Algebra & Number Theory

Volume 13
2019
No. 2

Essential dimension of inseparable field extensions

Zinovy Reichstein and Abhishek Kumar Shukla

ALGEBRA AND NUMBER THEORY 13:2 (2019)
dx.doi.org/10.2140/ant.2019.13.513

Essential dimension of inseparable field extensions

Zinovy Reichstein and Abhishek Kumar Shukla

Let k be a base field, K be a field containing k, and L/K be a field extension of degree n. The essential dimension $\mathrm{ed}(L/K)$ over k is a numerical invariant measuring "the complexity" of L/K. Of particular interest is

$$\tau(n) = \max\big\{\mathrm{ed}(L/K) \mid L/K \text{ is a separable extension of degree } n\big\},$$

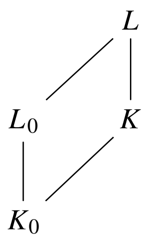
also known as the essential dimension of the symmetric group S_n. The exact value of $\tau(n)$ is known only for $n \leqslant 7$. In this paper we assume that k is a field of characteristic $p > 0$ and study the essential dimension of inseparable extensions L/K. Here the degree $n = [L : K]$ is replaced by a pair $(n, \boldsymbol{e})$ which accounts for the size of the separable and the purely inseparable parts of L/K, respectively, and $\tau(n)$ is replaced by

$$\tau(n, \boldsymbol{e}) = \max\big\{\mathrm{ed}(L/K) \mid L/K \text{ is a field extension of type } (n, \boldsymbol{e})\big\}.$$

The symmetric group S_n is replaced by a certain group scheme $G_{n,\boldsymbol{e}}$ over k. This group scheme is neither finite nor smooth; nevertheless, computing its essential dimension turns out to be easier than computing the essential dimension of S_n. Our main result is a simple formula for $\tau(n, \boldsymbol{e})$.

1. Introduction

Throughout this paper k will denote a base field. All other fields will be assumed to contain k. A field extension L/K of finite degree is said to descend to a subfield $K_0 \subset K$ if there exists an intermediate field $K_0 \subset L_0 \subset L$ such that L_0 and K generate L and $[L_0 : K_0] = [L : K]$. Equivalently, L is isomorphic to $L_0 \otimes_{K_0} K$ over K, as is shown in the diagram



The essential dimension of L/K (over k) is defined as

$$\mathrm{ed}(L/K) = \min\big\{\mathrm{trdeg}(K_0/k) \mid L/K \text{ descends to } K_0 \text{ and } k \subset K_0\big\}.$$

Reichstein was partially supported by National Sciences and Engineering Research Council of Canada Discovery grant 253424-2017. Shukla was partially supported by a graduate fellowship from the Science and Engineering Research Board of India.
MSC2010: 12F05, 12F15, 12F20, 20G10.
Keywords: inseparable field extension, essential dimension, group scheme in prime characteristic.

Essential dimension of separable field extensions was studied in [Buhler and Reichstein 1997]. Of particular interest is

$$\tau(n) = \max\left\{\mathrm{ed}(L/K) \mid L/K \text{ is a separable extension of degree } n \text{ and } k \subset K\right\}, \tag{1-1}$$

otherwise known as the essential dimension of the symmetric group S_n. It is shown in [Buhler and Reichstein 1997] that if $\mathrm{char}(k) = 0$, then $\lfloor n/2 \rfloor \leqslant \tau(n) \leqslant n-3$ for every $n \geqslant 5$.[1] A. Duncan [2010] later strengthened the lower bound as follows.

Theorem 1.1. *If* $\mathrm{char}(k) = 0$, *then* $\lfloor (n+1)/2 \rfloor \leqslant \tau(n) \leqslant n-3$ *for every* $n \geqslant 6$.

This paper is a sequel to [Buhler and Reichstein 1997]. Here we will assume that $\mathrm{char}(k) = p > 0$ and study inseparable field extensions L/K. The role of the degree, $n = [L : K]$ in the separable case, will be played by a pair $(n, \boldsymbol{e})$. The first component of this pair is the separable degree, $n = [S : K]$, where S is the separable closure of K in L. The second component is the so-called type $\boldsymbol{e} = (e_1, \dots, e_r)$ of the purely inseparable extension $[L : S]$, where $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r \geqslant 1$ are integers; see Section 4 for the definition. Note that the type $\boldsymbol{e} = (e_1, \dots, e_r)$ uniquely determines the inseparable degree $[L : S] = p^{e_1+\cdots+e_r}$ of L/K but not conversely. By analogy with (1-1) it is natural to define

$$\tau(n, \boldsymbol{e}) = \max\left\{\mathrm{ed}(L/K) \mid L/K \text{ is a field extension of type } (n, \boldsymbol{e}) \text{ and } k \subset K\right\}. \tag{1-2}$$

Our main result is the following:

Theorem 1.2. *Let k be a base field of characteristic $p > 0$, $n \geqslant 1$ and $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r \geqslant 1$ be integers, $\boldsymbol{e} = (e_1, \dots, e_r)$, and $s_i = e_1 + \cdots + e_i$ for $i = 1, \dots, r$. Then*

$$\tau(n, \boldsymbol{e}) = n \sum_{i=1}^{r} p^{s_i - i e_i}.$$

Some remarks are in order.

(1) Theorem 1.2 gives the exact value for $\tau(n, \boldsymbol{e})$. This is in contrast to the separable case, where Theorem 1.1 only gives estimates and the exact value of $\tau(n)$ is unknown for any $n \geqslant 8$.

(2) A priori, the integers $\mathrm{ed}(L/K)$, $\tau(n)$, and $\tau(n, \boldsymbol{e})$ all depend on the base field k. However, Theorem 1.2 shows that for a fixed $p = \mathrm{char}(k)$, $\tau(n, \boldsymbol{e})$ is independent of the choice of k.

(3) Theorem 1.2 implies that for any inseparable extension L/K of finite degree,

$$\mathrm{ed}(L/K) \leqslant \frac{1}{p}[L : K];$$

see Remark 5.3. This is again in contrast to the separable case, where Theorem 1.1 tells us that there exists an extension L/K of degree n such that $\mathrm{ed}(L/K) > \frac{1}{2}[L : K]$ for every odd $n \geqslant 7$ (assuming $\mathrm{char}(k) = 0$).

[1] These inequalities hold for any base field k of characteristic $\neq 2$. On the other hand, the stronger lower bound of Theorem 1.1, due to Duncan, is only known in characteristic 0.

(4) We will also show that the formula for $\tau(n, \boldsymbol{e})$ remains valid if we replace the essential dimension $\mathrm{ed}(L/K)$ in the definition (1-2) by the essential dimension at p, $\mathrm{ed}_p(L/K)$; see Theorem 7.1. For the definition of the essential dimension at a prime, see Section 5 in [Reichstein 2010] or Section 3 below.

The number $\tau(n)$ has two natural interpretations. On the one hand, $\tau(n)$ is the essential dimension of the functor Et_n which associates to a field K the set of isomorphism classes of étale algebras of degree n over K. On the other hand, $\tau(n)$ is the essential dimension of the symmetric group S_n. Recall that an étale algebra L/K is a direct product $L = L_1 \times \cdots \times L_m$ of separable field extensions L_i/K. Equivalently, an étale algebra of degree n over K can be thought of as a twisted K-form of the split algebra $k^n = k \times \cdots \times k$ (n times). The symmetric group S_n arises as the automorphism group of this split algebra, so that $\mathrm{Et}_n = H^1(K, \mathrm{S}_n)$; see Example 3.5.

Our proof of Theorem 1.2 relies on interpreting $\tau(n, \boldsymbol{e})$ in a similar manner. Here the role of the split étale algebra k^n will be played by the algebra $\Lambda_{n,\boldsymbol{e}}$, which is the direct product of n copies of the truncated polynomial algebra

$$\Lambda_{\boldsymbol{e}} = k[x_1, \ldots, x_r]/\big(x_1^{p^{e}_1}, \ldots, x_r^{p^{e_r}}\big).$$

Note that the k-algebra $\Lambda_{n,\boldsymbol{e}}$ is finite-dimensional, associative, and commutative, but not semisimple. Étale algebras over K will get replaced by K-forms of $\Lambda_{n,\boldsymbol{e}}$. The role of the symmetric group S_n will be played by the algebraic group scheme $G_{n,\boldsymbol{e}} = \mathrm{Aut}_k(\Lambda_{n,\boldsymbol{e}})$ over k. We will show that $\tau(n, \boldsymbol{e})$ is the essential dimension of $G_{n,\boldsymbol{e}}$, just like $\tau(n)$ is the essential dimension of S_n in the separable case. The group scheme $G_{n,\boldsymbol{e}}$ is neither finite nor smooth; however, much to our surprise, computing its essential dimension turned out to be easier than computing the essential dimension of S_n.

