JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 23, Number 3, July 2010, Pages 693–712
S 0894-0347(10)00661-2
Article electronically published on January 15, 2010

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

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 Fields/F of field extensions of F and field homomorphisms over F. Let $\mathcal{F} : \mathit{Fields}/F \to \mathit{Sets}$ be a functor (an "algebraic structure") and $K, E \in \mathit{Fields}/F$. 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 α*) 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 α under the map $\mathcal{F}(E) \to \mathcal{F}(E')$ coincides with the image of β under the map $\mathcal{F}(K) \to \mathcal{F}(E')$. The *essential p-dimension of α*, denoted $\mathrm{ed}_p^{\mathcal{F}}(\alpha)$, is the least transcendence degree $\mathrm{tr.deg}_F(K)$ over all fields of p-definition K of α. The *essential p-dimension of the functor $\mathcal{F}$* is

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

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

We write $\mathrm{ed}(\mathcal{F})$ for $\mathrm{ed}_0(\mathcal{F})$ and simply call $\mathrm{ed}(\mathcal{F})$ the *essential dimension of $\mathcal{F}$*. Clearly, $\mathrm{ed}(\mathcal{F}) \geq \mathrm{ed}_p(\mathcal{F})$ 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 $\mathcal{F}_G : \mathit{Fields}/F \to \mathit{Sets}$ taking a field E to the set of isomorphism classes of all G-torsors (principal homogeneous G-spaces) over $\mathrm{Spec}(E)$.

If $G = \mathbf{PGL}_n$ 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^r be the highest power of p dividing n. Then $\mathrm{ed}_p\big(\mathbf{PGL}_F(n)\big) = \mathrm{ed}_p\big(\mathbf{PGL}_F(p^r)\big)$ [12, Lemma 8.5.5]. Every central simple

Received by the editors December 8, 2008 and, in revised form, July 12, 2009.
2010 *Mathematics Subject Classification.* Primary 16K50, 20G15.
Key words and phrases. Essential p-dimension, Brauer group, algebraic tori.
The work has been supported by the NSF grant DMS #0652316.

E-algebra of degree p is cyclic over a finite field extension of degree prime to p; hence $\mathrm{ed}_p\big(\mathbf{PGL}_F(p)\big) = 2$ [12, Lemma 8.5.7] as we just need two parameters to define a cyclic algebra. It is shown in [9, Cor. 3.10] and [12, Th. 8.6] that $4 \le \mathrm{ed}_p\big(\mathbf{PGL}_F(p^2)\big) \le p^2+1$.

We prove the following:

Theorem 1.1. *Let p be a prime integer and F a field of characteristic different from p. Then*

$$\mathrm{ed}_p\big(\mathbf{PGL}_F(p^2)\big) = p^2+1.$$

Corollary 1.2 (Rost)**.** *If F is a field of characteristic different from 2, then* $\mathrm{ed}\big(\mathbf{PGL}_F(4)\big) = \mathrm{ed}_2\big(\mathbf{PGL}_F(4)\big) = 5$.

Proof. By Theorem 1.1, we have $\mathrm{ed}\big(\mathbf{PGL}_F(4)\big) \ge \mathrm{ed}_2\big(\mathbf{PGL}_F(4)\big) = 5$. On the other hand, $\mathrm{ed}\big(\mathbf{PGL}_F(4)\big) \le 5$ by [9]. □

We use the following notation:

F is a field, and $\Gamma = \mathrm{Gal}(F_{sep}/F)$ is the absolute Galois group of F.

$X(F)$ is the character group of Γ.

$\mathrm{Br}(F)$ is the Brauer group of F. For a field extension L/F, we write $\mathrm{Br}(L/F)$ for the relative Brauer group $\mathrm{Ker}\big(\mathrm{Br}(F)\to\mathrm{Br}(L)\big)$.

$\mathbb{G}_m$ denotes the multiplicative algebraic group $\mathrm{Spec}\,F[t,t^{-1}]$ 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 $R^{(1)}_{L/F}(\mathbb{G}_{m,L})$ for the torus of norm 1 elements in L.

If A is a central simple algebra over F, then $\mathrm{SB}(A)$ 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 ${}_{p^n}B$ 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 $X(E) = \mathrm{Mor}_F(\mathrm{Spec}(E), X)$ is the set of points of X over E. We write X_E for the scheme $X \times_F \mathrm{Spec}(E)$ over 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 Γ-lattice.

A torus P is *quasi-trivial* if P^* is a permutation lattice, i.e., if there is a Γ-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 $T = R^{(1)}_{L/F}(\mathbb{G}_{m,L})$ 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 $\sigma \in \mathrm{Gal}(L/F)$ and $u \in L^\times$.

Example 2.2. The torus $T = R^{(1)}_{L/F}(\mathbb{G}_{m,L})$ 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 $T\big(F(T)\big)/R$ is not trivial.

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

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

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

If $F' \subset F$ is a subfield and $\chi \in X(F')$, we write χ_F for the image of χ 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

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

takes $\chi \otimes a$ to the class $\chi \cup (a)$ of a cyclic algebra split by K. In fact, every element of $\mathrm{Br}(K/F)$ 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 $\theta : H^1(F, S) \xrightarrow{\sim} \mathrm{Br}(L/F)$. Let $\alpha \in H^1(F, S)$ and let S_α 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_α is an open subset of the Severi-Brauer variety $SB(A_\alpha)$ of a central simple F-algebra A_α of degree n such that $[A_\alpha] = \theta(\alpha)$ in $\mathrm{Br}(L/F)$. Moreover, S_α is trivial if and only if A_α is split.

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

2.3. **Bicyclic algebras and tori.** Let χ and η 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 $G = \mathrm{Gal}(K/F) \times \mathrm{Gal}(K'/F)$ acts naturally on L by automorphisms and G is generated by elements σ and τ 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., $I = \mathrm{Ker}(\varepsilon)$, where $\varepsilon : \Lambda \to \mathbb{Z}$ is defined by $\varepsilon(\rho) = 1$ for all $\rho \in G$. We have:

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

Consider the exact sequences of G-modules

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

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

(3) $$0 \to \Lambda/\mathbb{Z}N_G \xrightarrow{g} M \xrightarrow{h} \mathbb{Z}^2 \to 0,$$

where $N_G = \sum_{\rho\in G}\rho \in \Lambda$, $g(x+\mathbb{Z}N_G) = \big((\tau-1)x,(1-\sigma)x\big)$ and $h(x,y) = \big(\varepsilon(x)/p, \varepsilon(y)/p\big)$.

