Enseign. Math. (2) 71 (2025), 139–192
DOI 10.4171/LEM/1075

Hilbert's 13th problem for algebraic groups

Zinovy Reichstein

Abstract. The algebraic form of Hilbert's 13th problem asks for the resolvent degree $\mathrm{RD}(n)$ of the general polynomial $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$ of degree n, where $a_1, \dots, a_n$ are independent variables. The resolvent degree is the minimal integer d such that every root of $f(x)$ can be obtained in a finite number of steps, starting with $\mathbb{C}(a_1, \dots, a_n)$ and adjoining algebraic functions in $\leqslant d$ variables at each step. Recently Farb and Wolfson defined the resolvent degree $\mathrm{RD}_k(G)$ for every finite group G and any base field k of characteristic 0. In this setting $\mathrm{RD}(n) = \mathrm{RD}_{\mathbb{C}}(\mathrm{S}_n)$, where S_n denotes the symmetric group. In this paper we extend their definition of $\mathrm{RD}_k(G)$ to an arbitrary algebraic group G over an arbitrary field k. We investigate the dependency of this quantity on k and show that $\mathrm{RD}_k(G) \leqslant 5$ for any field k and any connected group G. The question whether $\mathrm{RD}_k(G)$ can be bigger than 1 for any field k and any algebraic group G over k (not necessarily connected) remains open.

Mathematics Subject Classification 2020: 20G10 (primary); 20G15 (secondary).

Keywords: resolvent degree, Hilbert's 13th problem, algebraic group, torsor.

1. Introduction

The algebraic forms of Hilbert's 13th problem asks for the resolvent degree $\mathrm{RD}(n)$, which is the smallest integer d such that a root of the general polynomial

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n$$

can be expressed as a composition of algebraic functions of at most d variables with complex coefficients. It is known that $\mathrm{RD}(n) = 1$ when $n \leqslant 5$, and that $1 \leqslant \mathrm{RD}(n) \leqslant n - \alpha(n)$, where $\alpha(n)$ is an unbounded but very slow growing function of n. Classical upper bounds of this form have been recently sharpened by Wolfson [51], Sutherland [45] and Heberle–Sutherland [25]. On the other hand, it is not known whether $\mathrm{RD}(n) > 1$ for any $n \geqslant 6$. For a brief informal introduction to Hilbert's 13th problem, see [34, Section 1]. For a more detailed discussion, see [17, 20].

Farb and Wolfson [20] defined the resolvent degree $\mathrm{RD}_k(G)$ for every finite group G over an arbitrary base field k of characteristic 0. In this setting $\mathrm{RD}(n) = \mathrm{RD}_{\mathbb{C}}(\mathrm{S}_n)$, and it is not known whether $\mathrm{RD}_k(G)$ can ever be > 1.

In this paper we extend their definition of $\mathrm{RD}_k(G)$ to an arbitrary algebraic group G (not necessarily finite, affine or smooth) defined over an arbitrary field k. Our definition proceeds in three steps. First we define the level of a finite field extension (Definition 4.1), then the resolvent degree of a functor (Definition 7.3), then the resolvent degree of an algebraic group (Definition 10.1). Our first main result is the following.

Theorem 1.1. *Let G be a connected algebraic group over a field k. Then:*

(a) $\mathrm{RD}_k(G) \leqslant 5$.

(b) *Moreover, if G has no simple components of type E_8, then* $\mathrm{RD}_k(G) \leqslant 1$.

Note that Theorem 1.1 was announced (in a weaker form and without proof) in Section 8 of my survey [34]. We will also investigate the dependence of $\mathrm{RD}_k(G)$ on the base field k. Our main results in this direction are Theorems 1.2 and 1.3 below.

Theorem 1.2. *Let G be an algebraic group defined over k. Then* $\mathrm{RD}_k(G) = \mathrm{RD}_{k'}(G_{k'})$ *for any field extension k'/k.*

The case where k' is algebraic over k is fairly straightforward (see Proposition 8.3 (b)); the main point here is that the extension k'/k can be arbitrary. In particular, if G is defined over $\mathbb{Z}$, when Theorem 1.2 tells us that $\mathrm{RD}_{k'}(G_{k'}) = \mathrm{RD}_k(G_k)$ for any two fields k and k' of the same characteristic. In arbitrary characteristic, we prove the following.

Theorem 1.3. *Let G be a smooth affine group scheme over $\mathbb{Z}$. Denote the connected component of G by G^0. Assume that G^0 is split reductive and G/G^0 is finite over $\mathbb{Z}$. Let k be a field of characteristic 0. Then $\mathrm{RD}_k(G_k) \geqslant \mathrm{RD}_{k_0}(G_{k_0})$ for any other field k_0.*

Theorem 1.3 bears a resemblance to [5, Theorem 2.4] and [35, Theorem 1.5], which assert analogous inequalities for essential dimension. The proofs in [5] and [35] study the behavior of essential dimension under specialization, and here we take a similar approach. In particular, Proposition 5.1, which underlies the proofs of both Theorems 1.2 and 1.3, resembles [35, Theorem 1.2]. Note, however, that this analogy is not perfect. The results we obtain for resolvent degree in this paper are stronger. Analogous results for essential dimension in [5] and [35] require additional assumptions. If we replace resolvent degree by essential dimension, then Theorem 1.3 will fail even in the case, where G is an abstract finite group; see [5, Example 3.1]. Similarly, Proposition 5.1 will fail if we replace the level by the essential dimension; see [35, Lemma 9.1 (c)].

We also remark that both Theorems 1.2 and 1.3 apply in the classical setting of Hilbert's 13th problem, where G is the symmetric group S_n (or any other abstract finite group), viewed as a group scheme over $\mathbb{Z}$.

A key role in our proof of Theorem 1.1 (b) will be played by a theorem of Tits, which asserts that if G is a simple group over k of any type other than E_8 and $T \to \mathrm{Spec}(K)$ is a G-torsor, then T can be "split by radicals," i.e., T splits over some radical extension of K; see Section 16. Tits asked whether the same is true for simple groups of type E_8. Using the arguments in Section 16, one readily sees that a positive answer to this question would imply the following.

Conjecture 1.4. $\mathrm{RD}_k(G) \leqslant 1$ for any connected algebraic group G over any field k.

Theorem 1.1 (a) (or more precisely, Proposition 16.1 (a)) may thus be viewed as a partial answer to Tits' question. Note that it is not known whether $\mathrm{RD}_k(G)$ can be > 1 for any field k and any algebraic group G defined over k (not necessarily connected).

The remainder of this paper is structured as follows. Sections 2 and 3 are devoted to preliminary material on essential dimension of finite-dimensional algebras and field extensions. Section 4 defines the level of a finite field extension and explores its elementary properties. Section 5 studies how the level changes under specialization. Section 6 introduces the level d closure of a field. The resolvent degree of a functor is introduced in Section 7. This notion parallels the notion of essential dimension of a functor, due to Merkurjev, Berhuy and Favi [1] but the type of functor we allow is more restrictive. Much of the work towards proving Theorems 1.1–1.3 is, in fact, done in the general setting of functors in Sections 8 and 9. Section 10 introduces the notion of resolvent degree of an algebraic group. In Section 11 we study the resolvent degree of infinitesimal groups and abelian varieties. The proof of Theorem 1.2 is completed in Section 12, the proof of Theorem 1.3 in Section 13, and the proof of Theorem 1.1 in Sections 14–16. In the last section we show that Conjecture 1.4 follows from a positive answer to a long-standing open question of Serre (Question 17.1).

The main focus of this paper is on the aspects of the subject which have not been previously investigated: resolvent degree of connected groups and dependence of resolvent degree on the base field. However, many of the preliminary results overlap with existing literature and some have classical roots. In particular, Section 4 overlaps with [20, Section 2], Section 10 with [20, Section 3]. Section 6 elaborates on the short note of Arnold and Shimura [6, pp. 45–46]; there is also some overlap between Section 14 and [51, Section 4]. I have tried to indicate these connections throughout the paper. I have also included independent characteristic-free proofs for most background results, with the goal of making the exposition largely self-contained. The arguments in this paper are mostly algebraic and valuation-theoretic, with only a few exceptions (e.g., in Section 14). I have not included references to classical literature; an interested reader can find them in [20] or [51, Appendix B].

2. Preliminaries on finite-dimensional algebras

Let K be a field and A be finite-dimensional K-algebra. We will say that A descends to a subfield K_0 of K if there exists a K_0-algebra A_0 such that $A \simeq_K A_0 \otimes_{K_0} K$. Here $\simeq_K$ stands for isomorphism of algebras over K. We will sometimes say that A/K descends to A_0/K_0.

Lemma 2.1. *Let $k \subset K$ be a field extension, A be a finite-dimensional K-algebra, and S a finite subset of A. Then there exist an intermediate subfield $k \subset K_0 \subset K$ and a finite-dimensional K_0-algebra A_0 over K_0 such that:*

- *K_0 finitely generated over k.*
- *A/K descends to A_0/K_0, i.e., A is K-isomorphic to $A_0 \otimes_{K_0} K$. In particular, we may identify A_0 with a K_0-subalgebra of A.*
- *$S \subset A_0$.*

Proof. Choose a K-vector space basis $b_1, \dots, b_n$ in A. Write $b_i \cdot b_j = \sum_{h=1}^n c_{ij}^h b_h$ for every $i, j = 1, \dots, n$ and $s = \sum_{h=1}^n \alpha_s^h b_h$ for every $s \in S$. Let

$$K_0 = k\big(c_{ij}^h, \alpha_s^h \mid i, j, h = 1, \dots, n \text{ and } s \in S\big)$$

and A_0 be the K_0-subalgebra of A generated by $b_1, \dots, b_n$. Then one readily sees that K_0 is finitely generated over k, the natural map $A_0 \otimes_{K_0} K \to A$ is an isomorphism over K, and $S \subset A_0$. ∎

Definition 2.2. Let K be a field containing k and A be a finite-dimensional K-algebra. The essential dimension $\mathrm{ed}_k(A/K)$ is the minimal value of the transcendence degree $\mathrm{trdeg}_k(K_0)$, where the minimum is taken over all intermediate fields $k \subset K_0 \subset K$ such that A/K descends to K_0.

Lemma 2.3. *Let K be a field containing k and A a finite-dimensional K-algebra. Then $\mathrm{ed}_k(A/K) < \infty$. Moreover, A/K descends to some A_0/K_0 such that K_0 is finitely generated over k and $\mathrm{ed}_k(A/K) = \mathrm{ed}_k(A_0/K_0) = \mathrm{trdeg}_k(K_0)$.*

Proof. Descend A/K to A_1/K_1 so that $d = \mathrm{trdeg}_k(K_1)$ is the smallest possible, i.e., $d = \mathrm{ed}_k(A/K)$. Note that a priori d is a non-negative integer or ∞. By Lemma 2.1,

A_1/K_1 further descends to A_0/K_0, where $k \subset K_0 \subset K_1$ and K_0 is finitely generated over k. By the minimality of d, $\mathrm{ed}_k(A/K) = \mathrm{ed}_k(A_1/K_1) = \mathrm{ed}_k(A_0/K_0) = \mathrm{trdeg}_k(K_0) = d$. Moreover, since K_0 is finitely generated over k, $d < \infty$. ■

Lemma 2.4. *Let $k \subset k' \subset K$ be fields and A be a finite-dimensional K-algebra. Then:*

(a) $\mathrm{ed}_{k'}(A/K) \leqslant \mathrm{ed}_k(A/K)$.

(b) *If k' is algebraic over k, then* $\mathrm{ed}_{k'}(A/K) = \mathrm{ed}_k(A/K)$.

(c) *There exists an intermediate field $k \subset l_0 \subset k'$ such that l_0 is finitely generated over k and* $\mathrm{ed}_l(A/K) = \mathrm{ed}_{k'}(A/K)$ *for any $l_0 \subset l \subset k'$.*

Proof. (a) Suppose A descends to a subfield $K_0 \subset K$ containing k such that $\mathrm{trdeg}_k(K_0)$ is as small as possible, i.e., $\mathrm{trdeg}_k(K_0) = \mathrm{ed}_k(A/K)$. Then A also descends to $k'K_0$, where the compositum is taken in K. Now $\mathrm{ed}_{k'}(A/K) \leqslant \mathrm{trdeg}_{k'}(k'K_0) \leqslant \mathrm{trdeg}_k(K_0) = \mathrm{ed}_k(A/K)$.

(b) In view of part (a), it suffices to show that $\mathrm{ed}_k(A/K) \leqslant \mathrm{ed}_{k'}(A/K)$. Indeed, A descends to some intermediate field $k' \subset K_0' \subset K$ such that $\mathrm{trdeg}_{k'}(K_0') = \mathrm{ed}_{k'}(A/K)$. If k' is algebraic over k, then $\mathrm{ed}_k(A/K) \leqslant \mathrm{trdeg}_k(K_0') = \mathrm{trdeg}_{k'}(K_0) = \mathrm{ed}_{k'}(A/K)$.

(c) By Lemma 2.3, A/K descends to some A_0/K_0 such that $k' \subset K_0 \subset K$, $\mathrm{ed}_{k'}(A/K) = \mathrm{ed}_{k'}(A_0/K_0) = \mathrm{trdeg}_{k'}(K_0)$ and K_0 is generated by finitely many elements over k', say $K_0 = k'(a_1, \dots, a_m)$.

Let $x_1, \dots, x_m$ be independent variables over k'. For each subset $I = \{i_1, \dots, i_r\} \subset \{1, 2, \dots, m\}$, such that the elements $a_{i_1}, \dots, a_{i_r}$ are algebraically dependent over k', choose a polynomial $0 \neq p_I(x_{i_1}, \dots, x_{i_r}) \in k'[x_{i_1}, \dots, x_{i_r}]$ such that $p_I(a_{i_1}, \dots, a_{i_r}) = 0$. Now choose an intermediate field $k \subset l_0 \subset k'$ such that l_0 is generated (over k) by the coefficients of the polynomials p_I for every such I. With this choice of l_0, any subset of $\{a_1, \dots, a_m\}$ which is algebraically dependent over k' remains algebraically dependent in l_0. In other words, $\mathrm{trdeg}_{l_0}(K_0) = \mathrm{trdeg}_{k'}(K_0)$ and thus

$$\mathrm{ed}_{l_0}(A/K) \leqslant \mathrm{trdeg}_{l_0}(K_0) = \mathrm{trdeg}_{k'}(K_0) = \mathrm{ed}_{k'}(A/K). \tag{1}$$

By part (a), $\mathrm{ed}_{l_0}(A/K) \geqslant \mathrm{ed}_l(A/K) \geqslant \mathrm{ed}_{k'}(A/K)$ for any intermediate field $l_0 \subset l \subset k'$. Now (1) tells us that both of these inequalities are, in fact, equalities, as desired. ■

3. Preliminaries on field extensions

We will be particularly interested in the case where the finite-dimensional K-algebra A is itself a field. In this case we will usually use the letter L in place of A and write $\mathrm{ed}_k(L/K)$ in place of $\mathrm{ed}_k(A/K)$.

Lemma 3.1. *Let $k \subset K \subset L$ be field extensions such that $[L : K] < \infty$.*

(a) *If $K^{\rm sep}$ is the separable closure of K in L, then $\mathrm{ed}_k(K^{\rm sep}/K) \leqslant \mathrm{ed}_k(L/K)$ and $\mathrm{ed}_k(L/K^{\rm sep}) \leqslant \mathrm{ed}_k(L/K)$.*

(b) *If L is separable over K, and $L^{\rm norm}$ is the normal closure of L, then $\mathrm{ed}_k(L/K) = \mathrm{ed}_k(L^{\rm norm}/K)$.*

(c) *Suppose $K \subset E \subset L$ is an intermediate extension. If E is separable over K, then $\mathrm{ed}_k(E/K) \leqslant \mathrm{ed}_k(L/K)$.*

Proof. (a) Suppose L/K descends to L_0/K_0. Denote the separable closure of K_0 in L_0 by $(K_0)^{\rm sep}$. Then $K^{\rm sep}/K$ descends to $K_0^{\rm sep}/K_0$, $L/K^{\rm sep}$ descends to $L_0/(K_0)^{\rm sep}$ and part (a) follows.

(b) is proved in [7, Lemma 2.3].

(c) In view of part (a), it suffices to show that $\mathrm{ed}_k(E/K) \leqslant \mathrm{ed}_k(K^{\rm sep}/K)$. In other words, we may replace L by $K^{\rm sep}$ and thus assume without loss of generality that L is separable over K. By (b), we may further replace L by its normal closure over K and thus assume that L is Galois over K. Then $E = L^H$, where H is a subgroup of $G = \mathrm{Gal}(L/K)$. By [7, Lemma 2.2], L/K descends to some L_0/K_0, where $k \subset K_0 \subset K$, $\mathrm{trdeg}_k(K_0) = \mathrm{ed}_k(L/K)$, and L_0 is a G-invariant subfield of L. Then E/K descends to L_0^H/K_0. This tells us that $\mathrm{ed}_k(E/K) \leqslant \mathrm{trdeg}_k(K_0) = \mathrm{ed}_k(L/K)$, as desired. ∎

We will say that a field extension L/K is simple if $[L : K] < \infty$ and L is generated by one element over K. In other words, $L \simeq K[x]/(f(x))$, where $f(x) \in K[x]$ is an irreducible polynomial over K. By the primitive element theorem, every finite separable extension is simple.

Lemma 3.2. *Suppose a field extension L/K of finite degree descends to L_0/K_0. Then L/K is simple if and only if L_0/K_0 is simple.*

Proof. One direction is obvious: if $L_0 = K_0(a)$ is simple, then $L = K(a)$ is also simple.

To prove the converse, assume that L/K is simple and set $n = [L : K] = [L_0 : K_0]$. If K_0 is a finite field, then so is L_0. In this case L_0/K_0 is separable and hence, simple. Thus, we may assume that K_0 is infinite. It suffices to show that L_0 contains an element of degree n over K_0. View L_0 as the set of K_0-points of the n-dimensional affine space $\mathbb{A}^n$, and L as the set of K-points of $\mathbb{A}^n$.

Let $X \subset \mathbb{A}^n$ be the subscheme of $\mathbb{A}^n$ determined by the condition that for $x \in \mathbb{A}^n_{K_0}$, $1, x, \dots, x^{n-1}$ are linearly dependent. More precisely, suppose $b_1, \dots, b_n$ is a K_0-basis of L_0. For simplicity, let us assume that $b_1 = 1$. Write

$$b_i b_j = \sum_{h=1}^{n} c_{ij}^h b_h, \tag{2}$$

where the structure constants c_{ij}^h lie in K_0. Set $x = x_1 b_1 + \cdots + x_n b_n$, where $x_1, \ldots, x_n$ are independent variables. Using formulas (2), for every $i \geqslant 0$ we can express x^i in the form $x^i = p_{i,1} b_1 + \cdots + p_{i,n} b_n$, where each $p_{i,j}$ is a polynomial in $x_1, \ldots, x_n$ with coefficients in K_0. We now define X to be the hypersurface in $\mathbb{A}^n_{K_0}$ cut out by the polynomial

$$\det \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,1} & p_{m,2} & \cdots & p_{m,n} \end{pmatrix} = 0.$$

For any field extension F/K_0, an F-point $(\alpha_1, \ldots, \alpha_n) \in X(F)$ represents an element $x = \alpha_1 b_1 + \cdots + \alpha_n b_n$ of $L_0 \otimes_{K_0} F$ such that $1, x, \ldots, x^{n-1}$ are linearly dependent over F.

In particular, $X(K_0)$ is the set of elements of L_0 of degree $\leqslant n-1$ over K_0 and $X(K)$ is the set of elements of L of degree $\leqslant n-1$ over K. We know that L/K is simple; hence, $X \subsetneq \mathbb{A}^n$. That is, $U = \mathbb{A}^n \setminus X$ is a non-empty Zariski open subscheme of $\mathbb{A}^n$ defined over K_0. Since K_0 is an infinite field, we conclude that $U(K_0) \neq \emptyset$. In other words, L_0/K_0 is simple, as claimed. ∎

Lemma 3.3. *Let $k \subset K \subset L$ be fields such that L/K is simple. Assume K'/K is another field extension (not necessarily finite), and $L' = K'L$ be a compositum of K' and L over K. Then* $\mathrm{ed}_k(L'/K') \leqslant \mathrm{ed}_k(L/K)$.

Note that Lemma 3.3 is immediate from the definition of $\mathrm{ed}_k(L/K)$ in the case, where $L' \simeq L \otimes_K K'$ or equivalently, $[L' : K'] = [L : K]$. The only (slight) complication arises from the fact that $[L' : K']$ may be smaller than $[L : K]$.

