) \\
\downarrow & & \downarrow \\
\text{Hom}_G(I, I) & \to & \text{Ext}_G^1(\mathbb{Z}, I) \\
\downarrow & & \downarrow \\
\text{Hom}_G(M, M) & \to & \text{Ext}_G^1(I, M) \\
\downarrow & & \downarrow \\
\text{Hom}_G(M, L(T')^\times) & \to & \text{Ext}_G^1(I, L(T')^\times) \\
\downarrow & & \downarrow \\
& & \text{Ext}_G^2(\mathbb{Z}, L(T')^\times).
\end{array}
$$

By [2] Ch. XIV, the images of $1_2$ and $-1_I$ agree in $\text{Ext}_G^1(\mathbb{Z}, I)$ and the images of $1_M$ and $-1_I$ agree in $\text{Ext}_G^2(I, M)$. It follows from [2] Ch. V, Prop. 4.1 that the upper square is anticommutative. The image of $1_2$ is equal to $\varphi(\xi)$ and the image of $1_M$ is equal to $[A'] + \text{Br}(F)$ in the right bottom corner.

Corollary 2.5. The class $p[A]$ in $\text{Br} F(T)$ does not belong to the image of $\text{Br}(F) \to \text{Br} F(T)$.

Proof. The image of $p[A]$ in $\text{Br} F(T')$ coincides with $p[A']$. Modulo the image of the map $\text{Br}(F) \to \text{Br} F(T')$, the class $p[A']$ is equal to $-\varphi(p\xi)$ and therefore, is nonzero as $\varphi$ is injective.

3. Degree of points of the norm 1 torus for a bicyclic field extension

3.1. Chow groups and push-forward homomorphism. Let $X$ be a scheme over a field $F$. We write $Z(X)$ for the group of algebraic cycles on $X$, i.e., the free abelian group generated by points of $X$. We write $\text{CH}(X)$ for the factor group of $Z(X)$ by the subgroup of cycles rationally equivalent to 0 (see [3] §1.3]). The groups $Z(X)$ and $\text{CH}(X)$ are graded by the dimension of points. If $x \in X$ is a point of dimension $i$, $[x]$ denotes the class of $x$ in $\text{CH}_i(X)$.

If $X$ is a variety of dimension $d$, then the group $\text{CH}_d(X)$ is infinite cyclic generated by the class of the generic point of $X$.

Let $f : X \to Y$ be a morphism of schemes over $F$. The push-forward homomorphism $f_* : Z(X) \to Z(Y)$ is a graded homomorphism defined by

$$f_*(x) = \begin{cases} [F(x) : F(y)] : y, & \text{if } [F(x) : F(y)] \text{ is finite;} \\ 0, & \text{otherwise,} \end{cases}$$

where $x \in X$ and $y = f(x)$. If $f$ is a proper morphism, then $f_*$ factors through the rational equivalence, defining the push-forward homomorphism $\text{CH}(X) \to \text{CH}(Y)$ still denoted by $f_*$ (see [3] §1.4]).

3.2. Degree of a point. Let $X$ be a scheme over a field $F$, $a \in X(E)$ a point over a field extension $E/F$ and $\{x\}$ the image of $a : \text{Spec}(E) \to X$. The dimension of $a$ is the integer $\dim(a) := \dim(x)$. If $f : X \to Y$ is a morphism of varieties over $F$ and
Let $a \in X(E)$ for a field extension $E/F$, we have $\dim(a) \geq \dim(f(a))$. If $d = \dim(a)$, we define the class $[a]$ of $a$ in $\text{CH}_d(X)$ as follows:

$$[a] := \begin{cases} [E : F(x)] \cdot [x], & \text{if } [E : F(x)] \text{ is finite;} \\ 0, & \text{otherwise.} \end{cases}$$

In addition, if $X$ is a variety, the degree of $a$ is the integer $\deg(a)$ satisfying $[a] = \deg(a) \cdot [x]$ if $\dim(a) = \dim(X)$ and $x$ is the generic point of $X$, and $\deg(a) = 0$ otherwise.

If $E'/E$ is a field extension and $a \in X(E)$, we write $a_{E'}$ for the image of $a$ in $X(E')$. If $E'/E$ is finite, we have $\deg(a_{E'}) = [E' : E] \cdot \deg(a)$.

If $E = F(X)$ is the function field of $X$ and $a \in X(E)$ is the generic point, then $\deg(a) = 1$.

**Proposition 3.1.** Let $f : X \to Y$ be a proper morphism of varieties over $F$ and let $a \in X(E)$ be a point over a field extension $E/F$. Then $[f(a)] = f_*(<[a]])$ in $\text{CH}(Y)$.

**Proof.** Let $\{x\}$ be the image of $a$ in $X$ and $y = f(x)$. If one of the field extensions $E/F(x)$ and $F(x)/F(y)$ is infinite, then $[f(a)] = 0$ and $f_*(<[a]]) = 0$. We may assume that $E$ is a finite extension of $F(y)$. Then

$$[f(a)] = [E : F(y)] \cdot [y] = [E : F(x)]([F(x) : F(y)] \cdot [y]) = [E : F(x)] \cdot f_*([x]) = f_*(<[a]])$$. 

If $Z$ is a scheme over $F$, we write $n(Z)$ for the gcd$[F(z) : F]$ over all closed points $z \in Z$.

**Example 3.2.** Let $T$ be an algebraic torus over $F$. We write $i(T)$ for the greatest common divisor of the integers $[E : F]$ over all finite field extensions $E/F$ such that $T$ is isotropic over $E$. If $X$ is a smooth complete geometrically irreducible variety containing $T$ as an open set, then $n(X \setminus T) = i(T)$ by [3 Lemme 12] (see also [10 Lemma 5.1]).

We shall need a variant of a push-forward homomorphism for morphisms that are not proper.

**Proposition 3.3.** Let $X$ be a complete variety over $F$, $U \subset X$ an open subvariety, $Z = X \setminus U$ and $f : U \to Y$ a morphism over $F$, where $Y$ is a variety of dimension $d$ over $F$. If $n = n(Z_{F(Y)})$, then the push-forward homomorphism on cycles $f_* : Z(U) \to Z(Y)$, followed by the projection $Z(Y) \to Z_d(Y) = \mathbb{Z}$, gives rise to a well-defined homomorphism

$$f_* : \text{CH}(U) \to \mathbb{Z}/n\mathbb{Z}$$

Moreover, for any point $a \in U(E)$ over a field extension $E/F$, one has $f_*([a]) = \deg(f(a))$ modulo $n$.

**Proof.** We define the map $f_*$ to be trivial on all homogeneous components $\text{CH}_i(U)$ except $i = d$, so we just need to define $f_*$ on $\text{CH}_d(U)$.

We claim that the image of the push-forward homomorphism

$$s_* : \text{CH}_d(Z \times Y) \to \text{CH}_d(Y) = \mathbb{Z}$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
for the projection $s : Z \times Y \to Y$ is contained in $n\mathbb{Z}$. Let $u \in Z \times Y$ be a point of dimension $d$. If $s(u)$ is not the generic point of $Y$, then $s_*(\{u\}) = 0$. Otherwise, $u$ is a closed point in $Z_{F(Y)} \subset Z \times Y$ and $s_*(\{u\})$ coincides with the degree of this closed point and hence is divisible by $n$. The claim is proven.

The map $s_*$ factors as $s_* = q_* \circ i_*$, where $i : Z \times Y \to X \times Y$ is the closed embedding and $q : X \times Y \to Y$ is the projection. By localization [4, §1.8], $\text{CH}_d(U \times Y)$ is canonically isomorphic to the cokernel of $i_*$. By the claim, $q_*$ gives rise to a homomorphism $\text{CH}_d(U \times Y) \to \mathbb{Z}/n\mathbb{Z}$. Composing it with the push-forward homomorphism for the closed embedding $(1_U, f) : U \to U \times Y$, we get the required homomorphism $f_* : \text{CH}_d(U) \to \mathbb{Z}/n\mathbb{Z}$. The last equality in the statement follows from Proposition 3.1 applied to $q$.

\[\square\]

**Example 3.4.** Let $T$ be an algebraic torus over $F$ and $n = i(T)$ (see Example 3.2). Then the structure morphism $T \to \text{Spec}(F)$ gives rise to a homomorphism $\text{CH}_d(T) \to \mathbb{Z}/n\mathbb{Z}$ that takes the class of a closed point $t \in T$ to $[F(t) : F]$ modulo $n$.