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

$$T(E) = \operatorname{Hom}_G\big(\Lambda/\mathbb{Z}N_G, (EL)^\times\big), \quad T'(E) = \operatorname{Hom}_G\big(M, (EL)^\times\big) \tag{4}$$

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:

$$\begin{array}{ccccccc}
 & & \operatorname{Hom}_G(\mathbb{Z}^2,(EL)^\times) & & & & \\
 & & \downarrow{\scriptstyle h^*} & \overset{\alpha}{\searrow} & & & \\
\operatorname{Hom}_G(\Lambda^2,(EL)^\times) & \longrightarrow & T'(E) & \longrightarrow & \operatorname{Br}(EL/E) & \longrightarrow & 0 \\
 & \underset{\beta}{\searrow} & \downarrow{\scriptstyle g^*} & & & & \\
 & & T(E) & & & & \\
 & & \downarrow & & & & \\
 & & 0 & & & &
\end{array}$$

It follows that the cokernels of α and β are naturally isomorphic. The image of $\alpha : E^{\times 2} \to \operatorname{Br}(EL/E)$ is the subgroup of *decomposable elements* $\operatorname{Br}_{dec}(EL/E)$ of $\operatorname{Br}(EL/E)$ generated by $\chi_E \cup (a)$ and $\eta_E \cup (b)$ with $a, b \in E^\times$.

The cokernel of $\beta : (EL)^{\times 2} \to T(E)$ is the group of R-equivalence classes $T(E)/R$ (see Example 2.1). We have proved:

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

$$T(E)/R \simeq \operatorname{Br}(EL/E)/\operatorname{Br}_{dec}(EL/E).$$

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 $\operatorname{Br}\big(L(T')/F(T')\big)$ modulo $\operatorname{Br}_{dec}\big(L(T')/F(T')\big)$. It follows that $p[A_{F(T')}] = p[A']$ in $\operatorname{Br} F(T')$.

The exact sequence of G-modules

$$0 \to L^\times \oplus M \to L(T')^\times \to \operatorname{Div}(T'_L) \to 0$$

induces an exact sequence

$$H^1\big(G, \operatorname{Div}(T'_L)\big) \to H^2(G, L^\times) \oplus H^2(G, M) \to H^2\big(G, L(T')^\times\big).$$

As $\operatorname{Div}(T'_L)$ is a permutation G-module, the first term in the sequence is trivial. Therefore, we get an injective homomorphism

$$\varphi : H^2(G, M) \to \operatorname{Br} F(T')/\operatorname{Br}(F).$$

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 ξ of order p^2.

Lemma 2.4. *We have* $\varphi(\xi) = -[A'] + \mathrm{Br}(F)$.

Proof. Consider the following diagram:

$$\begin{array}{ccccc}
 & & & & \mathrm{Hom}_G(\mathbb{Z},\mathbb{Z}) \\
 & & & & \downarrow \\
 & & \mathrm{Hom}_G(I,I) & \longrightarrow & \mathrm{Ext}^1_G(\mathbb{Z},I) \\
 & & \downarrow & & \downarrow \\
\mathrm{Hom}_G(M,M) & \longrightarrow & \mathrm{Ext}^1_G(I,M) & \longrightarrow & \mathrm{Ext}^2_G(\mathbb{Z},M) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_G\big(M,L(T')^\times\big) & \longrightarrow & \mathrm{Ext}^1_G\big(I,L(T')^\times\big) & \longrightarrow & \mathrm{Ext}^2_G\big(\mathbb{Z},L(T')^\times\big).
\end{array}$$

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

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

Proof. The image of $p[A]$ in $\mathrm{Br}\,F(T')$ coincides with $p[A']$. Modulo the image of the map $\mathrm{Br}(F) \to \mathrm{Br}\,F(T')$, the class $p[A']$ is equal to $-\varphi(p\xi)$ and therefore, is nonzero as φ 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 $\mathrm{Z}(X)$ for the group of algebraic cycles on X, i.e., the free abelian group generated by points of X. We write $\mathrm{CH}(X)$ for the factor group of $\mathrm{Z}(X)$ by the subgroup of cycles rationally equivalent to 0 (see [4, §1.3]). The groups $\mathrm{Z}(X)$ and $\mathrm{CH}(X)$ are graded by the dimension of points. If $x \in X$ is a point of dimension i, $[x]$ denotes the class of x in $\mathrm{CH}_i(X)$.

If X is a variety of dimension d, then the group $\mathrm{CH}_d(X)$ 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 $f_* : \mathrm{Z}(X) \to \mathrm{Z}(Y)$ is a graded homomorphism defined by

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

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 $\mathrm{CH}(X) \to \mathrm{CH}(Y)$ still denoted by f_* (see [4, §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 $a : \mathrm{Spec}(E) \to X$. The *dimension of* a is the integer $\dim(a) := \dim(x)$. If $f : X \to Y$ is a morphism of varieties over F and

$a \in X(E)$ for a field extension E/F, we have $\dim(a) \geq \dim\bigl(f(a)\bigr)$. If $d = \dim(a)$, we define the *class* $[a]$ *of* a in $\mathrm{CH}_d(X)$ 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 $\mathrm{CH}(Y)$.*

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

$$\begin{aligned} [f(a)] &= [E : F(y)] \cdot [y] \\ &= [E : F(x)]\bigl([F(x) : F(y)] \cdot [y]\bigr) \\ &= [E : F(x)] \cdot f_*([x]) \\ &= f_*([a]). \end{aligned}$$ ◻