Proof. Set $n = [L : K]$ and $d = \mathrm{ed}_k(L/K)$. Then L/K descends to some intermediate field $k \subset K_0 \subset K$ such that $\mathrm{trdeg}_k(K_0) = d$. That is, there exists a field extension L_0/K_0 such that $L \simeq_K L_0 \otimes_{K_0} K$, where $\simeq_{K_0}$ denotes an isomorphism of fields over K_0.

By Lemma 3.2, L_0/K_0 is simple. That is, $L_0 \simeq_{K_0} K_0[x]/(f(x))$, where $f(x) \in K_0[x]$ is a polynomial of degree n, irreducible over K_0. Then $L \simeq_K K[x]/(f(x))$. Now let $f(x) = f_1(x) \ldots f_r(x)$ be an irreducible decomposition of $f(x)$ over K'. A compositum L' of L and K' is isomorphic to $K'[x]/(f_i(x))$ for some i, say,

$L' \simeq_{K'} K'[x]/(f_1(x))$. Denote the degree of $f_1(x)$ by $n_1 = [L' : K']$ and the roots of f_1 in the algebraic closure of K by $\alpha_1, \dots, \alpha_{n_1}$. Since each α_i is a root of $f(x) \in K_0[x]$, each α_i algebraic over K_0. Hence, the coefficients of $f_1(x)$, being elementary symmetric polynomials in $\alpha_1, \dots, \alpha_{n_1}$, are also algebraic over K_0. This shows that $f_1(x) \in K_0^{\mathrm{alg}}[x]$, where K_0^{alg} is the algebraic closure of K_0 in K. In other words, L'/K' descends to K_0^{alg}. Consequently,

$$\mathrm{ed}_k(L'/K') \leqslant \mathrm{trdeg}_k\big(K_0^{\mathrm{alg}}\big) = \mathrm{trdeg}_k(K_0) = d = \mathrm{ed}_k(L/K),$$

as desired. ∎

Lemma 3.4. *Let $k \subset K \subset L$ be fields such that $[L : K] < \infty$. Then there exist intermediate extensions $K = K^{(0)} \subset K^{(1)} \subset \cdots \subset K^{(r)} = L$ such that $K^{(i)}/K^{(i-1)}$ is simple and* $\mathrm{ed}_k(K^{(i)}/K^{(i-1)}) \leqslant \mathrm{ed}_k(L/K)$ *for every $i = 1, \dots, r$.*

Proof. Set $d = \mathrm{ed}_k(L/K)$. By definition, L/K descends to L_0/K_0, where $k \subset K_0 \subset K$ and $\mathrm{trdeg}_k(K_0) = d$. Let $\alpha_1, \dots, \alpha_r$ be generators for L_0 over K_0 and set $K_0^{(i)} = K_0(\alpha_1, \dots, \alpha_i)$ and $K^{(i)} = K(\alpha_1, \dots, \alpha_i)$. We obtain the following diagram:

$$\begin{array}{ccccccc} K = K^{(0)} & \hookrightarrow & K^{(1)} & \hookrightarrow \cdots \hookrightarrow & K^{(r)} = L \\ | & & | & & | \\ K_0 = K_0^{(0)} & \hookrightarrow & K_0^{(1)} & \hookrightarrow \cdots \hookrightarrow & K_0^{(r)} = L_0. \end{array}$$

By our construction, the extension $K^{(i)}/K^{(i-1)}$ is simple for each $i = 1, \dots, r$. Moreover,

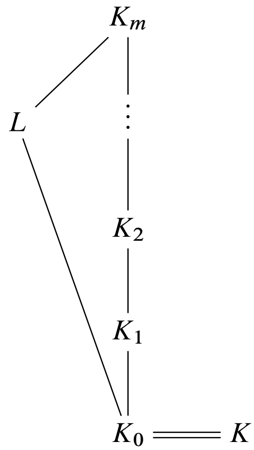
$$\mathrm{ed}_k\big(K^{(i)}/K^{i-1}\big) \leqslant \mathrm{trdeg}_k\big(K_0^{(i-1)}\big) = d$$

because $K^{(i)}/K^{(i-1)}$ descends to $K_0^{(i)}/K_0^{(i-1)}$ for each i. ∎

4. The level of a finite field extension

We now define the level of a field extension, following Dixmier [17, Section 2].

Definition 4.1. Let k be a base field, K be a field containing k, and L/K be a field extension of finite degree. I will say that L/K is of level $\leqslant d$ if there exists a diagram of field extensions

(3) 

such that $[K_i : K_{i-1}] < \infty$ and $\mathrm{ed}_k(K_i/K_{i-1}) \leqslant d$ for every $i = 1, \dots, m$. The level of L/K is the smallest such d; I will denote it by $\mathrm{lev}_k(L/K)$.

Remarks 4.2. (1) The same notion was introduced by Brauer [2] (in characteristic 0) under the name of resolvent degree. In this paper we will reserve the term "resolvent degree" for the resolvent degree of an object of a functor; see Definition 7.3. If L/K is a finite separable extension, then we may view L/K as an object of the functor of étale algebras, and the two notions coincide; see Example 7.5.

(2) (Cf. [20, Lemma 2.5.3].) If $k \subset K \subset L' \subset L$ and $[L : K] < \infty$, then $\mathrm{lev}_k(L'/K) \leqslant \mathrm{lev}_k(L/K)$. Indeed, any tower (3) showing that $\mathrm{lev}_k(L/K) \leqslant d$ also shows that $\mathrm{lev}_k(L'/K) \leqslant d$.

(3) (Cf. [20, Lemma 2.5.1].) Taking $m = 1$ and $K_1 = L$ in (3), we see that $\mathrm{lev}_k(L/K) \leqslant \mathrm{ed}_k(L/K)$.

(4) We may assume without loss of generality that each extension K_i/K_{i-1} in the tower (3) is simple. Indeed, by Lemma 3.4, we may replace K_i/K_{i-1} by a sequence of simple extensions without increasing the essential dimension.

(5) Definition 4.1 formalizes the classical notion of composition of algebraic functions. If K is a field of rational functions on some algebraic variety X defined over k, then it is natural to think of K_1 as being generated by algebraic (multi-valued) functions on X in $\leqslant \mathrm{ed}_k(K_1/K)$ variables, and K_i as being generated by compositions of i algebraic functions on X in $\leqslant \mathrm{lev}_k(L/K)$ variables.

(6) No examples where $\mathrm{lev}_k(L/K) > 1$ are known.

Lemma 4.3. *Assume that $k \subset k' \subset K \subset L$ are fields and $[L : K] < \infty$. Then:*

(a) (Cf. [20, Lemma 2.5.2].) $\mathrm{lev}_k(L/K) \geqslant \mathrm{lev}_{k'}(L/K)$.

(b) *Moreover, equality holds if k' is algebraic over k.*

(c) *Furthermore, there exists an intermediate field $k \subset l_0 \subset k'$ such that l_0 is finitely generated over k and $\mathrm{lev}_l(L/K) = \mathrm{lev}_{k'}(L/K)$ for every field l between l_0 and k'.*

Proof. Choose a tower $K = K_0 \subset K_1 \subset \cdots \subset K_m$, as in Definition 4.1, and apply parts (a), (b) and (c) of Lemma 2.4, respectively, to each intermediate extension K_i/K_{i-1}. In part (c), let l_i/k be a finitely generated field extension obtained by applying Lemma 2.4 (c) to K_i/K_{i-1}. Now set l_0 to be the compositum of $l_1, \ldots, l_m$ in k' over k. ∎

Lemma 4.4 (cf. [20, Lemma 2.5.3]). *Assume that $k \subset K \subset L$ are fields and $[L : K] < \infty$ and let $K \subset K'$ be another field extension (not necessarily finite). Then*

$$\mathrm{lev}_k(K'L/K') \leqslant \mathrm{lev}_k(L/K).$$

Here $K'L$ denotes an arbitrary compositum of K' and L over K.

Proof. Set $d = \mathrm{lev}_k(L/K)$ and choose a tower $K = K_0 \subset K_1 \subset \cdots \subset K_m$ as in Definition 4.1. By Remark 4.2 (4) we may assume that each intermediate extension K_i/K_{i-1} is simple. Now consider the tower

$$K' = K'_0 \subset K'_1 \subset \cdots \subset K'_m.$$

Here $K'_m = K'K_m$ is some compositum of K' and K_m, and for $i = 0, \ldots, m-1$, $K'_i = K'K_i$ is the compositum of K' and K_i in K'_m. Since $K \subset L \subset K_m$, $K'L$ embeds into $K'K_m$ over K. Since K_i/K_{i-1} is simple, Lemma 3.3 tells us that $\mathrm{ed}_k(K'_i/K'_{i-1}) \leqslant d$. We conclude that $\mathrm{lev}_k(K'L/K') \leqslant d$. ∎

Lemma 4.5. *Assume that $k \subset K \subset L$ are fields and $[L : K] < \infty$. Then $\mathrm{lev}_k(L/K) = 0$ if and only if L embeds in a compositum $\overline{k}K$ over k. In particular, if k is algebraically closed, then $\mathrm{lev}_k(L/K) = 0$ if and only if $L = K$.*

Proof. The second assertion is an immediate consequence of the first.

To prove the first assertion, suppose $L \subset \overline{k}K$. In other words, L/K is generated by elements $\alpha_1, \ldots, \alpha_m \in L$ which are algebraic over k. Consider the tower of simple extensions

$$k = k_0 \subset k_1 \subset \cdots \subset k_m,$$

where $k_i = k(\alpha_1, \dots, \alpha_s)$. Since $\operatorname{trdeg}_k(k_i) = 0$, we have $\operatorname{ed}_k(k_i/k_{i-1}) = 0$ for every $i = 1, \dots, m$. Now consider the tower

$$K = k_0 K \subset k_1 K \subset \cdots \subset k_m K = L.$$

By Lemma 3.3, $\operatorname{ed}_k(k_i K/k_{i-1}K) \leqslant \operatorname{ed}_k(k_i/k_{i-1}) = 0$. Thus, $\operatorname{lev}_k(L/K) = 0$.

Conversely, suppose $\operatorname{lev}_k(L/K) = 0$. Then there exists a tower (3) of field extensions such that $L \subset K_m$ (over K) and $\operatorname{ed}_k(K_i/K_{i-1}) = 0$ for each i. Consequently, K_i is generated over K_{i-1} by elements that are algebraic over k. This implies that K_m embeds in $\overline{k}K$ over K, and hence, so does L. ■

Recall that a finite field extension L/K is called radical if there exists a tower (3) such that $K_i = K_{i-1}(\lambda)$, where $\lambda^{n_i} \in K$ for some $n_i \geqslant 1$, $i = 1, \dots, m$.

Lemma 4.6. *Let K be a field containing k and L/K be a finite field extension. Assume that L/K is*

(a) *solvable,*

(b) *radical, or*

(c) *purely inseparable.*

Then $\operatorname{lev}_k(L/K) \leqslant 1$.

Proof. By definition L/K is solvable if there exists a tower $K = K_0 \subset K_1 \subset \cdots \subset K_m$, as in (3), such that L embeds into K_m over K and K_i is of the form $K_{i-1}(\lambda_i)$ for each $i = 1, \dots, m$, where λ_i is a root of a polynomial of the form

(i) $x^{n_i} - a_i$ or

(ii) $x^{n_i} - x - a_i$

for some positive integer n_i and $a_i \in K_{i-1}$.

Note that (i) covers the case, where λ_i is a root of unity ($a_i = 1$), and (ii) is only needed when $n_i = \operatorname{char}(k) > 0$. In both cases $K_i = k(\lambda)K_{i-1}$ and thus

$$\operatorname{ed}_k(K_i/K_{i-1}) \leqslant \operatorname{ed}_k(k(\lambda)/k(a_i)) \leqslant 1.$$

Here the first inequality follows from Lemma 3.3. The second inequality is obvious, since $\operatorname{trdeg}_k(k(a_i)) \leqslant 1$. Thus, $\operatorname{lev}_k(L/K) \leqslant 1$. This proves (a).

(b) is proved by the same argument, except that case (ii) does not occur.

(c) follows from (b) because every purely inseparable extension is radical. ■

Lemma 4.7 (cf. [20, Lemma 2.7]). *Let K be a field containing k and L/K and M/L be field extensions of finite degree. If* $\operatorname{lev}_k(L/K) \leqslant d$ *and* $\operatorname{lev}_k(M/L) \leqslant d$, *then*

$$\operatorname{lev}_k(M/K) \leqslant d.$$

Proof. Choose a tower $K = K_0 \subset K_1 \subset \cdots \subset K_m$ for L/K as in (3), and a similar tower $L = L_0 \subset L_1 \subset \cdots \subset L_n$ for M/L. That is, L embeds into K_m over K, M embeds into L_n over L, $\mathrm{ed}_k(K_i/K_{i-1}) \leqslant d$ and $\mathrm{ed}_k(L_j/L_{j-1}) \leqslant d$ for every $i = 1, \dots, m$ and $j = 1, \dots, n$. By Remark 4.2 (4) we may assume that all intermediate extensions K_i/K_{i-1} and L_j/L_{j-1} are simple. Let $\overline{K}$ be an algebraic closure of K. Fix embeddings $K_m \hookrightarrow \overline{K}$ and $L_n \hookrightarrow \overline{K}$ and consider the tower of simple extensions

$$K_0 \subset K_1 \subset \cdots \subset K_m = K_m L_0 \subset K_m L_1 \subset \cdots \subset K_m L_n,$$

where $K_m L_i$ is the compositum of K_m and L_i in $\overline{K}$. Clearly, $M \subset L_n \subset K_m L_n$. Thus, it suffices to show that

(i) $\mathrm{ed}_k(K_i/K_{i-1}) \leqslant d$ for every $i = 1, \dots, m$ and

(ii) $\mathrm{ed}_k(K_m L_j/K_m L_{j-1}) \leqslant d$ for every $j = 1, \dots, n$.

(i) follows from our choice of the tower $K_0 \subset K_1 \subset \cdots \subset K_m$. On the other hand, by Lemma 3.3, $\mathrm{ed}_k(K_m L_j/K_m L_{j-1}) \leqslant \mathrm{ed}_k(L_j/L_{j-1})$, and by our choice of the tower $L_0 \subset L_1 \cdots \subset L_n$, $\mathrm{ed}_k(L_j/L_{j-1}) \leqslant d$ for every $j = 1, \dots, n$. This proves (ii). ■

Lemma 4.8 (cf. [20, Lemma 2.11]). *Let $k \subset K \subset L$ be fields. Assume that the field extension L/K is finite and separable. Denote the normal closure of L over K by L^{norm}. Then $\mathrm{lev}_k(L/K) = \mathrm{lev}_k(L^{\mathrm{norm}}/K)$.*

Proof. By Remark 4.2 (2), $\mathrm{lev}_k(L/K) \leqslant \mathrm{lev}_k(L^{\mathrm{norm}}/K)$. We will thus focus on proving the opposite inequality.

Set $d = \mathrm{lev}(L/K)$. By the primitive element theorem, $L \simeq_K K[x]/f(x)$ for some irreducible polynomial $f(x) \in K[x]$. Then $f(x)$ splits into a product of linear factors over L^{norm}. Denote its roots in L^{norm} by $\alpha_1, \dots, \alpha_n$. Set $L_i = K(\alpha_1, \dots, \alpha_i)$; in particular, $L_0 = K$. We claim that $\mathrm{lev}_k(L_i/L_{i-1}) \leqslant d$ for each $i = 1, \dots, n$. If we can prove this claim, then applying Lemma 4.7 recursively, we obtain the desired inequality

$$\mathrm{lev}_k(L^{\mathrm{norm}}/K) = \mathrm{lev}_k(L_n/K) \leqslant d = \mathrm{lev}_k(L/K).$$

It thus remains to prove the claim. Since L_i is a composite of L_{i-1} and $K(\alpha_i) \simeq_K L$ for each i, Lemma 4.4 tells us that

$$\mathrm{lev}_k(L_i/L_{i-1}) = \mathrm{lev}(L_{i-1}K(\alpha_i)/L_{i-1}) \leqslant \mathrm{lev}_k(K(\alpha_i)/K) = \mathrm{lev}_k(L/K) = d,$$

as claimed. ■

Proposition 4.9 (cf. [20, Lemma 2.12]). *Let $k \subset K \subset L$ be fields, where $[L : K] < \infty$. Assume that $\mathrm{lev}_k(L/K) \leqslant d$. Then the tower*

$$K = K_0 \subset \cdots \subset K_m$$

of field extensions in Definition 4.1 can be chosen to have the following additional properties.

(a) *Each field extension K_i/K_{i+1} is simple and either separable or purely inseparable.*

(b) *If K_i/K_{i-1} is separable, then it is Galois.*

(c) *If K_i/K_{i-1} is Galois, then* $\mathrm{Gal}(K_i/K_{i-1})$ *is a finite simple group.*

Proof. We will start with a tower $K = K_0 \subset K_1 \subset \cdots \subset K_m$ of Definition 4.1. By Remark 4.2 (4), we may assume that each intermediate extension K_i/K_{i-1} is simple. We will now modify this tower in three steps (a), (b) and (c), so that it acquires properties (a), (b), and (c) from the statement of the proposition, respectively. At each stage m may increase and the fields K_i may change, but every K_i/K_{i-1} will remain simple, the largest field K_m will either get larger or stay the same (and in particular, it will continue to contain L), and the maximal value of $\mathrm{ed}_k(K_i/K_{i-1})$ will not increase (so that it will remain $\leqslant d$).

(a) Let K_{i-1}^{sep} be the separable closure of K_{i-1} in K_i. If K_i/K_{i-1} is neither separable nor purely inseparable, i.e., $K_{i-1} \subsetneq K_{i-1}^{\mathrm{sep}} \subsetneq K_i$, we insert K_{i-1}^{sep} between K_{i-1} and K_i. Note that $K_i/K_{i-1}^{\mathrm{sep}}$ is simple because K_i/K_{i-1} is, and $K_{i-1}^{\mathrm{sep}}/K_{i-1}$ is simple by the primitive element theorem. Now relabel $K_0, K_1, \ldots$ to absorb the newly inserted fields. By our construction each K_i/K_{i-1} is simple and either separable or purely inseparable. The maximal value of $\mathrm{ed}_k(K_i/K_{i-1})$ does not increase by Lemma 3.1 (a).

(b) If K_1/K_0 is purely inseparable, do nothing. If K_1/K_0 is separable, replace K_1 by its normal closure K_1^{norm} and K_i by $K_1^{\mathrm{norm}}K_i$ for each $i \geqslant 2$. All newly created extensions K_1^{norm}/K_0 and $K_1^{\mathrm{norm}}K_i/K_1^{\mathrm{norm}}K_{i-1}$ ($i \geqslant 2$), remain simple and either separable or purely inseparable. Moreover, for every $i \geqslant 2$, $\mathrm{ed}_k(K_1^{\mathrm{norm}}/K_0) = \mathrm{ed}_k(K_1/K_0)$ by Lemma 3.1 (b) and $\mathrm{ed}_k(K_1^{\mathrm{norm}}K_i/K_1^{\mathrm{norm}}K_{i-1}) \leqslant \mathrm{ed}_k(K_i/K_{i-1})$ by Lemma 3.3.

Now relabel $K_0, K_1, \ldots$ and do the same for the extension K_2/K_1. That is, if K_2/K_1 is purely inseparable, then do nothing. If K_2/K_1 is separable, replace K_2 by its normal closure K_2^{norm}, and K_i by $K_2^{\mathrm{norm}}K_i$ for every $i \geqslant 3$. Proceed recursively: do the same thing for the extension K_3/K_2, then (after suitably modifying $K_3, \ldots, K_m$) for the extension K_4/K_3, etc. When all of these modifications are completed, the resulting tower $K = K_0 \subset K_1 \subset \cdots \subset K_m$ will have properties (a) and (b).

(c) If K_i/K_{i-1} is purely inseparable, do nothing. If it is Galois and $G = \mathrm{Gal}(K_i/K_{i-1})$ is simple, again do nothing. If not – say if G has a proper normal subgroup N – insert K_i^N between K_{i-1} and K_i. By Lemma 3.1 (c), $\mathrm{ed}_k(K_i/K_i^N)$ and

$\mathrm{ed}_k(K_i^N/K_{i-1})$ are both $\leqslant \mathrm{ed}_k(K_i/K_{i-1})$. Thus, the maximal value of $\mathrm{ed}_k(K_i/K_{i-1})$ does not increase. Proceeding recursively, we arrive at a tower of field extensions satisfying (a), (b) and (c). ∎

5. Extensions of valued fields

Throughout this section we will assume the following:

(1) $k \subset K \subset L$ are fields and $[L : K] < \infty$.