The remainder of this paper is structured as follows. Sections 2 and 3 contain preliminary results on finite-dimensional algebras, their automorphism groups, and essential dimension. In Section 4 we recall the structure theory of inseparable field extensions. Section 6 is devoted to versal algebras. The upper bound of Theorem 1.2 is proved in Section 5; alternative proofs are outlined in Section 8. The lower bound of Theorem 1.2 is established in Section 7; our proof relies on the inequality (7-2) due to D. Tossici and A. Vistoli [2013]. Finally, in Section 9 we prove a stronger version of Theorem 1.2 in the special case where $n = 1$, $e_1 = \cdots = e_r$, and k is perfect.

2. Finite-dimensional algebras and their automorphisms

Recall that in the introduction we defined the essential dimension of a field extension L/K of finite degree, where K contains k. The same definition is valid for any finite-dimensional algebra A/K. That is, we say that A descends to a subfield K_0 if there exists a K_0-algebra A_0 such that $A_0 \otimes_{K_0} K$ is isomorphic to A (as a K-algebra). The essential dimension $\mathrm{ed}(A)$ is then the minimal value of $\mathrm{trdeg}(K_0/k)$, where the minimum is taken over the intermediate fields $k \subset K_0 \subset K$ such that A descends to K_0.

Here by a K-algebra A we mean a K-vector space with a bilinear "multiplication" map $m : A \times A \to A$. Later on we will primarily be interested in commutative associative algebras with 1, but at this stage m can be arbitrary: we will not assume that A is commutative or associative or has an identity element. (For example, one can talk of the essential dimension of a finite-dimensional Lie algebra A/K.) Recall that to each basis $x_1, \dots, x_n$ of A one can associate a set of n^3 structure constants $c_{ij}^h \in K$, where

$$x_i \cdot x_j = \sum_{h=1}^{n} c_{ij}^h x_h. \tag{2-1}$$

Lemma 2.1. *Let A be an n-dimensional K-algebra with structure constants c_{ij}^h (relative to some K-basis of A). Suppose a subfield $K_0 \subset K$ contains c_{ij}^h for every $i, j, h = 1, \dots, n$. Then A descends to K_0. In particular*, $\mathrm{ed}(A) \leqslant \mathrm{trdeg}(K_0/k)$.

Proof. Let A_0 be the K_0-vector space with basis $b_1, \dots, b_n$. Define the K_0-algebra structure on A_0 by (2-1). Clearly $A_0 \otimes_{K_0} K = A$, and the lemma follows. □

The following lemma will be helpful to us in the sequel.

Lemma 2.2. *Suppose $k \subset K \subset S$ are field extensions, such that S/K is separable of degree n. Let A be a finite-dimensional algebra over S. If A descends to a subfield S_0 of S such that $K(S_0) = S$, then*

$$\mathrm{ed}(A/K) \leqslant n\, \mathrm{trdeg}(S_0/k).$$

Here $\mathrm{ed}(A/K)$ *is the essential dimension of A, viewed as a K-algebra.*

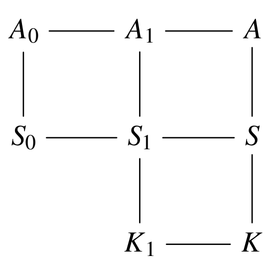
Proof. By our assumption there exists an S_0-algebra A_0 such that $A = A_0 \otimes_{S_0} S$.

Denote the normal closure of S over K by S^{norm}, and the associated Galois groups by $G = \mathrm{Gal}(S^{\mathrm{norm}}/K)$ and $H = \mathrm{Gal}(S^{\mathrm{norm}}/S) \subset G$. Now define $S_1 = k(g(s) \mid s \in S_0,\ g \in G)$. Choose a transcendence basis $t_1, \dots, t_d$ for S_0 over k, where $d = \mathrm{trdeg}(S_0/k)$. Clearly S_1 is algebraic over $k(g(t_i) \mid g \in G,\ i = 1, \dots, d)$. Since H fixes every element of S, each t_i has at most $[G : H] = n$ distinct translates of the form $g(t_i)$, $g \in G$. This shows that $\mathrm{trdeg}(S_1/k) \leqslant nd$.

Now let $K_1 = S_1^G \subset K$ and $A_1 = A_0 \otimes_{K_0} K_1$. Since S_1 is algebraic over K_1, we have

$$\mathrm{trdeg}(K_1/k) = \mathrm{trdeg}(S_1/k) \leqslant nd.$$

Examining the diagram



we see that A/K descends to K_1, and the lemma follows. □

Now let Λ be a finite-dimensional k-algebra with multiplication map $m : \Lambda \times \Lambda \to \Lambda$. The general linear group $\mathrm{GL}_k(\Lambda)$ acts on the vector space $\Lambda^* \otimes_k \Lambda^* \otimes_k \Lambda$ of bilinear maps $\Lambda \times \Lambda \to \Lambda$. The automorphism group scheme $G = \mathrm{Aut}_k(\Lambda)$ of Λ is defined as the stabilizer of m under this action. It is a closed subgroup scheme of $\mathrm{GL}_k(\Lambda)$ defined over k. The reason we use the term “group scheme” here, rather than “algebraic group”, is that G may not be smooth; see the Remark after Lemma III.1.1 in [Serre 1997].

Proposition 2.3. *Let Λ be a commutative finite-dimensional local k-algebra with residue field k, and $G = \mathrm{Aut}_k(\Lambda)$ be its automorphism group scheme. Then the natural map*

$$f : G^n \rtimes \mathrm{S}_n \to \mathrm{Aut}_k(\Lambda^n)$$

is an isomorphism. Here $G^n = G \times \cdots \times G$ (n times) acts on $\Lambda^n = \Lambda \times \cdots \times \Lambda$ (n times) componentwise and S_n acts by permuting the factors.

Before proceeding with the proof of the proposition, recall that an element α of a ring R is called an idempotent if $\alpha^2 = \alpha$.

Lemma 2.4. *Let Λ be a commutative finite-dimensional local k-algebra with residue field k and R be an arbitrary commutative k-algebra with 1. Then the only idempotents of $\Lambda_R = \Lambda \otimes_k R$ are those in R (more precisely in $1 \otimes R$).*

Proof. By Lemma 6.2 in [Waterhouse 1979], the maximal ideal M of Λ consists of nilpotent elements. Tensoring the natural projection $\Lambda \to \Lambda/M \simeq k$ with R, we obtain a surjective homomorphism $\Lambda_R \to R$ whose kernel again consists of nilpotent elements. By Proposition 7.14 in [Jacobson 1980], every idempotent in R lifts to a unique idempotent in Λ_R, and the lemma follows. □

Proof of Proposition 2.3. Let $\alpha_i = (0, \dots, 1, \dots, 0)$ where 1 appears in the i-th position. Then $\bigoplus_{i=1}^n R\alpha_i$ is an R-subalgebra of Λ_R^n.

Let $f \in \mathrm{Aut}_R(\Lambda_R^n)$. Since each α_i is an idempotent in Λ_R^n, so is each $f(\alpha_i)$. The components of each $f(\alpha_i)$ are idempotents in Λ_R. By Lemma 2.4, they lie in R. Thus, $f(\alpha_i) \in \bigoplus_{i=1}^n R\alpha_i$ for every $i = 1, \dots, n$. As a result, we obtain a morphism

$$\mathrm{Aut}_R(\Lambda_R^n) \xrightarrow{\tau_R} \mathrm{Aut}_R\left(\bigoplus_{i=1}^n R\alpha_i\right) = S_n(R).$$

For the second equality, see, e.g., p. 59 in [Waterhouse 1979]. These maps are functorial in R and thus give rise to a morphism $\tau : \mathrm{Aut}(\Lambda^n) \to \mathrm{S}_n$ of group schemes over k. The kernel of τ is $\mathrm{Aut}(\Lambda)^n$, and τ clearly has a section. The proposition follows. □

Remark 2.5. The assumption that Λ is commutative in Proposition 2.3 can be dropped, as long as we assume that the center of Λ is a finite-dimensional local k-algebra with residue field k. The proof proceeds along similar lines, except that we restrict f to an automorphism of the center $Z(\Lambda^n) = Z(\Lambda)^n$ and apply Lemma 2.4 to $Z(\Lambda)$, rather than Λ itself. This more general variant of Proposition 2.3 will not be needed in the sequel.

Remark 2.6. On the other hand, the assumption that the residue field of Λ is k cannot be dropped. For example, if Λ is a separable field extension of k of degree d, then $\mathrm{Aut}_k(\Lambda^n)$ is a twisted form of

$$\mathrm{Aut}_{\bar{k}}(\Lambda^n \otimes_k \bar{k}) = \mathrm{Aut}_{\bar{k}}(\bar{k}^{dn}) = \mathrm{S}_{nd}.$$

Here $\bar{k}$ denotes the separable closure of k. Similarly, $\mathrm{Aut}_k(\Lambda)^n \rtimes \mathrm{S}_d$ is a twisted form of $(\mathrm{S}_d)^n \rtimes \mathrm{S}_n$. For $d, n > 1$, these groups have different orders, so they cannot be isomorphic.