### 3.3. Chow groups of tori and Severi-Brauer varieties

Let $p$ be a prime integer and let $Z$ be the product of $r$ copies of the projective space $\mathbb{P}_F(W)$, where $W$ is a vector space of dimension $n > 0$ over $F$. Then

$$\text{CH}(Z) = Z[h] := Z[h_1, h_2, \ldots, h_r],$$

with $h_i^n = 0$ for all $i$, where $h_i$ is the pull-back on $Z$ of the class of a hyperplane on the $i$th factor of $Z$. Moreover, $Z[h]$ is the factor ring of the polynomial ring on the variables $t_1, t_2, \ldots, t_r$ by the ideal generated by $t_1^n, t_2^n, \ldots, t_r^n$. Note that the homogeneous $i$th component $Z[h]_i$ is trivial if $i > r(n-1)$ and $Z[h]_{r(n-1)} = Z h^{n-1}$, where $h := h_1 h_2 \cdots h_r$.

Let $K/F$ be a Galois field extension with a cyclic Galois group $H$ of prime order $p$ and let $\sigma$ be a generator of $H$. Let $V$ be a vector space of dimension $n > 0$ over $K$. Consider the variety $X = R_{K/F}(\mathbb{P}^r_K(V))$ over $F$. Then $X_K$ is the product of $p$ copies of $\mathbb{P}^r_K(V)$. The group $H$ acts on the product by cyclic permutation of the factors. We have the graded ring homomorphism

$$\text{CH}(X) \to \text{CH}(X_K) = Z[h],$$

where $h = (h_1, h_2, \ldots, h_p)$.

The group $H$ acts on $Z[h]$ permuting cyclically the $h_i$’s. Hence the image of the map $\text{CH}(X) \to Z[h]$ is contained in the subring $Z[h]^H$ of $H$-invariant elements, so we have the graded ring homomorphism

$$\text{CH}(X) \to Z[h]^H$$

(which is in fact an isomorphism). The image of an element $\alpha \in \text{CH}(X)$ in $Z[h]^H$ is denoted by $\bar{\alpha}$. For example, if $\alpha$ is the class of the subscheme $R_{K/F}(\mathbb{P}^r_K(W))$ of $X$, where $W$ is a $K$-subspace of $V$ of codimension $i = 0, 1, \ldots, n-1$, then $\bar{\alpha} = h^i$.

Consider the trace homomorphism

$$\text{tr} : Z[h] \to Z[h]^H$$

defined by $\text{tr}(x) = \sum_{i=0}^{p-1} \sigma^i(x)$. We write $I$ for the image of $\text{tr}$. Clearly, $I$ is a graded ideal in $Z[h]^H$. Note that

$$\text{(5) } (Z[h]^H)_j = \begin{cases} I_j, & \text{if } p \text{ does not divide } j; \\ \mathbb{Z} h^i + I_j, & \text{if } j = pi. \end{cases}$$
It follows that $\mathbb{Z}[h]^{H}$ is generated by $I$ and $h^i$, $i = 0, 1, \ldots, n - 1$ as an abelian group. Moreover, $ph^i \in I$ for all $j$ and $I_{p(n - 1)} = p\mathbb{Z}h^{n - 1}$.

Let $A$ be a central simple algebra over $K$ of degree $n$ and let $Y = R_{K/F}(SB(A))$, where $SB(A)$ is the Severi-Brauer variety of $A$ over $K$. The function field $E$ of $Y$ splits $A$ and is linearly disjoint with $K/F$. Therefore, $Y_E \simeq X_E$ and we have the ring homomorphism

$$CH(Y) \to CH(Y_E) \simeq CH(X_E) \to \mathbb{Z}[h]^H.$$  

The image of an element $\alpha \in CH(Y)$ in $\mathbb{Z}[h]^H$ is denoted by $\bar{\alpha}$.

**Proposition 3.5.** Let $K/F$ be a cyclic field extension of prime degree $p$, let $A$ be a nonsplit central simple $K$-algebra of degree $p$ and $Y = R_{K/F}(SB(A))$. Then the image of the map $CH(Y) \to \mathbb{Z}[h]^H$ is contained in $\mathbb{Z} + I$.

**Proof.** Consider a more general situation: $A$ is a central simple $K$-algebra of index $p$ and degree $n$. Let $\alpha \in CH(Y)$. We shall prove in the cases 1 and 2 below that $\bar{\alpha} \in \mathbb{Z} + I$. By (2), we may assume that $\alpha \in CH^{p_1}(Y)$ for $i = 1, 2, \ldots, n - 1$. Let $a \in \mathbb{Z}$ be such that $\bar{\alpha} \equiv ah$ modulo $I$. It suffices to prove that $a$ is divisible by $p$.

**Case 1.** $i = n - 1$. We have $\bar{\alpha} = bh^{n-1}$ for some $b \equiv a$ modulo $p$ as $I_{p(n - 1)} = p\mathbb{Z}h^{n-1}$. Since $h^{n-1}$ is the class of a rational point of $Y$ over a splitting field and the degree of every closed point of $Y$ is divisible by $p$, we have $h \in p\mathbb{Z}$. Therefore, $a \in p\mathbb{Z}$.

**Case 2.** $i$ divides $n - 1$. Write $n - 1 = ij$. We have $\alpha^j \in CH^{p(n-1)}(Y)$ and $\alpha^j \equiv a^j h^{n-1}$ modulo $I$. By Case 1, $a^j$ and hence $a$ is divisible by $p$.

Now assume that $A$ is a central division $K$-algebra of degree $p$ and $\alpha \in CH^{p_1}(Y)$ with $i = 1, 2, \ldots, p - 1$. We shall prove that $\bar{\alpha} \in I$. Write $ik + pm = 1$ for some integers $k$ and $m > 0$. The Severi-Brauer variety $SB(M_m(A))$ can be identified with the variety of the reduced rank $1$ right $A$-submodules in the free right $A$-module $A^m$. The projection to the last component $A$ of $A^m$ gives rise to a rational morphism $SB(M_m(A)) \to SB(A)$ that is defined on the complement $U$ of the variety $SB(M_{m-1}(A))$ embedded into $SB(M_m(A))$ as a closed subvariety via the inclusion $A^{m-1} \to A^m$, $(a_1, \ldots, a_{m-1}) \mapsto (a_1, \ldots, a_{m-1}, 0)$. Moreover, the projection $U \to SB(A)$ is a vector bundle.

Let $Y' = R_{K/F}(SB(M_m(A)))$ and $U' = R_{K/F}(U)$. Then $U'$ is an open subscheme of $Y'$ and the natural morphism $U' \to Y$ is a vector bundle. Hence we have a surjective homomorphism

$$CH(Y') \to CH(U') \simeq CH(Y).$$

Moreover, the diagram

$$\begin{array}{c}
CH(Y') \longrightarrow CH(Y) \\
\downarrow \downarrow \\
\mathbb{Z}[h]^H \longrightarrow \mathbb{Z}[h]^H,
\end{array}$$

where the bottom map takes a monomial $h^{\alpha}$ to $h^{\alpha}$ if $\alpha_i < p$ for all $i$ and to $0$ otherwise, is commutative. Lift $\alpha$ to an element $\alpha' \in CH^{p_1}(Y')$. As $i$ divides $pm - 1$, By Case 2 applied to the algebra $M_m(A)$, we have $\bar{\alpha}' \in I'$. Since the bottom map in the diagram takes $I'$ to $I$, we have $\bar{\alpha} \in I$. $\square$
Let $K'/F$ be a cyclic field extension of degree $p$ and
\[ S = (R_{K'/F}^1(\mathbb{G}_m,K'))^r \simeq (R_{K'/F}(\mathbb{G}_m,K')/\mathbb{G}_m)^r \]
for some $r > 0$. We view the variety of the group $S$ as an open subset of $Z := \mathbb{P}_F(K')^r$. Hence the restriction gives a surjective ring homomorphism
\[ (\mathbb{Z}/p\mathbb{Z})[h] = \text{Ch}(Z) \rightarrow \text{Ch}(S), \]
where $h = (h_1, h_2, \ldots, h_r)$, $h_i^p = 0$ for all $i$, and we write Ch for the Chow groups modulo $p$. We shall also write $\bar{h}_i$ for the image of $h_i$ in $\text{Ch}^1(S)$. The class in $\text{Ch}^r(p^{r-1})(S)$ of a rational point of $S$ is equal to $\bar{h}^{p-1}$, where $\bar{h} = \bar{h}_1\bar{h}_2\cdots\bar{h}_r \in \text{Ch}^0(S)$. As $i(S) = p$, we have $\bar{h}^{p-1} \neq 0$ by Example 3.2.