(2) K and L are complete relative to a discrete valuation $\nu\colon L^* \to \mathbb{Z}$.

(3) We will denote the residue fields of k, K and L by k_ν, K_ν and L_ν, respectively.

Note that we do not require k to be complete. Our goal is to compare $\mathrm{lev}_k(L/K)$ to $\mathrm{lev}_{k_\nu}(L_\nu/K_\nu)$. Our main result is as follows.

Proposition 5.1. $\mathrm{lev}_{k_\nu}(L_\nu/K_\nu) \leqslant \max\{\mathrm{lev}_k(L/K), 1\}$.

Our proof of Proposition 5.1 will rely on the following lemma comparing the essential dimensions of L/K and L_ν/K_ν.

Lemma 5.2. *In addition to notational conventions (1), (2), (3), assume that L/K is a Galois extension, and the Galois group $H = \mathrm{Gal}(L/K)$ is a finite simple group.*

(a) *Then one of the following holds.*

  (i) *L/K is totally ramified and L_ν is purely inseparable over K_ν; or*

  (ii) *L/K is totally unramified and L_ν/K_ν is an H-Galois extension, where the H-action on L_ν is induced from the H-action on L.*

(b) *Moreover, if H is non-abelian and L/K is totally unramified, then*

$$\mathrm{ed}_{k_\nu}(L_\nu/K_\nu) \leqslant \mathrm{ed}_k(L/K).$$

Proof of Lemma 5.2. (a) Since K is complete, ν is the unique valuation of L lying over $\nu_{|K^*}$; see [38, Proposition II.2.3 and Corollary II.2.2]. Thus, ν remains invariant under the action of H, and this action descends to L_ν. In other words, the decomposition group $D_\nu(L/K)$ is all of H. Let K_{un}/K be the largest unramified subextension of L/K; it exists by [38, Corollary 3 to Theorem III.5.3]. Clearly K_{un} is invariant under the action of H. Hence, $\mathrm{Gal}(L/K_{\mathrm{un}})$ is a normal subgroup of H. Since H is simple, there are only two possibilities: either

(i) $K_{\mathrm{un}} = K$, i.e., L/K is totally ramified; or

(ii) $K_{\mathrm{un}} = L$, i.e., L/K is unramified.

In case (i), L_ν is purely inseparable over K_ν by [38, Corollary 3 to Theorem III.5.3]. In case (ii), the natural homomorphism

$$H = D_\nu(L/K) \to \mathrm{Aut}(L_\nu/K_\nu)$$

is, in fact, an isomorphism of finite groups; see [38, Theorem III.5.3]. On the other hand, since L/K is unramified, $[L_\nu : K_\nu] = [L : K] = |H|$. This tells us that L_ν is Galois over K_ν with Galois group H.

(b) Now assume that H is a non-abelian simple group, and we are in case (ii). Set $d = \mathrm{ed}_k(L/K)$. By definition, L/K descends to L_0/K_0, where $k \subset K_0 \subset K$ and $\mathrm{trdeg}_k(K_0) = d$. By [7, Lemma 2.2], we may assume that L_0 is invariant under H. Recall that $L = L_0 \otimes_{K_0} K$. Since H acts faithfully on L and trivially on K, it acts faithfully on L_0. The valuation ν restricts to an H-invariant discrete valuation on L_0, and the H-action on L_0 descends to an H-action on the residue field $(L_0)_\nu$. Note however that a priori L_0 and K_0 may not be complete, and L_0/K_0 may be ramified.

We claim that H acts faithfully of $(L_0)_\nu$. Let us assume for a moment that this claim has been established. Then L_ν/K_ν descends to $(L_0)_\nu/(K_0)_\nu$, where $(K_0)_\nu$ denotes the residue field of K_0. Indeed, the image of the natural map $(L_0)_\nu \otimes_{(K_0)_\nu} K_\nu \to L_\nu$ is surjective by the Galois correspondence, and hence, is an isomorphism, because $[(L_0)_\nu : (K_0)_\nu] = |H| = [L_\nu : K_\nu]$. We thus conclude, that

$$\mathrm{ed}_{k_\nu}(L_\nu/K_\nu) \leqslant \mathrm{trdeg}_{k_\nu}(K_0)_\nu \leqslant \mathrm{trdeg}_k(K_0) = d,$$

as desired. Here the second inequality follows from [5, Lemma 2.1], which is a special case of Abhyankar's lemma.

It remains to prove the claim. For each $d \geqslant 0$, let $L_0^{\geqslant d} = \{a \in L^* \mid \nu(a) \geqslant d\} \cup \{0\}$. In particular, $L_0^{\geqslant 0}$ is the valuation ring of ν in L_0, $L_0^{\geqslant 1}$ is the maximal ideal, and $L_0^{\geqslant 0}/L_0^{\geqslant 1}$ is, by definition, the residue field $(L_0)_\nu$. Let I_d be the kernel of the H-action on $L_0^{\geqslant 0}/L_0^{\geqslant d+1}$. Then $I_0 \supset I_1 \supset I_2 \supset \cdots$ is a decreasing sequence of normal subgroups of H. Since H is simple, each I_d is either all of H or 1. Our goal is to show that $I_0 = 1$. Assume the contrary: $I_0 = H$. Consider two possibilities.

- $\mathrm{char}((L_0)_\nu) = 0$. In this case $I_0 = H$ is a cyclic group; see [38, Corollary IV.2.2] or [5, Lemma 2.2 (a)]. This contradicts our assumption that H is non-abelian.
- $\mathrm{char}((L_0)_\nu) = p > 0$. In this case $I_0 = H$ is of the form $P \ltimes C$, where P is a p-group and C is a cyclic group of order prime to p; see [38, Corollary IV.2.4]. Once again, this contradicts our assumption that H is simple and non-abelian.

This completes the proof of the claim and thus of Lemma 5.2. ∎

Proof of Proposition 5.1. Let $d = \mathrm{lev}_k(L/K)$. By Definition 4.1 there exists a tower

$$K = K_0 \subset K_1 \subset \cdots \subset K_m$$

of finite field extensions, where L embeds in K_m over K and $\mathrm{ed}_k(K_i/K_{i-1}) \leqslant d$ for each $i = 1, \ldots, m$. Since K is complete, so are $K_1, \ldots, K_m$; see [38, Proposition II.2.3]. By Proposition 4.9 we may assume that each K_{i+1}/K_i is simple and either purely inseparable or Galois with $\mathrm{Gal}(K_{i+1}/K_i)$ a finite simple group. Passing to residue fields, we obtain a tower

$$K_\nu = (K_0)_\nu \subset (K_1)_\nu \subset \cdots \subset (K_m)_\nu$$

such that L_ν embeds into $(K_m)_\nu$ over k_ν. In view of Lemma 4.7 it now suffices to show that

$$\mathrm{lev}_{k_\nu}((K_i)_\nu/(K_{i-1})_\nu) \leqslant \max\{d, 1\} \quad \text{for each } i = 1, \ldots, m. \tag{4}$$

If K_i/K_{i-1} is purely inseparable, then $(K_i)_\nu/(K_{i-1})_\nu$ is again purely inseparable. By Lemma 4.6 (c), $\mathrm{lev}_{k_\nu}((K_i)_\nu/(K_{i-1})_\nu) \leqslant 1$, and (4) holds.

From now on we may assume that K_i/K_{i-1} is Galois, and $H = \mathrm{Gal}(K_i/K_{i-1})$ is a simple group. By Lemma 5.2 (a), L/K is either totally ramified or unramified.

If L/K is totally ramified, then $(K_i)_\nu/(K_{i-1})_\nu$ is again purely inseparable, so that $\mathrm{lev}_{k_\nu}((K_i)_\nu/(K_{i-1})_\nu) \leqslant 1$, and (4) holds, as above.

Note also that if H is abelian, then by Lemma 4.6 (a), $\mathrm{lev}_{k_\nu}((K_i)_\nu/(K_{i-1})_\nu) \leqslant 1$, and once again, (4) holds.

We may thus assume that H is simple and non-abelian and L/K is unramified. In this case

$$\mathrm{lev}_{k_\nu}((K_i)_\nu/(K_{i-1})_\nu) \leqslant \mathrm{ed}_{k_\nu}((K_i)_\nu/(K_{i-1})_\nu) \leqslant \mathrm{ed}_k(K_i/K_{i-1}) \leqslant d,$$

and once again, (4) follows. Here the first inequality is given by Remark 4.2 (3) and the second by Lemma 5.2 (b). ∎

6. The level d closure of a field

Definition 6.1. Let K be a field containing k, $\overline{K}$ be an algebraic closure of K and $d \geqslant 1$ be an integer. We define the level d closure $K^{(d)}$ of K in $\overline{K}$ to be the compositum of all intermediate extensions $K \subset L \subset \overline{K}$ such that $[L : K] < \infty$ and $\mathrm{lev}_k(L/K) \leqslant d$. Clearly $K^{(1)} \subset K^{(2)} \subset K^{(3)} \subset \cdots$. Up to isomorphism (over K) the level d closure $K^{(d)}$ depends only on K and not on the choice of $\overline{K}$. We will say that K is closed at level d if $K = K^{(d)}$, i.e., if K has no non-trivial extensions of level $\leqslant d$.

Remark 6.2. If $d = 0$, then $K^{(0)} = \overline{k}K$, where $\overline{k}$ denotes the algebraic closure of k and the compositum is taken in $\overline{K}$. In particular, K is closed at level 0 if and only if K contains an algebraic closure of k. This follows directly from Lemma 4.5.

In the case, where k is an algebraically closed field and $K = k(x_1, \dots, x_n)$ is a purely transcendental extension, Definition 6.1 appeared in the short note of Arnold and Shimura in [6, pp. 45–46]. In this section we will explore the properties of level d closure. Our main result is Proposition 6.3 below. I assume that Arnold and Shimura had something like Proposition 6.3 in mind, through I have not encountered any explicit statements along these lines in the literature.

Proposition 6.3. *Let $k \subset K \subset E$ be fields and $d \geqslant 0$ be an integer.*

(a) *Consider an intermediate field $K \subset L \subset \overline{K}$ such that $[L : K] < \infty$. Then* $\operatorname{lev}_k(L/K) \leqslant d$ *if and only if $L \subset K^{(d)}$.*

(b) *$K^{(d)} \subset E^{(d)}$. Moreover, if E is a finite extension of K and* $\operatorname{lev}_k(E/K) \leqslant d$, *then equality holds, $K^{(d)} = E^{(d)}$.*

(c) *$E^{(d)} = \bigcup E^{(d)}_{\text{f.g.}}$, where the union is taken over the intermediate fields $K \subset E_{\text{f.g.}} \subset E$ with $E_{\text{f.g.}}$ finitely generated over K.*

(d) *$(K^{(d)})^{(n)} = K^{(n)}$ for every $n \geqslant d$. In particular, $K^{(d)}$ is closed at level d.*

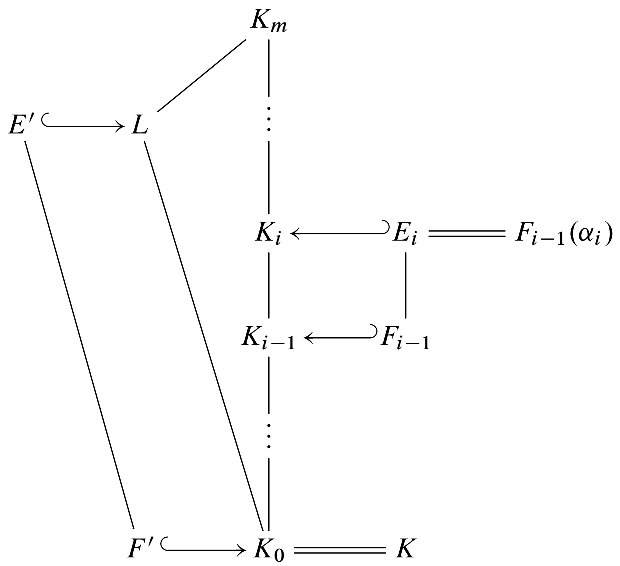
Our proof of Proposition 6.3 will rely on the following lemma.

Lemma 6.4. *Let $k \subset K \subset L$ be field extensions such that $[L : K] < \infty$. Then L/K descends to some L'/K', where K' is finitely generated over k and* $\operatorname{lev}_k(L'/K') = \operatorname{lev}_k(L/K)$.

Proof. Set $d = \operatorname{lev}_k(L/K)$ and choose a tower $K = K_0 \subset K_1 \subset \cdots \subset K_m$ of field extensions such that L embeds into K_m over K, $[K_i : K_{i-1}] < \infty$, and $\operatorname{ed}_k(K_i/K_{i-1}) \leqslant d$ for each i, as in Definition 4.1. By Remark 4.2 (4), we may assume that each intermediate extension K_i/K_{i-1} is simple.

By Lemma 2.3, K_i/K_{i-1} descends to some E_i/F_{i-1}, where $E_i \subset K_i$, $k \subset F_{i-1} \subset K_{i-1}$, F_{i-1} is finitely generated over k and $\operatorname{trdeg}_k(F_{i-1}) = \operatorname{ed}_k(E_i/F_{i-1}) = \operatorname{ed}_k(K_i/K_{i-1}) \leqslant d$. Let G_{i-1} be a finite set of generators for F_{i-1} over k. By Lemma 3.2, E_i/F_{i-1} is simple, say, $E_i = F_{i-1}(\alpha_i)$.

Similarly, by Lemma 2.1, the field extension L/K descends to E'/F', where the intermediate field $k \subset F' \subset K$ is finitely generated over k. Let H be a finite set of generators for F' over k and B be an F'-vector space basis for E'. These notations are summarized in the diagram below, where $\hookrightarrow$ indicates descent.



By Lemma 2.1, K_m/K descends to some K'_m/K' such that $k \subset K' \subset K$, K' is finitely generated over k and K'_m contains the finite subset

$$G_0 \cup \cdots \cup G_{m-1} \cup \{\alpha_1, \ldots, \alpha_m\} \cup H \cup B$$

of K_m. Consider the tower

$$K' = K'_0 \subset K'_1 \subset \cdots \subset K'_m, \tag{5}$$

where $K'_i = K'_m \cap K_i$ for each i. Note that K'_{i-1} contains k and G_{i-1} and hence, $k(G_{i-1}) = F_{i-1}$. Moreover, since K'_i contains K'_{i-1} and α_i, it also contains $F_{i-1}(\alpha_i) = E_i$.

Since K_m/K descends to K'_m/K', we have

$$\begin{aligned} &[K'_m : K'_{m-1}] \cdot [K'_{m-1} : K'_{m-2}] \cdots [K'_1 : K'_0] = [K'_m : K'], \\ &[K_m : K] = [K_m : K_{m-1}] \cdot [K_{m-1} : K_{m-2}] \cdots [K_1 : K_0]. \end{aligned} \tag{6}$$

On the other hand, since $\alpha_i \in K'_i$ has degree $[E_i : F_{i-1}] = [K_i : K_{i-1}]$ over K_{i-1}, it has degree $\geqslant [K_i : K_{i-1}]$ over K'_{i-1}. Thus, $[K'_i : K'_{i-1}] \geqslant [K_i : K_{i-1}]$ for each i. In view of (6), we conclude that $[K'_i : K'_{i-1}] = [K_i : K_{i-1}]$ for each i. In other words, K_i/K_{i-1} descends to K'_i/K'_{i-1} which, in turn, descends to E_i/F_{i-1}. Thus,

$$\mathrm{ed}_k(K'_i/K'_{i-1}) \leqslant \mathrm{ed}_k(E_i/F_{i-1}) = \mathrm{trdeg}_k(F_{i-1}) \leqslant d.$$

Finally, note that $K' = K'_0$ contains H and thus K' contains $k(H) = F'$. Set $L' = K'_m \cap L$. Since K'_m contains B, this tells us that L/K descends to L'/K'. By our construction, $L' = K'_m \cap L$ embeds into K'_m over K'. The tower (5) now shows that $\mathrm{lev}_k(L'/K') \leqslant d$, as desired. ∎

Proof of Proposition 6.3. (a) If $\mathrm{lev}_k(L/K) \leqslant d$, then $L \subset K^{(d)}$ by the definition of $K^{(d)}$. Conversely, if $L \subset K^{(d)}$ and $[L:K] < \infty$, then L is contained in a compositum $L_1 L_2 \ldots L_n$ of finitely many finite extensions L_i/K such that $\mathrm{lev}_k(L_i/K) \leqslant d$ for each i. Using Lemmas 4.4 and 4.7 recursively, we see that

$$\mathrm{lev}_k(L/K) \leqslant \mathrm{lev}(L_1 \ldots L_n/K) \leqslant d.$$

(b) Recall that $K^{(d)}$ is generated by finite extensions L/K of level $\leqslant d$. In order to prove that $K^{(d)} \subset E^{(d)}$ it suffices to show that every such L is contained in $E^{(d)}$. This follows from the inequality $\mathrm{lev}_k(LE/E) \leqslant \mathrm{lev}_k(L/K)$ of Lemma 4.4.

Now suppose E is a finite extension of K and $\mathrm{lev}_k(E/K) \leqslant d$. We want to prove that in this case $E^{(d)} \subset K^{(d)}$. It suffices to show that every finite extension M/E of level $\leqslant d$ lies in $K^{(d)}$, i.e., $\mathrm{lev}_k(M/K) \leqslant d$. This follows from Lemma 4.7.

(c) Set $U = \bigcup E_{\mathrm{f.g.}}^{(d)}$. By part (b), $E_{\mathrm{f.g.}}^{(d)} \subset E^{(d)}$ for each finitely generated field $K \subset E_{\mathrm{f.g.}} \subset E$. Hence, $U \subset E^{(d)}$. To prove the opposite inclusion, we proceed in four steps.

Step 1: We reduce to the case, where $K = k$. Indeed, every intermediate field $k \subset E_0 \subset E$ such that E_0 is finitely generated over k lies in $E_1 = KE_0$ which is finitely generated over K. By part (b), $E_0^{(d)} \subset E_1^{(d)} \subset U$. Thus,

$$\bigcup E_0^{(d)} \subset U \subset E^{(d)}$$

where the first union is over finitely generated subextensions $k \subset E_0 \subset E$. If we know that $\bigcup E_0^{(d)}$ equals $E^{(d)}$, then both of these inclusions are equalities, and in particular, $U = E^{(d)}$, as desired. This shows that we may assume without loss of generality that $K = k$. We will do so for the remainder of the proof of part (c).

Step 2: We claim that U is a subfield of $E^{(d)}$. Indeed, suppose $x_1 \in E_1^{(d)}$ and $x_2 \in E_2^{(d)}$, where $k \subset E_i \subset E$ and E_i is finitely generated over k for $i = 1, 2$. Assume $x_1 \neq 0$. We want to show that $x_1 \pm x_2$, $x_1 \cdot x_2$ and x_1^{-1} all lie in U. Indeed, the composite $E_3 = E_1 E_2$ of E_1 and E_2 in E is also finitely generated over k. Hence, $E_3^{(d)}$ is contained in U. By part (b), $x_1 \in E_1^{(d)} \subset E_3^{(d)}$ and $x_2 \in E_2^{(d)} \subset E_3^{(d)}$. We conclude that $x_1 \pm x_2$, $x_1 \cdot x_2$ and $x_1^{-1} \in E_3^{(d)} \subset U$, as desired.

Step 3: U contains E. This is because U contains $k(x)$ for every $x \in E$.

Step 4: We will now complete the proof of the desired inclusion $E^{(d)} \subset U$.

Indeed, it suffices to show that U contains every finite extension L/E such that $\mathrm{lev}_k(L/E) \leqslant d$. Recall that by Lemma 6.4, L/E descends to L_0/E_0 for some field $k \subset E_0 \subset E$ such that E_0 is finitely generated over k and $\mathrm{lev}_k(L_0/E_0) = \mathrm{lev}_k(L/E) \leqslant d$. Thus, $L_0 \subset E_0^{(d)} \subset U$. Since U is a subfield of $\overline{E}$ containing both E and L_0, it contains $L = EL_0$.

This completes the proof of Step 4 and thus of part (c).

(d) Part (b) tells us that $K^{(n)} \subset (K^{(d)})^{(n)} = (K^{(n)})^{(n)}$. Thus, it suffices to show that $(K^{(n)})^{(n)} = K^{(n)}$, i.e., that $K^{(n)}$ is closed at level n. In other words, we may assume without loss of generality that $n = d$.