3. Essential dimension of a functor

In the sequel we will need the following general notion of essential dimension, due to A. Merkurjev [Berhuy and Favi 2003]. Let $\mathcal{F} : \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor from the category of field extensions K/k to the category of sets. Here k is assumed to be fixed throughout, and K ranges over all fields containing k. We say that an object $a \in \mathcal{F}(K)$ descends to a subfield $K_0 \subset K$ if a lies in the image of the natural restriction map $\mathcal{F}(K_0) \to \mathcal{F}(K)$. The essential dimension $\mathrm{ed}(a)$ of a is defined as the minimal value of $\mathrm{trdeg}(K_0/k)$, where $k \subset K_0$ and a descends to K_0. The essential dimension of the functor $\mathcal{F}$, denoted by $\mathrm{ed}(\mathcal{F})$, is the supremum of $\mathrm{ed}(a)$ for all $a \in F(K)$, and all fields K in Fields_k.

If l is a prime, there is also a related notion of essential dimension at l, which we denote by ed_l. For an object $a \in \mathcal{F}$, we define $\mathrm{ed}_l(a)$ as the minimal value of $\mathrm{ed}(a')$, where a' is the image of a in $\mathcal{F}(K')$, and the minimum is taken over all field extensions K'/K such that the degree $[K' : K]$ is finite and prime to l. The essential dimension $\mathrm{ed}_l(\mathcal{F})$ of the functor $\mathcal{F}$ at l is defined as the supremum of $\mathrm{ed}_l(a)$ for all $a \in F(K)$ and all fields K in Fields_k. Note that the prime l in this definition is unrelated to $p = \mathrm{char}(k)$; we allow both $l = p$ and $l \neq p$.

Example 3.1. Let G be a group scheme over a base field k and $\mathcal{F}_G : K \to H^1(K, G)$ be the functor defined by

$$\mathcal{F}_G(K) = \{\text{isomorphism classes of } G\text{-torsors } T \to \mathrm{Spec}(K)\}.$$

Here by a torsor we mean a torsor in the flat (fppf) topology. If G is smooth, then $H^1(K, G)$ is the first Galois cohomology set, as in [Serre 1997]; see Section II.1. The essential dimension $\mathrm{ed}(G)$ is, by definition, $\mathrm{ed}(\mathcal{F}_G)$, and similarly for the essential dimension $\mathrm{ed}_l(G)$ of G at prime l. These numerical invariants of G have been extensively studied; see, e.g., [Merkurjev 2009] or [Reichstein 2010] for a survey.

Example 3.2. Define the functor $\mathrm{Alg}_n : K \to H^1(K, G)$ by

$$\mathrm{Alg}_n(K) = \{\text{isomorphism classes of } n\text{-dimensional } K\text{-algebras}\}.$$

If A is an n-dimensional algebra, and $[A]$ is its class in $\mathrm{Alg}_n(K)$, then $\mathrm{ed}([A])$ coincides with $\mathrm{ed}(A)$ defined at the beginning of Section 2. By Lemma 2.1, $\mathrm{ed}(\mathrm{Alg}_n) \leqslant n^3$; the exact value is unknown (except for very small n).

We will now restrict our attention to certain subfunctors of Alg_n which are better understood.

Definition 3.3. Let Λ/k be a finite-dimensional algebra and K/k be a field extension (not necessarily finite or separable). We say that an algebra A/K is a *K-form* of Λ if there exists a field L containing K such that $\Lambda \otimes_k L$ is isomorphic to $A \otimes_K L$ as an L-algebra. We will write

$$\mathrm{Alg}_\Lambda : \mathrm{Fields}_k \to \mathrm{Sets}$$

for the functor which sends a field K/k to the set of K-isomorphism classes of K-forms of Λ.

Proposition 3.4. *Let Λ be a finite-dimensional k-algebra and $G = \mathrm{Aut}_k(\Lambda) \subset \mathrm{GL}(\Lambda)$ be its automorphism group scheme. Then the functors Alg_Λ and $\mathcal{F}_G = H^1(*, G)$ are isomorphic. In particular, $\mathrm{ed}(\mathrm{Alg}_\Lambda) = \mathrm{ed}(G)$ and $\mathrm{ed}_l(\mathrm{Alg}_\Lambda) = \mathrm{ed}_l(G)$ for every prime l.*

Proof. For the proof of the first assertion, see Proposition X.2.4 in [Serre 1979] or Proposition III.2.2.2 in [Knus 1991]. The second assertion is an immediate consequence of the first, since isomorphic functors have the same essential dimension. □

Example 3.5. The K-forms of $\Lambda_n = k \times \cdots \times k$ (n times) are called étale algebras of degree n. An étale algebra L/K of degree n is a direct products of separable field extensions,

$$L = L_1 \times \cdots \times L_r, \quad \text{where } \sum_{i=1}^{r} [L_i : K] = n.$$

The functor Alg_{Λ_n} is usually denoted by Et_n. The automorphism group $\mathrm{Aut}_k(\Lambda_n)$ is the symmetric group S_n, acting on Λ_n by permuting the n factors of k; see Proposition 2.3. Thus, $\mathrm{Et}_n = H^1(K, \mathrm{S}_n)$; see, e.g., Examples 2.1 and 3.2 in [Serre 2003].

4. Field extensions of type (n, e)

Let L/S be a purely inseparable extension of finite degree. For $x \in L$ we define the exponent of x over S as the smallest integer e such that $x^{p^e} \in S$. We will denote this number by $e(x, S)$. We will say that $x \in L$ is *normal* in L/S if $e(x, S) = \max\{e(y, S) \mid y \in L\}$. A sequence $x_1, \ldots, x_r$ in L is called normal if each x_i is normal in L_i/L_{i-1} and $x_i \notin L_{i-1}$. Here $L_i = S(x_1, \ldots, x_{i-1})$ and $L_0 = S$. If $L = S(x_1, \ldots, x_r)$, where $x_1, \ldots, x_r$ is a normal sequence in L/S, then we call $x_1, \ldots, x_r$ a *normal generating sequence* of L/S. We will say that this sequence is *of type* $\boldsymbol{e} = (e_1, \ldots, e_r)$ if $e_i := e(x_i, L_{i-1})$ for each i. Here $L_i = S(x_1, \ldots, x_i)$, as above. It is clear that $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r$.

Proposition 4.1 (G. Pickert [1949]). *Let L/S be a purely inseparable field extension of finite degree.*

(a) *For any generating set Λ of L/S there exists a normal generating sequence $x_1, \ldots, x_r$ with each $x_i \in \Lambda$.*

(b) *If $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$ are two normal generating sequences for L/S, of types $(e_1, \ldots, e_r)$ and $(f_1, \ldots, f_s)$, respectively, then $r = s$ and $e_i = f_i$ for each $i = 1, \ldots, r$.*

Proof. For modern proofs of both parts, see Propositions 6 and 8 in [Rasala 1971] or Lemma 1.2 and Corollary 1.5 in [Karpilovsky 1989]. □

Proposition 4.1 allows us to talk about the *type* of a purely inseparable extension L/S. We say that L/S is of type $\boldsymbol{e} = (e_1, \ldots, e_r)$ if it admits a normal generating sequence $x_1, \ldots, x_r$ of type $\boldsymbol{e}$.

Now suppose L/K is an arbitrary inseparable (but not necessarily purely inseparable) field extension L/K of finite degree. Denote the separable closure of K in L by S. We will say that L/K is of type $(n, \boldsymbol{e})$ if $[S : K] = n$ and the purely inseparable extension L/S is of type $\boldsymbol{e}$.

Remark 4.2. Note that we will assume throughout that $r \geqslant 1$, i.e., that L/K is not separable. In particular, a finite field K does not admit an extension of type $(n, \boldsymbol{e})$ for any n and $\boldsymbol{e}$.

Remark 4.3. It follows from Proposition 4.1 that L/K cannot be generated by fewer than r elements. Note also that the integer r can be determined directly, without constructing a normal generating sequence. Indeed, by Theorem 6 in [Becker and MacLane 1940], $[L : K(L^p)] = p^r$. Here $K(L^p)$ denotes the subfield of L generated by L^p and K.

Lemma 4.4. *Let $n \geqslant 1$ and $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r \geqslant 1$ be integers. Then there exist*

(a) *a separable field extension E/F of degree n with $k \subset F$ and*

(b) *a field extension L/K of type $(n, \boldsymbol{e})$ with $k \subset K$ and $\boldsymbol{e} = (e_1, \dots, e_r)$.*

In particular, this lemma shows that the maxima in definitions (1-1) and (1-2) are taken over a nonempty set of integers.

Proof. (a) Let $x_1, \dots, x_n$ be independent variables over k. Set $E = k(x_1, \dots, x_n)$ and $F = E^C$, where C is the cyclic group of order n acting on E by permuting the variables. Clearly E/F is a Galois (and hence, separable) extension of degree n.