**Proposition 3.6.** The map $(\mathbb{Z}/p\mathbb{Z})[h] \rightarrow \text{Ch}(S)$ is a ring isomorphism.

**Proof.** Suppose that $f(\bar{h}_1, \bar{h}_2, \ldots, \bar{h}_r) = 0$ for a nonzero homogeneous polynomial $f$ over $\mathbb{Z}/p\mathbb{Z}$. Suppose that a monomial $\bar{h}_1^{\alpha_1} \cdots \bar{h}_r^{\alpha_r}$ enters $f$ with a nonzero coefficient. Multiplying the equality by $\bar{h}_1^{\beta_1} \cdots \bar{h}_r^{\beta_r}$ with $\beta_i = p - 1 - \alpha_i$, we get $\bar{h}^{p-1} = 0$, a contradiction.

For an element $\alpha$ in $\text{Ch}(S)$ we shall write $\bar{\alpha}$ for the corresponding element in $(\mathbb{Z}/p\mathbb{Z})[h]$.

Consider the homomorphism $f : S \times S \rightarrow S$ defined by $f(x, y) = xy^{-1}$. Recall that as $i(S) = p$, by Example 3.3 and Proposition 3.6, we have the homomorphism
\[ f_* : \text{CH}_{r(p-1)}(S \times S) \rightarrow (\mathbb{Z}/p\mathbb{Z}). \]

**Lemma 3.7.** For any $\alpha \in \text{Ch}^i(S)$ and $\beta \in \text{Ch}^j(S)$ with $i + j = r(p - 1)$, we have
\[ \bar{\alpha} \cdot \bar{\beta} = f_*(\alpha \times \beta)h^{p-1} \]
in $(\mathbb{Z}/p\mathbb{Z})[h]$.

**Proof.** It suffices to consider the case when $\alpha$ and $\beta$ are monomials in $\bar{h}_i$. As both sides of the equality commute with products, we may assume that $r = 1$, i.e., $S = R_{K'/F}(\mathbb{G}_m,K')/\mathbb{G}_m$, and $\alpha = \bar{h}^i$, $\beta = \bar{h}^j$. The cycles $\alpha$ and $\beta$ are represented by $\mathbb{P}(U) \cap S$ and $\mathbb{P}(W) \cap S$, where $U$ and $W$ are $F$-subspaces of $K'$ of codimensions $i$ and $j$, respectively. The fiber of the restriction
\[ f' : (\mathbb{P}(U) \cap S) \times (\mathbb{P}(W) \cap S) \rightarrow S \]
of $f$ over a point $s$ of $S$ is isomorphic to $\mathbb{P}(U \cap sW) \cap S$. The vector space $U \cap sW$ is one-dimensional for a generic $s$; hence $f'$ is a birational isomorphism and $f'_*(\alpha \times \beta) = 1 + p\mathbb{Z}$. On the other hand, $\bar{\alpha} \cdot \bar{\beta} = \bar{h}^i \cdot \bar{h}^j = h^{p-1}$. \hfill $\square$

Let $L/F$ be a bicyclic field extension of degree $p^2$ and $T = R_{L/F}^1(\mathbb{G}_m,L)$. Choose a subfield $K$ of $L$ of degree $p$ over $F$ and let $t \in K^\times$ be an element with $N_{K/F}(t) = 1$; i.e., $t$ is an $F$-point of the torus $R_{K/F}^1(\mathbb{G}_m,K)$. Write $S_t$ for the fiber of the norm homomorphism $T \rightarrow R_{K/F}^1(\mathbb{G}_m)$ over $t$. The variety $S_t$ is a principal homogeneous space of the torus $S = R_{K/F}^1(\mathbb{G}_m,K)$.

The variety $S_t$ is canonically isomorphic to an open subscheme of the variety $Y := R_{K/F}(\text{SB}(A_t))$ for a central simple $K$-algebra $A_t$ of degree $p$ (see Section 2.2). Over the function field $E$ of SB($A_t$) over $K$, the varieties $S_t$ and $S$ become isomorphic to the torus $(R_{L/E}^1(\mathbb{G}_m,E))^p$, where $LE = L \otimes_K E$, so we can apply
the constructions considered above to the torus $S_E$ over $E$. In particular, we have that the element $\bar{\alpha} \in (\mathbb{Z}/p\mathbb{Z})[h]$ is well defined for any cycle $\alpha$ on $S_t$ and $S$.

Consider the morphism

$$f : S_t \times S \to S_t, \quad f(x, y) = xy^{-1}.$$  

We have defined the homomorphism (see (6)):

$$f_* : \text{CH}_{p(p-1)}(S_t \times S) \to \text{CH}_{p(p-1)}((S_t)E \times S_E) \to \mathbb{Z}/p\mathbb{Z}.$$  

**Proposition 3.8.** Suppose that the principal homogeneous space $S_t$ is not trivial. Then $f_*(\alpha \times \bar{h}^j) = 0$ for any $\alpha \in \text{CH}^{p(p-j-1)}(S_t)$ and $j = 0, 1, \ldots, p-2$.

**Proof.** As $S_t$ is not trivial, the algebra $A_t$ is not split. We can lift $\alpha$ to a cycle $\beta$ in $\text{Ch}(Y)$. By Proposition 3.3, $\beta$ belongs to the image $I$ of the ideal $I$ in $(\mathbb{Z}/p\mathbb{Z})[h]^H$. It follows that $\alpha \cdot h^j = \beta \cdot h^j \in I_{p(p-1)} = 0$. Lemma 3.7 (applied to the field extension $E$ of $F$ and $r = p$) shows that $f_*(\alpha \times h^j) = 0$. \qed

3.4. A key proposition. Let $p$ be a prime integer, $L/F$ a bicyclic field extension of degree $p^2$, $G = \text{Gal}(L/F)$, $\sigma$ and $\tau$ generators of $G$. Consider the tori $T = R_{L/F}(\mathbb{G}_{m,L})$ of norm 1 elements in $L/F$ and $P = R_{L/F}(\mathbb{G}_{m,L})/\mathbb{G}_m$, both of dimension $d := p^2 - 1$. The torus $T$ (respectively, $P$) becomes isotropic over a field extension $E/F$ if and only if $E \otimes_F L$ is not a field. It follows that $i(T) = i(P) = i(T \times P) = p$.

Consider the morphisms $f$ and $g$ from $T \times P$ to $T$ defined by $f(t, v) = t$ and $g(t, v) = \sigma(t)\tau(v)/v$. By Proposition 3.3 and Example 3.2, $f$ and $g$ give rise to well-defined homomorphisms $f_*$ and $g_*$ from $\text{CH}_d(T \times P)$ to $\mathbb{Z}/p\mathbb{Z}$.

**Proposition 3.9.** The maps $f_*$ and $g_*$ coincide.

**Proof.** The torus $P$ is an open subscheme in the projective space $\mathbb{P}_F(L)$; hence the ring $\text{CH}(P)$ is generated by the restriction to $P$ of the class $e$ of a hyperplane in $\mathbb{P}_F(L)$. Moreover, by the Projective Bundle Theorem [4, Th. 3.3], $\text{CH}_d(T \times P)$ coincides with the sum of subgroups $\text{CH}_i(T) \times e^i$ over all $i = 0, 1, \ldots, d$.

Let $\beta \in \text{CH}_d(T)$. It suffices to show that $f_*(\beta \times e^i) = g_*(\beta \times e^i)$ for any $i = 0, 1, \ldots, d$. If $i = d$, the class $e^d$ is represented by the identity point 1 of $P$. The equality follows from the fact that $f$ and $g$ coincide on $T \times \{1\}$.