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 $f_* : \mathrm{Z}(U) \to \mathrm{Z}(Y)$, followed by the projection $\mathrm{Z}(Y) \to \mathrm{Z}_d(Y) = \mathbb{Z}$, gives rise to a well-defined homomorphism*

$$f_\star : \mathrm{CH}(U) \to \mathbb{Z}/n\mathbb{Z}.$$

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

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

We claim that the image of the push-forward homomorphism

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

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], $\mathrm{CH}_d(U \times Y)$ is canonically isomorphic to the cokernel of i_*. By the claim, q_* gives rise to a homomorphism $\mathrm{CH}_d(U \times Y) \to \mathbb{Z}/n\mathbb{Z}$. Composing it with the push-forward homomorphism for the closed embedding $(1_U, f) : U \to U \times Y$, we get the required homomorphism $f_\star : \mathrm{CH}_d(U) \to \mathbb{Z}/n\mathbb{Z}$. The last equality in the statement follows from Proposition 3.1 applied to q. □

Example 3.4. Let T be an algebraic torus over F and $n = i(T)$ (see Example 3.2). Then the structure morphism $T \to \mathrm{Spec}(F)$ gives rise to a homomorphism $\mathrm{CH}_0(T) \to \mathbb{Z}/n\mathbb{Z}$ 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

$$\mathrm{CH}(Z) = \mathbb{Z}[\mathbf{h}] := \mathbb{Z}[h_1, h_2, \dots, h_r],$$

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 ith factor of Z. Moreover, $\mathbb{Z}[\mathbf{h}]$ is the factor ring of the polynomial ring on the variables $t_1, t_2, \dots, t_r$ by the ideal generated by $t_1^n, t_2^n, \dots, t_r^n$. Note that the homogeneous ith component $\mathbb{Z}[\mathbf{h}]_i$ is trivial if $i > r(n-1)$ and $\mathbb{Z}[\mathbf{h}]_{r(n-1)} = \mathbb{Z}h^{n-1}$, where $h := h_1 h_2 \cdots h_p$.

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

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

where $\mathbf{h} = (h_1, h_2, \dots, h_p)$.

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

$$\mathrm{CH}(X) \to \mathbb{Z}[\mathbf{h}]^H$$

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

Consider the trace homomorphism

$$\mathrm{tr} : \mathbb{Z}[\mathbf{h}] \to \mathbb{Z}[\mathbf{h}]^H$$

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

$$\big(\mathbb{Z}[\mathbf{h}]^H\big)_j = \begin{cases} I_j, & \text{if } p \text{ does not divide } j; \\ \mathbb{Z}h^i + I_j, & \text{if } j = pi. \end{cases} \tag{5}$$

It follows that $\mathbb{Z}[\mathbf{h}]^H$ is generated by I and h^i, $i = 0, 1, \dots, n-1$ as an abelian group. Moreover, $ph^j \in I$ 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 $Y = R_{K/F}\big(\mathrm{SB}(A)\big)$, where $\mathrm{SB}(A)$ 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

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

The image of an element $\alpha \in \mathrm{CH}(Y)$ in $\mathbb{Z}[\mathbf{h}]^H$ 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 $Y = R_{K/F}\big(\mathrm{SB}(A)\big)$. Then the image of the map $\mathrm{CH}(Y) \to \mathbb{Z}[\mathbf{h}]^H$ 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 $\alpha \in \mathrm{CH}(Y)$. We shall prove in the cases 1 and 2 below that $\bar{\alpha} \in \mathbb{Z} + I$. By (5), we may assume that $\alpha \in \mathrm{CH}^{pi}(Y)$ for $i = 1, 2, \dots, n-1$. Let $a \in \mathbb{Z}$ be such that $\bar{\alpha} \equiv ah^i$ 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 $b \in p\mathbb{Z}$. Therefore, $a \in p\mathbb{Z}$.

Case 2. i divides $n-1$. Write $n-1 = ij$. We have $\alpha^j \in \mathrm{CH}^{p(n-1)}(Y)$ 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 $\alpha \in \mathrm{CH}^{pi}(Y)$ with $i = 1, 2, \dots, p-1$. We shall prove that $\bar{\alpha} \in I$. Write $ik + pm = 1$ for some integers k and $m > 0$. The Severi-Brauer variety $\mathrm{SB}(M_m(A))$ 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 $\mathrm{SB}(M_m(A)) \to \mathrm{SB}(A)$ that is defined on the complement U of the variety $\mathrm{SB}(M_{m-1}(A))$ embedded into $\mathrm{SB}(M_m(A))$ as a closed subvariety via the inclusion $A^{m-1} \to A^m$, $(a_1, \dots, a_{m-1}) \mapsto (a_1, \dots, a_{m-1}, 0)$. Moreover, the projection $U \to \mathrm{SB}(A)$ is a vector bundle.

Let $Y' = R_{K/F}\big(\mathrm{SB}(M_m(A))\big)$ 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

$$\mathrm{CH}(Y') \to \mathrm{CH}(U') \simeq \mathrm{CH}(Y).$$

Moreover, the diagram

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

where the bottom map takes a monomial $\mathbf{h}'^{\alpha}$ to $\mathbf{h}^{\alpha}$ if $\alpha_i < p$ for all i and to 0 otherwise, is commutative. Lift α to an element $\alpha' \in \mathrm{CH}^{pi}(Y')$. 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

$$S = \big(R^{(1)}_{K'/F}(\mathbb{G}_{m,K'})\big)^r \simeq \big(R_{K'/F}(\mathbb{G}_{m,K'})/\,\mathbb{G}_m\big)^r$$

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

$$(\mathbb{Z}/p\mathbb{Z})[\mathbf{h}] = \mathrm{Ch}(Z) \to \mathrm{Ch}(S),$$

where $\mathbf{h} = (h_1, h_2, \dots, h_r)$, $h_i^p = 0$ for all i, and we write Ch for the Chow groups modulo p. We shall also write $\tilde{h}_i$ for the image of h_i in $\mathrm{Ch}^1(S)$. The class in $\mathrm{Ch}^{r(p-1)}(S)$ of a rational point of S is equal to $\tilde{h}^{p-1}$, where $\tilde{h} = \tilde{h}_1\tilde{h}_2\cdots\tilde{h}_r \in \mathrm{Ch}^p(S)$. As $i(S) = p$, we have $\tilde{h}^{p-1} \neq 0$ by Example 3.4.