(b) Let E/F be as in part (a) and $y_1, \dots, y_r$ be independent variables over F. Set $L = E(y_1, \dots, y_r)$ and $K = F(z_1, \dots, z_r)$, where $z_i = y_i^{p^{e_i}}$. One readily checks that $S = E(z_1, \dots, z_n)$ is the separable closure of K in L and L/S is a purely inseparable extension of type $\boldsymbol{e}$. □

Now suppose $n \geqslant 1$ and $\boldsymbol{e} = (e_1, \dots, e_r)$ are as above, with $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r \geqslant 1$. The following finite-dimensional commutative k-algebras will play an important role in the sequel:

$$\Lambda_{n,\boldsymbol{e}} = \Lambda_{\boldsymbol{e}} \times \cdots \times \Lambda_{\boldsymbol{e}} \quad (n \text{ times}), \qquad \text{where } \Lambda_{\boldsymbol{e}} = k[x_1, \dots, x_r]/(x_1^{p^{e_1}}, \dots, x_r^{p^{e_r}}) \tag{4-1}$$

is a truncated polynomial algebra.

Lemma 4.5. *$\Lambda_{n,\boldsymbol{e}}$ is isomorphic to $\Lambda_{m,\boldsymbol{f}}$ if and only if $m = n$ and $\boldsymbol{e} = \boldsymbol{f}$.*

Proof. One direction is obvious: if $m = n$ and $\boldsymbol{e} = \boldsymbol{f}$, then $\Lambda_{n,\boldsymbol{e}}$ is isomorphic to $\Lambda_{m,\boldsymbol{f}}$

To prove the converse, note that $\Lambda_{\boldsymbol{e}}$ is a finite-dimensional local k-algebra with residue field k. By Lemma 2.4, the only idempotents in $\Lambda_{\boldsymbol{e}}$ are 0 and 1. This readily implies that the only idempotents in $\Lambda_{n,\boldsymbol{e}}$ are of the form $(\epsilon_1, \dots, \epsilon_n)$, where each ϵ_i is 0 or 1, and the only minimal idempotents are

$$\alpha_1 = (1, 0, \dots, 0), \quad \dots, \quad \alpha_n = (0, \dots, 0, 1).$$

(Recall that idempotents α and β are called *orthogonal* if $\alpha\beta = \beta\alpha = 0$. If α and β are orthogonal, then one readily checks that $\alpha + \beta$ is also an idempotent. An idempotent is *minimal* if it cannot be written as a sum of two orthogonal idempotents.)

If $\Lambda_{n,\boldsymbol{e}}$ and $\Lambda_{m,\boldsymbol{f}}$ are isomorphic, then they have the same number of minimal idempotents; hence, $m = n$. Denote the minimal idempotents of $\Lambda_{m,\boldsymbol{f}}$ by

$$\beta_1 = (1, 0, \dots, 0), \quad \dots, \quad \beta_m = (0, \dots, 0, 1).$$

A k-algebra isomorphism $\Lambda_{n,\boldsymbol{e}} \to \Lambda_{m,\boldsymbol{f}}$ takes α_1 to β_j for some $j = 1, \dots, n$ and, hence, induces a k-algebra isomorphism between $\alpha_1 \Lambda_{n,\boldsymbol{e}} \simeq \Lambda_{\boldsymbol{e}}$ and $\beta_j \Lambda_{m,\boldsymbol{f}} \simeq \Lambda_{\boldsymbol{f}}$. To complete the proof, we appeal to Proposition 8 in [Rasala 1971], which asserts that $\Lambda_{\mathbf{e}}$ and $\Lambda_{\boldsymbol{f}}$ are isomorphic if and only if $\boldsymbol{e} = \boldsymbol{f}$. □

Lemma 4.6. *Let L/K be a field extension of finite degree. Then the following are equivalent.*

(a) *L/K is of type $(n, \boldsymbol{e})$.*

(b) *L is a K-form of $\Lambda_{n,\boldsymbol{e}}$. In other words, $L \otimes_K K'$ is isomorphic to $\Lambda_{n,\boldsymbol{e}} \otimes_k K'$ as a K'-algebra for some field extension K'/K.*

Proof. (a) $\Longrightarrow$ (b). Assume L/K is a field extension of type $(n, \boldsymbol{e})$. Let S be the separable closure of K in L and K' be an algebraic closure of S (which is also an algebraic closure of K). Then

$$L \otimes_K K' = L \otimes_S (S \otimes_K K') = (L \otimes_S K') \times \cdots \times (L \otimes_S K') \quad (n \text{ times}).$$

On the other hand, by [Rasala 1971, Theorem 3], $L \otimes_S K'$ is isomorphic to $\Lambda_{\boldsymbol{e}}$ as a K'-algebra, and part (b) follows.

(b) $\Longrightarrow$ (a). Assume $L \otimes_K K'$ is isomorphic to $\Lambda_{n,\boldsymbol{e}} \otimes_k K'$ as a K'-algebra for some field extension K'/K. After replacing K' by a larger field, we may assume that K' contains the normal closure of S over K. Since $\Lambda_{n,\boldsymbol{e}} \otimes_k K'$ is not separable over K', L is not separable over K. Thus, L/K is of type $(m, \boldsymbol{f})$ for some $m \geqslant 1$ and $\boldsymbol{f} = (f_1, \dots, f_s)$ with $f_1 \geqslant f_2 \geqslant \cdots \geqslant f_s \geqslant 1$. As shown above, this implies that $L \otimes_K K''$ is isomorphic to $\Lambda_{m,\boldsymbol{f}} \otimes_k K''$ for a suitable field extension K''/K. After enlarging K'', we may assume without loss of generality that $K' \subset K''$. We conclude that $\Lambda_{n,\boldsymbol{e}} \otimes_k K''$ is isomorphic to $\Lambda_{m,\boldsymbol{f}} \otimes_k K''$ as a K''-algebra. By Lemma 4.5, with k replaced by K'', this is only possible if $(n, \boldsymbol{e}) = (m, \boldsymbol{f})$. □

5. Proof of the upper bound of Theorem 1.2

In this section we will prove the following proposition.

Proposition 5.1. *Let $n \geqslant 1$, $\boldsymbol{e} = (e_1, \dots, e_r)$, where $e_1 \geqslant \cdots \geqslant e_r \geqslant 1$, and $s_i = e_1 + \cdots + e_i$ for $i = 1, \dots, r$. Then*

$$\tau(n, \boldsymbol{e}) \leqslant n \sum_{i=1}^{r} p^{s_i - i e_i}.$$

Our proof of Proposition 5.1 will be facilitated by the following lemma.

Lemma 5.2. *Let K be an infinite field of characteristic p, q be a power of p, S/K be a separable field extension of finite degree, and $0 \neq a \in S$. Then there exists an $s \in S$ such that as^q is a primitive element for S/K.*

Proof. Assume the contrary. It is well known that there are only finitely many intermediate fields between K and S; see, e.g., [Lang 1984, Theorem V.4.6]. Denote the intermediate fields properly contained in S by $S_1, \dots, S_n \subsetneq S$, and let $\mathbb{A}_K(S)$ be the affine space associated to S. (Here we view S as a K-vector space.) The nongenerators of S/K may now be viewed as K-points of the finite union

$$Z = \bigcup_{i=1}^{n} \mathbb{A}_K(S_i).$$

Since we are assuming that every element of S of the form as^q is a nongenerator, and K is an infinite field, the image of the K-morphism $f : \mathbb{A}(S) \to \mathbb{A}(S)$ given by $s \mapsto as^q$ lies in $Z = \bigcup_{i=1}^{n} \mathbb{A}_K(S_i)$. Since $\mathbb{A}_K(S)$ is irreducible, we conclude that the image of f lies in one of the affine subspaces $\mathbb{A}_K(S_i)$, say in $\mathbb{A}_K(S_1)$. Equivalently, $as^q \in S_1$ for every $s \in S$. Setting $s = 1$, we see that $a \in S_1$. Dividing $as^q \in S_1$ by $0 \neq a \in S_1$, we conclude that $s^q \in S_1$ for every $s \in S$. Thus, S is purely inseparable over S_1, contradicting our assumption that S/K is separable. □

Proof of Proposition 5.1. Let L/K be a field extension of type $(n, \boldsymbol{e})$. Our goal is to show that $\operatorname{ed}(L/K) \leqslant n \sum_{j=1}^{r} p^{s_j - je_j}$. By Remark 4.2, K is infinite.

Let S be the separable closure of K in L and $x_1, \ldots, x_r$ be a normal generating sequence for the purely inseparable extension L/S of type $\boldsymbol{e}$. Set $q_i = p^{e_i}$. Recall that by the definition of normal sequence, $x_1^{q_1} \in S$. We are free to replace x_1 by $x_1 s$ for any $0 \neq s \in S$; clearly $x_1 s, x_2, \ldots, x_r$ is another normal generating sequence. By Lemma 5.2, we may choose $s \in S$ so that $(x_1 s)^{q_1}$ is a primitive element for S/K. In other words, we may assume without loss of generality that $x_1^{q_1}$ is a primitive element for S/K.