Let $E = K^{(d)}$. We want to show that $E^{(d)} = K^{(d)}$. By part (c), it suffices to show that $L^{(d)} = K^{(d)}$ for every intermediate extension $K \subset L \subset E = K^{(d)}$, where L is finitely generated (or equivalently, finite) over K. Since $K \subset L \subset K^{(d)}$, part (a) tells us that $\mathrm{lev}_k(L/K) \leqslant d$. The desired equality, $L^{(d)} = K^{(d)}$, is now given by the second assertion in part (b). ∎

Corollary 6.5. *Suppose $K \in \mathrm{Fields}_k$ is closed at level $d \geqslant 1$. Then K is perfect and solvably closed.*

Proof. Suppose L/K is a solvable or purely inseparable extension. Our goal is to show that $K = L$. Indeed, by Lemma 4.6, $\mathrm{lev}_k(L/K) \leqslant 1$. By Proposition 6.3 (a), $K \subset L \subset K^{(d)}$. Since K is closed at level d, $K^{(d)} = K$ and thus $K = L$. ∎

Remark 6.6. Let G be a finite group of resolvent degree 1. (For the definition of the resolvent degree of a group, see Section 10.) Then Proposition 6.3 (a) tells us that if K is closed at level $d \geqslant 1$, then K does not admit a Galois extensions L/K with Galois group G. In particular, there do not exist Galois extensions L/K with Galois group A_5 or $\mathrm{PSL}_2(\mathbb{F}_7)$; see Example 14.3.

7. The resolvent degree of a functor

Essential dimension can be defined for a broader class of objects, beyond finite field extensions. The following definition is due to Merkurjev, Berhuy and Favi [1]. Let k be a base field, and $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}$ be a functor from the category of field extensions K/k to the category of sets. All functors in this paper will be assumed to be covariant. We think of $\mathcal{F}$ as specifying the type of object we are considering, and $\mathcal{F}(K)$ as the set of objects of this type defined over K. Given a field extension $k \subset K \subset K'$, we think of the natural map $\mathcal{F}(K) \to \mathcal{F}(K')$ as base change. The image of $\alpha \in \mathcal{F}(K)$ under this map will be denoted by $\alpha_{K'}$.

Definition 7.1. Any object $\alpha \in \mathcal{F}(K)$ in the image of the natural map $\mathcal{F}(K_0) \to \mathcal{F}(K)$ is said to *descend* to K_0. The essential dimension $\mathrm{ed}_k(\alpha)$ is defined as the minimal value of $\mathrm{trdeg}_k(K_0)$, where the minimum is taken over all intermediate fields $k \subset K_0 \subset K$ such that α descends to K_0.

Example 7.2. Consider the functor $\mathrm{Alg}\colon \mathrm{Fields}_k \to \mathrm{Sets}$, where $\mathrm{Alg}(K)$ is the set of isomorphism classes of finite-dimensional K-algebras. Here the natural map $\mathrm{Alg}(K) \to \mathrm{Alg}(K')$ takes a K-algebra A to the K'-algebra $K' \otimes_K A$. Let $K \in \mathrm{Fields}_k$ and A be a finite-dimensional K-algebra. If we view A as an object in $\mathcal{F}(K)$, then $\mathrm{ed}_k(A)$ given by Definition 7.1 is the same as $\mathrm{ed}_k(A/K)$ given by Definition 2.2.

Our goal now is to define the resolvent degree of a functor $\mathcal{F}$ in a similar manner (but under more restrictive assumptions on $\mathcal{F}$). Let $\mathcal{F}$ be a covariant functor from the category Fields_k of field extensions K/k to

$$\text{the category } \ \mathrm{Sets}' \ \text{ of sets with a marked element.}$$

We will denote the marked element in $\mathcal{F}(K)$ by 1 and will refer to it as being "split." We will say that a field extension L/K splits an object $\alpha \in \mathcal{F}(K)$ if $\alpha_L = 1$. Let us assume that

$$\text{(7)} \quad \text{for every field } K/k \text{ and every } \alpha \in \mathcal{F}(K), \quad \alpha \text{ can be split by a field extension } L/K \text{ of finite degree.}$$

Note that this is a strong condition on $\mathcal{F}$; in particular, it implies that $\mathcal{F}(K) = \{1\}$ whenever K is algebraically closed.

Definition 7.3. Let $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'$ be a functor satisfying condition (7), K/k be a field extension and $\alpha \in \mathcal{F}(K)$.

(a) The resolvent degree $\mathrm{RD}_k(\alpha)$ is the minimal integer $d \geqslant 0$ such that α is split by a finite field extension L/K of level d (or equivalently, of level $\leqslant d$).

(b) The resolvent degree $\mathrm{RD}_k(\mathcal{F})$ of the functor $\mathcal{F}$ is the maximal value of $\mathrm{RD}_k(\alpha)$, as K ranges over all fields containing k and α ranges over $\mathcal{F}(K)$.

Remarks 7.4. (1) Note that the level $\mathrm{lev}_k(L/K)$ plays a similar role in Definition 7.3 to the role played by the transcendence degree $\mathrm{trdeg}_k(K_0)$ in Definition 7.1.

(2) Condition (7) ensures that $\mathrm{RD}_k(\alpha)$ is finite for every $K \in \mathrm{Fields}_k$ and every $\alpha \in \mathcal{F}(K)$. On the other hand, $\mathrm{RD}_k(\mathcal{F})$ can a priori be infinite, even though no examples where $\mathrm{RD}_k(\mathcal{F}) > 1$ are known.

Example 7.5. Consider the functor $\acute{\mathrm{E}}\mathrm{t}_n\colon \mathrm{Fields}_k \to \mathrm{Sets}'$, where $\acute{\mathrm{E}}\mathrm{t}(K)$ is the set of isomorphism classes of n-dimensional étale algebras L/K. Recall that an n-dimensional étale algebra L is a direct product of the form $L = L_1 \times \cdots \times L_r$, where each L_i is a finite separable field extension of K and $[L_1 : K] + \cdots + [L_r : K] = n$. The marked element in $\text{Ét}_n(K)$ is the split algebra $K \times K \times \cdots \times K$ (n times).

(a) If L/K is a separable field extension of degree n, and $[L]$ is its class in $\text{Ét}_n(K)$, then $\text{RD}_k([L]) = \text{lev}_k(L/K)$.

(b) (Cf. [20, Lemma 2.6].) More generally, if $L = L_1 \times \cdots \times L_r$ is a direct product of separable extensions of K as above, and $[L]$ is its class in $\text{Ét}_n(K)$, then $\text{RD}_k([L]) = \max_{i=1,\dots,r} \text{lev}_k(L_i/K)$.

(c) $\text{RD}_k(\text{Ét}) = \max \text{lev}_k(L/K)$, where the maximum is taken over all separable field extensions L/K of degree $\leqslant n$.

Proof. (a) By the primitive element theorem, $L \simeq_K K[x]/(f(x))$, where $f(x) \in K[x]$ is an irreducible separable polynomial of degree n. A field extension L'/K splits $[L]$ if and only if $f(x)$ splits as a product of linear factors over L'. Equivalently, L' splits L if and only if L' contains the normal closure L^{norm} of L over K. By Remark 4.2 (2),

$$\text{RD}_k([L]) = \min\{\text{lev}_k(L'/K) \mid L^{\text{norm}} \subset L'\} = \text{lev}_k(L^{\text{norm}}/K).$$

On the other hand, by Lemma 4.8, $\text{lev}_k(L^{\text{norm}}/K) = \text{lev}_k(L/K)$.

(b) A field extension L'/K splits $[L]$ if and only if it splits each $[L_i] \in \text{Ét}_{[L_i:K]}(K)$. Hence, by part (a), $\text{RD}_k([L]) \geqslant \max_{i=1,\dots,r} \text{RD}_k([L_i]) = \max_{i=1,\dots,r} \text{lev}_k(L_i/K)$. To prove the opposite inequality, take L' to be the compositum of L_i over K. Then L' splits $[L]$. Moreover, combining Lemmas 4.4 and 4.7, we obtain

$$\text{RD}_k([L]) \leqslant \text{lev}_k(L'/K) \leqslant \max_{i=1,\dots,r} \text{lev}_k(L_i/K).$$

(c) is an immediate consequence of (b). ∎

Lemma 7.6. *Let $\mathcal{F}\colon \text{Fields}_k \to \text{Sets}'$ be a functor satisfying condition* (7)*, K/k be a field extension and $\alpha \in \mathcal{F}(K)$. Then:*

(a) $\text{RD}_k(\alpha_{K'}) \leqslant \text{RD}_k(\alpha)$ *for any field K' containing K.*

(b) $\text{RD}_k(\alpha) \leqslant \text{ed}_k(\alpha)$.

(c) $\text{RD}_k(\mathcal{F}) \leqslant \text{ed}_k(\mathcal{F})$.

Proof. (a) If α is split by a finite extension L/K such that $\text{lev}_k(L/K) = d$, then $\alpha_{K'}$ is split by the finite extension $K'L/K'$ of level $\text{lev}_k(K'L/K') \leqslant d$; see Lemma 4.4.

(b) Set $d = \text{ed}_k(\alpha)$. Then α descends to $\alpha_0 \in \mathcal{F}(K_0)$ for some intermediate field $k \subset K_0 \subset K$ such that $\text{trdeg}_k(K_0) = d$. Since $\mathcal{F}$ satisfies condition (7), α_0 is split by some finite extension L_0/K_0. Now

$$\text{RD}_k(\alpha) \leqslant \text{RD}_k(\alpha_0) \leqslant \text{lev}_k(L_0/K_0) \leqslant \text{ed}_k(L_0/K_0) \leqslant d,$$

as desired. Here the first inequality follows from part (a), the second from the definition of $\mathrm{RD}_k(\alpha_0)$, the third from Remark 4.2 (3), and the fourth from the fact that $\mathrm{trdeg}_k(K_0) = d$.

(c) is an immediate consequence of (b). ∎

Lemma 7.7. *Let $k \subset k' \subset K$ be field extensions, Let $\mathcal{F} : \mathrm{Fields}_k \to \mathrm{Sets}'$ be a functor satisfying condition (7) and $\alpha \in \mathcal{F}(K)$. Then:*

(a) $\mathrm{RD}_k(\alpha) \geqslant \mathrm{RD}_{k'}(\alpha)$.

(b) *Moreover, equality holds if k' is algebraic over k.*

(c) *Furthermore, there exists an intermediate field $k \subset l_0 \subset k'$ such that l_0 is finitely generated over k and $\mathrm{RD}_l(\alpha) = \mathrm{RD}_{k'}(\alpha)$ for every field l between l_0 and k'.*

Proof. For every finite extension L/K splitting α, we have $\mathrm{lev}_k(L/K) \geqslant \mathrm{lev}_{k'}(L/K)$. Moreover, equality holds if k' is algebraic over k; see Lemma 4.3. This proves (a) and (b).

For part (c), choose a splitting extension L/K such that $d = \mathrm{lev}_{k'}(L/K)$ assumes its minimal possible value, $d = \mathrm{RD}_{k'}(\alpha)$. Now choose l_0 as in Lemma 4.3 (c). Then for any intermediate field $l_0 \subset l \subset k'$,

$$\mathrm{RD}_l(\alpha) \leqslant \mathrm{lev}_l(L/K) = \mathrm{lev}_{k'}(L/K) = d = \mathrm{RD}_{k'}(\alpha).$$

Combining this inequality with the inequality of part (a), we conclude that $\mathrm{RD}_l(\alpha) = \mathrm{RD}_{k'}(\alpha)$. ∎

Lemma 7.8. *If k is algebraically closed, then $\mathrm{RD}_k(\alpha) > 0$ for any $K \in \mathrm{Fields}_k$ and any $1 \neq \alpha \in \mathcal{F}(K)$. In particular, $\mathrm{RD}_k(\mathcal{F}) = 0$ if and only if $\mathcal{F}$ is the trivial functor, i.e., if and only if $\mathcal{F}(K) = 1$ for every $K \in \mathrm{Fields}_k$.*

Proof. Immediate from Lemma 4.5 and our standing assumption that $\mathcal{F}$ satisfies condition (7). ∎

Lemma 7.9. *Let $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ be functors $\mathrm{Fields}_k \to \mathrm{Sets}'$ satisfying (7).*

(a) *Suppose $\mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3$ is an exact sequence.*[1] *Then*

$$\mathrm{RD}_k(\mathcal{F}_2) \leqslant \max\{\mathrm{RD}_k(\mathcal{F}_1), \mathrm{RD}_k(\mathcal{F}_3)\}.$$

(b) *If a morphism $\mathcal{F}_1 \to \mathcal{F}_2$ of functors has trivial kernel, then $\mathrm{RD}_k(\mathcal{F}_1) \leqslant \mathrm{RD}_k(\mathcal{F}_2)$.*

(c) *If a morphism $\mathcal{F}_2 \to \mathcal{F}_3$ of functors is surjective, then $\mathrm{RD}_k(\mathcal{F}_3) \leqslant \mathrm{RD}_k(\mathcal{F}_2)$.*

[1] This means that $\mathcal{F}_1(K) \to \mathcal{F}_2(K) \to \mathcal{F}_3(K)$ is an exact sequence in Sets' for every field K/k.

(d) *If* $1 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 1$ *is a short exact sequence, then*

$$\mathrm{RD}(\mathcal{F}_2) = \max\{\mathrm{RD}_k(\mathcal{F}_1), \mathrm{RD}_k(\mathcal{F}_3)\}.$$

In particular, $\mathrm{RD}_k(\mathcal{F}_1 \times \mathcal{F}_3) = \max\{\mathrm{RD}_k(\mathcal{F}_1), \mathrm{RD}_k(\mathcal{F}_3)\}$.

Proof. (a) Suppose $\alpha \in \mathcal{F}_2(K)$ for some field K/k. Denote the image of α in $\mathcal{F}_3(K)$ by β. After passing to an extension L/K of level $\leqslant \mathrm{RD}(\mathcal{F}_3)$, we may assume that β is split. Hence, $\alpha_L \in \mathcal{F}_2(L)$ is the image of some $\gamma \in \mathcal{F}_1(L)$. A further extension L'/L of level $\leqslant \mathrm{RD}(\mathcal{F}_1)$ splits γ. Thus, the composite extension $K \subset L \subset L'$ splits α, i.e., $\alpha_{L'} = 1$. We conclude that

$$\begin{aligned}\mathrm{RD}_k(\alpha) &\leqslant \mathrm{lev}_k(L'/K)\\ &\leqslant \max\{\mathrm{lev}_k(L/K), \mathrm{lev}_k(L'/L)\} \leqslant \max\{\mathrm{RD}_k(\mathcal{F}_1), \mathrm{RD}_k(\mathcal{F}_3)\},\end{aligned}$$

where the inequality in the middle follows from Lemma 4.7. Taking the maximum over all fields K/k and all objects $\alpha \in \mathcal{F}_2(K)$, we conclude that $\mathrm{RD}(\mathcal{F}_2) \leqslant \max\{\mathrm{RD}_k(\mathcal{F}_1), \mathrm{RD}_k(\mathcal{F}_3)\}$.

(b) and (c): Apply part (a) to the exact sequences $1 \to \mathcal{F}_1 \to \mathcal{F}_2$ and $\mathcal{F}_2 \to \mathcal{F}_3 \to 1$, respectively.

(d) For the first assertion combine the inequalities of (a), (b) and (c). The second assertion is a special case of the first with $\mathcal{F}_3 = \mathcal{F}_1 \times \mathcal{F}_2$. ■

Proposition 7.10. *Let A be a diagonalizable group (i.e., a closed subgroup of the split torus* $\mathbb{G}_m^d$*) defined over k. Then the functor* $H^2(*, A)$ *satisfies condition* (7) *and*

$$\mathrm{RD}_k(H^2(*, A)) \leqslant 1.$$

Proof. First, let us consider the special case, where $A = \mathbb{G}_m$. Recall that $H^2(K, \mathbb{G}_m)$ is in a natural (functorial) bijection with the Brauer group $\mathrm{Br}(K)$. Thus, it suffices to show that every central simple algebra A over every $F \in \mathrm{Fields}_k$ can be split by a solvable extension of K. By the primary decomposition theorem we may assume without loss of generality that the index of A is a prime power, p^r. If $\mathrm{char}(k) \neq p$, then the Merkurjev–Suslin theorem tells us that A can be split by a solvable extension of K; see [23, Corollary 2.5.9]. If $p = \mathrm{char}(k)$, then by a theorem of Albert [23, Theorem 9.1.8], A is Brauer-equivalent to a cyclic algebra and thus can be split by a cyclic (and hence, once again, solvable) field extension of K. This completes the proof in the case where $A = \mathbb{G}_m$.

If $A = \mu_n$, then $H^2(*, \mu_n) \simeq {}_n\mathrm{Br}(K)$, where ${}_n\mathrm{Br}(K)$ is the n-torsion subgroup of $\mathrm{Br}(K)$, and the same argument applies.

In general, we write A as a direct product $A_1 \times_k \cdots \times_k A_r$, where each A_i is k-isomorphic to $\mathbb{G}_m$ or μ_n for some integer n. Then $H^2(*, A) = H^2(*, A_1) \times \cdots \times H^2(*, A_r)$, and the desired conclusion follows from Lemma 7.9 (d). ■

Remark 7.11. If $A \neq 1$ in Proposition 7.10, then equality holds: $\mathrm{RD}_k(H^2(*, A)) = 1$.

To prove this, we readily reduce to the case, where $A = \mu_n$ for some $n \geqslant 2$. In this case, assume the contrary. Then for every $K \in \mathrm{Fields}_k$, every $\alpha \in H^2(K, \mu_n)$ can be split by a finite extension L/K of level 0. In particular, by Remark 6.2, if K contains $\bar{k}$, then K is closed at level 0, i.e., there are no non-trivial finite extensions L/K of level 0 and thus $H^2(K, \mu_n) = 1$. On the other hand, it is well known that if $K = \bar{k}(x, y)$, where x and y are variables, the symbol algebra $(x, y)_n$ represents a non-trivial class in $H^2(K, \mu_n)$, a contradiction. ∎

Remark 7.12. Using the norm residue isomorphism theorem (formerly known as the Bloch–Kato conjecture) in place of the Merkurjev–Suslin theorem, one shows in the same manner that $\mathrm{RD}_k(H^d(*, \mu_n)) \leqslant 1$ for every $n \geqslant 1$ not divisible by $\mathrm{char}(k)$ and every $d \geqslant 1$, and that equality holds when $n \geqslant 2$.

8. Functors preserving direct limits

In this section we will assume that our functor $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'$ respects direct limits. Examples include Galois cohomology functors $H^1(*, G)$, where G is an algebraic group over k, as well as $H^d(*, G)$ for every $d \geqslant 2$, if G is abelian. For such functors $\mathcal{F}$ the study of resolvent degree can be facilitated by using the notion of level d closure of field introduced in Section 6.

Proposition 8.1. *Assume that a functor $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'$ satisfies condition (7) and respects direct limits. Let $K \in \mathrm{Fields}_k$ and $\alpha \in \mathcal{F}(K)$. Then:*

(a) $\mathrm{RD}_k(\alpha) \leqslant d$ *if and only if α splits over $K^{(d)}$, i.e., $\alpha_{K^{(d)}} = 1$.*

(b) $\mathrm{RD}_k(\mathcal{F}) \leqslant d$ *if and only if $\mathcal{F}(K) = 1$ for every field K closed at level d.*

(c) *Suppose* $\mathrm{RD}_k(\alpha_{K^{(d)}}) \leqslant m$. *Then* $\mathrm{RD}_k(\alpha) \leqslant \max\{d, m\}$.

(d) *Suppose* $\mathrm{RD}_k(\beta) \leqslant m$ *for every field $E \in \mathrm{Fields}_k$ closed at level d and every $\beta \in \mathcal{F}(E)$. Then* $\mathrm{RD}_k(\mathcal{F}) \leqslant \max\{d, m\}$.

Proof. (a) Suppose $\mathrm{RD}_k(\alpha) \leqslant d$. Then α splits over a finite extension L of K such that $\mathrm{lev}_k(L/K) \leqslant d$. By definition of $K^{(d)}$, L embeds into $K^{(d)}$ over K. Hence, $\alpha_{K^{(d)}} = 1$. Conversely, suppose α splits over $K^{(d)}$. Since $\mathcal{F}$ respects direct limits, α splits over some subextension $K \subset L \subset K^{(d)}$ such that $[L : K] < \infty$. By Proposition 6.3 (a), $\mathrm{lev}_k(L/K) \leqslant d$. Thus, $\mathrm{RD}_k(\alpha) \leqslant d$.