Now assume that $i < d$. In this case, $f_*(\beta \times e^i) = 0$ and we need to show that $g_*(\beta \times e^i) = 0$.

Let $K$ be the subfield of $\sigma$-invariant elements in $L$ of degree $p$ over $F$. We have $pk + 1 \leq p^2 - i \leq p(k + 1)$ for some integer $k = 0, \ldots, p - 1$. Consider a $K$-linear subspace $W$ of $L$ of $K$-dimension $k$ such that $K \cap W = 0$. Let $V$ be an $F$-subspace of $L$ of dimension $p^2 - i$ over $F$ such that

$$F \oplus W \subset V \subset K \oplus W.$$  

The class of $P \cap \mathbb{P}(V)$ in $\text{CH}^i(P)$ is equal to $e^i$.

The torus $S := R_{K/F}(R_{L/K}(\mathbb{G}_{m,L}))$ is the kernel of the norm homomorphism $T \to T_1 := R_{K/F}(\mathbb{G}_{m,K})$, so we have an exact sequence

$$(7) \quad 1 \to S \to T \to T_1 \to 1.$$
By Hilbert Theorem 90, $S \simeq R_{K/F}(R_{L/K}(\mathbb{G}_{m,L})/\mathbb{G}_{m,K})$. We view $S$ as an open subscheme of $R_{K/F}(\mathbb{P}_K(L))$. The map $g$ factors as follows:

$$T \times P \overset{1 \times l}{\longrightarrow} T \times S \overset{g}{\longrightarrow} T,$$

where $l : P \rightarrow S$ is defined by $l(v) = v/\sigma(v)$ and $r(t, s) = ts^{-1}$. The image of $P \cap \mathbb{P}_F(K \oplus W)$ under $l$ is the variety $S \cap R_{K/F}(\mathbb{P}_K(K \oplus W))$ of dimension $pk$ in $S \simeq R_{K/F}(R_{L/K}(\mathbb{G}_{m,L})/\mathbb{G}_{m,K})$. Therefore, if $p^2 - 1 > pk + 1$, then $\dim(P \cap \mathbb{P}(V)) > pk$, but the dimension of the image of $P \cap \mathbb{P}(V)$ under $l$ is at most $pk$, so $P \cap \mathbb{P}(V)$ loses dimension under $l$; therefore, $g_*(\beta \times e^1) = 0$.

It remains to consider the case $p^2 - 1 = pk + 1$, $k = 1, \ldots, p - 1$, i.e., $V = F \oplus W$. Since the map $P \cap \mathbb{P}(V) \rightarrow R_{K/F}(\mathbb{P}_K(K \oplus W))$ given by $l$ is a birational isomorphism, and the class of $R_{K/F}(\mathbb{P}_K(K \oplus W))$ in $CH(S)$ is equal to $h^{p-1}$, where $h \in CH^0(S)$ is the class given by a $K$-hyperplane in $L$, it suffices to show that $r_*(\beta \times h^{p-1}) = 0$.

Let $S_t$ be the fiber of the norm homomorphism $T \rightarrow T_1$ over the generic point $t$ of $T_1$, so $S_t$ is a principal homogeneous space of $S$ over the function field $F(T_1)$. Denote by $r' : S_t \times S \rightarrow S_t$ the morphism given by $r'(x, s) = xs^{-1}$. Thus we have a commutative diagram

$$
\begin{array}{ccc}
S_t \times S & \xrightarrow{r'} & S_t \\
\downarrow q & & \downarrow m \\
T \times S & \xrightarrow{r} & T,
\end{array}
$$

where $m$ is the canonical morphism and $q = m \times 1_S$. It follows that $r_*$ factors as the composition

$$CH_d(T \times S) \xrightarrow{q^*} CH_{p-1}(S_t \times S) \xrightarrow{r'^*} \mathbb{Z}/p\mathbb{Z}.$$ 

Thus, it suffices to show that $r'^*(\alpha \times h^{p-1}) = 0$ for any $\alpha \in CH^k(S_t)$. This follows from Proposition 3.8 applied to the torus $S$ over the field $F(T_1)$ (with $j = p - k - 1$) if we show that $S_t$ is a nontrivial principal homogeneous space of $S$. Suppose that $S_t$ has a point over $F(T_1)$. It follows that the exact sequence (1) splits rationally; i.e., the torus $T$ is birationally isomorphic to the product $S \times T_1$ and hence is a rational variety. But $T$ is not rational (see Example 2.2), a contradiction.  

3.5. Invariance of the degree under $R$-equivalence.

**Theorem 3.10.** Let $p$ be a prime integer, $L/F$ a bicyclic field extension of degree $p^2$ and $T = R_{L/F}^1(\mathbb{G}_{m,L})$. Let $M/F$ be a field extension and let $t$ and $t'$ be $R$-equivalent points in $T(M)$. Then $\deg(t) \equiv \deg(t') \pmod{p}$.

**Proof.** We have $t' = t \cdot \sigma(u)u^{-1} \cdot \tau(v)v^{-1}$ for some $u, v \in (LM)^\times$ (see Example 2.1). Let $t'' = t \cdot \sigma(u)u^{-1}$. It suffices to prove that $\deg(t) = \deg(t'')$ and $\deg(t') = \deg(t'')$ in $\mathbb{Z}/p\mathbb{Z}$. We shall prove the first equality (the second being similar). So replacing $t''$ by $t'$ we may assume that $t' = t \cdot \sigma(u)u^{-1}$.

Consider the point $w = (t, u)$ in $(T \times P)(M)$ and two morphisms $f$ and $g$ from $T \times P$ to $T$ as in Section 3.4. We have $f(w) = t$ and $g(w) = t'$. By Propositions 3.3 and 3.4, we have in $\mathbb{Z}/p\mathbb{Z}$:

$$\deg(t) = \deg f(w) = f_*(|w|) = g_*(|w|) = \deg g(w) = \deg(t').$$

\[\square\]
4. Essential $p$-dimension of $\text{PGL}(p^d)$

Let $F$ be a field and $p$ a prime integer different from $\text{char}(F)$.

4.1. Characters, central simple algebras and discrete valuations. Let $v$ be a discrete valuation on a field extension $E$ over $F$, $N$ the residue field, and $\widehat{E}$ the completion of $E$. Then $N$ is a field extension of $F$.

Let $C$ be a finite Galois module over $F$ of order a power of $p$. There is an exact sequence of Galois cohomology groups $\mathbb{[5, Prop. 8.2]}$:

\[ 0 \to H^i(N, C) \to H^i(\widehat{E}, C) \to H^{i+1}(N, C(-1)) \to 0. \]

Taking $i = 1$ and $C = \mathbb{Z}/p^n\mathbb{Z}$ for some $n$, we get an exact sequence

\[ 0 \to p\cdot X(N) \xrightarrow{i} p\cdot X(\widehat{E}) \xrightarrow{\partial} \text{Hom}_{\Gamma}(\mu_{p^n}, \mathbb{Z}/p^n\mathbb{Z}) \to 0, \]

where $\mu_{p^n}$ is the $\Gamma$-module of $p^n$th roots of unity.

Let $\chi \in X(F)$. Recall that $F(\chi)/F$ is a cyclic field extension of degree $\text{ord}(\chi)$ with the choice of a generator of $\text{Gal}(F(\chi)/F)$. The group $X(N)$ is identified with the character group of the maximal unramified field extension of $\widehat{E}$. For a character $\chi \in p\cdot X(N)$, we write $\widehat{\chi}$ for the corresponding character in $p\cdot X(\widehat{E})$.

Taking $i = 2$ and $C = \mu_{p^n}$ for all $n$, we get an exact sequence

\[ 0 \to \text{Br}(N)\{p\} \xrightarrow{i} \text{Br}(\widehat{E})\{p\} \xrightarrow{\partial} X(N)\{p\} \to 0. \]

The first map preserves indices of algebras. For a central simple algebra $C$ over $N$ with $C \in \text{Br}(N)\{p\}$ let $\widehat{C}$ be a central simple algebra over $\widehat{E}$ of the same degree representing the image of $[C]$ under $i$. For example, if $[C] = \chi + (u)$ for some $\chi \in X(N)\{p\}$ and a unit $u \in \widehat{E}$, then $[\widehat{C}] = \widehat{\chi} + (u)$.