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

Proof. Suppose that $f(\tilde{h}_1, \tilde{h}_2, \dots, \tilde{h}_r) = 0$ for a nonzero homogeneous polynomial f over $\mathbb{Z}/p\mathbb{Z}$. Suppose that a monomial $h_1^{\alpha_1}\cdots h_r^{\alpha_r}$ enters f with a nonzero coefficient. Multiplying the equality by $\tilde{h}_1^{\beta_1}\cdots\tilde{h}_r^{\beta_r}$ with $\beta_i = p-1-\alpha_i$, we get $\tilde{h}^{p-1} = 0$, a contradiction. □

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

Consider the homomorphism $f : S \times S \to S$ defined by $f(x, y) = xy^{-1}$. Recall that as $i(S) = p$, by Example 3.2 and Proposition 3.3, we have the homomorphism

$$f_\star : \mathrm{CH}_{r(p-1)}(S \times S) \to \mathbb{Z}/p\mathbb{Z}. \tag{6}$$

Lemma 3.7. *For any $\alpha \in \mathrm{Ch}^i(S)$ and $\beta \in \mathrm{Ch}^j(S)$ with $i + j = r(p-1)$, we have*

$$\bar{\alpha}\cdot\bar{\beta} = f_\star(\alpha\times\beta)h^{p-1}$$

in $(\mathbb{Z}/p\mathbb{Z})[\mathbf{h}]$.

Proof. It suffices to consider the case when α and β are monomials in $\tilde{h}_i$. 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 $\alpha = \tilde{h}^i$, $\beta = \tilde{h}^j$. The cycles α and β 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

$$f' : \big(\mathbb{P}(U)\cap S\big)\times\big(\mathbb{P}(W)\cap S\big) \to S$$

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 $f_\star(\alpha\times\beta) = 1 + p\mathbb{Z}$. On the other hand, $\bar{\alpha}\cdot\bar{\beta} = h^i\cdot h^j = h^{p-1}$. □

Let L/F be a bicyclic field extension of degree p^2 and $T = R^{(1)}_{L/F}(\mathbb{G}_{m,L})$. 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 $R^{(1)}_{K/F}(\mathbb{G}_{m,K})$. Write S_t for the fiber of the norm homomorphism $T \to R^{(1)}_{K/F}(\mathbb{G}_m)$ over t. The variety S_t is a principal homogeneous space of the torus $S = R_{K/F}\big(R^{(1)}_{L/K}(\mathbb{G}_{m,L})\big) \simeq R_{K/F}\big(R_{L/K}(\mathbb{G}_{m,L})/\,\mathbb{G}_{m,K}\big)$.

The variety S_t is canonically isomorphic to an open subscheme of the variety $Y := R_{K/F}\big(\mathrm{SB}(A_t)\big)$ for a central simple K-algebra A_t of degree p (see Section 2.2). Over the function field E of $\mathrm{SB}(A_t)$ over K, the varieties S_t and S become isomorphic to the torus $\big(R^{(1)}_{LE/E}(\mathbb{G}_{m,LE})\big)^p$, 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 $\bar{\alpha} \in (\mathbb{Z}/p\mathbb{Z})[\mathbf{h}]$ is well defined for any cycle α on S_t and S.

Consider the morphism

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

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

$$f_\star : \mathrm{CH}_{p(p-1)}(S_t \times S) \to \mathrm{CH}_{p(p-1)}\big((S_t)_E \times S_E\big) \to \mathbb{Z}/p\mathbb{Z}.$$

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

Proof. As S_t is not trivial, the algebra A_t is not split. We can lift α to a cycle β in $\mathrm{Ch}(Y)$. By Proposition 3.5, $\bar{\beta}$ belongs to the image $\tilde{I}$ of the ideal I in $(\mathbb{Z}/p\mathbb{Z})[\mathbf{h}]^H$. It follows that $\bar{\alpha} \cdot h^j = \bar{\beta} \cdot h^j \in \tilde{I}_{p(p-1)} = 0$. Lemma 3.7 (applied to the field extension E of F and $r = p$) shows that $f_\star(\alpha \times \tilde{h}^j) = 0$. □

3.4. **A key proposition.** Let p be a prime integer, L/F a bicyclic field extension of degree p^2, $G = \mathrm{Gal}(L/F)$, σ and τ generators of G. Consider the tori $T = R^{(1)}_{L/F}(\mathbb{G}_{m,L})$ 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 $g(t, v) = t\sigma(v)/v$. By Proposition 3.3 and Example 3.2, f and g give rise to well-defined homomorphisms $f_\star$ and $g_\star$ from $\mathrm{CH}_d(T \times P)$ to $\mathbb{Z}/p\mathbb{Z}$.

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

Proof. The torus P is an open subscheme in the projective space $\mathbb{P}_F(L)$; hence the ring $\mathrm{CH}(P)$ 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], $\mathrm{CH}_d(T \times P)$ coincides with the sum of subgroups $\mathrm{CH}_i(T) \times e^i$ over all $i = 0, 1, \dots, d$.

Let $\beta \in \mathrm{CH}_i(T)$. It suffices to show that $f_\star(\beta \times e^i) = g_\star(\beta \times e^i)$ for any $i = 0, 1, \dots, d$. If $i = d$, the class e^i 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, $f_\star(\beta \times e^i) = 0$ and we need to show that $g_\star(\beta \times e^i) = 0$.

Let K be the subfield of σ-invariant elements in L of degree p over F. We have $pk + 1 \le p^2 - i \le p(k+1)$ for some integer $k = 0, \dots, p-1$. 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 $\mathrm{CH}^i(P)$ is equal to e^i.

The torus $S := R_{K/F}\big(R^{(1)}_{L/K}(\mathbb{G}_{m,L})\big)$ is the kernel of the norm homomorphism $T \to T_1 := R^{(1)}_{K/F}(\mathbb{G}_{m,K})$, so we have an exact sequence

$$(7) \qquad 1 \to S \to T \to T_1 \to 1.$$

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

$$T \times P \xrightarrow{1_T \times l} T \times S \xrightarrow{r} T,$$

where $l : P \to S$ 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 $S \cap R_{K/F}\big(\mathbb{P}_K(K \oplus W)\big)$ of dimension pk in $S \simeq R_{K/F}\big(R_{L/K}(\mathbb{G}_{m,L})/\,\mathbb{G}_{m,K}\big)$. Therefore, if $p^2 - i > pk+1$, then $\dim\big(P \cap \mathbb{P}(V)\big) > pk$, 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, $g_\star(\beta \times e^i) = 0$.