(b) Suppose $\mathrm{RD}_k(\mathcal{F}) \leqslant d$ and $K \in \mathrm{Fields}_k$ is closed at level d. By part (a), any $\alpha \in \mathcal{F}(K)$ splits over $K^{(d)}$. By Proposition 6.3 (d), $K^{(d)} = K$ and thus $\alpha = 1$. This shows that $\mathcal{F}(K) = 1$.

Conversely, assume $\mathcal{F}(K) = 1$ whenever $K \in \mathrm{Fields}_k$ is closed at level d. Let F be an arbitrary field containing k and $\alpha \in \mathcal{F}(F)$. By our assumption (with $K = F^{(d)}$), $\alpha_{F^{(d)}} = 1$. Since $\mathcal{F}$ respects direct limits, $\alpha_E = 1$ for some $F \subset E \subset F^{(d)}$, where E is finitely generated over F, i.e., $[E : F] < \infty$. By Proposition 6.3 (a), $\mathrm{lev}_k(E/F) \leqslant d$. Hence, $\mathrm{RD}_k(\alpha) \leqslant d$.

(c) Let $n = \max\{d, m\}$. In view of part (a), our goal is to show that $\alpha_{K^{(n)}} = 1$. Set $E = K^{(d)}$. By Proposition 6.3 (d), E is closed at level d and $E^{(n)} = K^{(n)}$. By our assumption, $\mathrm{RD}_k(\alpha_E) \leqslant m$. By part (a), $\alpha_{E^{(m)}} = 1$. Since $E^{(m)} \subset E^{(n)}$, we conclude that $\alpha_{K^{(n)}} = \alpha_{E^{(n)}} = 1$.

(d) is an immediate consequence of (c). ∎

Definition 8.2. Let $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'$ be a functor. For any field k' containing k, we define $\mathcal{F}_{k'}\colon \mathrm{Fields}_{k'} \to \mathrm{Sets}'$ to be the restriction of $\mathcal{F}$ to $\mathrm{Fields}_{k'}$. In other words, $\mathcal{F}_{k'}(K)$ is only defined if K contains k', and for such K, $\mathcal{F}_{k'}(K) = \mathcal{F}(K)$.

Proposition 8.3. *Assume that a functor* $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'$ *satisfies condition* (7).

(a) *If k'/k is a field extension, then the functor $\mathcal{F}_{k'}$ also satisfies condition* (7) *and* $\mathrm{RD}_k(\mathcal{F}) \geqslant \mathrm{RD}_{k'}(\mathcal{F}_{k'})$.

(b) *Moreover, if k'/k is an algebraic field extension and $\mathcal{F}$ respects direct limits, then* $\mathrm{RD}_k(\mathcal{F}) = \mathrm{RD}_{k'}(\mathcal{F}_{k'})$.

Proof. Let $K \in \mathrm{Fields}_k$ and $\alpha \in \mathcal{F}(K)$.

(a) The first assertion is obvious from Definition 8.2. To prove the second assertion, it suffices to show that

$$\mathrm{RD}_k(\alpha) \geqslant \mathrm{RD}_k(\alpha_{k'K}) \geqslant \mathrm{RD}_{k'}(\alpha_{k'K}), \tag{8}$$

where $k'K$ is a compositum of k' and K. Indeed, the maximal value of the left-hand side over all $K \in \mathrm{Fields}_k$ and all $\alpha \in \mathcal{F}(K)$ is $\mathrm{RD}_k(\mathcal{F})$, whereas the maximal value of the right-hand side is $\mathrm{RD}_{k'}(\mathcal{F}_{k'})$. The first inequality in (8) follows from Lemma 7.6 (a) and the second from Lemma 7.7 (a).

(b) Here it suffices to show that

$$\mathrm{RD}_k(\alpha) = \mathrm{RD}_k(\alpha_{k'K}) = \mathrm{RD}_{k'}(\alpha_{k'K}). \tag{9}$$

The second equality follows from Lemma 7.7 (b). To prove the first inequality, it suffices to show that

$$K^{(d)} = (k'K)^{(d)} \tag{10}$$

for every $d \geqslant 0$. Indeed, if we can prove this, then α is split by $K^{(d)}$ if and only if $\alpha_{k'K}$ is split by $(k'K)^{(d)}$, and the desired equality follows from Proposition 8.1 (a).

To prove (10), note that by Remark 6.2, $K \subset k'K \subset K^{(0)}$. By Proposition 6.3,

$$K^{(d)} \subset (k'K)^{(d)} \subset (K^{(0)})^{(d)} = K^{(d)},$$

and (10) follows. ■

Example 8.4. Let $\text{Ét}_n : \text{Fields}_k \to \text{Sets}'$ be the functor of n-dimensional étale algebras introduced in Example 7.5. If $d \geqslant \text{RD}_k(\text{Ét}_n)$, and $K \in \text{Fields}_k$ is closed at level d, then every polynomial of degree $\leqslant n$ splits into a product of linear factors over K.

Proof. If $n = 1$, the assertion is vacuous, so we may assume that $n \geqslant 2$. One readily checks that the functor $(\text{Ét}_n)_{\overline{k}}$ is non-trivial for any $n \geqslant 2$. Hence,

$$\text{RD}_k(\text{Ét}_n) \geqslant \text{RD}_{\overline{k}}\big((\text{Ét}_n)_{\overline{k}}\big) \geqslant 1,$$

where $\overline{k}$ denotes an algebraic closure of k, the first inequality follows from Proposition 8.3 (a), and the second from Lemma 7.8. Thus, $d \geqslant 1$. By Corollary 6.5, K is perfect.

It remains to show that there does not exist an irreducible polynomial $f(x) \in K[x]$ of degree m for any $2 \leqslant m \leqslant n$. Indeed, assume the contrary. Then

$$E = K[x]/(f(x)) \times \underbrace{K \times \cdots \times K}_{n-m \text{ times}}$$

is a non-split étale algebra of degree n. On the other hand, $\text{Ét}_n(K) = 1$ by Proposition 8.1 (b), i.e., every étale algebra of degree n over K is split, a contradiction. ■

Remark 8.5. Proposition 8.3 (b) may fail if

(a) the functor $\mathcal{F}$ is not required to respect direct limits or if

(b) the field k' is not required to be algebraic over k.

Proof. Our counterexamples in parts (a) and (b) will both rely on the following construction. Let $\mathcal{F} : \text{Fields}_k \to \text{Sets}'$ be a functor and Λ be a collection of fields $K \subset \text{Fields}_k$ closed under inclusion. That is, if $L \in \Lambda$ and $K \subset L$, then $K \in \Lambda$. Set $\mathcal{F}^{\Lambda} : \text{Fields}_k \to \text{Sets}'$ by

$$\mathcal{F}^{\Lambda}(K) = \begin{cases} \mathcal{F}(K), & \text{if } K \in \Lambda, \\ \{1\}, & \text{if } K \notin \Lambda. \end{cases}$$

If $K \subset L$ is a field extension, the natural map $\mathcal{F}^{\Lambda}(K) \to \mathcal{F}^{\Lambda}(L)$ is defined to be the same as the natural map $\mathcal{F}(K) \to \mathcal{F}(L)$ if $L \in \Lambda$ and to be the trivial map (sending every element of $\mathcal{F}(K)$ to 1) if $L \notin \Lambda$. It is easy to see that $\mathcal{F}^{\Lambda}$ is well defined.

Moreover, if $\mathcal{F}$ satisfies condition (7), then so does $\mathcal{F}^{\Lambda}$. Informally, we think of $\mathcal{F}^{\Lambda}$ as a truncation of $\mathcal{F}$.

The starting point for both parts is a functor $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'_k$ which satisfies (7), respects direct limits, and such that $\mathrm{RD}_k(\mathcal{F}) \geqslant 1$. There are many examples of such functors, e.g., $\mathcal{F} = H^2(*, \mathbb{G}_m)$; see Remark 7.11. Choose a field $K \in \mathrm{Fields}_k$ and an object $\alpha \in \mathcal{F}(K)$ such that $\mathrm{RD}_k(\alpha) \geqslant 1$. Since $\mathcal{F}$ respects direct limits, α descends to $\alpha_0 \in \mathcal{F}(K_0)$ for some intermediate field $k \subset K_0 \subset K$ such that K_0 is finitely generated over k. By Lemma 7.6 (a), $\mathrm{RD}_k(\alpha_0) \geqslant \mathrm{RD}_k(\alpha) \geqslant 1$. After replacing K by K_0 and α by α_0, we may assume that K is finitely generated over k.

(a) Consider the truncated functor $\mathcal{F}^{\Lambda}$, where

$$\Lambda = \{K/k \mid K \text{ is finitely generated over } k\}.$$

Note that $\mathrm{RD}_k(\alpha) \geqslant 1$ whether we view α as an object in $\mathcal{F}$ or $\mathcal{F}^{\Lambda}$. On the other hand, if the algebraic closure $\overline{k}$ is not finitely generated over k (e.g., if $k = \mathbb{Q}$), then no field containing $\overline{k}$ can be finitely generated over k. This tells us that the truncated functor $\mathcal{F}^{\Lambda}_{\overline{k}}$ is the trivial functor and consequently, $\mathrm{RD}_{\overline{k}}(\mathcal{F}^{\Lambda}_{\overline{k}}) = 0$. We conclude that Proposition 8.3 (b) fails for $\mathcal{F}^{\Lambda}$ if $k' = \overline{k}$.

(b) Set $m = \mathrm{trdeg}_k(K)$ and consider the truncated functor $\mathcal{F}^{\Lambda}$, where

$$\Lambda = \{K/k \mid \mathrm{trdeg}_k(K) \leqslant m\}.$$

The functor $\mathcal{F}^{\Lambda}$ continues to satisfy condition (7) and to respect direct limits. If $\mathrm{trdeg}_k(k') > m$, then $\mathcal{F}^{\Lambda}_{k'}$ is trivial and thus $\mathrm{RD}_{k'}(\mathcal{F}^{\Lambda}) = 0$. On the other hand, $\mathrm{RD}_k(\alpha) \geqslant 1$ whether we view α as an object in $\mathcal{F}$ or $\mathcal{F}^{\Lambda}$. In summary, $\mathrm{RD}_k(\mathcal{F}^{\Lambda}) \geqslant 1$, $\mathrm{RD}_{k'}(\mathcal{F}^{\Lambda}_{k'}) = 0$, and Proposition 8.3 (b) fails for $\mathcal{F}^{\Lambda}$. ∎

9. Change of base field

As we saw in Remark 8.5 (b), Proposition 8.3 (b) fails if k' is not assumed to be algebraic over k. In this section we will show that under an additional condition on the functor $\mathcal{F}$, the equality of Proposition 8.3 (b) can be (largely) salvaged for an arbitrary field extension k'/k. The condition we will impose on $\mathcal{F}$ is as follows:

(11) The natural map $\mathcal{F}(E) \to \mathcal{F}\big(E((t))\big)$ has trivial kernel for every perfect field E containing k.

Note that this is almost the same as condition (*) considered by Merkurjev in [29, Section 3]. The only difference is that condition (*) requires injectivity of the map (11) for every field E, not necessarily perfect. As is pointed out in [29], this condition is natural and is often satisfied.

Proposition 9.1. *Assume that a functor* $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'$ *satisfies conditions* (7) *and* (11) *and respects direct limits. Then*

$$\mathrm{RD}_{k'}(\mathcal{F}_{k'}) \leqslant \mathrm{RD}_k(\mathcal{F}) \leqslant \max\{\mathrm{RD}_{k'}(\mathcal{F}_{k'}), 1\}$$

for any field extension k'/k*.*

The remainder of this section will be devoted to proving Proposition 9.1. We begin with the following lemma.

Lemma 9.2. *Assume that a functor* $\mathcal{F}\colon \mathrm{Fields}_k \to \mathrm{Sets}'$ *satisfies condition* (7) *and respects direct limits. Let* k'/k *be a field extension,* $K \in \mathrm{Fields}_k$ *and* $\alpha \in \mathcal{F}(K)$*. Then there exists an intermediate field* $k \subset l \subset k'$ *such that* l *is finitely generated over* k *and* $\mathrm{RD}_l(\alpha_{lK}) = \mathrm{RD}_{k'}(\alpha_{k'K})$*. Here* $k'K$ *is some compositum of* k' *and* K *over* k*. The compositum* lK *is taken in* $k'K$*.*

Proof. For any intermediate field $k \subset l \subset k'$, we have

$$\mathrm{RD}_l(\alpha_{lK}) \geqslant \mathrm{RD}_l(\alpha_{k'K}) \geqslant \mathrm{RD}_{k'}(\alpha_{k'K});$$

see (8). Our goal is to show that the opposite inequality holds for a suitably chosen intermediate field $k \subset l \subset k'$, where l is finitely generated over k.

Set $d = \mathrm{RD}_{k'}(\alpha_{k'K})$. By Lemma 7.7 (c) there exists an intermediate extension $k \subset l_0 \subset k'$ such that l_0 is finitely generated over k, and $d = \mathrm{RD}_l(\alpha_{k'K})$ for any intermediate field $l_0 \subset l \subset k'$. After replacing k by l_0 and α by α_{l_0K}, we may assume without loss of generality that $k = l_0$. In particular, $d = \mathrm{RD}_k(\alpha_{k'K})$. By Proposition 8.1 (a), α splits over $(k'K)^{(d)}$. Since $\mathcal{F}$ preserves direct limits, α splits over $L^{(d)}$ for some intermediate extension $K \subset L \subset k'K$ such that L is finitely generated over K. Any such L is contained in lK for some intermediate field $k \subset l \subset k'$, where l is finitely generated over k. Thus, α splits over $(lK)^{(d)}$. By Proposition 8.1 (a) this implies that $\mathrm{RD}_l(\alpha_{lK}) \leqslant d$, as claimed. ∎

Proof of Proposition 9.1. The first inequality $\mathrm{RD}_{k'}(\mathcal{F}_{k'}) \leqslant \mathrm{RD}_k(\mathcal{F})$ is proved in Proposition 8.3 (a). We will thus focus on proving the second inequality. Let K be a field containing k and $\alpha \in \mathcal{F}(K)$. Our goal is to show that

$$\mathrm{RD}_k(\alpha) \leqslant \max\{\mathrm{RD}_{k'}(\alpha_{k'K}), 1\}. \tag{12}$$

If we can prove this, then taking the maximum over all $K \in \mathrm{Fields}_k$ and all $\alpha \in \mathcal{F}(K)$, we will obtain the desired inequality $\mathrm{RD}_k(\mathcal{F}) \leqslant \max\{\mathrm{RD}_{k'}(\mathcal{F}_{k'}), 1\}$.

We begin by reducing to the case where k' is finitely generated over k. Indeed, choose l as in Lemma 9.2. That is, l is finitely generated over k and $\mathrm{RD}_l(\alpha_{lK}) = \mathrm{RD}_{k'}(\alpha_{k'K})$. For the purpose of proving (12) we may now replace k' by l.

From now on we will assume k' is finitely generated over k. Choose a transcendence basis $t_1, \dots, t_n$ for k'/k and set $k_i = k(t_1, \dots, t_i)$, so that k' is algebraic over k_n. By (9),

$$\mathrm{RD}_{k_n}(\alpha_{k_n K}) = \mathrm{RD}_{k_n}(\alpha_{k' K}) = \mathrm{RD}_{k'}(\alpha_{k' K}).$$

Thus, we may further replace k' by k_n. It remains to show that

$$\mathrm{RD}_k(\alpha) \leqslant \max\{\mathrm{RD}_{k(t)}(\alpha_{K(t)}), 1\}, \tag{13}$$

where t is a variable. Indeed, applying this inequality recursively, we readily deduce (12):

$$\mathrm{RD}_k(\alpha) \leqslant \max\{\mathrm{RD}_{k_1}(\alpha_{k_1 K}), 1\} \leqslant \cdots \leqslant \max\{\mathrm{RD}_{k_n}(\alpha_{k_n K}), 1\}.$$

(Recall that here $k' = k_n$.)

The remainder of the proof will be devoted to establishing the inequality (13). First observe that we may assume without loss of generality that K is closed at level 1. Indeed, let $K^{(1)}$ be the level 1 closure of K. By Proposition 8.1 (c),

$$\mathrm{RD}_k(\alpha) \leqslant \max\{\mathrm{RD}_k(\alpha_{K^{(1)}}), 1\}$$

and by Lemma 7.6 (a),

$$\mathrm{RD}_{k(t)}(\alpha_{K^{(1)}(t)}) \leqslant \mathrm{RD}_{k(t)}(\alpha_{K(t)}),$$

where $K^{(1)}$ is the level 1 closure of K. These inequalities show that in the course of proving (13), we may replace K by $K^{(1)}$ and α by $\alpha_{K^{(1)}}$. In other words, for the purpose of proving (13), we may assume that K is closed at level 1. In particular, we may assume that K is a perfect field; see Corollary 6.5.

We now proceed with the proof of (13) under the assumption that K is a perfect field. First we observe that by Lemma 7.6 (a), $\mathrm{RD}_{k(t)}(\alpha_{K((t))}) \leqslant \mathrm{RD}_{k(t)}(\alpha_{K(t)})$. Thus, we only need to show that

$$\mathrm{RD}_k(\alpha) \leqslant \max\{\mathrm{RD}_{k(t)}(\alpha_{K((t))}), 1\}.$$

Set $d = \mathrm{RD}_{k(t)}(\alpha_{K((t))})$. By definition there exists a finite field extension $L/K((t))$ such that $\alpha_L = 1$ and $\mathrm{lev}_{k(t)}(L/K((t))) = d$.

The field $K((t))$ carries a natural discrete valuation $\nu\colon K((t))^* \to \mathbb{Z}$ with uniformizer t, trivial on K. Lift ν to a discrete valuation $L^* \to \frac{1}{e}\mathbb{Z}$, where e is the ramification index. By abuse of notation I will continue to denote this lifted valuation by ν. I will denote the residue field of L relative to this valuation by L_ν.

Note that since $K((t))$ is complete with respect to ν, so is L; see [38, Proposition II.2.3]. Moreover, since K is perfect, so is L_ν. Note also that we are in equal characteristic situation here:

$$\mathrm{char}(L_\nu) = \mathrm{char}(K) = \mathrm{char}(k) = \mathrm{char}(k(t)) = \mathrm{char}(K((t))) = \mathrm{char}(L).$$

By the Cohen structure theorem [13, Theorem 15], the local ring of ν in L is isomorphic to the power series ring $L_\nu[[s]]$ in one variable over L_ν; cf. also [38, Section II.4]. Hence, L is isomorphic to the field of Laurent series $L_\nu((s))$. Since $\alpha_L = 1$ and L_ν is perfect, the natural map

$$\mathcal{F}(L_\nu) \to \mathcal{F}(L_\nu((s))) = \mathcal{F}(L)$$

has trivial kernel, by our assumption (11). We conclude that $\alpha_{L_\nu} = 1$. In other words, L_ν/K is a splitting extension for α. By Proposition 5.1,

$$\mathrm{RD}_k(\alpha) \leqslant \mathrm{lev}_k(L_\nu/K) \leqslant \max\{\mathrm{lev}_k(L/K((t))), 1\} = \max\{d, 1\},$$

where K is the residue field of $K((t))$. This completes the proof of Proposition 9.1. ∎

10. The resolvent degree of an algebraic group

Let G be an algebraic group over k, not necessarily affine, smooth or connected. Of particular interest to us will be the functor $H^1(*, G)$ whose objects over K are isomorphism classes of G-torsors over $\mathrm{Spec}(K)$. Here torsors are assumed to be locally trivial in the flat (fppf) topology. If G is smooth over k, this is equivalent to being trivial in the étale topology; see [31, Remark 4.8 (a)]. For every field K containing k, the set $H^1(K, G)$ has a marked element, represented by the split G-torsor $G_K \to \mathrm{Spec}(K)$, where $G_K = G \times_{\mathrm{Spec}(k)} \mathrm{Spec}(K)$. The functor $H^1(*, G)$ satisfies condition (7).

Definition 10.1. Define $\mathrm{ed}_k(G) = \mathrm{ed}_k(H^1(*, G))$ and $\mathrm{RD}_k(G) = \mathrm{RD}_k(H^1(*, G))$.

The essential dimension $\mathrm{ed}_k(G)$ of an algebraic group G/k has been much studied; for an overview, see [30, 33, 34]. If G is an abstract finite group (viewed as an algebraic group over k) and $\mathrm{char}(k) = 0$, our definition of $\mathrm{RD}_k(G)$ above coincides with the definition given by Farb and Wolfson [20]. To the best of my knowledge, $\mathrm{RD}_k(G)$ has not been previously investigated for other algebraic groups G/k.

In view of Proposition 8.3 (b), passing from G to $G_{\bar{k}}$ does not change the resolvent degree. Thus from now on we will assume that k is algebraically closed.