The choice of a prime element $\pi$ in $\widehat{E}$ yields a splitting of the sequence $\mathbb{[10]}$ by sending a character $\chi$ to the class of the cyclic algebra $\widehat{\chi} + (\pi)$. Thus for every central simple algebra $A$ over $\widehat{E}$ we can write

$[A] = [C] + ([\widehat{\chi}] + (\pi))$

in $\text{Br}(\widehat{E})$ for a unique $[C] \in \text{Br}(N)\{p\}$ and $\chi = \partial([A])$. Moreover (see $\mathbb{[6, Th. 5.15(a)]}$ or $\mathbb{[10, Prop. 2.4]}$),

\[ \text{ind}(A) = \text{ord}(\chi) \cdot \text{ind}(C_{N(\chi)}). \]

Let $E'/E$ be a finite field extension and $v'$ a discrete valuation on $E'$ extending $v$ with residue field $N'$. Then for any $[A] \in \text{Br}(E)\{p\}$ one has

\[ \partial_{v'}([A_{E'}]) = e \cdot \partial_v([A])_{N'}. \]

where $e$ is the ramification index of $E'/E$ $\mathbb{[3, Prop. 8.2]}$.

4.2. The functors $\mathcal{F}_1$ and $\mathcal{F}_2$. We define the functors $\mathcal{F}_1$ and $\mathcal{F}_2$ from the category $\text{Fields}/F$ of field extensions of $F$ to the category $\text{Sets}$ as follows. Let $E/F$ be a field extension. Then $\mathcal{F}_1(E)$ is the set of isomorphism classes of central simple $E$-algebras of degree $p^2$. Thus, $d_{p}(\mathcal{F}_1) = d_{p}(\text{PGL}_F(p^2))$.

Let $\mathcal{S}_2(E)$ be the class of pairs $(B, K)$, where $B$ is a central simple algebra of degree $p^2$ over $E$ and $K$ is a cyclic étale $E$-algebra of degree $p$ such that $\text{ind}(B_K) \leq p$; i.e., $K$ is isomorphic to an $E$-subalgebra of $B$. We say that the pairs $(B_1, K_1)$ and $(B_2, K_2)$ are equivalent if $K_1 \simeq K_2$ over $E$ and $[B_1] - [B_2] \in \text{Br}(K_1/E) = \mathbb{Z}/p\mathbb{Z}$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Let $\text{Br}(K_2/E)$. Let $\mathcal{F}_2(E)$ be the set of equivalence classes in $\mathcal{S}_2(E)$. We write $[B, K]$ for the class in $\mathcal{F}_2(E)$ of a pair $(B, K)$.

Let $(B, K) \in \mathcal{S}_2(E)$ with $K$ a field and let $\chi \in X(E)$ be a character (of order $p$) such that $K = E(\chi)$ (see Section 2.2). As $\text{ind}(B_K) \leq p$, there is a central simple algebra $C$ over the function field $E(y)$ ($y$ is a variable) of degree $p^2$ such that

$$[C] = [B_{E(y)}] + (\chi_{E(y)} \cup (y))$$

in $\text{Br}(E(y))$.

Consider the following condition $(\ast)$ on the pair $(B, K)$ in $\mathcal{S}_2(E)$ and the character $\chi$:

For any finite field extension $N/E$ of degree prime to $p$, the class of the algebra $B_N$ in $\text{Br}(N)$ cannot be written in the form $[B_N] = \rho \cup (s)$ for some $s \in N^\times$ and a character $\rho \in X(N)$ of order $p^2$ such that $p \cdot \rho$ is a multiple of $\chi_N$.

**Proposition 4.1.** Let $\chi \in X(E)$ be a character of prime order $p$, $K = E(\chi)$, and let $B$ be a central simple algebra of degree $p^2$ over $E$ such that $(B, K) \in \mathcal{S}_2(E)$ and $(B, K)$ together with $\chi$ satisfy the condition $(\ast)$. Then

$$\text{ed}^p_1([C]) \geq \text{ed}^p_2([B, K]) + 1$$

for the algebra $C$ defined by (13).

**Proof.** Let $M/E(y)$ be a finite field extension of degree prime to $p$, $M_0 \subset M$ a subfield over $F$ and $[C_0] \in \mathcal{F}_1(M_0)$ such that

$$[(C_0)_M] = [C_M]$$

in $\mathcal{F}_1(M)$ and $\text{ed}^p_1([C]) = \text{tr. deg.}_F(M_0)$.

We have $[C] \in \mathcal{F}_1(E(y))$ and $\partial([C]) = \chi$, where $\partial$ is taken with respect to the discrete valuation $\nu$ on $E(y)$ associated to $y$ (see Section 4.1). We extend $\nu$ to a discrete valuation $\nu'$ on $M$ with ramification index $e'$ and inertia degree both prime to $p$ (see [1] Lemma 1.1). Thus, the residue field $N$ of $\nu'$ is a finite extension of $E$ of degree prime to $p$. Let $v_0$ be the restriction of $\nu'$ to $M_0$ and $N_0$ its residue field. As $[N : E]$ is not divisible by $p$, it follows from (12) that $\partial([C_M]) = e' \cdot \chi_N \neq 0$. Hence the algebra $C_M$ is ramified; i.e., the class of $C_M$ does not belong to the image of the map $\text{Br}(O) \to \text{Br}(M)$, where $O$ is the valuation ring of $v'$. It follows that $C_0$ is also ramified; therefore $v_0$ is nontrivial and hence $v_0$ is a discrete valuation on $M_0$.

Let $\chi_0 = \partial([C_0]) \in X(N_0\{p\})$ and $K_0 = N_0(\chi_0)$. Choose a prime element $\pi_0$ in $M_0$ and write

$$[(C_0)_{\widehat{M}_0}] = [\widehat{B}_0] + (\widehat{\chi}_0 \cup (\pi_0))$$

in $\text{Br}(\widehat{M}_0)$, where $B_0$ is a central simple algebra over $N_0$ (see Section 4.1). By (11),

$$\text{ind}(C_0) = \text{ord}(\chi_0) \cdot \text{ind}(B_0)_{K_0}.$$

Let $e$ be the ramification index of $M/M_0$ and let $\pi$ be a prime element in $M$. Write $\pi_0 = u \pi^e$ and $y = v \pi^e$ with $u$ and $v$ units in $M$.

It follows from (14) and (12) that

$$e' \cdot \chi_N = \partial([C_M]) = \partial([C_0]_{M}) = e \cdot \partial(\chi_0)_{N} = e \cdot (\chi_0)_{N}.$$

Recall that $e'$ is relatively prime to $p$. It follows that $\chi_N$ is a multiple of $(\chi_0)_{N}$.

In particular, $\text{ord}(\chi_0)_{N}$ is divisible by $p$. 
It follows from (14), (15) and (17) that
\begin{equation}
[(\hat{B}_0)_N] + ((\hat{\chi}_0)_N \cup (u)) = [\hat{B}_N] + (\hat{\chi}_N \cup (\bar{v}))
\end{equation}
in $\text{Br}(\hat{M})$; hence
\begin{equation}
[(B_0)_N] + ((\chi_0)_N \cup (\bar{u})) = [B_N] + (\chi_N \cup (\bar{v}))
\end{equation}
in $\text{Br}(N)$.

Since $\text{ind}(C_0) \leq p^2$, it follows from (11) and (16) that $\text{ord}(\chi_0)$ divides $p^2$.

**Case 1.** $\text{ord}(\chi_0)_N = p^2$. By (16), $\text{ind}(B_0)_{K_0} = 1$, i.e., $B_0$ is split over $K_0$; hence $[B_0] = \chi_0 \cup (s_0)$ for some $s_0 \in N^\times$. It follows from (19) that $[B_N] = (\chi_0)_N \cup (s)$ for some $s \in N^\times$. Since $\text{ord}(\chi_0)_N = p^2$, the character $p \cdot (\chi_0)_N$ is a multiple of $\chi_N$ by (17). Hence $(B, K)$ and $\chi$ do not satisfy the condition (*), a contradiction.