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

Let S_t be the fiber of the norm homomorphism $T \to T_1$ 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

$$r' : S_t \times S \to S_t$$

the morphism given by $r'(x,s) = xs^{-1}$. Thus we have a commutative diagram

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

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

$$\mathrm{CH}_d(T \times S) \xrightarrow{q^*} \mathrm{CH}_{p(p-1)}(S_t \times S) \xrightarrow{r'_\star} \mathbb{Z}/p\mathbb{Z}.$$

Thus, it suffices to show that $r'_\star(\alpha \times h^{p-k-1}) = 0$ for any $\alpha \in \mathrm{CH}^{pk}(S_t)$. 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 (7) 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 $T = R^{(1)}_{L/F}(\mathbb{G}_{m,L})$. Let M/F be a field extension and let t and t' be R-equivalent points in $T(M)$. Then* $\deg(t) \equiv \deg(t')$ *modulo 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 3.9, we have in $\mathbb{Z}/p\mathbb{Z}$:

$$\deg(t) = \deg f(w) = f_\star([w]) = g_\star([w]) = \deg g(w) = \deg(t'). \qquad \square$$

4. Essential p-dimension of $\mathbf{PGL}(p^2)$

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

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 [5, §7.9]:

$$0 \to H^i(N,C) \xrightarrow{i} H^i(\widehat{E},C) \xrightarrow{\partial} H^{i-1}\big(N, C(-1)\big) \to 0. \tag{8}$$

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

$$0 \to {}_{p^n}\mathsf{X}(N) \xrightarrow{i} {}_{p^n}\mathsf{X}(\widehat{E}) \xrightarrow{\partial} \mathrm{Hom}_\Gamma(\mu_{p^n}, \mathbb{Z}/p^n\mathbb{Z}) \to 0, \tag{9}$$

where μ_{p^n} is the Γ-module of p^nth roots of unity.

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

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

$$0 \to \mathrm{Br}(N)\{p\} \xrightarrow{i} \mathrm{Br}(\widehat{E})\{p\} \xrightarrow{\partial} \mathsf{X}(N)\{p\} \to 0. \tag{10}$$

The first map preserves indices of algebras. For a central simple algebra C over N with $C \in \mathrm{Br}(N)\{p\}$ 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 $[C] = \chi \cup (\bar{u})$ for some $\chi \in \mathsf{X}(N)\{p\}$ and a unit $u \in \widehat{E}$, then $[\widehat{C}] = \widehat{\chi} \cup (u)$.

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

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

in $\mathrm{Br}(\widehat{E})$ for a unique $[C] \in \mathrm{Br}(N)\{p\}$ and $\chi = \partial\big([A]\big)$. Moreover (see [6, Th. 5.15(a)] or [14, Prop. 2.4]),

$$\mathrm{ind}(A) = \mathrm{ord}(\chi) \cdot \mathrm{ind}(C_{N(\chi)}). \tag{11}$$

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

$$\partial_{v'}\big([A_{E'}]\big) = e \cdot \partial_v([A])_{N'}, \tag{12}$$

where e is the ramification index of E'/E [5, 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 *Fields*$/F$ of field extensions of F to the category *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, $\mathrm{ed}_p(\mathcal{F}_1) = \mathrm{ed}_p\big(\mathbf{PGL}_F(p^2)\big)$.

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 $\mathrm{ind}(B_K) \leq p$; 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 $[B_1]-[B_2] \in \mathrm{Br}(K_1/E) =$

$\mathrm{Br}(K_2/E)$. 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 $\mathrm{ind}(B_K)\le p$, there is a central simple algebra C over the function field $E(y)$ (y is a variable) of degree p^2 such that

$$[C]=[B_{E(y)}]+\big(\chi_{E(y)}\cup(y)\big) \tag{13}$$

in $\mathrm{Br}\big(E(y)\big)$.

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

For any finite field extension N/E of degree prime to p, the class of the algebra B_N in $\mathrm{Br}(N)$ 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 χ_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 χ satisfy the condition $(*)$. Then*

$$\mathrm{ed}_p^{\mathcal{F}_1}([C])\ge\mathrm{ed}_p^{\mathcal{F}_2}([B,K])+1$$

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

$$[(C_0)_M]=[C_M] \tag{14}$$

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

We have $[C]\in\mathcal{F}_1\big(E(y)\big)$ and $\partial\big([C]\big)=\chi$, where ∂ is taken with respect to the discrete valuation v on $E(y)$ associated to y (see Section 4.1). We extend v to a discrete valuation v' on M with ramification index e' and inertia degree both prime to p (see [7, 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 $\partial([C_M])=e'\cdot\chi_N\neq0$. Hence the algebra C_M is ramified; i.e., the class of C_M does not belong to the image of the map $\mathrm{Br}(O)\to\mathrm{Br}(M)$, 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 $\chi_0=\partial\big([C_0]\big)\in X(N_0)\{p\}$ and $K_0=N_0(\chi_0)$. Choose a prime element π_0 in M_0 and write

$$[(C_0)_{\widehat{M_0}}]=[\widehat{B}_0]+\big(\widehat{\chi}_0\cup(\pi_0)\big) \tag{15}$$

in $\mathrm{Br}(\widehat{M_0})$, where B_0 is a central simple algebra over N_0 (see Section 4.1). By (11),

$$\mathrm{ind}(C_0)=\mathrm{ord}(\chi_0)\cdot\mathrm{ind}(B_0)_{K_0}. \tag{16}$$

Let e be the ramification index of M/M_0 and let π 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

$$e'\cdot\chi_N=\partial\big([C_M]\big)=\partial\big([(C_0)_M]\big)=e\cdot\partial\big([C_0]\big)_N=e\cdot(\chi_0)_N. \tag{17}$$

Recall that e' is relatively prime to p. It follows that χ_N is a multiple of $(\chi_0)_N$. In particular, $\mathrm{ord}(\chi_0)_N$ is divisible by p.