Example 10.2. The functor $\mathrm{Ét}_n$ introduced in Example 7.5 is isomorphic to $H^1(*, \mathrm{S}_n)$ and thus $\mathrm{RD}_k(\mathrm{Ét}_n) = \mathrm{RD}_k(\mathrm{S}_n)$. By Example 7.5,

$$\mathrm{RD}_k(\mathrm{S}_n) = \max\ \mathrm{lev}_k(L/K).$$

The algebraic form of Hilbert's 13th problem asks for the value of $\mathrm{RD}(n) = \mathrm{RD}_{\mathbb{C}}(\mathrm{S}_n)$.

Remark 10.3. Recall that the classical definition of $\mathrm{RD}(n)$ is motivated by wanting to express a root of a general polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ as a composition of algebraic functions in $\leqslant d$ variables. This is equivalent to finding the smallest integer d such that the 0-cycle in $\mathbb{A}^1_K$ given by $f(x) = 0$ has an L-point, for some field extension L/K of level $\leqslant d$. If G is an algebraic group over k, K is a field containing k and $T \to \mathrm{Spec}(K)$ is a G-torsor, then our definition of $\mathrm{RD}_k(T)$ retains this flavor. Indeed, saying that T is split by L is equivalent to saying that T has an L-point.

Remark 10.4 (cf. [20, Lemma 3.2]). Let G be an algebraic group defined over a field k, K be a field containing k, and $\alpha\colon T \to \mathrm{Spec}(K)$ be a G-torsor. Setting $\mathcal{F} = H^1(*, G)$ in Lemma 7.6, we obtain the inequalities $\mathrm{RD}_k(\alpha) \leqslant \mathrm{ed}_k(\alpha)$ and $\mathrm{RD}_k(G) \leqslant \mathrm{ed}_k(G)$.

Remark 10.5 (cf. [20, Lemma 3.13]). Let G be a finite group and H be a subgroup. We will view G and H as algebraic groups over k. The long exact sequence in Galois cohomology associated to $1 \to H \xrightarrow{i} G$ (see [40, Section I.5.4]) readily show that the induced morphism $i_*\colon H^1(*, H) \to H^1(*, G)$ has trivial kernel. By Lemma 7.9 (b), we conclude that $\mathrm{RD}_k(H) \leqslant \mathrm{RD}_k(G)$.

Example 10.6 (cf. [20, Corollary 3.4]). If G is a solvable finite group, then $\mathrm{RD}_k(G) \leqslant 1$. Indeed, every element of $H^1(K, G)$ can be split by a solvable extension L/K, and a solvable extension has level $\leqslant 1$ by Lemma 4.6 (a). Moreover, if we further assume that $G \neq 1$, then $\mathrm{RD}_k(G) = 1$. This follows from Lemma 7.8 and Proposition 8.3 (b).

Recall that an algebraic group G defined over a field k is called special if $H^1(*, G)$ is the trivial functor, i.e., $H^1(K, G) = 1$ for every field K containing k. This notion is due to Serre [37]. (Note that [37] is reprinted in [41].)

Lemma 10.7. *Let G be an algebraic group over an algebraically closed field k. Then:*

(a) *G is special if and only if* $\mathrm{RD}_k(G) = 0$.

(b) *If G is connected and solvable, then* $\mathrm{RD}_k(G) = 0$.

(c) *If G is the general linear group* GL_n*, the special linear group* SL_n *or the symplectic group* Sp_{2n}*, then* $\mathrm{RD}_k(G) = 0$ *for any $n \geqslant 1$.*

Proof. (a) By Lemma 7.8, $\mathrm{RD}_k(G) = 0$ if and only if $H^1(*, G)$ is the trivial functor, i.e., if and only if G is special.

(b) Every connected solvable group is special; see [37, Section 4.4 (a)].

(c) GL_n is special by Hilbert's Theorem 90. For SL_n and Sp_{2n}, see [37, Section 4.4 (b) and (c)], respectively. ■

We now record several simple but useful observations about the behavior of resolvent degree in exact sequences of groups.

Proposition 10.8. *Consider a short exact sequence of algebraic groups*

$$1 \to A \to B \to C \to 1 \tag{14}$$

defined over a field k. Then:

(a) (Cf. [20, Theorem 3.3].) $\mathrm{RD}_k(B) \leqslant \max\{\mathrm{RD}_k(A), \mathrm{RD}_k(C)\}$.

(b) (Cf. [20, Theorem 3.3].) *If B is isomorphic to the direct product $A \times C$, then* $\mathrm{RD}_k(B) = \max\{\mathrm{RD}_k(A), \mathrm{RD}_k(C)\}$.

(c) *If G is a diagonalizable algebraic group over k, then* $\mathrm{RD}_k(G) \leqslant 1$.

(d) *Suppose (14) is a central short exact sequence and A is diagonalizable over k. Then*

$$\mathrm{RD}_k(B) \leqslant \max\{\mathrm{RD}_k(C), 1\} \quad \textit{and} \quad \mathrm{RD}_k(C) \leqslant \max\{\mathrm{RD}_k(B), 1\}.$$

Proof. (a) follows from Lemma 7.9 (a) applied to the exact sequence of functors $H^1(*, A) \to H^1(*, B) \to H^1(*, C)$ induced by (14).

(b) follows from Lemma 7.9 (d), since in this case the functor $H^1(*, B)$ is isomorphic to $H^1(*, A) \times H^1(*, C)$.

(c) Write G as a product $G_1 \times \cdots \times G_r$, where each G_i is isomorphic either to $\mathbb{G}_m$ or μ_n for some $n \geqslant 2$. By part (b), it suffices to show that $\mathrm{RD}_k(G_i) \leqslant 1$ for each i. Now recall that $\mathrm{RD}_k(\mathbb{G}_m) = 0$ by Lemma 10.7 (b). On the other hand, $\mathrm{RD}_k(\mu_n) \leqslant \mathrm{ed}_k(\mu_n)$ by Remark 10.4, and $\mathrm{ed}_k(\mu_n) = 1$ for every $n \geqslant 2$; see, e.g., [30, Example 3.5].

(d) To prove the first inequality, combine parts (a) and (c). The second inequality follows from Lemma 7.9 (a) applied to the exact sequences of functors $H^1(*, B) \to H^1(*, C) \to H^2(*, A)$ induced by (14). Recall that $\mathrm{RD}_k(H^2(*, A)) \leqslant 1$ by Proposition 7.10. ■

Corollary 10.9. *Let G be a connected reductive affine algebraic group, T be a split maximal torus of G, N be the normalizer of T in G, and $W = N/T$ be the Weyl group. Then*

$$\mathrm{RD}_k(W) \geqslant \mathrm{RD}_k(N) \geqslant \mathrm{RD}_k(G).$$

Proof. By [11, Corollary 5.3] the natural morphism $H^1(K, N) \to H^1(K, G)$ is surjective; see also [40, Lemma III.4.3.6]. Hence, $\mathrm{RD}_k(N) = \mathrm{RD}(H^1(*, N)) \geqslant \mathrm{RD}_k(H^1(*, G)) = \mathrm{RD}_k(G)$ by Lemma 7.9 (c).

The inequality $\mathrm{RD}_k(W) \geqslant \mathrm{RD}_k(N)$ follows from Proposition 10.8 (a) applied to the exact sequence $1 \to T \to N \to W \to 1$. Note that by Lemma 10.7 (b), $\mathrm{RD}_k(T) = 0$. ■

11. The resolvent degree of an abelian variety

In this section we will assume that the base field k is algebraically closed. This assumption is harmless in view of Proposition 8.3 (b).

Recall that for every algebraic group G defined over k, there exists a smooth (i.e., reduced) subgroup G_{red} such that $G(k) = G_{\mathrm{red}}(k)$; see [15, Exp. $\mathrm{VI_A}$, Section 0.2].

Lemma 11.1. *Let K be a field containing k and let $i\colon G_{\mathrm{red}} \hookrightarrow G$ be the natural inclusion and $i_*\colon H^1(K, G_{\mathrm{red}}) \to H^1(K, G)$ be the induced map in cohomology. Then:*

(a) *i_* is injective.*

(b) *If K is a perfect field, then i_* is bijective.*

Proof. Let $\gamma \in H^1(K, G)$. By [40, Section I.5.4, Corollary 2], the fiber of $(i_*)^{-1}(\gamma)$ may be identified with the set of orbits of ${}_\gamma G(K)$ in $({}_\gamma G/{}_\gamma G_{\mathrm{red}})(K)$.[2] Here ${}_\gamma G$ denotes the twist of G by a cocycle representing γ, and similarly for G_{red}. Since the homogeneous space G/G_{red} is purely inseparable over $\mathrm{Spec}(k)$, the homogeneous space ${}_\gamma G/{}_\gamma G_{\mathrm{red}}$ is purely inseparable over $\mathrm{Spec}(K)$. (To see this, pass to a splitting field of γ.) Thus, ${}_\gamma G/{}_\gamma G_{\mathrm{red}}$ can have at most one $\mathrm{Spec}(K)$-point. This shows that the fiber of $(i_*)^{-1}(\gamma)$ has at most one element, proving (a). If K is perfect, then the homogeneous space ${}_\gamma G/{}_\gamma G_{\mathrm{red}}$ has exactly one K-point. In this case the fiber of $(i_*)^{-1}(\gamma)$ has exactly one element for every $\gamma \in H^1(K, G_{\mathrm{red}})$. This proves (b). ■

Recall that an infinitesimal group is a connected 0-dimensional group. Non-trivial infinitesimal groups exist only in prime characteristic.

Proposition 11.2. *Let G be an algebraic group over k. Then:*

(a) $\mathrm{RD}_k(G) \leqslant \max\{\mathrm{RD}_k(G_{\mathrm{red}}), 1\}$.

(b) *If G be an infinitesimal group over k, then* $\mathrm{RD}_k(G) \leqslant 1$.

(c) *Let G be a 0-dimensional abelian group over k (not necessarily smooth or connected). Then* $\mathrm{RD}_k(G) \leqslant 1$.

Proof. (a) In view of Proposition 8.1 (d), it suffices to show that $\mathrm{RD}_k(\alpha) \leqslant \mathrm{RD}_k(G_{\mathrm{red}})$ for every field K/k such that K is closed at level 1 and every $\alpha \in H^1(K, G)$. Indeed, every such field K is perfect; see Corollary 6.5. Thus by Lemma 11.1, α is the image of some $\beta \in H^1(K, G_{\mathrm{red}})$. Every field extension of K which splits β also splits α. This tells us that

$$\mathrm{RD}_k(\alpha) \leqslant \mathrm{RD}_k(\beta) \leqslant \mathrm{RD}_k(G_{\mathrm{red}}),$$

[2] In [40] only étale cohomology is considered. The same argument works for flat cohomology.

as claimed.

(b) If G is infinitesimal, then $G_{\mathrm{red}} = 1$. Thus, $\mathrm{RD}_k(G_{\mathrm{red}}) = 0$, and $\mathrm{RD}_k(G) \leqslant 1$ by part (a).

(c) Consider the exact sequence $1 \to G^0 \to G \to G/G^0 \to 1$. The group G^0 is infinitesimal; thus $\mathrm{RD}_k(G^0) \leqslant 1$ by part (b). On the other hand, by [15, Exp. VI_{A}, Proposition 5.5.1], G/G^0 is étale. Since k is algebraically closed, this tells us that G/G^0 is constant, i.e., is isomorphic to an abstract finite abelian group, viewed as an algebraic group over k. In particular, $\mathrm{RD}_k(G/G^0) \leqslant 1$ by Example 10.6. Applying Proposition 10.8 (a) to the exact sequence $1 \to G^0 \to G \to G/G^0 \to 1$, we obtain $\mathrm{RD}_k(G) \leqslant 1$. ∎

Proposition 11.3. *Let A be an abelian variety over k. Then* $\mathrm{RD}_k(A) \leqslant 1$.

Proof. Let K be a field containing k. Recall that $H^1(K, A)$, the Weil–Châtelet group of A_K, is torsion; see [28, p. 663]. Thus, it suffices to show that $\mathrm{RD}_k(H^1(*, A)[d]) \leqslant 1$ for every integer $d \geqslant 1$. Examining the exact sequence in cohomology associated to

$$1 \longrightarrow A[d] \longrightarrow A \xrightarrow{\times d} A \longrightarrow 1$$

we conclude that $H^1(*, A[d])$ surjects onto $H^1(*, A)[d]$; see [42, Section VIII.2]. (In [42], A is assumed to be an elliptic curve, but the same argument goes through for an abelian variety of arbitrary dimension.) Lemma 7.9 (c) now tells us that

$$\mathrm{RD}_k\big(H^1(*, A)[d]\big) \leqslant \mathrm{RD}_k\big(H^1(*, A[d])\big) \stackrel{\text{def}}{=} \mathrm{RD}_k(A[d]).$$

Since $A[d]$ is a 0-dimensional abelian group over k, $\mathrm{RD}_k(A[d]) \leqslant 1$ by Proposition 11.2 (c). Thus, $\mathrm{RD}_k(H^1(*, A)[d]) \leqslant 1$ for every $d \geqslant 1$, as claimed. ∎

12. Proof of Theorem 1.2

Setting $\mathcal{F}$ to be the non-abelian cohomology functor $H^1(*, G)$ in Proposition 8.3 (b), we obtain $\mathrm{RD}_k(G) = \mathrm{RD}_{\overline{k}}(G)$ and $\mathrm{RD}_{k'}(G) = \mathrm{RD}_{\overline{k'}}(G_{\overline{k'}})$, where $\overline{k}$ is the algebraic closure of k and similarly for k'. After replacing k and k' by $\overline{k}$ and $\overline{k'}$, we may assume that k and k' are algebraically closed.

The following two lemmas will allow us to complete the proof by appealing to Proposition 9.1. Lemma 12.1 tells us that the conditions of Proposition 9.1 are satisfied by the non-abelian cohomology functor $\mathcal{F} = H^1(*, G)$ and thus

$$\mathrm{RD}_{k'}(G_{k'}) \leqslant \mathrm{RD}_k(G) \leqslant \{\mathrm{RD}_{k'}(G_{k'}), 1\}.$$

This yields the desired equality, $\mathrm{RD}_k(G) = \mathrm{RD}_{k'}(G_{k'})$, assuming $\mathrm{RD}_{k'}(G_{k'}) \geqslant 1$. Lemma 12.2 shows that this equality also holds when $\mathrm{RD}_{k'}(G_{k'}) = 0$.

Lemma 12.1. *Let k be algebraically closed field and G be an algebraic group over k. Then the natural map $H^1(E,G) \to H^1(E((t)),G)$ has trivial kernel for every perfect field E containing k.*

Proof. We begin by reducing the problem to the case where G is smooth. Indeed, let G_{red} be the associated smooth group. Consider the following diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & H^1(E,G_{\text{red}}) & \longrightarrow & H^1(E,G) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H^1(E((t)),G_{\text{red}}) & \longrightarrow & H^1(E((t)),G), & & \end{array}$$

where the bottom row is exact by Lemma 11.1 (a) and the top row is exact by Lemma 11.1 (b). (Recall that we are assuming E to be perfect.) An easy diagram chase shows that if the left vertical map has trivial kernel, then so does the right vertical map. In other words, if the lemma holds for G_{red}, then it also holds for G. From now on we will assume that G is smooth.

Now suppose $\alpha \in H^1(E,G)$ lies in the kernel of the map $H^1(E,G) \to H^1(E((t)),G)$. This means that the G-torsor $\pi\colon T \to \operatorname{Spec}(E)$ representing α splits over $\operatorname{Spec}(E((t)))$. In other words, $\pi_{E[[t]]}\colon T \times \operatorname{Spec}(E[[t]]) \to \operatorname{Spec}(E[[t]])$ has a section $s\colon \operatorname{Spec}(E((t))) \to T \times \operatorname{Spec}(E((t)))$ over the generic point of $\operatorname{Spec}(E[[t]])$.

We would like to show that this section extends to all of $\operatorname{Spec}(E[[t]])$. If we manage to do this, then restricting to the closed point of $\operatorname{Spec}(E[[t]])$ (i.e., setting $t = 0$), we obtain an E-point on T. This shows that T is split, i.e., $\alpha = [T] = 1$ in $H^1(E,G)$, as desired.

To prove that s can be extended to all of $\operatorname{Spec}(E[[t]])$, it is natural to appeal to the valuative criterion for properness. If G is proper over $\operatorname{Spec}(k)$ (i.e., the identity component of G is an abelian variety), then T is proper over $\operatorname{Spec}(K)$, a desired lifting exists by the valuative criterion for properness, and the proof is complete. In general, T is not proper over $\operatorname{Spec}(K)$, so the valuative criterion for properness does not apply. Nevertheless, we will now see that a variant of this argument still goes through, if we modify T slightly as follows.

By Chevalley's structure theorem [12, 14] there exists a unique connected smooth normal affine k-subgroup $N = G^0_{\text{aff}}$ of G^0 such that the quotient G^0/N is an abelian variety. Since G is smooth and k is an algebraically closed field, N is smooth, connected and normal in G, and G/N is proper over $\operatorname{Spec}(k)$; see [3, Theorem 4.2 and Remark 4.3].

Let B be a Borel subgroup (i.e., a maximal connected solvable subgroup) of N. Then the homogeneous space N/B is proper over $\operatorname{Spec}(k)$. Consequently, G/B is proper over G/N. Since G/N is proper over $\operatorname{Spec}(k)$, we conclude that G/B is proper over Spec(k) and hence, T/B is proper over Spec(K). Now the valuative criterion for properness tells us that the section

$$s\colon \mathrm{Spec}\big(E((t))\big) \to T_{\mathrm{Spec}(E[\![t]\!])} \to (T/B)_{\mathrm{Spec}(E[\![t]\!])}$$

extends to Spec$(E[\![t]\!])$. Restricting to the closed point of Spec$(E[\![t]\!])$, we obtain an E-point on T/B. Denote this point by $p\colon \mathrm{Spec}(E) \to T/B$. The preimage of this E-point under the natural map $T \to T/B$ is a B-torsor over Spec(E). Since B is connected and solvable, it is special; see Lemma 10.7 (b). Thus, this B-torsor is split, i.e., has an E-point. This shows that T has an E-point, i.e., T is split over E, as desired. ∎

Lemma 12.2. *Let $k \subset k'$ be algebraically closed fields and G be an algebraic group over k. Then the following conditions are equivalent.*

(a) $\mathrm{RD}_{k'}(G_{k'}) = 0$;

(b) *$G_{k'}$ is a special group;*

(c) *$G_{k'}$ is affine, and* $\mathrm{ed}_{k'}(G_{k'}) = 0$;

(d) *G is affine, and* $\mathrm{ed}_k(G) = 0$;

(e) *G is a special group;*

(f) $\mathrm{RD}_k(G) = 0$.

Proof. (a) $\Longleftrightarrow$ (b) and (e) $\Longleftrightarrow$ (f) by Lemma 10.7 (a).

(b) $\Longrightarrow$ (c): Suppose $G_{k'}$ is special, i.e., $H^1(*, G_{k'})$ is the trivial functor. Then clearly $\mathrm{ed}_{k'}(G_{k'}) = \mathrm{ed}_{k'}(H^1(*, G_{k'})) = 0$. Moreover, a special group is affine; see [37, Theorem 4.1].

(c) $\Longleftrightarrow$ (d): G is affine if and only if $G_{k'}$ is affine. Moreover, since k is algebraically closed and G is an affine group over k, we have $\mathrm{ed}_k(G) = \mathrm{ed}_{k'}(G_{k'})$; see [4, Proposition 2.14] or [49, Example 4.10].

(d) $\Longrightarrow$ (e) by [30, Proposition 3.16].

(f) $\Longrightarrow$ (a): By Proposition 8.3 (a) with $\mathcal{F} = H^1(*, G)$, $\mathrm{RD}_k(G) \geqslant \mathrm{RD}_{k'}(G_{k'})$. In particular, if $\mathrm{RD}_k(G) = 0$, then $\mathrm{RD}_{k'}(G_{k'}) = 0$. ∎

13. Proof of Theorem 1.3

Our proof of Theorem 1.3 will rely on the following proposition.

Proposition 13.1. *Let D be a discrete valuation ring with fraction field k and residue field k_0. Let G be a smooth affine group scheme over D. Assume that the connected* *component G^0 is reductive and the component group G/G^0 is finite over D. If* $\mathrm{char}(k) = 0$ *and* $\mathrm{char}(k_0) = p > 0$*, assume further that the absolute ramification index of D is* 1*. Then*

$$\mathrm{RD}_{k_0}(G_{k_0}) \leqslant \max\{\mathrm{RD}_k(G_k), 1\}.$$

Recall that the absolute ramification index of D is defined as $\nu(p)$, where $\nu: k^* \to \mathbb{Z}$ is the discrete valuation.