By the structure theorem of Pickert, each $x_i^{q_i}$ lies in $S[x_1^{q_i}, \ldots, x_{i-1}^{q_i}]$, where $q_i = p^{e_i}$ [Rasala 1971, Theorem 1]. In other words, for each $i = 1, \ldots, r$,

$$x_i^{q_i} = \sum a_{d_1,\ldots,d_{i-1}} x_1^{q_i d_1} \cdots x_{i-1}^{q_i d_{i-1}} \tag{5-1}$$

for some $a_{d_1,\ldots,d_{i-1}} \in S$. Here the sum is taken over all integers $d_1, \ldots, d_{i-1}$, where each $0 \leqslant d_j < p^{e_j - e_i}$. Note that for $i = 1$ (5-1) reduces to

$$x_1^{q_1} = a_\varnothing,$$

for some $a_\varnothing \in S$. By Lemma 2.1, L (viewed as an S-algebra), descends to

$$S_0 = k(a_{d_1,\ldots,d_{i-1}} \mid i = 1, \ldots, r \text{ and } 0 \leqslant d_j < p^{e_j - e_i}).$$

Note that for each $i = 1, \ldots, r$, there are exactly

$$p^{e_1 - e_i} \cdot p^{e_2 - e_i} \cdot \cdots \cdot p^{e_{i-1} - e_i} = p^{s_i - ie_i}$$

choices of the subscripts $d_1, \ldots, d_{i-1}$. Hence, S_0 is generated over k by $\sum_{i=1}^{r} p^{s_i - ie_i}$ elements and consequently,

$$\operatorname{trdeg}(S_0/k) \leqslant \sum_{i=1}^{r} p^{s_i - ie_i}.$$

Moreover, since S_0 contains $a_\varnothing = x_1^q$, which is a primitive element for S/K, we conclude that $K(S_0) = S$. Thus, Lemma 2.2 can be applied to $A = L$; it yields $\operatorname{ed}(L/K) \leqslant n \operatorname{trdeg}(S_0/k)$, and the proposition follows. □

Remark 5.3. Suppose L/K is an extension of type $(n, \boldsymbol{e})$, where $e = (e_1, \dots, e_r)$. Here, as usual, K is assumed to contain the base field k of characteristic $p > 0$. Dividing both sides of the inequality in Proposition 5.1 by $[L : K] = np^{e_1+\cdots+e_r}$, we readily deduce that

$$\frac{\mathrm{ed}(L/K)}{[L:K]} \leqslant \frac{\tau(n)}{[L:K]} \leqslant \sum_{i=1}^{r} p^{-ie_i - e_{i+1} - \cdots - e_r} \leqslant \frac{r}{p^r} \leqslant \frac{1}{p}.$$

In particular, $\mathrm{ed}(L/K) \leqslant \frac{1}{2}[L : K]$ for any inseparable extension $[L : K]$ of finite degree, in any (positive) characteristic. As we pointed out in the introduction, this inequality fails in characteristic 0 (even for $k = \mathbb{C}$).

6. Versal algebras

Let K be a field and A be a finite-dimensional associative K-algebra with 1. Every $a \in A$ gives rise to the K-linear map $l_a : A \to A$ given by $l_a(x) = ax$ (left multiplication by a). Note that $l_{ab} = l_a \cdot l_b$. It readily follows from this that a has a multiplicative inverse in A if and only if l_a is nonsingular.

Proposition 6.1. *Let l be a prime integer and Λ be a finite-dimensional associative k-algebra with* 1. *Assume that there exists a field extension K/k and a K-form A of Λ such that A is a division algebra. Then*:

(a) *There exists a field K_{ver} containing k and a K_{ver}-form A_{ver} of Λ such that*

$$\mathrm{ed}(A_{\mathrm{ver}}) = \mathrm{ed}(\mathrm{Alg}_\Lambda), \quad \mathrm{ed}_l(A_{\mathrm{ver}}) = \mathrm{ed}_l(\mathrm{Alg}_\Lambda) \quad \textit{for every prime integer } l, \quad \textit{and}$$

A_{ver} is a division algebra.

(b) *If G is the automorphism group scheme of Λ, then*

$$\mathrm{ed}(G) = \mathrm{ed}(\mathrm{Alg}_\Lambda) = \max\{\mathrm{ed}(A/K) \mid A \textit{ is a } K\textit{-form of } \Lambda \textit{ and a division algebra}\},$$
$$\mathrm{ed}_l(G) = \mathrm{ed}_l(\mathrm{Alg}_\Lambda) = \max\{\mathrm{ed}_l(A/K) \mid A \textit{ is a } K\textit{-form of } \Lambda \textit{ and a division algebra}\}.$$

Here the subscript "ver" is meant to indicate that $A_{\mathrm{ver}}/K_{\mathrm{ver}}$ is a versal object for $\mathrm{Alg}_\Lambda = H^1(*, G)$. For a discussion of versal torsors, see Section I.5 in [Serre 2003] or [Duncan and Reichstein 2015].

Proof. (a) We begin by constructing a versal G-torsor $T_{\mathrm{ver}} \to \mathrm{Spec}(K_{\mathrm{ver}})$. Recall that $G = \mathrm{Aut}_k(\Lambda)$ is defined as a closed subgroup of the general linear group $\mathrm{GL}_k(\Lambda)$. This general linear group admits a generically free linear action on some vector space V (e.g., we can take $V = \mathrm{End}_k(\Lambda)$, with the natural left G-action). Restricting to G we obtain a generically free representation $G \to \mathrm{GL}(V)$. We can now choose a dense open G-invariant subscheme $U \subset V$ over k which is the total space of a G-torsor $\pi : U \to B$; see, e.g., Example 5.4 in [Serre 2003]. Passing to the generic point of B, we obtain a G-torsor $T_{\mathrm{ver}} \to \mathrm{Spec}(K_{\mathrm{ver}})$, where K_{ver} is the function field of B over k. Then $\mathrm{ed}(T_{\mathrm{ver}}/K_{\mathrm{ver}}) = \mathrm{ed}(G)$ (see, e.g., Section 4 in [Berhuy and Favi 2003]) and $\mathrm{ed}_l(T_{\mathrm{ver}}/K_{\mathrm{ver}}) = \mathrm{ed}_l(G)$ (see Lemma 6.6 in [Reichstein and Youssin 2000] or Theorem 4.1 in [Merkurjev 2009]).

Let $T \to \mathrm{Spec}(K)$ be the torsor associated to the K-algebra A and A_{ver} be the K_{ver}-algebra associated to $T_{\mathrm{ver}} \to \mathrm{Spec}(K_{\mathrm{ver}})$ under the isomorphism between the functors Alg_Λ and $H^1(*, G)$ of Proposition 3.4.

By the characteristic-free version of the no-name lemma, proved in [Reichstein and Vistoli 2006, §2], $T \times V$ is G-equivariantly birationally isomorphic to $T \times \mathbb{A}^d_k$, where $d = \dim V$ and G acts trivially on $\mathbb{A}^d_k$. In other words, we have a Cartesian diagram of rational maps defined over k:

$$\begin{array}{ccccc} & & T \times \mathbb{A}^d & \overset{\simeq}{\dashrightarrow} \; T \times V & \overset{\mathrm{pr}_2}{\dashrightarrow} \; U \\ & & \big\downarrow & & \big\downarrow \\ \mathbb{A}^d_K & = & \mathrm{Spec}(K) \times \mathbb{A}^d & \dashrightarrow & B \end{array}$$

Here all direct products are over $\mathrm{Spec}(k)$, and pr_2 denotes the rational G-equivariant projection map taking $(t, v) \in T \times V$ to $v \in V$ for $v \in U$. The map $\mathrm{Spec}(K) \times \mathbb{A}^d \dashrightarrow B$ in the bottom row is induced from the dominant G-equivariant map $T \times \mathbb{A}^d \dashrightarrow U$ on top. Passing to generic points, we obtain an inclusion of field $K_{\mathrm{ver}} \hookrightarrow K(x_1, \dots, x_d)$ such that the induced map $H^1(K_{\mathrm{ver}}, G) \to H^1(K(x_1, \dots, x_d), G)$ sends the class of $T_{\mathrm{ver}} \to \mathrm{Spec}(K_{\mathrm{ver}})$ to the class associated to $T \times \mathbb{A}^d \to \mathbb{A}^d_K$. Under the isomorphism of Proposition 3.4 between the functors Alg_Λ and $\mathcal{F}_G = H^1(*, G)$, this translates to

$$A_{\mathrm{ver}} \otimes_{K_{\mathrm{ver}}} K(x_1, \dots, x_d) \simeq A \otimes_K K(x_1, \dots, x_d)$$

as $K(x_1, \dots, x_d)$-algebras.

For simplicity we will write $A(x_1, \dots, x_d)$ in place of $A \otimes_K K(x_1, \dots, x_d)$. Since A is a division algebra, so is $A(x_1, \dots, x_d)$. Thus, the linear map $l_a : A(x_1, \dots, x_d) \to A(x_1, \dots, x_d)$ is nonsingular (i.e., has trivial kernel) for every $a \in A_{\mathrm{ver}}$. Hence, the same is true for the restriction of l_a to A_{ver}. We conclude that A_{ver} is a division algebra. Remembering that A_{ver} corresponds to T_{ver} under the isomorphism of functors between Alg_Λ and $\mathcal{F}_G$, we see that

$$\begin{aligned} \mathrm{ed}(A_{\mathrm{ver}}) &= \mathrm{ed}(T_{\mathrm{ver}}/K_{\mathrm{ver}}) = \mathrm{ed}(G) = \mathrm{ed}(\mathrm{Alg}_\Lambda), \\ \mathrm{ed}_l(A_{\mathrm{ver}}) &= \mathrm{ed}_l(T_{\mathrm{ver}}/K_{\mathrm{ver}}) = \mathrm{ed}_l(G) = \mathrm{ed}_l(\mathrm{Alg}_\Lambda), \end{aligned}$$

as desired.