It follows from (14), (15) and (17) that

$$[\widehat{(B_0)}_N] + \big(\widehat{(\chi_0)}_N \cup (u)\big) = [\widehat{B}_N] + \big(\widehat{\chi}_N \cup (v)\big) \tag{18}$$

in $\mathrm{Br}(\widehat{M})$; hence

$$[(B_0)_N] + \big((\chi_0)_N \cup (\bar{u})\big) = [B_N] + \big(\chi_N \cup (\bar{v})\big) \tag{19}$$

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

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

Case 1. $\mathrm{ord}(\chi_0)_N = p^2$. By (16), $\mathrm{ind}(B_0)_{K_0} = 1$, i.e., B_0 is split over K_0; hence $[B_0] = \chi_0 \cup (s_0)$ for some $s_0 \in N_0^\times$. It follows from (19) that $[B_N] = (\chi_0)_N \cup (s)$ for some $s \in N^\times$. Since $\mathrm{ord}(\chi_0)_N = p^2$, the character $p \cdot (\chi_0)_N$ is a multiple of χ_N by (17). Hence (B, K) and χ do not satisfy the condition $(*)$, a contradiction.

Case 2. $\mathrm{ord}(\chi_0)_N = p$. 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 η_0 is of order p in $X(N_0)$. The characters χ_N and $(\chi_0)_N$ generate the same subgroup in $X(N)$. It follows that

$$K_0 \otimes_{N_0} N \simeq N\big((\chi_0)_N\big) = N(\chi_N) \simeq K \otimes_E N. \tag{20}$$

By (16), we have $\mathrm{ind}(B_0)_{K_0} \le p$. 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

$$[B_N] - [(B_0)_N] \in \mathrm{Br}(K \otimes_E N/N).$$

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,

$$\mathrm{ed}_p^{\mathcal{F}_1}\big([C]\big) = \mathrm{tr.deg}_F(M_0) \ge \mathrm{tr.deg}_F(N_0) + 1 \ge \mathrm{ed}_p^{\mathcal{F}_2}\big([B, K]\big) + 1. \qquad \square$$

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 χ_N. Then $[C_{N(y)}] = \rho_{N(y)} \cup (sy^{pi})$ for some i; i.e., the algebra $C_{N(y)}$ is also cyclic. With an appropriate choice of ρ 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, $[A] \in \mathrm{Br}(L/E)$. 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 $[A_1] - [A_2] \in \mathrm{Br}_{dec}(L_1/E) = \mathrm{Br}_{dec}(L_2/E)$ (see Section 2.3). 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 $\mathrm{Br}(L/E)/\mathrm{Br}_{dec}(L/E)$ as a subset of $\mathcal{F}_3(E)$ identifying the class of an algebra A with $[A, L]$.

Let χ and η in $X(F)$ be linearly independent characters of order p and let E/F be a field extension such that χ_E and η_E are linearly independent in $X(E)$. Let $(A, L) \in S_3(E)$ and set $K = E(\chi)$ and $L = E(\chi, \eta) := K(\eta)$. As A is split by L, there is a central simple algebra B over the function field $E(x)$ (x is a variable) of degree p^2 such that

$$[B] = [A_{E(x)}] + \big(\eta_{E(x)} \cup (x)\big) \tag{21}$$

in $\mathrm{Br}\big(E(x)\big)$. We have $\big(B, K(x)\big) \in \mathcal{S}_2\big(E(x)\big)$.

Proposition 4.3. *Let $\chi, \eta \in X(F)$ be characters of order p, E/F a field extension such that χ_E and η_E are linearly independent in $X(E)$, $K = E(\chi)$, $L = E(\chi, \eta)$, A a central simple algebra of degree p^2 over E such that $(A, L) \in \mathcal{S}_3(E)$. Then*

$$\mathrm{ed}_p^{\mathcal{F}_2}\big([B, K(x)]\big) \geq \mathrm{ed}_p^{\mathcal{F}_3}\big([A, L]\big) + 1$$

for the algebra B defined by (21).

Proof. Let $M/E(x)$ be a finite field extension of degree prime to p, $M_0 \subset M$ a subfield over F and $[B_0, R_0] \in \mathcal{F}_2(M_0)$ such that $\mathrm{ed}_p^{\mathcal{F}_2}\big([B, K(x)]\big) = \mathrm{tr.deg}_F(M_0)$ and

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

in $\mathcal{F}_2(M)$. The last equality means that $R := K(x) \otimes_{E(x)} M \simeq R_0 \otimes_{M_0} M$ and

$$[B_M] = [(B_0)_M] + \big(\chi_M \cup (f)\big) \tag{22}$$

in $\mathrm{Br}(M)$ for some $f \in M^\times$. Hence there is a character $\rho \in X(M_0)$ 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 $[B_0, R_0]$ by $[B_0, R_0]_{M_1}$, we may assume that $\rho = \chi_{M_0}$, i.e., $R_0 = M_0(\chi)$.

We have $\partial\big([B]\big) = \eta$, where ∂ 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 [7, 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

$$e' \cdot \eta_N = \partial([B_M]) = \partial([(B_0)_M]) + k \cdot \chi_N, \tag{23}$$

where $k = v'(f)$. Note that the characters χ_N and η_N are linearly independent in $X(N)$ 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 $\eta_0 = \partial([B_0]) \in X(N_0)\{p\}$. Choose a prime element π_0 in M_0 and write

$$[(B_0)_{\widehat{M}_0}] = [\widehat{A}_0] + \big(\widehat{\eta}_0 \cup (\pi_0)\big) \tag{24}$$

in $\mathrm{Br}(\widehat{M_0})$, where A_0 is a central simple algebra over N_0. By (11),

$$\mathrm{ind}(B_0) = \mathrm{ord}(\eta_0) \cdot \mathrm{ind}(A_0)_{N_0(\eta_0)}. \tag{25}$$

Let e be the ramification index of M/M_0 and let π be a prime element in M. Write $\pi_0 = u\pi^e$, $x = v\pi^{e'}$ and $f = w\pi^k$ with u, v and w units in M. It follows from (23) that

$$e' \cdot \eta_N = e \cdot (\eta_0)_N + k \cdot \chi_N. \tag{26}$$

As e' is relatively prime to p, η_N belongs to the subgroup of $X(N)$ generated by $(\eta_0)_N$ and χ_N, and $(\eta_0)_N \neq 0$ since χ_N and η_N are linearly independent. In particular, p divides $\operatorname{ord}(\eta_0)_N$.