**Case 2.** $\text{ord}(\chi_0)_N = p$. As $p\eta_0$ is split by $N$, we can view the field $N_1 := N_0(p\eta_0)$ as a subfield of $N$. Replacing $N_0$ by $N_1$ and $B_0$ by $(B_0)_{N_1}$, we may assume that $\eta_0$ is of order $p$ in $X(N_0)$. The characters $\chi_N$ and $(\chi_0)_N$ generate the same subgroup in $X(N)$. It follows that
\begin{equation}
K_0 \otimes_{N_0} N \simeq N((\chi_0)_N) = N(\chi_N) \simeq K \otimes_{E} N.
\end{equation}

By (19), we have $\text{ind}(B_0)_{K_0} \leq p$. Therefore, we may assume that $\deg(B_0) = p^2$ and hence $(B_0, K_0) \in \mathcal{S}_2(N_0)$. It follows from (19) that
\begin{equation}
[B_N] - [(B_0)_N] \in \text{Br}(K \otimes_{E} N/N).
\end{equation}

By (20), the pairs $(B_N, K \otimes_{E} N)$ and $((B_0)_N, K_0 \otimes_{N_0} N) = (B_0, K_0)_N$ are equivalent in $\mathcal{S}_2(N)$. It follows that the class of $[B, K]$ in $\mathcal{F}_2(E)$ is $p$-defined over $N_0$; therefore,
\begin{equation}
\text{ed}^{\mathcal{F}_1}_p([C]) = \text{tr. deg}_p(M_0) \geq \text{tr. deg}_p(N_0) + 1 \geq \text{ed}^{\mathcal{F}_2}_p([B, K]) + 1.
\end{equation}

**Remark 4.2.** The statement of Proposition 4.1 is no longer true if we don’t assume the condition (*). Indeed, let $[B_N] = \rho \cup (s)$ for a finite field extension $N/E$ of degree prime to $p$, some $s \in N^\times$ and a character $\rho \in X(N)$ of order $p^2$ such that $p \cdot \rho$ is a multiple of $\chi_N$. Then $[C_{N(y)}] = \rho_{N(y)} \cup (sy^p)$ for some $y$; i.e., the algebra $C_{N(y)}$ is also cyclic. With an appropriate choice of $\rho$ and $s$ (and the assumption that the base field contains a primitive root of unity of degree $p^2$) both classes $[B, K]$ and $[C]$ have essential $p$-dimension 2.

**4.3. The functor $\mathcal{F}_3$.** Let $E/F$ be a field extension and let $\mathcal{S}_3(E)$ be the class of pairs $(A, L)$, where $A$ is a central simple algebra of degree $p^2$ over $E$ and $L$ is a bicyclic étale $E$-algebra of dimension $p^2$ such that $L$ splits $A$; i.e., $L$ is isomorphic to an $E$-subalgebra of $A$, or, equivalently, $[A] \in \text{Br}(L/E)$. We say that the pairs $(A_1, L_1)$ and $(A_2, L_2)$ in $\mathcal{S}_3(E)$ are equivalent if $L_1 \simeq L_2$ and $[A_1] - [A_2] \in \text{Br}_{\text{dec}}(L_1/E) = \text{Br}_{\text{dec}}(L_2/E)$ (see Section 4.2). Let $\mathcal{F}_3(E)$ be the set of equivalence classes in $\mathcal{S}_3(E)$. We write $[A, L]$ for the equivalence class of $(A, L)$ in $\mathcal{F}_3(E)$.

Let $L$ be a bicyclic étale $E$-algebra of dimension $p^2$. We view the factor group $\text{Br}(L/E)/\text{Br}_{\text{dec}}(L/E)$ as a subset of $\mathcal{F}_3(E)$ identifying the class of an algebra $A$ with $[A, L]$.

Let $\chi$ and $\eta$ in $X(F)$ be linearly independent characters of order $p$ and let $E/F$ be a field extension such that $\chi_E$ and $\eta_E$ are linearly independent in $X(E)$. Let $(A, L) \in \mathcal{S}_3(E)$ and set $K = E(\chi)$ and $L = E(\chi, \eta) := K(\eta)$. As $A$ is split by $L$, 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
there is a central simple algebra $B$ over the function field $E(x)$ ($x$ is a variable) of degree $p^2$ such that

$$[B] = [A_{E(x)}] + (\eta_{E(x)} \cup (x))$$

in $\text{Br}(E(x))$. We have $(B, K(x)) \in S_2(E(x))$.

**Proposition 4.3.** Let $\chi, \eta \in \mathcal{X}(F)$ be characters of order $p$, $E/F$ a field extension such that $\chi_E$ and $\eta_E$ are linearly independent in $\mathcal{X}(E)$, $K = E(\chi)$, $L = E(\chi, \eta)$, $A$ a central simple algebra of degree $p^2$ over $E$ such that $(A, L) \in S_3(E)$. Then

$$\text{ed}_p^F([B, K(x)]) \geq \text{ed}_p^F([A, L]) + 1$$

for the algebra $B$ defined by (21).

**Proof.** Let $M/E(x)$ be a finite field extension of degree prime to $p$, $M_0 \subseteq M$ a subfield over $F$ and $[B_0, R_0] \in F_2(M_0)$ such that $\text{ed}_p^F([B, K(x)]) = \text{tr.deg}_F(M_0)$ and

$$[B_0, R_0]_M = [B, K(x)]_M$$

in $F_2(M)$. The last equality means that $R := K(x) \otimes_{E(x)} M \simeq R_0 \otimes_{M_0} M$ and

$$[B_M] = ([B_0]_M) + (\chi_M \cup (f))$$

in $\text{Br}(M)$ for some $f \in M^\times$. Hence there is a character $\rho \in \mathcal{X}(M_0)$ such that $R_0 \simeq M_0(\rho)$ and $\rho_M = \chi_M$. Therefore, we can view the field $M_1 := M_0(\rho - \chi_{M_0})$ as a subfield of $M$. Replacing $M_0$ by $M_1$ and $[B_0, R_0]_M$ by $[B_0, R_0]_{M_1}$, we may assume that $\rho = \chi_{M_0}$, i.e., $R_0 = M_0(\chi)$. We have $\partial([B]) = \eta$, where $\partial$ is taken with respect to the discrete valuation $v$ on $E(x)$ associated to $x$. We extend the discrete valuation $v$ on $E(x)$ to a discrete valuation $v'$ on $M$ with ramification index $e'$ and inertia degree both prime to $p$ (see [21 Lemma 1.1]). Thus, the residue field $N$ of $v'$ is a finite extension of $E$ of degree prime to $p$. Let $v_0$ be the restriction of $v'$ to $M_0$ and $N_0$ its residue field. As $[N : E]$ is not divisible by $p$, it follows from (12) that $\partial([B_M]) = e' \cdot \eta_N \neq 0$. Hence the algebra $B_M$ is ramified. It follows from (22) and (12) that

$$e' \cdot \eta_N = \partial([B_M]) = \partial(([B_0]_M)) + k \cdot \chi_N,$$

where $k = v'(f)$. Note that the characters $\chi_N$ and $\eta_N$ are linearly independent in $\mathcal{X}(N)$ since $[N : E]$ is not divisible by $p$. It follows that $\partial(([B_0]_M)) \neq 0$ and then $B_0$ is ramified; therefore $v_0$ is nontrivial and hence $v_0$ is a discrete valuation on $M_0$.

As $R = KM$, the valuation $v'$ on $M$ extends to a discrete valuation on $R$ such that $R/M$ is unramified.

Let $\eta_0 = \partial([B_0]) \in \mathcal{X}(N_0)\{p\}$. Choose a prime element $\pi_0$ in $M_0$ and write

$$([B_0]_{\tilde{M}_0}) = [\tilde{A}_0] + ([\eta_0] \cup (\pi_0))$$

in $\text{Br}(\tilde{M}_0)$, where $A_0$ is a central simple algebra over $N_0$. By (11),

$$\text{ind}(B_0) = \text{ord}(\eta_0) \cdot \text{ind}(A_0)_{N_0(\eta_0)}.$$  

Let $e$ be the ramification index of $M/M_0$ and let $\pi$ be a prime element in $M$. Write $\pi = u\pi^e$, $x = v\pi^e$ and $f = w\pi^k$ with $u$, $v$ and $w$ units in $M$. It follows from (23) that

$$e' \cdot \eta_N = e \cdot (\eta_0)_N + k \cdot \chi_N.$$
As $e'$ is relatively prime to $p$, $\eta_N$ belongs to the subgroup of $X(N)$ generated by $(\eta_0)_N$ and $\chi_N$, and $(\eta_0)_N \neq 0$ since $\chi_N$ and $\eta_N$ are linearly independent. In particular, $p$ divides $\text{ord}(\eta_0)_N$.