(b) The first equality in both formulas follows from Proposition 3.4, and the second from part (a). □

We will now revisit the finite-dimensional k-algebras $\Lambda_{\boldsymbol{e}}$ and $\Lambda_{n,\boldsymbol{e}} = \Lambda_{\boldsymbol{e}} \times \cdots \times \Lambda_{\boldsymbol{e}}$ (n times) defined in Section 4; see (4-1). We will write

$$G_{n,\boldsymbol{e}} = \mathrm{Aut}(\Lambda_{n,\boldsymbol{e}}) \subset \mathrm{GL}_k(\Lambda_{n,\boldsymbol{e}})$$

for the automorphism group scheme of $\Lambda_{n,\boldsymbol{e}}$ and $\mathrm{Alg}_{n,\boldsymbol{e}}$ for the functor $\mathrm{Alg}_{\Lambda_{n,\boldsymbol{e}}} : \mathrm{Fields}_k \to \mathrm{Sets}$. Recall that this functor associates to a field K/k the set of isomorphism classes of K-forms of $\Lambda_{n,\boldsymbol{e}}$.

Replacing essential dimension by essential dimension at a prime l in the definitions (1-1) and (1-2), we set

$$\begin{aligned} \tau_l(n) &= \max\big\{\mathrm{ed}_l(L/K) \mid L/K \text{ is a separable field extension of degree } n \text{ and } k \subset K\big\}, \\ \tau_l(n, \boldsymbol{e}) &= \max\big\{\mathrm{ed}_l(L/K) \mid L/K \text{ is a field extension of type } (n, \boldsymbol{e}) \text{ and } k \subset K\big\}. \end{aligned}$$

Corollary 6.2. *Let l be a prime integer. Then*:

(a) $\mathrm{ed}(\mathrm{S}_n) = \mathrm{ed}(\mathrm{Et}_n) = \tau(n)$ *and* $\mathrm{ed}_l(\mathrm{S}_n) = \mathrm{ed}_l(\mathrm{Et}_n) = \tau_l(n)$. *Here* Et_n *is the functor of n-dimensional étale algebras*, *as in Example 3.5*.

(b) $\mathrm{ed}(G_{n,\boldsymbol{e}}) = \mathrm{ed}(\mathrm{Alg}_{n,\boldsymbol{e}}) = \tau(n, \boldsymbol{e})$ *and* $\mathrm{ed}_l(G_{n,\boldsymbol{e}}) = \mathrm{ed}_l(\mathrm{Alg}_{n,\boldsymbol{e}}) = \tau_l(n, \boldsymbol{e})$.

Proof. (a) Recall that étale algebras are, by definition, commutative and associative with identity. For such algebras "division algebra" is the same as "field". By Lemma 4.4(a) there exists a separable field extension E/F of degree n with $k \subset F$. The desired equality follows from Proposition 6.1(b).

(b) The same argument as in part (a) goes through, with part (a) of Lemma 4.4 replaced by part (b). □

Remark 6.3. The value of $\mathrm{ed}_l(\mathrm{S}_n)$ is known for every integer $n \geqslant$ and every prime $l \geqslant 2$:

$$\mathrm{ed}_l(\mathrm{S}_n) = \begin{cases} \lfloor n/l \rfloor & \text{if } \mathrm{char}(k) \neq l, \\ 1 & \text{if } \mathrm{char}(k) = l \leqslant n, \\ 0 & \text{if } \mathrm{char}(k) = l > n. \end{cases}$$

See respectively [Meyer and Reichstein 2009, Corollary 4.2], [Reichstein and Vistoli 2018, Theorem 1], and either [Meyer and Reichstein 2009, Lemma 4.1] or [Reichstein and Vistoli 2018, Theorem 1].

7. Conclusion of the proof of Theorem 1.2

In this section we will prove Theorem 1.2 in the following strengthened form.

Theorem 7.1. *Let k be a base field of characteristic $p > 0$, $n \geqslant 1$ and $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r \geqslant 1$ be integers*, *$\boldsymbol{e} = (e_1, \ldots, e_r)$, and $s_i = e_1 + \cdots + e_i$ for $i = 1, \ldots, r$. Then*

$$\tau_p(n, \boldsymbol{e}) = \tau(n, \boldsymbol{e}) = n \sum_{i=1}^{r} p^{s_i - i e_i}.$$

By definition $\tau_p(n, \boldsymbol{e}) \leqslant \tau(n, \boldsymbol{e})$ and by Proposition 5.1, $\tau(n, \boldsymbol{e}) \leqslant n \sum_{i=1}^{r} p^{s_i - i e_i}$. Moreover, by Corollary 6.2(b), $\tau_p(n, \boldsymbol{e}) = \mathrm{ed}_p(G_{n,\boldsymbol{e}})$. It thus remains to show that

$$\mathrm{ed}_p(G_{n,\boldsymbol{e}}) \geqslant n \sum_{i=1}^{r} p^{s_i - i e_i}. \tag{7-1}$$

Our proof of (7-1) will be based on the general inequality, due to Tossici and Vistoli [2013],

$$\mathrm{ed}_p(G) \geqslant \dim \mathrm{Lie}(G) - \dim G \tag{7-2}$$

for any group scheme G of finite type over a field k of characteristic p. Now recall that $G_{\boldsymbol{e}} = \mathrm{Aut}_k(\Lambda_{\boldsymbol{e}})$, and $G_{n,\boldsymbol{e}} = \mathrm{Aut}_k(\Lambda_{n,\boldsymbol{e}})$, where $\Lambda_{n,\boldsymbol{e}} = \Lambda_{\boldsymbol{e}}^n$. Since $\Lambda_{\boldsymbol{e}}$ is a commutative local k-algebra with residue field k, Proposition 2.3 tells us that $G_{n,\boldsymbol{e}} = G_{\boldsymbol{e}}^n \rtimes \mathrm{S}_n$ (see also Proposition 5.1 in [Sancho de Salas 2000]). We conclude that

$$\dim G_{n,\boldsymbol{e}} = n \dim G_{\boldsymbol{e}} \quad \text{and} \quad \dim \mathrm{Lie}(G_{n,\boldsymbol{e}}) = n \dim \mathrm{Lie}(G_{\boldsymbol{e}}).$$

Substituting these formulas into (7-2), we see that the proof of the inequality (7-1) (and thus of Theorem 7.1) reduces to the following:

Proposition 7.2. *Let* $\boldsymbol{e} = (e_1, \dots, e_r)$, *where* $e_1 \geqslant \cdots \geqslant e_r \geqslant 1$ *are integers. Then*

(a) $\dim \mathrm{Lie}(G_{\boldsymbol{e}}) = rp^{e_1+\cdots+e_r}$, *and*

(b) $\dim G_{\boldsymbol{e}} = rp^{e_1+\cdots+e_r} - \sum_{i=1}^{r} p^{s_i - ie_i}$.

The remainder of this section will be devoted to proving Proposition 7.2. We will use the following notations.

(1) We fix the type $\boldsymbol{e} = (e_1, \dots, e_r)$ and set $q_i = p^{e_i}$.

(2) The infinitesimal group scheme α_{p^j} over a commutative ring S of characteristic p is defined as the kernel of the j-th power of the Frobenius map, $\mathbb{G}_a \to \mathbb{G}_a$, $x \mapsto x^{p^j}$, viewed as a homomorphism of group schemes over S. We will be particularly interested in the case where $S = \Lambda_{\boldsymbol{e}}$.

(3) Suppose X is a scheme over Λ, where Λ is a finite-dimensional commutative k-algebra. We will denote the Weil restriction of the Λ-scheme X to k by $R_{\Lambda/k}(X)$. For generalities on Weil restriction, see Chapter 2 and the Appendix in [Milne 2017].

(4) We will denote by $\mathrm{End}(\Lambda_{\boldsymbol{e}})$ the functor

$$\mathrm{Comm}_k \to \mathrm{Sets}, \qquad R \to \mathrm{End}_{R\text{-alg}}(\Lambda_{\boldsymbol{e}} \otimes_k R)$$

of algebra endomorphisms of $\Lambda_{\boldsymbol{e}}$. Here Comm_k denotes the category of commutative associative k-algebras with 1 and Sets denotes the category of sets.

Lemma 7.3. (a) *The functor* $\mathrm{End}(\Lambda_{\boldsymbol{e}})$ *is represented by an irreducible, nonreduced, affine* k*-scheme* $X_{\boldsymbol{e}}$.

(b) $\dim X_{\boldsymbol{e}} = rp^{e_1+\cdots+e_r} - \sum_{i=1}^{r} p^{s_i - ie_i}$.