It follows from (22), (24) and (26) that

$$[\widehat{(A_0)}_N] + \big(\widehat{(\eta_0)}_N \cup (u)\big) + \big(\widehat{\chi}_M \cup (w)\big) = [\widehat{A}_N] + \big(\widehat{\eta}_N \cup (v)\big) \tag{27}$$

in $\operatorname{Br}(\widehat{M})$; hence

$$[(A_0)_N] + \big((\eta_0)_N \cup (\bar{u})\big) + \big(\chi_N \cup (\bar{w})\big) = [A_N] + \big(\eta_N \cup (\bar{v})\big) \tag{28}$$

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

Since $\operatorname{ind}(B_0) \leq p^2$, it follows from (25) that $\operatorname{ord}(\eta_0) \leq p^2$.

Case 1. $\operatorname{ord}(\eta_0)_N = \operatorname{ord}(\eta_0) = p^2$. It follows from (26) 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 $s_0 \in M_0^\times$. It follows from (24) that $[B_0]_{\widehat{M}_0} = \widehat{\eta}_0 \cup (s_0\pi_0)$ in $\operatorname{Br}(\widehat{M}_0)$; hence $[B_0]_{\widehat{M}_0(\chi)} = \widehat{(\eta_0)}_{N_0(\chi)} \cup (s_0\pi_0)$ in $\operatorname{Br}\big(\widehat{M}_0(\chi)\big)$. As

$$\operatorname{ind}(B_0)_{\widehat{M}_0(\chi)} \leq \operatorname{ind}(B_0)_{M_0(\chi)} = \operatorname{ind}(B_0)_{R_0} \leq p,$$

the order of $(\eta_0)_{N_0(\chi)}$ is at most p, i.e., $p\eta_0$ is a multiple of χ_{N_0}. As e is divisible by p, it follows from (26) that η_N is a multiple of χ_N, a contradiction.

Case 2. $\operatorname{ord}(\eta_0)_N = p$. It follows from (26) that $(e,p) = 1$ and $(\eta_0)_N$ belongs to the subgroup generated by χ_N and η_N. Moreover,

$$\langle \chi_N, (\eta_0)_N \rangle = \langle \chi_N, \eta_N \rangle$$

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

$$[(B_0)_{\widehat{R}_0}] = [\widehat{(A_0)}_{K_0}] + \big(\widehat{(\eta_0)}_{K_0} \cup (\pi_0)\big).$$

As $(B_0, R_0) \in \mathcal{S}_2(M_0)$, we have $\operatorname{ind}(B_0)_{R_0} \leq p$. Since η_0 is not a multiple of χ_{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 η_0 is of order p in $X(N_0)$.

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

$$L_0 \otimes_{N_0} N = N\big(\chi, \eta_0\big) = N(\chi, \eta) = L \otimes_E N \tag{29}$$

is a bicyclic field extension of degree p^2 and hence so is the extension L_0/N_0. In particular, χ_{N_0} and η_0 generate a subgroup of order p^2 in $X(N_0)$.

As A_0 is split by L_0, we may assume that $\deg(A_0) = p^2$ and hence $(A_0, L_0) \in \mathcal{S}_3(N_0)$.

It follows from (28) that $[A_N] - [(A_0)_N] \in \operatorname{Br}_{dec}(L \otimes_E N/N)$. By (29), the pairs $(A_N, L \otimes_E N)$ and $\big((A_0)_N, L_0 \otimes_{N_0} N\big) = (A_0, L_0)_N$ are equivalent in $\mathcal{S}_3(N)$. Then the class $[A, L]$ in $\mathcal{F}_3(E)$ is p-defined over N_0; therefore,

$$\operatorname{ed}_p^{\mathcal{F}_2}([B, K(x)]) = \operatorname{tr.deg}_F(M_0) \geq \operatorname{tr.deg}_F(N_0) + 1 \geq \operatorname{ed}_p^{\mathcal{F}_3}([A, L]) + 1. \qquad \square$$

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 $t \in T\big(F(T)\big)$ be the generic point and let $[A, L(T)]$ be the corresponding element in $\mathcal{F}_3\big(F(T)\big)$ via the isomorphism between $T\big(F(T)\big)/R$ and $\operatorname{Br}(L(T)/F(T))/\operatorname{Br}_{dec}(L(T)/F(T))$ in Proposition 2.3.

Proposition 4.4. $\operatorname{ed}_p^{\mathcal{F}_3}\big([A, L(T)]\big) \geq p^2 - 1$.

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 $\deg(t) = 1$; therefore, $\deg(t_M)$ is not divisible by p as $[M : F(T)]$ is prime to p. By Theorem 3.10, $\deg((t_0)_M) \equiv \deg(t_M)$ modulo p; hence $\deg((t_0)_M) \neq 0$. 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 $\rho(t_0)_M$ generate a subfield in LM over L of the transcendence degree $\dim(T) = p^2 - 1$. 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 $T = R^{(1)}_{L/F}(\mathbb{G}_{m,L})$. 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*

$$\operatorname{ed}_p\big(\mathbf{PGL}_F(p^2)\big) = p^2 + 1.$$

Proof. Recall that $\operatorname{ed}_p\big(\mathbf{PGL}_F(p^2)\big) = \operatorname{ed}_p(\mathcal{F}_1)$. 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 $\big(B, KE(x)\big) \in \mathcal{S}_2(E(x))$

with

$$[B] = [A_{E(x)}] + \big(\eta_{E(x)} \cup (x)\big) \tag{30}$$

in $\mathrm{Br}(E(x))$ and the algebra C of degree p^2 over $E(x, y)$ with

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

in $\mathrm{Br}\big(E(x, y)\big)$.

We claim that the pair $\big(B, KE(x)\big)$ in $\mathcal{S}_2\big(E(x)\big)$ and the character $\chi_{E(x)}$ satisfy the condition $(*)$. Let $N/E(x)$ be a finite field extension of degree prime to p with $[B_N] = \rho \cup (s)$ in $\mathrm{Br}(N)$ 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 χ_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 χ_N and the extension $\widehat{N}(\chi)/\widehat{N}$ is unramified, the ramification index e of $\widehat{N}(\rho)/\widehat{N}$ is either 1 or p.