It follows from (22), (24) and (20) that

\[(A_0)_N + (\hat{\eta}_N \cup \hat{\hat{v}}) = \hat{A}_N + (\hat{\eta}_N \cup \hat{v})\]

in $\text{Br}(\hat{M})$; hence

\[(A_0)_N + (\hat{\eta}_N \cup \hat{\hat{v}}) = (A_0)_N + (\hat{\eta}_N \cup \hat{v})\]

in $\text{Br}(N)$.

Since $\text{ind}(B_0) \leq p^2$, it follows from (24) that $\text{ord}(\eta_0) \leq p^2$.

Case 1. $\text{ord}(\eta_0)_N = \text{ord}(\eta_0) = p^2$. It follows from (20) that $e$ is divisible by $p$. By (25), $A_0$ is split over $N_0(\eta_0)$; hence $[A_0] = \eta_0 \cup (\bar{s}_0)$ for some $s_0 \in M_0^*$. It follows from (21) that $[B_0]_{\hat{M}_0} = \hat{\eta}_0 \cup (\bar{s}_0 \pi_0)$ in $\text{Br}(\hat{M}_0)$; hence $[B_0]_{\hat{M}_0(\chi)} = \hat{\eta}_0 N_0(\chi) \cup (\bar{s}_0 \pi_0)$ in $\text{Br}(\hat{M}_0(\chi))$. As

\[\text{ind}(B_0)_{\hat{M}_0(\chi)} \leq \text{ind}(B_0)_{M_0(\chi)} = \text{ind}(B_0)_{R_0} \leq p,\]

the order of $(\eta_0)_{N_0(\chi)}$ is at most $p$, i.e., $p \eta_0$ is a multiple of $\chi_{N_0}$. As $e$ is divisible by $p$, it follows from (20) that $\eta_N$ is a multiple of $\chi_N$, a contradiction.

Case 2. $\text{ord}(\eta_0)_N = p$. It follows from (20) that $(e, p) = 1$ and $(\eta_0)_N$ belongs to the subgroup generated by $\chi_N$ and $\eta_N$. Moreover,

\[(\chi_N, (\eta_0)_N) = (\chi_N, \eta_N)\]

in $X(N)$. Let $K_0 = N_0(\chi)$. It follows from (24) that

\[[B_0]_{R_0} = [(A_0)_{K_0}] + (\hat{\eta}_0)_{K_0} \cup (\pi_0)\]

As $(B_0, R_0) \in S_2(M_0)$, we have $\text{ind}(B_0)_{R_0} \leq p$. Since $\eta_0$ is not a multiple of $\chi_{N_0}$, the character $(\eta_0)_{K_0}$ is nontrivial, and it follows from (11) that $A_0$ is split by $K_0(\eta_0)$.

As $p \eta_0$ is split by $N$, we can view the field $N_1 := N_0(p \eta_0)$ as a subfield of $N$. Replacing $N_0$ by $N_1$ and $A_0$ by $(A_0)_{N_1}$, we may assume that $\eta_0$ is of order $p$ in $X(N_0)$.

Let $L_0 = N_0(\chi, \eta_0) = K_0(\eta_0)$. Then

\[(L_0 \otimes_{N_0} N) = N(\chi, \eta_0) = N(\chi, \eta) = L \otimes_E N\]

is a bicyclic field extension of degree $p^2$ and hence so is the extension $L_0/N_0$. In particular, $\chi_{N_0}$ and $\eta_0$ generate a subgroup of order $p^2$ in $X(N_0)$.

As $A_0$ is split by $L_0$, we may assume that $\text{deg}(A_0) = p^2$ and hence $(A_0, L_0) \in S_3(N_0)$.

It follows from (20) that $[A_N] - [(A_0)_N] \in \text{Br}_{dec}(L \otimes_E N/N)$. By (20), the pairs $(A_N, L \otimes_E N)$ and $(A_0)_N, L_0 \otimes_{N_0} N) = (A_0, L_0)_N$ are equivalent in $S_3(N)$. Then the class $[A, L]$ in $F_3(E)$ is $p$-defined over $N_0$; therefore,

\[\text{ed}^{T_2}_p([B, K(x)]) = \text{tr. deg}_F(M_0) \geq \text{tr. deg}_F(N_0) + 1 \geq \text{ed}^{T_2}_p([A, L]) + 1.\]
Let \( L/F \) be a bicyclic field extension of degree \( p^2 \). Write \( T \) for the torus over \( F \) of norm 1 elements for the field extension \( L/F \). Let \( t \in T(F(T)) \) be the generic point and let \( [A, L(T)] \) be the corresponding element in \( \mathcal{F}_3(F(T)) \) via the isomorphism between \( T(F(T))/R \) and \( \operatorname{Br}(L(T)/F(T))/\operatorname{Br}_{dec}(L(T)/F(T)) \) in Proposition 2.3.

**Proposition 4.4.** \( \operatorname{ed}_{p^3}([A, L(T)]) \geq p^2 - 1 \).

**Proof.** Let \( M/F(T) \) be a field extension of degree prime to \( p \), \( M_0 \subset M \) a subfield over \( F \) and \( [A_0, L_0] \in \mathcal{F}_3(M_0) \) such that \( [A_0, L_0]_M = [A, L(T)]_M \). We need to prove that \( \operatorname{tr.deg}_F(M_0) \geq p^2 - 1 \). Set \( LM = L \otimes_F M \). As \( L_0 \otimes_{M_0} M \simeq LM \), we may assume that \( L_0 \subset LM \).

Let \( T_0 \) be the torus over \( M_0 \) of norm 1 elements for the extension \( L_0/M_0 \). We have \( (T_0)_M \simeq T_M \). Consider the commutative diagram

\[
\begin{array}{ccc}
T_0(M_0)/R & \longrightarrow & T(M)/R \\
\downarrow & & \downarrow \\
\mathcal{F}_3(M_0) & \longrightarrow & \mathcal{F}_3(M),
\end{array}
\]

where the vertical injective maps are given by the isomorphisms in Proposition 2.3. The pair \([A_0, L_0]\) belongs to the image of the left vertical map in the diagram. Hence there exists an element \( t_0 \in T_0(M_0) \) such that \( (t_0)_M \) in \( T_0(M) = T(M) \) is \( R \)-equivalent to \( t_M \). We have \( \operatorname{deg}(t) = 1 \); therefore, \( \operatorname{deg}(t_M) \) is not divisible by \( p \) as \([M : F(T)]\) is prime to \( p \). By Theorem 3.10 \( \operatorname{deg}((t_0)_M) = \operatorname{deg}(t_M) \) modulo \( p \); hence \( \operatorname{deg}((t_0)_M) \neq 0 \). It follows that \((t_0)_M\), viewed as a morphism \( \operatorname{Spec}(M) \to T \), is dominant. Therefore, there is a field homomorphism \( F(T) \to M \) over \( F \) taking \( t \) to \((t_0)_M\). The elements \( \rho(t) \) over all \( \rho \in G := \operatorname{Gal}(L/F) \) generate the field \( L(T) \) over \( L \). Hence the elements \( \rho(t)_M \) generate a subfield in \( LM \) over \( L \) of the transcendence degree \( \operatorname{dim}(T) = p^2 - 1 \). As \( t_0 \in L_0 \) and \( L_0 \) is normal over \( M_0 \) and hence is \( G \)-invariant, the elements \( \rho(t_0) \) generate a subfield in \( L_0 \) over \( F \) of the transcendence degree \( p^2 - 1 \). It follows that \( \operatorname{tr.deg}_F(L_0) \geq p^2 - 1 \); hence \( \operatorname{tr.deg}_F(M_0) \geq p^2 - 1 \).

**Remark 4.5.** Let \( L \) be a bicyclic field extension of degree \( p^2 \) of a field \( F \) of arbitrary characteristic and let \( T = \mathcal{R}_{L/F}^1(\mathbb{G}_m, L) \). A similar argument as the one in the proof of Proposition 4.4 shows that \( \operatorname{ed}_p(T/R) = p^2 - 1 \), where \( T/R \) is the functor taking a field \( E \) to \( T(E)/R \).