Proof. First observe that we may replace D by its completion $\widehat{D}$. Indeed, denote the fraction field of $\widehat{D}$ by $\widehat{k}$. Then $k \subset \widehat{k}$, and the residue field k_0 remains unchanged. By Proposition 8.3 (a), $\mathrm{RD}_{\widehat{k}}(G_{\widehat{k}}) \leqslant \mathrm{RD}_k(G_k)$. Thus, it suffices to show that $\mathrm{RD}_{k_0}(G_{k_0}) \leqslant \max\{\mathrm{RD}_{\widehat{k}}(G_{\widehat{k}}), 1\}$.

After replacing D by $\widehat{D}$, we may assume that D is complete. Under the assumptions of the proposition, $D = W(k_0)$; see [38, Sections II.4–5]. Here for any field K_0 containing k_0 we define $W(K_0)$ to be the ring of power series $K_0[\![t]\!]$ if $\mathrm{char}(k) = \mathrm{char}(k_0)$ and the ring of Witt vectors with coefficients in K_0 if $\mathrm{char}(k) = 0$ and $\mathrm{char}(k_0) = p > 0$; see [38, Section II.6].

Now let K_0 be a field containing k_0 and $\pi: T_0 \to \mathrm{Spec}(K_0)$ be a G_{k_0}-torsor. Set $R = W(K_0)$. Recall that R is a complete local ring relative to a valuation $\nu: R \to \mathbb{Z}$ with residue field K_0, extending the valuation on D. By [16, Exp. XXIV, Proposition 8.1], the natural map $H^1(R, G) \to H^1(K_0, G)$ is bijective. In particular, there exists a G_R-torsor $\pi_R: T \to \mathrm{Spec}(R)$ which restricts to π over the closed point $\mathrm{Spec}(K_0) \to \mathrm{Spec}(R)$. Let K be the field of fractions of $R = W(K_0)$ and $\pi_K: T_K \to \mathrm{Spec}(K)$ be the restriction of π to the generic point of $\mathrm{Spec}(R)$. Our goal is to show that

$$\mathrm{RD}_{k_0}(T_{K_0}) \leqslant \max\{\mathrm{RD}_k(T_K), 1\}. \tag{15}$$

This inequality tells us that $\mathrm{RD}_{k_0}(T_{K_0}) \leqslant \max\{\mathrm{RD}_k(G_k), 1\}$. Taking the maximum of the left-hand side over all $K_0 \in \mathrm{Fields}_{k_0}$ and all G_{k_0}-torsors $T_0 \to \mathrm{Spec}(K_0)$, we arrive at $\mathrm{RD}_{k_0}(G_{k_0}) \leqslant \max\{\mathrm{RD}_k(G_k), 1\}$, as desired.

It remains to prove the inequality (15). By the definition of $d = \mathrm{RD}_k(T_K)$ there exists a finite field extension L/K such that L splits T_K and $\mathrm{lev}_k(L/K) \leqslant d$. The valuation ν extends from K and to L. Once again, by abuse of notation I will continue to denote this extended valuation by $\nu: L^* \to \mathbb{Z}$. I will also denote the valuation ring for this valuation by S and the residue field by L_0. Now consider the diagram of natural morphisms

$$
\begin{array}{ccc}
T_S & \longrightarrow & T_L \\
\downarrow & H^1(S, G_S) \hookrightarrow H^1(L, G_L) & \\
& \downarrow & \\
T_{L_0} & H^1(L_0, G_{L_0}). &
\end{array}
\tag{16}
$$

The horizontal map is injective by [35, Lemma 3.3 (b)]. Note that the assumptions of Theorem 1.3, that G^0 is reductive and G/G^0 is finite over D (and hence, over R and over S), are used to ensure that [35, Lemma 3.3 (b)] applies.

Since T_K splits over $\mathrm{Spec}(L)$, the injectivity of the horizontal map in (16) tells us that T splits over $\mathrm{Spec}(S)$. Consequently, T_{K_0} splits over $\mathrm{Spec}(L_0)$. This tells us that

$$\mathrm{RD}_{k_0}(T_{K_0}) \leqslant \mathrm{lev}_{k_0}(L_0/K_0) \leqslant \max\{\mathrm{lev}_k(L/K), 1\} \leqslant \max\{d, 1\},$$

where the middle inequality is given by Proposition 5.1. This completes the proof of the inequality (15) and thus of Proposition 13.1. ■

We now proceed with the proof of Theorem 1.3. If $\mathrm{char}(k) = \mathrm{char}(k_0)$, then by Theorem 1.2, $\mathrm{RD}_k(G_k) = \mathrm{RD}_F(G_F) = \mathrm{RD}_{k_0}(G_{k_0})$, where F is the prime field. Thus, we may assume without loss of generality that $\mathrm{char}(k) = 0$ and $\mathrm{char}(k_0) = p > 0$. Moreover, we are free to replace k by any field of characteristic 0 and k_0 by any field of characteristic p.

If $\mathrm{RD}_k(G_k) \geqslant 1$ for some (and thus every) field of characteristic 0, then the desired inequality $\mathrm{RD}_{k_0}(G_{k_0}) \leqslant \mathrm{RD}_k(G_k)$ readily follows from Proposition 13.1, applied to the group scheme G_D, where $D = W(k_0) =$ the ring of Witt vectors with coefficients in k_0.

I will treat the case where $\mathrm{RD}_k(G_k) = 0$ separately, as in the previous section. Once again, we are free to choose k to be any field of characteristic 0 and k_0 to be any field of characteristic p. In particular, we may assume that both k and k_0 are algebraically closed. Now by Lemma 10.7 (a), it suffices to show that if G_k is special, then G_{k_0} is special.

Indeed, if G_k is special, then G_k is connected [37, Theorem 4.1]. Hence, G and G_{k_0} are also connected. On the other hand, since k and k_0 are algebraically closed, we may appeal to the classification of special groups over an algebraically closed field due to Grothendieck [24, Theorem 3]. According to this classification, G_k is special if and only if its derived subgroup is a direct product $G_1 \times \cdots \times G_r$, where each G_i is a simply connected simple group of type A or C. This property is encoded into the root datum, which is the same for G_k, G, and G_{k_0}; see [16, Exp. XXV, Section 1]. (Note that this is the only step in the proof of Theorem 1.3 which uses the assumption that G^0 is split.) We conclude that G_k is special if and only if G_{k_0} is special. This finishes the proof of Theorem 1.3. ■

Remark 13.2. Our proof of Proposition 13.1 relies on [35, Lemma 3.3 (b)], which asserts that the horizontal homomorphism in diagram (16) is injective. This lemma is a variant of the Grothendieck–Serre conjecture over a Henselian discrete valuation ring. A theorem of Nisnevich [32], establishing the Grothendieck–Serre conjecture in this context, is a key ingredient in the proof of [35, Lemma 3.3 (b)] and thus of Proposition 13.1 and Theorem 1.3 in this paper.

14. Upper bounds on the resolvent degree of a group

Consider an action of a linear algebraic group G on an algebraic variety X (not necessarily connected) defined over a field k. We will say that this action is generically free if there exists a dense G-invariant open subset $U \subset X$ such that the scheme-theoretic stabilizer G_u is trivial for every geometric point $u \in U$. In this section we will prove the following.

Proposition 14.1. *Let G be a closed subgroup of* PGL_{n+1} *defined over k. Suppose there exists a G-invariant closed subvariety X of $\mathbb{P}^n$ of degree a and dimension b.*

(a) (Cf. [51, Proposition 4.11].) *If the G-action on X is generically free, then*

$$\mathrm{RD}_k(G) \leqslant \max\{b - \dim(G), \mathrm{RD}_k(\mathrm{S}_a), 1\},$$

where S_a denotes the symmetric group on a letters.

(b) *Suppose there exists a G-invariant quadric hypersurface $Q \subset \mathbb{P}(V)$ of rank r such that* $\dim(Q \cap X) = b - 1$. *Assume further the G-action on $Q \cap X$ is generically free, and $b \geqslant \lfloor \frac{r+1}{2} \rfloor$. Then*

$$\mathrm{RD}_k(G) \leqslant \max\{b - 1 - \dim(G), \mathrm{RD}_k(\mathrm{S}_a), 1\}.$$

Remark 14.2. (1) Note that $\mathrm{RD}_k(\mathrm{S}_a) \geqslant 1$ if $a \geqslant 2$. Thus, for $a \geqslant 2$, the conclusions of parts (a) and (b) simplify to $\mathrm{RD}_k(G) \leqslant \max\{b - \dim(G), \mathrm{RD}_k(\mathrm{S}_a)\}$ and $\mathrm{RD}_k(G) \leqslant \max\{b - \dim(G) - 1, \mathrm{RD}_k(\mathrm{S}_a)\}$, respectively.

(2) By the rank r of Q we mean the rank of some (and thus any) quadratic form defining Q. The maximal value of r is $n + 1$; it is attained when Q is non-singular. In particular, the condition that $b \geqslant \lfloor \frac{r+1}{2} \rfloor$ is automatically satisfied if $b \geqslant \lfloor \frac{n+2}{2} \rfloor$. If X is a hypersurface, i.e., $b = n - 1$, then it is automatically satisfied whenever $n \geqslant 3$.

(3) Note that by Theorem 1.2, $\mathrm{RD}_k(\mathrm{S}_a) = \mathrm{RD}_{\mathbb{C}}(\mathrm{S}_a)$ for any field k of characteristic 0 and $\mathrm{RD}_k(\mathrm{S}_a) \leqslant \mathrm{RD}_{\mathbb{C}}(\mathrm{S}_a)$ for any field k of positive characteristic. Thus, $\mathrm{RD}_k(\mathrm{S}_a)$ can be replaced by $\mathrm{RD}_{\mathbb{C}}(\mathrm{S}_a)$ in the statement of the proposition.

Example 14.3. (1) If we take $X = \mathbb{P}^n$ in part (a), we obtain $\mathrm{RD}_k(G) \leqslant n - \dim(G)$. In particular, if an abstract finite group G has an n-dimensional faithful projective representation over k, then $\mathrm{RD}_k(G) \leqslant n$. (The G-action on $\mathbb{P}^n$ is automatically generically free in this case.) In particular, since the alternating group A_a acts faithfully on $\mathbb{P}^1$ for $a \leqslant 5$, we obtain $\mathrm{RD}_k(\mathrm{A}_a) \leqslant 1$ for every $a \leqslant 5$. Similarly, since A_6 and A_7 have complex projective representations of dimension 2 and 3, respectively, we deduce classical upper bounds $\mathrm{RD}_{\mathbb{C}}(\mathrm{A}_6) \leqslant 2$ and $\mathrm{RD}_{\mathbb{C}}(\mathrm{A}_7) \leqslant 3$; see [17, Sections 3 and 4], [20, Theorem 5.6].

Note also that $\mathrm{RD}_k(\mathrm{S}_n) = \mathrm{RD}_k(\mathrm{A}_n)$ for any $n \geqslant 3$; this follows from Proposition 10.8 (a) applied to the exact sequence $1 \to \mathrm{A}_n \to \mathrm{S}_n \to \mathbb{Z}/2\mathbb{Z} \to 1$.

(2) More generally, the classical upper bound $\mathrm{RD}_k(\mathrm{S}_n) \leqslant n - 4$ for any $n \geqslant 5$ can be deduced from Proposition 14.1 (b) as follows. Consider the $(n-1)$-dimensional subspace of k^n given by $x_1 + x_2 + \cdots + x_n = 0$. The group S_n acts on this space by permuting the coordinates. This yields an embedding $\mathrm{S}_n \hookrightarrow \mathrm{PGL}_{n-2}$. The desired inequality now follows from Proposition 14.1 (b), where we take X to be the cubic hypersurface given by $s_3 = 0$ and Q to be the quadric $s_2 = 0$; see Remark 14.2 (2). Here s_i denotes the ith elementary symmetric polynomial in $x_1, \ldots, x_n$.

(3) The group $G = \mathrm{PSL}_2(\mathbb{F}_7)$ acts faithfully on the quartic curve $X \subset \mathbb{P}^2$ given by $x^3y + y^3z + z^3x = 0$ (the Klein quartic). By Proposition 14.1 (a),

$$\mathrm{RD}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_7)) \leqslant \max\{1, \mathrm{RD}_{\mathbb{C}}(\mathrm{S}_4), 1\} = 1.$$

This inequality was known to Felix Klein; for an alternative proof and historical references, see [19, Proposition 4.13 (2)].

None of the upper bounds in Example 14.3 are new; the point here is that they can all be deduced from Proposition 14.1 in a uniform way. The remainder of this section will be devoted to proving Proposition 14.1. We begin with two lemmas.

Lemma 14.4. *Let k be a field, $K \in \mathrm{Fields}_k$ be closed at level d, and $\emptyset \neq X \subset \mathbb{P}^n$ be a projective variety of degree $\leqslant a$ defined over K. If $d \geqslant \max\{\mathrm{RD}_k(\mathrm{S}_a), 1\}$, then:*

(a) *K-points are dense in X.*

(b) *Assume further that $Q \subset \mathbb{P}^n$ is a quadric hypersurface of rank r defined over K and $\dim(X) \geqslant \lfloor \frac{r+1}{2} \rfloor$. Then K-points are dense in $X \cap Q$.*

Proof. (a) We argue by induction on n. The base case, where $n = 1$, reduces to the assertion that every non-constant homogeneous polynomial $f(x, y) \in K[x, y]$ of degree $\leqslant a$ splits into a product of linear factors over K. This assertion follows from Example 8.4. (Recall that $\mathrm{RD}_k(\mathrm{S}_n) = \mathrm{RD}_k(\mathrm{\acute{E}t}_n)$; see Example 10.2.)

For the induction step, assume $n \geqslant 2$ and consider the incidence variety

$$\begin{array}{ccc} & I = \{(p, L) \in X \times \widehat{\mathbb{P}}^n \mid p \in L\} & \\ \swarrow^{\pi_1} & & \searrow^{\pi_2} \\ X & & \widehat{\mathbb{P}}^n, \end{array}$$

where $\widehat{\mathbb{P}}^n$ is the dual projective space parametrizing hyperplanes in $\mathbb{P}^n$ and π_1, π_2 are projections to the first and second factor, respectively. Clearly π_1 is surjective; there is a hyperplane in $\mathbb{P}^n$ through every point of X. By the induction assumption, K-points are dense $\pi_2^{-1}(L)$ for every $L \in \widehat{\mathbb{P}}^n(K)$. Since K-points are dense in $\widehat{\mathbb{P}}^n$, we conclude that K-points are dense in I. Projecting them to X via π_1, we see that K-points are dense in X, as desired.

(b) Since K is closed at level $d \geqslant 1$, every quadratic form splits over K. That is, Q is the zero locus of a split quadratic form $q(x_0, \dots, x_n)$ of rank r over K. Let $m = \lfloor \frac{r}{2} \rfloor + (n + 1 - r)$ and $\mathrm{Gr}_q(m, n + 1)$ be the isotropic Grassmannian of maximal isotropic subspaces of q. In other words, $\mathrm{Gr}_q(m, n + 1)$ parametrizes linear subspaces of (projective) dimension $m - 1$ which are contained in Q. Since q is split, K-points are dense in $\mathrm{Gr}_q(m, n + 1)$. Consider the incidence variety

$$\begin{array}{ccc} & I = \big\{(p, L) \in (Q \cap X) \times \mathrm{Gr}_q(m, n + 1) \mid p \in L\big\} & \\ \swarrow^{\pi_1} & & \searrow^{\pi_2} \\ Q \cap X & & \mathrm{Gr}_q(m, n + 1). \end{array}$$

Note that there exists a maximal isotropic subspace through every point of Q; in particular, π_1 is surjective. On the other hand, our assumption that $\dim(X) \geqslant \lfloor \frac{r+1}{2} \rfloor$ ensures that $\dim(L) + \dim(X) = (m - 1) + \dim(X) \geqslant n$ and thus $L \cap X \neq \emptyset$ for every $L \in \mathrm{Gr}_q(m, n + 1)$. This tells us that π_2 is surjective. The fiber $\pi_1^{-1}(L) = L \cap X$ of a K-rational point L of $\mathrm{Gr}_q(m, n + 1)$ is a closed subvariety of degree $\leqslant a$ in $L \simeq \mathbb{P}^{m-1}$ defined over K. By part (a), K-points are dense in every such fiber. Since K-points are dense in $\mathrm{Gr}_q(m, n + 1)$, we conclude that K-points are dense in I. Projecting them to $Q \cap X$ via π_1, we see that K-points are dense in $Q \cap X$ as well. ∎

Lemma 14.5. *Consider a generically free action of an algebraic group G on an algebraic variety X defined over a field k. Supposed that K-points are dense in the* *twisted variety* ${}_TX$ *for every field* K *containing* k*, closed at level* d *and every* G*-torsor* $T \to \operatorname{Spec}(K)$*. Then* $\mathrm{RD}_k(G) \leqslant \max\{d, \dim(X) - \dim(G)\}$.

Proof. Let K/k be a field closed at level d and $T \to \operatorname{Spec}(K)$ be a G-torsor. By Proposition 8.1 (c) it suffices to show that

$$\mathrm{RD}_k(T) \leqslant \dim(X) - \dim(G). \tag{17}$$

After replacing X by a suitable G-invariant union of its irreducible components, we may assume that G transitively permutes the irreducible components of X. In this case there exists a G-invariant dense open subvariety $U \subset X$, which is the total space of a G-torsor $U \to B$. By our assumption ${}_TU$ has a K-point. Equivalently, there exists a G-equivariant map $T \to U$ defined over k; see, e.g., [18, Proof of Theorem 1.1 (a) on p. 508]. This implies that $\mathrm{ed}_k(T) \leqslant \dim(B) = \dim(X) - \dim(G)$. The desired inequality (17) now follows from the inequality $\mathrm{RD}_k(T) \leqslant \mathrm{ed}_k(T)$ of Remark 10.4. ∎

Proof of Proposition 14.1. (a) Set $d = \max\{\mathrm{RD}_k(\mathrm{S}_a), 1\}$. Suppose a field $K \in \mathrm{Fields}_k$ is closed at level d. By Lemma 14.5 it suffices to show that K-points are dense in ${}_TX$ for every G-torsor $T \to \operatorname{Spec}(K)$.

Note that the G-equivariant closed immersion $X \hookrightarrow \mathbb{P}(V)$ induces a natural closed immersion ${}_TX \hookrightarrow {}_T\mathbb{P}(V)$ of K-varieties. Here ${}_T\mathbb{P}(V)$ is a Brauer–Severi variety over K. Since K is closed at level $d \geqslant 1$, every Brauer–Severi variety over K is split. (This is because the underlying Brauer class in $H^2(K, \mathbb{G}_m)$ has resolvent degree $\leqslant 1$; see Proposition 7.10.) Thus, ${}_TX$ is a closed subvariety of $\mathbb{P}(V)_K$. The degree of ${}_TX$ in $\mathbb{P}(V)_K$ is a, same as the degree of X in $\mathbb{P}(V)$. (To see this, pass to $\overline{K}$.) By Lemma 14.4 (a), K-points are dense in ${}_TX$. The desired inequality, $\mathrm{RD}(G) \leqslant \{d, \dim(X) - \dim(G)\}$, now follows from Lemma 14.5.

(b) The argument here is the same as in part (a), with Lemma 14.4 (b) used to show that K-points are dense in ${}_T(Q \cap X)$. ∎

15. Upper bounds on the resolvent degree of some reflection groups

The purpose of this section is to prove the following.

Proposition 15.1. *Let* W *be Weyl group of the simple Lie algebra (or equivalently, a simple algebraic group) of type* E_i*. Here* $i = 6$*,* 7 *or* 8*. Let* k *be an arbitrary field. Then* $\mathrm{RD}_k(W) \leqslant i - 3$.

The inequality $\mathrm{RD}_k(W) \leqslant 5$, where W is the Weyl group of E_8, will play an important role in the proof of Theorem 1.1. We will only supply a proof of Proposition 15.1 in this case (for $i = 8$). The other two inequalities (where $i = 6$ and 7) will not be used in this paper. They are proved by a minor modification of the same argument; we leave the details as an exercise for the reader.

Note that by Theorem 1.2, $\mathrm{RD}_{\mathbb{C}}(W_i) = \mathrm{RD}_{\mathbb{Q}}(W_i) = \mathrm{RD}_k(W_i)$ for any field k of characteristic 0. Moreover, by Theorem 1.3, $\mathrm{RD}_k(W_i) \leqslant \mathrm{RD}_{\mathbb{C}}(W_i)$ for any field k of characteristic p. Thus, for the purpose of proving Theorem 15.1, we may assume that $k = \mathbb{C}$. This places us into the setting of Springer's classic paper on complex reflection groups [43].