Case 1. $e = 1$. We have $\rho_{\widehat{N}} = \widehat{\mu}$ for a character $\mu \in X(P)$ of order p^2. By (30), we have

$$e'\eta_P = \partial([B_{\widehat{N}}]) = v(s)\mu_P.$$

As ρ_P is of order p^2, the character $p \cdot \mu_P$ is a multiple of χ_N. On the other hand, $p \cdot \mu$ is a multiple of χ_P by assumption; i.e., χ_P and η_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 $P^\times/P^{\times p}$. Let π be a prime element in N and ν the corresponding character of order p in $X(N)$. We can write $\rho = \widehat{\mu} + l\nu$ for some character $\mu \in X(P)$ of order p^2 and an integer l prime to p. Noting that $\chi_N = p \cdot \rho = p \cdot \widehat{\mu}$, we have $p \cdot \mu = \chi_P$.

Write $s = u\pi^j$ for a unit u in N. Then

$$[B_N] = \rho \cup (s) = (\widehat{\mu} + l\nu) \cup (u\pi^j) = \widehat{\mu} \cup (u) + (j\widehat{\mu}) \cup (\pi) + \nu \cup (w), \tag{31}$$

where $w = (-1)^{lj}u^l$. Let ϵ be the character in $X(P)$ of exponent p corresponding to $\bar{w}$. As $\nu \cup (w) + \widehat{\epsilon} \cup (\pi) = 0$, it follows from (30) that

$$e'\eta_P = \partial([B_{\widehat{N}}]) = j\mu - \epsilon.$$

Since μ 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 χ and η are defined over F. It follows that the classes of $\bar{w}$ and $\bar{u}$ belong to the image of $F^\times/F^{\times p}$ in $P^\times/P^{\times p}$. By (30) and (31),

$$p[A_P] = p(\mu \cup (\bar{u})) = \chi_P \cup (\bar{u}) \in \mathrm{Im}\big(\mathrm{Br}(F) \to \mathrm{Br}(N)\big).$$

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 $\mathrm{Br}(F) \to \mathrm{Br}(E)$. This contradicts Corollary 2.5. Thus, we have checked the condition $(*)$.

By Propositions 4.1, 4.3 and 4.4,

$$\begin{aligned}\mathrm{ed}_p\big(\mathbf{PGL}_F(p^2)\big) = \mathrm{ed}_p(\mathcal{F}_1) &\geq \mathrm{ed}_p^{\mathcal{F}_1}([C]) \geq \mathrm{ed}_p^{\mathcal{F}_2}([B, KE(x)]) + 1 \\ &\geq \mathrm{ed}_p^{\mathcal{F}_3}\big([A, LE]\big) + 2 \geq (p^2 - 1) + 2 = p^2 + 1.\end{aligned}$$

We shall show that $\mathrm{ed}_p(\mathcal{F}) \leq p^2 + 1$. 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 [13, 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 $\operatorname{ed}_p(\mathcal{F}_1) \leq \operatorname{ed}_p(\mathcal{F}_1')$ [11, Prop. 1.3]. So it suffices to show that $\operatorname{ed}(\mathcal{F}_1') \leq p^2 + 1$.

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

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

Choose a G-homomorphism $\varphi : M \to L^\times$ corresponding to $[A]$ in $\operatorname{Br}(L/E)$. Since $\operatorname{rank}(M) = p^2 + 1$, the image of φ is contained in $L_0^\times$, where L_0 is a G-invariant subfield of L with $\operatorname{tr.deg}_F(L_0) \leq p^2 + 1$. Note that G acts faithfully on M. Modifying φ by an element in the image of the map $\operatorname{Hom}_G(\Lambda^2, L^\times) \to \operatorname{Hom}_G(M, L^\times)$, we may assume that G acts faithfully on the image of φ and hence on L_0. Thus L_0 is a Galois extension of $E_0 := (L_0)^G$ with Galois group G, and φ defines a central simple E_0-algebra A_0 with $[A_0] \in \operatorname{Br}(L_0/E_0)$ such that $A_0 \otimes_{F_0} E \simeq A$. Thus, A is defined over E_0; hence

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

References

[1] G. Berhuy and G. Favi, *Essential dimension: A functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330 (electronic). MR2029168 (2004m:11056)

[2] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1999, with an appendix by David A. Buchsbaum, reprint of the 1956 original. MR1731415 (2000h:18022)

[3] J.-L. Colliot-Thélène and J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. (4) **10** (1977), no. 2, 175–229. MR0450280 (56:8576)

[4] W. Fulton, *Intersection theory*, Springer-Verlag, Berlin, 1984. MR732620 (85k:14004)

[5] R. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in Galois cohomology*, American Mathematical Society, Providence, RI, 2003. MR1999383 (2004f:11034)

[6] B. Jacob and A. Wadsworth, *Division algebras over Henselian fields*, J. Algebra **128** (1990), no. 1, 126–179. MR1031915 (91d:12006)

[7] N. Karpenko and A. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508. MR2393078 (2009b:12009)

[8] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society, Providence, RI, 1998, with a preface in French by J. Tits. MR1632779 (2000a:16031)

[9] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670. MR2009442 (2004j:16022)

[10] A. Merkurjev, *R-equivalence on three-dimensional tori and zero-cycles*, Algebra Number Theory **2** (2008), no. 1, 69–89. MR2377363 (2009j:19006)

[11] A. Merkurjev, Essential dimension, *Proceedings of the International Conference on the Algebraic and Arithmetic Theory of Quadratic Forms*, Frutillar, Chile, December 13-19, 2007, Contemp. Math., 493, *Amer. Math. Soc., Providence, R.I.*, 2009, 299-326. MR2537108

[12] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056, with an appendix by János Kollár and Endre Szabó. MR1782331 (2001k:14088)

[13] L. Rowen and D. Saltman, *Prime-to-p extensions of division algebras*, Israel J. Math. **78** (1992), no. 2-3, 197–207. MR1194966 (93k:12006)

[14] J.-P. Tignol, *Sur les classes de similitude de corps à involution de degré* 8, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 20, A875–A876. MR0498496 (58:16605)

[15] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs, vol. 179, American Mathematical Society, Providence, RI, 1998, Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ]. MR1634406 (99g:20090)

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

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