(c) $\dim T_\gamma(X_{\boldsymbol{e}}) = rp^{e_1+\cdots+e_r}$ *for any* k*-point* γ *of* $X_{\boldsymbol{e}}$. *Here* $T_\gamma(X_{\boldsymbol{e}})$ *denotes the tangent space to* $X_{\boldsymbol{e}}$ *at* γ.

Proof. An endomorphism F in $\mathrm{End}(\Lambda_{\boldsymbol{e}})(R)$ is uniquely determined by the images

$$F(x_1), F(x_2), \dots, F(x_r) \in \Lambda_{\boldsymbol{e}}(R)$$

of the generators $x_1, \dots, x_r$ of $\Lambda_{\boldsymbol{e}}$. These elements of $\Lambda_{\boldsymbol{e}}$ satisfy $F(x_i)^{q_i} = 0$. Conversely, any r elements $F_1, \dots, F_r$ in $\Lambda_{\boldsymbol{e}} \otimes R$ satisfying $F_i^{q_i} = 0$ give rise to an algebra endomorphism F in $\mathrm{End}(\Lambda_{\boldsymbol{e}})(R)$. We thus have

$$\begin{aligned} \mathrm{End}(\Lambda_{\boldsymbol{e}})(R) &= \mathrm{Hom}_{R\text{-alg}}(\Lambda_{\boldsymbol{e}} \otimes_k R, \Lambda_{\boldsymbol{e}} \otimes R) \\ &\cong \alpha_{q_1}(\Lambda_{\boldsymbol{e}} \otimes R) \times \cdots \times \alpha_{q_r}(\Lambda_{\boldsymbol{e}} \otimes R) \\ &\cong R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_1})(R) \times \cdots \times R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_r})(R) \\ &\cong \prod_{i=1}^{r} R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_i})(R). \end{aligned}$$

We conclude that $\mathrm{End}(\Lambda_{\boldsymbol{e}})$ is represented by an affine k-scheme $X_{\boldsymbol{e}} = \prod_{i=1}^{r} R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_i})$. Note that $X_{\boldsymbol{e}}$ is isomorphic to $\prod_{i=1}^{r} R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_i})$ as a k-scheme only, not as a group scheme. To complete the proof of the lemma it remains to establish the following assertions, claimed for all $q_j \in \{q_1, \dots, q_r\}$:

(a′) $R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j})$ is irreducible.

(b′) $\dim R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j}) = p^{e_1+\cdots+e_r} - p^{s_j - je_j}$.

(c′) $\dim T_\gamma(R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j})) = p^{e_1+\cdots+e_r}$ for any k-point γ of $R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j})$.

To prove (a′), (b′), and (c′), we will write out explicit equations for $R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j})$ in $R_{\Lambda_{\boldsymbol{e}}/k}(\mathbb{A}^1) \simeq \mathbb{A}_k(\Lambda_{\boldsymbol{e}})$. We will work in the basis $\{x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}\}$ of monomials in $\Lambda_{\boldsymbol{e}}$, where $0 \leqslant i_1 < q_1, 0 \leqslant i_2 < q_2, \dots, 0 \leqslant i_r < q_r$. Over $\Lambda_{\boldsymbol{e}}$, α_{q_j} is cut out (scheme-theoretically) in $\mathbb{A}^1$ by the single equation $t^{q_j} = 0$, where t is a coordinate function on $\mathbb{A}^1$. Since $x_i^{q_i} = 0$ for every i, writing

$$t = \sum y_{i_1,\dots,i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}$$

and expanding

$$t^{q_j} = \sum y_{i_1,\dots,i_r}^{q_j} x_1^{q_j i_1} x_2^{q_j i_2} \cdots x_r^{q_j i_r}$$

we see that the only monomials appearing in the above sum are those for which

$$q_j i_1 < q_1, \quad q_j i_2 < q_2, \quad \dots, \quad q_j i_r < q_r.$$

Thus, $R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j})$ is cut out (again, scheme-theoretically) in $R_{\Lambda_{\boldsymbol{e}}/k}(\mathbb{A}^1) \simeq \mathbb{A}(\Lambda_{\boldsymbol{e}})$ by

$$y_{i_1,\dots,i_{j-1},0,\dots,0}^{q_j} = 0 \quad \text{for } 0 \leqslant i_1 < \frac{q_1}{q_j}, \quad \dots, \quad 0 \leqslant i_{j-1} < \frac{q_{j-1}}{q_j},$$

where $y_{i_1,\dots,i_r}$ are the coordinates in $\mathbb{A}(\Lambda_{\boldsymbol{e}})$. In other words, $R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j})$ is the subscheme of $R_{\Lambda_{\boldsymbol{e}}/k}(\mathbb{A}^1) \simeq \mathbb{A}_k(\Lambda_{\boldsymbol{e}}) \simeq \mathbb{A}_k^{p^{e_1+\cdots+e_r}}$ cut out (again, scheme-theoretically) by q_j-th powers of

$$\frac{q_1}{q_j} \frac{q_2}{q_j} \cdots \frac{q_{j-1}}{q_j} = p^{s_j - je_j}$$

distinct coordinate functions. The reduced scheme $R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_j})_{\mathrm{red}}$ is thus isomorphic to an affine space of dimension $p^{e_1+\cdots+e_r} - \sum_{j=1}^{r} p^{s_j - je_j}$. On the other hand, since q_j is a power of p, the Jacobian criterion tells us that the tangent space to $R_{\Lambda_{\boldsymbol{e}}/k}(\alpha_{q_l})$ at any k-point is the same as the tangent space to $\mathbb{A}(\Lambda_{\boldsymbol{e}}) = \mathbb{A}^{p^{e_1+\cdots+e_r}}$, and (a′), (b′), and (c′) follow. □

Conclusion of the proof of Proposition 7.2. The automorphism group scheme $G_{\boldsymbol{e}}$ is the group of invertible elements in $\mathrm{End}(\Lambda_{\boldsymbol{e}})$. In other words, the natural diagram

$$\begin{array}{ccc} G_{\boldsymbol{e}} & \longrightarrow & \mathrm{GL}_N \\ \downarrow & & \downarrow \\ \mathrm{End}(\Lambda_{\boldsymbol{e}}) & \longrightarrow & \mathrm{Mat}_{N\times N} \end{array}$$

where $N = \dim \Lambda_{\boldsymbol{e}} = p^{e_1+\cdots+e_r}$, is Cartesian. Hence, $G_{\boldsymbol{e}}$ is an open subscheme of $X_{\boldsymbol{e}}$. Since $X_{\boldsymbol{e}}$ is irreducible, Proposition 7.2 follows from Lemma 7.3. This completes the proof of Proposition 7.2 and thus of Theorem 7.1. □

8. Alternative proofs of Theorem 1.2

The proof of the lower bound of Theorem 1.2 given in Section 7 is the only one we know. However, we have two other proofs for the upper bound (Proposition 5.1), in addition to the one given in Section 5. In this section we will briefly outline these arguments for the interested reader.

Our first alternative proof of Proposition 5.1 is based on an explicit construction of the versal algebra A_{ver} of type $(n, \boldsymbol{e})$ whose existence is asserted by Proposition 6.1. This construction is via generators and relations, by taking "the most general" structure constants in (5-1). Versality of A_{ver} constructed this way takes some work to prove; however, once versality is established, it is easy to see directly that A_{ver} is a field and thus

$$\tau(n, \boldsymbol{e}) = \text{ed}(A_{\text{ver}}) \leqslant \text{trdeg}(K_{\text{ver}}/k) = n \sum_{i=1}^{r} p^{s_i - ie_i}.$$

Our second alternative proof of Proposition 5.1 is based on showing that the natural representation of $G_{n,\boldsymbol{e}}$ on $V = \Lambda_{n,\boldsymbol{e}}^r$ is generically free. Intuitively speaking, this is clear: $\Lambda_{n,e}$ is generated by r elements as a k-algebra, so r-tuples of generators of $\Lambda_{n,\boldsymbol{e}}$ are dense in V and have trivial stabilizer in $G_{n,\boldsymbol{e}}$. The actual proof involves checking that the stabilizer in general position is trivial scheme-theoretically and not just on the level of points. Once generic freeness of this linear action is established, the upper bound of Proposition 5.1 follows from the inequality

$$\text{ed}(G_{n,\boldsymbol{e}}) \leqslant \dim V - \dim G_{n,\boldsymbol{e}};$$

see, e.g., Proposition 4.11 in [Berhuy and Favi 2003]. To deduce the upper bound of Proposition 5.1 from this inequality, recall that

- $\tau(n, \boldsymbol{e}) = \text{ed}(G_{n,\boldsymbol{e}})$ (see Corollary 6.2(b)),
- $\dim V = r \dim \Lambda_{n,\boldsymbol{e}} = nr \dim \Lambda_{\mathbf{e}} = nrp^{e_1+\cdots+e_r}$ (clear from the definition), and
- $\dim G_{n,\boldsymbol{e}} = n \dim G_{\boldsymbol{e}} = nrp^{e_1+\cdots+e_r} - n \sum_{i=1}^r p^{s_i - ie_i}$ (see Proposition 7.2(b)).