### 4.4. The main theorem.

**Theorem 4.6.** Let \( p \) be a prime integer and \( F \) a field of characteristic different from \( p \). Then

\[
\operatorname{ed}_p(\mathbb{PGL}(p^2)) = p^2 + 1.
\]

**Proof.** Recall that \( \operatorname{ed}_p(\mathbb{PGL}(p^2)) = \operatorname{ed}_p(\mathcal{F}_1) \). First we prove the inequality \( \operatorname{ed}_p(\mathcal{F}_1) \geq p^2 + 1 \). We may replace \( F \) by any field extension. In particular, we may assume that there are linearly independent characters \( \chi, \eta \in X(F) \) of order \( p \); hence \( L := F(\chi, \eta)/F \) is a bicyclic field extension of degree \( p^2 \). Set \( K = F(\chi) \) and \( K' = F(\eta) \). Let \( T \) be the norm 1 torus for the extension \( L/F \) and set \( E := F(T) \). Let \([A, LE]\) be the element of \( \mathcal{F}_3(E) \) corresponding to the generic point \( t \in T(E) \) via the isomorphism in Proposition 2.3. Consider the pair \((B, KE(x)) \in S_2(E(x)) \)
with
\[(30) \quad \begin{aligned}
[B] &= [A_{E(x)}] + (\eta_{E(x)} \cup (x)) \\
[C] &= [B_{E(x,y)}] + (\chi_{E(x,y)} \cup (y))
\end{aligned}
\]
in $\text{Br}(E(x,y))$. We claim that the pair $(B, KE(x))$ in $S_2(E(x))$ and the character $\chi_{E(x)}$ satisfy the condition $(\ast)$. Let $N/E(x)$ be a finite field extension of degree prime to $p$ with $[B_N] = \rho \cup (s)$ in $\text{Br}(N)$ for some $s \in N^\times$ and a character $\rho \in X(N)$ of order $p^2$ such that $p \cdot \rho$ is a multiple of $\chi_N$. Extend the discrete valuation of the field $F(x)$ associated to $x$ to a discrete valuation $v$ on $N$ with the ramification index $e'$ prime to $p$ and residue field $P$ of degree prime to $p$ over $E$. As $p \cdot \rho$ is a multiple of $\chi_N$ and the extension $\hat{N}(\chi)/\hat{N}$ is unramified, the ramification index $e$ of $\hat{N}(\rho)/\hat{N}$ is either 1 or $p$.

**Case 1.** $e = 1$. We have $\rho_{\hat{N}} = \hat{\mu}$ for a character $\mu \in X(P)$ of order $p^2$. By (30), we have
\[e' \eta_P = \partial([B_{\hat{N}}]) = v(s)\mu_P.\]
As $\rho_P$ is of order $p^2$, the character $p \cdot \mu_P$ is a multiple of $\chi_N$. On the other hand, $p \cdot \mu$ is a multiple of $\chi_P$ by assumption; i.e., $\chi_P$ and $\eta_P$ are linearly dependent, a contradiction.

**Case 2.** $e = p$. It follows that $P$ contains primitive roots of unity of degree $p$ (see [9]), so we can identify $pX(P)$ with $P^s/P^{sp}$. Let $\pi$ be a prime element in $N$ and $\nu$ the corresponding character of order $p$ in $X(N)$. We can write $\rho = \hat{\mu} + lv$ for some character $\mu \in X(P)$ of order $p^2$ and an integer $l$ prime to $p$. Noting that $\chi_N = p \cdot \rho = p \cdot \hat{\mu}$, we have $p \cdot \mu = \chi_P$.

Write $s = u\pi^j$ for some integer $u$ in $N$. Then
\[(31) \quad \begin{aligned}
[B_N] &= \rho \cup (s) = (\hat{\mu} + lv) \cup (u\pi^j) = \hat{\mu} \cup (u) + (j\hat{\mu}) \cup (\pi) + \nu \cup (w),
\end{aligned}\]
where $w = (-1)^j\eta_\pi^j$. Let $\epsilon$ be the character in $X(P)$ of exponent $p$ corresponding to $\hat{w}$. As $\nu \cup (w) + \epsilon \cup (\pi) = 0$, it follows from (30) that
\[e' \eta_P = \partial([B_{\hat{N}}]) = j\mu - \epsilon.
\]
Since $\mu$ is of order $p^2$, we have $j = pk$ for some integer $k$. Hence $\epsilon = kp \cdot \mu - e' \eta_P = k\chi_P - e' \eta_P$. Note that the characters $\chi$ and $\eta$ are defined over $F$. It follows that the classes of $\hat{w}$ and $\hat{u}$ belong to the image of $F^s/F^{sp}$ in $P^s/P^{sp}$. By (30) and (31),
\[p[A_P] = p(\mu \cup (\hat{u})) = \chi_P \cup (\hat{u}) \in \text{Im}(\text{Br}(F) \rightarrow \text{Br}(N)).\]
Taking the corestriction for the extension $P/E$ of degree prime to $p$, we see that the class $p[A]$ belongs to the image of the map $\text{Br}(F) \rightarrow \text{Br}(E)$. This contradicts Corollary (2.3). Thus, we have checked the condition $(\ast)$.

By Propositions (4.1), (4.3) and (4.4),
\[\begin{aligned}
ed_p(\text{PGL}_F(p^2)) &= ed_p(F_1) \geq ed_p^p([C]) \geq ed_p^p([B, KE(x)]) + 1 \\
&\geq ed_p^p([A, LE]) + 2 \geq (p^2 - 1) + 2 = p^2 + 1.
\end{aligned}\]

We shall show that $ed_p(F) \leq p^2 + 1$. As mentioned in the introduction, this was shown in [9, Cor. 3.10(a)]. For completeness, we give the argument here.
Let $\mathcal{F}_1(E)$ be the set of isomorphism classes of central simple $E$-algebras of degree $p^2$ that are crossed products with the group $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. So $\mathcal{F}_1$ is a subfunctor of $\mathcal{F}_1$. By [8 Th. 1.2], for every $[A] \in \mathcal{F}_1(E)$ there is a finite field extension $E'/E$ of degree prime to $p$ such that $[A_{E'}] \in \mathcal{F}_1(E')$. Hence the inclusion of $\mathcal{F}_1'$ into $\mathcal{F}_1$ is $p$-surjective (see [11]). It follows that $\text{ed}_p(\mathcal{F}_1') \leq \text{ed}_p(\mathcal{F}_1)$ [11 Prop. 1.3]. So it suffices to show that $\text{ed}(\mathcal{F}_1') \leq p^2 + 1$.

Let $E/F$ be a field extension and $[A] \in \mathcal{F}_1(E)$. Then $[A] \in \text{Br}(L/E)$ for a bicyclic field extension $L/F$ of degree $p^2$ with Galois group $G$ generated by $\sigma$ and $\tau$. The exact sequence (2) yields an epimorphism

$$\text{Hom}_G(M, L^\times) \to \text{Br}(L/E).$$

Choose a $G$-homomorphism $\varphi : M \to L^\times$ corresponding to $[A]$ in $\text{Br}(L/E)$. Since $\text{rank}(M) = p^2 + 1$, the image of $\varphi$ is contained in $L_0$, where $L_0$ is a $G$-invariant subfield of $L$ with $\text{tr.deg}_F(L_0) \leq p^2 + 1$. Note that $G$ acts faithfully on $M$. Modifying $\varphi$ by an element in the image of the map $\text{Hom}_G(A^2, L^\times) \to \text{Hom}_G(M, L^\times)$, we may assume that $G$ acts faithfully on the image of $\varphi$ and hence on $L_0$. Thus $L_0$ is a Galois extension of $E_0 := (L_0)^G$ with Galois group $G$, and $\varphi$ defines a central simple $E_0$-algebra $A_0$ with $[A_0] \in \text{Br}(L_0/E_0)$ such that $A_0 \otimes_{E_0} E \simeq A$. Thus, $A$ is defined over $E_0$; hence

$$\text{ed}(\mathcal{F}_1([A])) \leq \text{tr. deg}_F(E_0) = \text{tr. deg}_F(L_0) \leq p^2 + 1. \quad \square$$

**References**


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90095-1555

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