9. The case, where $e_1 = \cdots = e_r$

In the special case where $n = 1$ and $e_1 = \cdots = e_r$, Theorem 1.2 tells us that $\tau(n, \boldsymbol{e}) = r$. In this section, we will give a short proof of the following stronger assertion under the assumption that k is perfect.

Proposition 9.1. *Let $\boldsymbol{e} = (e, \ldots, e)$ (r times) and L/K be purely inseparable extension of type $\boldsymbol{e}$, with $k \subset K$. Assume that the base field k is perfect. Then* $\text{ed}_p(L/K) = \text{ed}(L/K) = r$.

The assumption that k is perfect is crucial here. Indeed, by Lemma 4.4(b), there exists a field extension L/K of type $\boldsymbol{e}$. If we do not require k to be perfect, then we may set $k = K$. In this case $\text{ed}(L/K) = 0$, and the proposition fails.

The remainder of this section will be devoted to proving Proposition 9.1. We begin with two reductions.

(1) It suffices to show that

$$\mathrm{ed}(L/K) = r \quad \text{for every field extension } L/K \text{ of type } \boldsymbol{e}; \tag{9-1}$$

the identity $\mathrm{ed}_p(L/K)$ will then follow. Indeed, $\mathrm{ed}_p(L/K)$ is defined as the minimal value of $\mathrm{ed}(L'/K')$ taken over all finite extensions K'/K of degree prime to p. Here $L' = L \otimes_K K'$. Since $[L : K]$ is a power of p, L' is a field, so (9-1) tells us that $\mathrm{ed}(L'/K') = r$.

(2) The proof of the upper bound,

$$\mathrm{ed}(L/K) \leqslant r, \tag{9-2}$$

is the same as in Section 5, but in this special case the argument is much simplified. For the sake of completeness we reproduce it here. Let $x_1, \ldots, x_r$ be a normal generating sequence for L/K. By a theorem of Pickert [Rasala 1971, Theorem 1], $x_1^q, \ldots, x_r^q \in K$, where $q = p^e$. Set $a_i = x_i^q$ and $K_0 = k(a_1, \ldots, a_r)$. The structure constants of L relative to the K-basis $x_1^{d_1} \cdots x_r^{d_r}$ of L, with $0 \leqslant d_1, \ldots, d_r \leqslant q-1$ all lie in K_0. Clearly $\mathrm{trdeg}(K_0/k) \leqslant r$; the inequality (9-2) now follows from Lemma 2.1.

It remains to prove the lower bound, $\mathrm{ed}(L/K) \geqslant r$. Assume the contrary: L/K descends to L_0/K_0 with $\mathrm{trdeg}(K_0/k) < r$. By Lemma 2.1, L_0/K_0 further descends to L_1/K_1, where K_1 is finitely generated over k. By Lemma 4.6, L_1/K_1 is a purely inseparable extension of type $\boldsymbol{e}$. After replacing L/K by L_1/K_1, it remains to prove the following:

Lemma 9.2. *Let k be a perfect field and K/k be a finitely generated field extension of transcendence degree $< r$. There does not exist a purely inseparable field extension L/K of type $\boldsymbol{e} = (e_1, \ldots, e_r)$, where $e_1 \geqslant \cdots \geqslant e_r \geqslant 1$.*

Proof. Assume the contrary. Let $a_1, \ldots, a_s$ be a transcendence basis for K/k. That is, $a_1, \ldots, a_s$ are algebraically independent over k, K is algebraic and finitely generated (hence, finite) over $k(a_1, \ldots, a_s)$, and $s \leqslant r-1$. By Remark 4.3,

$$[L : L^p] \geqslant [L : (L^p \cdot K)] = p^r. \tag{9-3}$$

On the other hand, since $[L : k(a_1, \ldots, a_s)] < \infty$, Theorem 3 in [Becker and MacLane 1940] tells us that

$$[L : L^p] = [k(a_1, \ldots, a_s) : k(a_1, \ldots, a_s)^p] = [k(a_1, \ldots, a_s) : k(a_1^p, \ldots, a_s^p)] = p^s < p^r. \tag{9-4}$$

Note that the second equality relies on our assumption that k is perfect. The contradiction between (9-3) and (9-4) completes the proof of Lemma 9.2 and thus of Proposition 9.1. □

Acknowledgements

We are grateful to Madhav Nori, Julia Pevtsova, Federico Scavia, and Angelo Vistoli for stimulating discussions.

References

[Becker and MacLane 1940] M. F. Becker and S. MacLane, "The minimum number of generators for inseparable algebraic extensions", *Bull. Amer. Math. Soc.* **46** (1940), 182–186. MR Zbl

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

[Buhler and Reichstein 1997] J. Buhler and Z. Reichstein, "On the essential dimension of a finite group", *Compositio Math.* **106**:2 (1997), 159–179. MR Zbl

[Duncan 2010] A. Duncan, "Essential dimensions of A_7 and S_7", *Math. Res. Lett.* **17**:2 (2010), 263–266. MR Zbl

[Duncan and Reichstein 2015] A. Duncan and Z. Reichstein, "Versality of algebraic group actions and rational points on twisted varieties", *J. Algebraic Geom.* **24**:3 (2015), 499–530. MR Zbl

[Jacobson 1980] N. Jacobson, *Basic algebra, II*, W. H. Freeman, San Francisco, 1980. MR Zbl

[Karpilovsky 1989] G. Karpilovsky, *Topics in field theory*, North-Holland Math. Studies **155**, North-Holland, Amsterdam, 1989. MR Zbl

[Knus 1991] M.-A. Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der Math. Wissenschaften **294**, Springer, 1991. MR Zbl

[Lang 1984] S. Lang, *Algebra*, 2nd ed., Addison-Wesley, Reading, MA, 1984. MR Zbl

[Merkurjev 2009] A. S. Merkurjev, "Essential dimension", pp. 299–325 in *Quadratic forms: algebra, arithmetic, and geometry*, edited by R. Baeza et al., Contemp. Math. **493**, Amer. Math. Soc., Providence, RI, 2009. MR Zbl

[Meyer and Reichstein 2009] A. Meyer and Z. Reichstein, "The essential dimension of the normalizer of a maximal torus in the projective linear group", *Algebra Number Theory* **3**:4 (2009), 467–487. MR Zbl

[Milne 2017] J. S. Milne, *Algebraic groups*, Cambridge Studies in Adv. Math. **170**, Cambridge Univ. Press, 2017. MR Zbl

[Pickert 1949] G. Pickert, "Inseparable Körpererweiterungen", *Math. Z.* **52** (1949), 81–136. MR Zbl

[Rasala 1971] R. Rasala, "Inseparable splitting theory", *Trans. Amer. Math. Soc.* **162** (1971), 411–448. MR Zbl

[Reichstein 2010] Z. Reichstein, "Essential dimension", pp. 162–188 in *Proceedings of the International Congress of Mathematicians, II* (Hyderabad, 2010), edited by R. Bhatia et al., Hindustan Book Agency, New Delhi, 2010. MR Zbl

[Reichstein and Vistoli 2006] Z. Reichstein and A. Vistoli, "Birational isomorphisms between twisted group actions", *J. Lie Theory* **16**:4 (2006), 791–802. MR Zbl

[Reichstein and Vistoli 2018] Z. Reichstein and A. Vistoli, "Essential dimension of finite groups in prime characteristic", *C. R. Math. Acad. Sci. Paris* **356**:5 (2018), 463–467. MR Zbl

[Reichstein and Youssin 2000] Z. Reichstein and B. Youssin, "Essential dimensions of algebraic groups and a resolution theorem for G-varieties", *Canad. J. Math.* **52**:5 (2000), 1018–1056. MR Zbl

[Sancho de Salas 2000] P. J. Sancho de Salas, "Automorphism scheme of a finite field extension", *Trans. Amer. Math. Soc.* **352**:2 (2000), 595–608. MR Zbl

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Math. **67**, Springer, 1979. MR Zbl

[Serre 1997] J.-P. Serre, *Galois cohomology*, Springer, 1997. MR Zbl

[Serre 2003] J.-P. Serre, "Cohomological invariants, Witt invariants, and trace forms", pp. 1–100 in *Cohomological invariants in Galois cohomology*, Univ. Lecture Ser. **28**, Amer. Math. Soc., Providence, RI, 2003. MR

[Tossici and Vistoli 2013] D. Tossici and A. Vistoli, "On the essential dimension of infinitesimal group schemes", *Amer. J. Math.* **135**:1 (2013), 103–114. MR Zbl

[Waterhouse 1979] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Math. **66**, Springer, 1979. MR Zbl

Communicated by Susan Montgomery
Received 2018-06-28 Accepted 2018-12-24

reichst@math.ubc.ca *Department of Mathematics, University of British Columbia, Vancouver, BC, Canada*

abhisheks@math.ubc.ca *Department of Mathematics, University of British Columbia, Vancouver, BC, Canada*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US $385/year for the electronic version, and $590/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 13 No. 2 2019