We now proceed with the proof of Proposition 15.1 for $i = 8$ and $k = \mathbb{C}$. Consider the natural representation $W \hookrightarrow \mathrm{GL}(V) = \mathrm{GL}_8$ where V is a Cartan subalgebra of E_8. The kernel Z of the corresponding projective representation $W \to \mathrm{PGL}(V)$ is the center of W; it is a cyclic group of order 2. We will denote the non-trivial element of Z by z and the image of W in $\mathrm{PGL}(V)$ by $\overline{W} = W/Z$.

Recall that the ring of invariants $\mathbb{C}[V]^W$ is a polynomial ring over $\mathbb{C}$ in 8 variables. The generators f_2, f_8, f_{12}, f_{14}, f_{18}, f_{20}, f_{24} and f_{30} are called basic invariants; each f_i is a homogeneous G-invariant polynomial of degree i. These basic invariants are not unique but their degrees are. That is, if $\mathbb{C}[V]^G$ is generated by 8 homogeneous elements $g_1, \dots, g_8$, then the degrees of $g_1, \dots, g_8$ are

$$2,\ 8,\ 12,\ 14,\ 18,\ 20,\ 24,\ 30. \tag{18}$$

These integers are called the fundamental degrees of W.

Our strategy is to apply Proposition 14.1 (b) with $G = \overline{W}$, $X \subset \mathbb{P}(V) = \mathbb{P}^7$ the hypersurface $f_8 = 0$ and $Q \subset \mathbb{P}^7$ the quadric hypersurface $f_2 = 0$. Denote the affine cones of Q and X by Q^{aff} and X^{aff}, respectively.

Lemma 15.2. *The following statements hold:*

(a) *W transitively permutes the irreducible components of $Q \cap X$ (or equivalently, the irreducible components of $Q^{\mathrm{aff}} \cap X^{\mathrm{aff}}$).*

(b) *Each irreducible component of $Q \cap X$ is of dimension* 5.

Lemma 15.3. *The action of $\overline{W}$ on $Q \cap X$ is generically free.*

Assume for a moment that we have established these two lemmas. Then Proposition 14.1 (b) tells us that

$$\mathrm{RD}_{\mathbb{C}}(\overline{W}) \leqslant \max\{\dim(X) - 1, \mathrm{RD}_{\mathbb{C}}(\mathrm{S}_8)\} = \max\{5, 4\} = 5.$$

Here I used the fact that $\mathrm{RD}_{\mathbb{C}}(\mathrm{S}_8) \leqslant 4$; see [20, Theorem 5.6] or Example 14.3 (2). Applying Proposition 10.8 (a) to the exact sequence $1 \to Z \to W \to \overline{W} \to 1$, we conclude that

$$\mathrm{RD}_{\mathbb{C}}(W) \leqslant \max\{\mathrm{RD}_{\mathbb{C}}(\overline{W}), \mathrm{RD}_{\mathbb{C}}(Z)\} \leqslant \max\{5, 1\} = 5,$$

as desired. It thus remains to prove Lemmas 15.2 and 15.3.

Proof of Lemma 15.2. The natural inclusion $\mathbb{C}[f_2, f_8, \dots, f_{30}] = \mathbb{C}[V]^W \hookrightarrow \mathbb{C}[V]$ induces the categorical quotient map $\pi \colon V \to \mathbb{A}^8$ given by $\pi \colon v \to (f_2(v), f_8(v), \dots, f_{30}(v))$. Note that π is a finite morphism, and the fibers of $\mathbb{C}$-points of $\mathbb{A}^8$ are precisely the W-orbits in V. By definition, Q^{aff} and X^{aff} the preimages of coordinate hyperplanes H_1 and H_2 in $\mathbb{A}^8$ given by $x_1 = 0$ and $x_2 = 0$, respectively. Both (a) and (b) now follows from the fact that $H_1 \cap H_2 \simeq \mathbb{A}^6$ is irreducible of dimension 6. ■

Proof of Lemma 15.3. Assume the contrary: the $\overline{W}$-action on $Q \cap X$ is not generically free. This means that $Q^{\mathrm{aff}} \cap X^{\mathrm{aff}}$ is covered by the union of eigenspaces $V(g, \zeta)$, where g ranges over $W \setminus Z$ and ζ ranges over the roots of unity in $\mathbb{C}$. Here

$$V(g, \zeta) = \{v \in V \mid g(v) = \zeta v\}$$

stands for the ζ-eigenspace of g, as in [43].

If ζ is a primitive root of unity of degree d, then $\dim(V(g, \zeta)) \leqslant a(d)$, where $a(d)$ is the number of fundamental degrees (18) divisible by d; see [43, Theorem 3.4]. By inspection we see that $a(d) \leqslant 4$ for any $d \geqslant 3$, with equality for $d = 3, 4, 6$. Thus, the union of eigenspaces

$$\bigcup_{\deg(\zeta) \geqslant 3}^{g \in W \setminus Z} V(g, \zeta)$$

is at most 4-dimensional. Since every irreducible component of $Q^{\mathrm{aff}} \cap X^{\mathrm{aff}}$ is of dimension 6 (see Lemma 15.2 (b)), $Q^{\mathrm{aff}} \cap X^{\mathrm{aff}}$ is, in fact, covered by the union of $V(g, \pm 1) = V^g$, as g ranges over $W \setminus Z$. Since $V(g, -1) = V(zg, 1)$ for each g, we conclude that

$$V^{\text{non-free}} = \bigcup_{g \in W \setminus Z} V(g, 1)$$

covers one of the irreducible components of $Q^{\mathrm{aff}} \cap X^{\mathrm{aff}}$. Clearly $V^{\text{non-free}}$ is W-invariant. By Lemma 15.2 (a), if it covers one irreducible component of $Q^{\mathrm{aff}} \cap X^{\mathrm{aff}}$, it covers all of them. In other words,

$$Q^{\mathrm{aff}} \cap X^{\mathrm{aff}} \subset \bigcup_{1 \neq g \in W} V(g, 1).$$

Thus, in order to produce a contradiction, it suffices to exhibit one point $v \in V$ such that

(i) $\mathrm{Stab}_W(v) = \{1\}$ or equivalently, $v \notin V(g, 1)$ for any $1 \neq g \in W$; and

(ii) $v \in Q^{\mathrm{aff}} \cap X^{\mathrm{aff}}$ of equivalently, $f_2(v) = f_8(v) = 0$.

By [43, p. 177, Table 3], W has a regular element of order 3. This means that $V(g, \zeta_3)$ contains a regular vector v, where ζ_3 is a primitive cube root of unity. Recall that a vector in V is called regular if it is not contained in any reflecting hyperplane, and that for any regular vector v, the stabilizer $\mathrm{Stab}_W(v) = \{1\}$; see [43, Proposition 4.1]. Moreover, if f_d is one of the fundamental invariants, then

$$f_d(v) = f_d(gv) = f_d(\zeta_3 v) = \zeta_3^d f_d(v).$$

In particular, $f_d(v) = 0$ when $d = 2$ and 8. Thus, the regular vector v satisfies conditions (i) and (ii). This completes the proof of Lemma 15.3 and thus of Proposition 15.1 for $i = 8$. ∎

16. Proof of Theorem 1.1

Once again, by Theorem 1.2, we may replace k by its algebraic closure and thus assume without loss of generality that k is algebraically closed.

Reduction to the case, where G is smooth. By Proposition 11.2 (a),

$$\mathrm{RD}_k(G) \leqslant \max\{\mathrm{RD}_k(G_{\mathrm{red}}), 1\},$$

where G_{red} is the underlying smooth group. Thus, in order to prove Theorem 1.1 for G, it suffices to prove it for G_{red}.

Reduction to the case, where G is affine. We may now assume that G is smooth. By Chevalley's structure theorem [12, 14] there exists a unique connected smooth normal affine k-subgroup G_{aff} of G such that the quotient G/G^{aff} is an abelian variety. By Proposition 11.3, $\mathrm{RD}_k(G/G^{\mathrm{aff}}) \leqslant 1$. Applying Proposition 10.8 (a) to the exact sequence $1 \to G_{\mathrm{aff}} \to G \to G/G^{\mathrm{aff}} \to 1$, we obtain $\mathrm{RD}_k(G) \leqslant \max\{\mathrm{RD}_k(G_{\mathrm{aff}}), 1\}$. Thus, in order to prove Theorem 1.1 for G, it suffices to prove it for G_{aff}.

Reduction to the case, where G is semisimple. We may now assume that G is affine. Let $\mathrm{Rad}(G)$ be the radical of G, i.e., the largest connected solvable normal subgroup of G. Denote the quotient (semisimple) group by G^{ss} and consider the natural exact sequence $1 \to \mathrm{Rad}(G) \to G \to G^{ss} \to 1$. By Lemma 10.7 (b), $\mathrm{RD}_k(\mathrm{Rad}(G)) = 0$. Proposition 10.8 (a) now tells us that $\mathrm{RD}_k(G) \leqslant \mathrm{RD}_k(G^{ss})$. Thus, in order to prove Theorem 1.1 for G, it suffices to prove it for G^{ss}.

Reduction to the case, where G is almost simple. We will now assume that G is semisimple. Then G isogenous to the direct product $\widetilde{G} = G_1 \times \cdots \times G_r$ of its minimal connected normal subgroups. That is, there exists a central exact sequence

$$1 \to A \to \widetilde{G} \to G \to 1,$$

where A is a finite subgroup of a maximal torus of $\widetilde{G}$; see [44, Section 9.6.1]. Since we are assuming that k is algebraically closed, this tells us that A is a finite diagonalizable group. Hence, $\mathrm{RD}_k(A) \leqslant 1$ by Proposition 10.8 (c). The minimal connected normal subgroups $G_1, \ldots, G_r$ are (almost) simple; see [26, Section 27.5]. Proposition 10.8(d) (d) now tells us that it suffices to prove Theorem 1.1 for $\widetilde{G} = G_1 \times \cdots \times G_r$. Applying Proposition 10.8 (b) recursively, we see that

$$\mathrm{RD}_k(G_1 \times \cdots \times G_r) = \max\{\mathrm{RD}_k(G_1), \ldots, \mathrm{RD}_k(G_r)\}.$$

Thus, in order to prove Theorem 1.1 for G, it suffices to prove it for each (almost) simple group G_i.

From now on we will assume that G is (almost) simple. To complete the proof of Theorem 1.1, it remains to establish the following.

Proposition 16.1. *Let k be an algebraically closed field and G an almost simple group defined over k. Then*

(a) $\mathrm{RD}_k(G) \leqslant 5$ *if G is of type E_8, and*

(b) $\mathrm{RD}_k(G) \leqslant 1$ *if G is of any other type.*

Proof. (a) Let G be a simple group of type E_8 and let W_8 be the Weyl group of G. Then

$$\mathrm{RD}_k(G) \leqslant \mathrm{RD}_k(W_8) \leqslant 5,$$

where the first inequality is given by Corollary 10.9, and the second by Proposition 15.1.

(b) Tits [46, Section 2] showed that if G is a simple group of any type other than E_8, then G has no non-trivial torsors over any field K, closed under taking radicals. (Note that [46] is reprinted in [48].) In particular, there are no non-trivial G-torsors over any field K closed at level 1. By Proposition 8.1 (b) this implies that $\mathrm{RD}_k(G) \leqslant 1$, as claimed.

For the sake of completeness we will give a short direct proof of part (b), using the terminology of this paper. We begin with two preliminary observations. First, recall that since we are working over an algebraically closed field k, every almost simple algebraic group over k is split and consequently descends to $\mathbb{Z}$. Using

Theorems 1.2 and 1.3, we may assume without loss of generality that $k = \mathbb{C}$ is the field of complex numbers. This assumption will allow us to avoid some of the subtle points of the arguments in [46, Section 2] which only come up in prime characteristic.

Our second preliminary observation is that if G_1 and G_2 are almost simple groups of the same type, then they are isogenous and hence, by Proposition 10.8 (d),

$$\mathrm{RD}_{\mathbb{C}}(G_1) \leqslant \max\{\mathrm{RD}_{\mathbb{C}}(G_2), 1\} \quad \text{and} \quad \mathrm{RD}_{\mathbb{C}}(G_2) \leqslant \max\{\mathrm{RD}_{\mathbb{C}}(G_1), 1\}.$$

Consequently, Proposition 16.1 (b) holds for G_1 if and only if it holds for G_2. In other words, it suffices to prove that $\mathrm{RD}_{\mathbb{C}}(G) \leqslant 1$ for one almost simple group G of each type (other than E_8).

G is of type A_r or C_r. Here we can take G to be $G = \mathrm{SL}_{r+1}$ and $G = \mathrm{Sp}_{2r}$, respectively. By Lemma 10.7 (c), $\mathrm{RD}_k(G) = 0$ in both cases.

G is of type B_r or D_r. Here we take G to be the special orthogonal group $G = \mathrm{SO}_n$, which is of type B_r if $n = 2r + 1$ and of type D_r if $n = 2r$. By [27, (29.29)], $H^1(K, G)$ can be represented by n-dimensional quadratic forms q of discriminant 1 over K. In a suitable basis, $q(x_1, \dots, x_n) = a_1 x^2 + \dots + a_n x_n^2$ for some $a_1, \dots, a_n$. Thus, q splits over $L = K(\sqrt{a_1}, \dots, \sqrt{a_n})$. Clearly $\mathrm{RD}_{\mathbb{C}}(L/K) \leqslant 1$, and thus $\mathrm{RD}_{\mathbb{C}}(G) \leqslant 1$, as claimed.

G is of type G_2 and F_4. In both cases the only primes dividing $|W|$ are 2 and 3. By Burnside's theorem, W is solvable.[3] Thus, $\mathrm{RD}_k(G) \leqslant \mathrm{RD}_k(W) \leqslant 1$, where the first inequality follows from Corollary 10.9 and the second from Example 10.6.

G is a simply connected group of type E_6. By [22, Example 9.12], G has a subgroup S isomorphic to $F_4 \times \mu_3$ such that the map $H^1(K, S) \to H^1(K, G)$ is surjective; see [22, Section 23]. Here F_4 denotes the simply connected group of type F_4. By Lemma 7.9 (c), $\mathrm{RD}_{\mathbb{C}}(S) = \mathrm{RD}_{\mathbb{C}}\, H^1(*, S) \geqslant \mathrm{RD}_{\mathbb{C}}\, H^1(*, G) = \mathrm{RD}_{\mathbb{C}}(G)$. Since we know that $\mathrm{RD}_{\mathbb{C}}(F_4) \leqslant 1$,

$$\mathrm{RD}_{\mathbb{C}}(G) \leqslant \mathrm{RD}_{\mathbb{C}}(S) = \mathrm{RD}_{\mathbb{C}}(F_4 \times \mu_3) = \max\{\mathrm{RD}_{\mathbb{C}}(F_4), \mathrm{RD}_{\mathbb{C}}(\mu_3)\} = 1.$$

G is a simply connected group of type E_7. By [22, Example 12.3], G has a subgroup $\widetilde{S}$ isomorphic to $E_6 \rtimes \mu_4$ such that the map $H^1(K, \widetilde{S}) \to H^1(K, G)$ is

[3] One can also see this directly, without appealing to Burnside's theorem.

surjective; see [22, Section 23]. Here E_6 denotes the simply connected group of type E_6. Once again, by Lemma 7.9 (c), $\mathrm{RD}_{\mathbb{C}}(\widetilde{S}) \geqslant \mathrm{RD}_{\mathbb{C}}(G)$. Since we know that $\mathrm{RD}_{\mathbb{C}}(E_6) \leqslant 1$, we conclude that $\mathrm{RD}_{\mathbb{C}}(G) \leqslant \mathrm{RD}_{\mathbb{C}}(\widetilde{S}) = \mathrm{RD}_{\mathbb{C}}(E_6 \rtimes \mu_4) = \max\{\mathrm{RD}_{\mathbb{C}}(E_6), \mathrm{RD}_{\mathbb{C}}(\mu_4)\} = 1$.

This completes the proof of Proposition 16.1 and thus of Theorem 1.1. ∎

Remark 16.2. For simply connected groups G of type G_2, F_4, E_6 and E_7, the inequality $\mathrm{RD}_{\mathbb{C}}(G) \leqslant 1$ of Proposition 16.1 (b) can also be deduced from a theorem of Garibaldi which asserts that for these groups the Rost invariant $H^1(*, G) \to H^3(*, \mathbb{Z}/n_G\mathbb{Z}(2))$ has trivial kernel; see [21, Theorem 0.5] or [9].

17. Can the inequality of Theorem 1.1 be strengthened?

Recall that Conjecture 1.4 asserts that the inequality $\mathrm{RD}_k(G) \leqslant 5$ of Theorem 1.1 can be strengthened to $\mathrm{RD}_k(G) \leqslant 1$. In this final section we will show that this conjecture follows from a positive answer to a long-standing open question of Serre [39, Question 2] stated below.

Question 17.1. Let K be a field, H be a smooth algebraic group over K, and $T \to \mathrm{Spec}(K)$ be an H-torsor. Suppose $K_1, \dots, K_r$ are field extensions of K of degrees $d_1, \dots, d_r$, respectively, such that

- $d_1, \dots, d_r$ are relatively prime integers, i.e., $\gcd(d_1, \dots, d_r) = 1$; and
- each K_i splits T, i.e., $T_{K_i} = 1$ in $H^1(K_i, H)$.

Then T is split over K.

Note that for $r = 1$ this is obvious, since in this case the gcd assumption forces $K_1 = K$. For a detailed discussion of Question 17.1, we refer the reader to [50].

Proposition 17.2. *Assume that Question 17.1 has a positive answer in the following special situation: K is a solvably closed field containing $\mathbb{C}$ and H is the split simple group of type E_8 over K. Then $\mathrm{RD}_k(G) \leqslant 1$ for every field k and every connected algebraic group G over k.*

Proof. It suffices to show that, under the assumption of the proposition, the inequality $\mathrm{RD}_k(E_8) \leqslant 5$ of Proposition 16.1 (a) can be strengthened to $\mathrm{RD}_k(E_8) \leqslant 1$. If we can do this, then the argument of Section 16 will go through unchanged to show that $\mathrm{RD}_k(G) \leqslant 1$ for every field k and every connected algebraic group G over k.

By Theorems 1.2 and 1.3 we may further assume that $k = \mathbb{C}$, as we did in the proof of Proposition 16.1. By Proposition 8.1 (b) it suffices to show that every E_8-torsor

$T \to \mathrm{Spec}(K)$ is split for every field $K \in \mathrm{Fields}_{\mathbb{C}}$, closed at level 1 (over $\mathbb{C}$). In fact, we will show that this is the case whenever K is solvably closed; cf. Corollary 6.5. By a theorem of Tits [47], T is split by a finite field extension $K_{\geqslant 7}/K$ such that

$$\text{the only primes dividing } [K_{\geqslant 7} : K] \text{ are } 2, 3 \text{ and } 5;$$

see also [50]. (Note that this step is valid for every K; we do not use the assumption that K is solvably closed here.)

Now observe that since K is solvably closed, the norm residue isomorphism theorem tells us that $H^d(K, \mu_n) = 1$ for every $d, n \geqslant 1$; cf. Remark 7.12. In particular, the class of T lies in the kernel of the Rost invariant $R\colon H^1(K, E_8) \to H^3(K, \mu_{60})$. Theorems of Chernousov now tell us that

$$T \text{ is split by a finite extension } K_3/K \text{ such that } 3 \nmid [K_3 : K];$$

and

$$T \text{ is split by a finite extension } K_5/K \text{ such that } 5 \nmid [K_5 : K];$$

see [8, 10]. Finally, T also lies in the kernel of the Semenov invariant

$$H^1(*, E_8)_0 \to H^3(*, \mu_2),$$

where $H^1(*, E_8)_0$ denote the kernel of the mod 4 Rost invariant, $15R$. Consequently, by [36, Theorem 8.7]

$$T \text{ is split by a finite extension } K_2/K \text{ such that } 2 \nmid [K_2 : K].$$

In summary, T can be split by finite extensions K_2, K_3, K_5 and $K_{\geqslant 7}$ of K whose degrees are relatively prime. The assumption of the proposition now tells us that T is split over K, as desired. ∎

Remark 17.3. Note that the Semenov invariant is only defined in characteristic 0. In prime characteristic our proof of Proposition 17.2 relies on Theorem 1.3.

Acknowledgments. The author is grateful to Jesse Wolfson, the editor, and the anonymous referee for helpful detailed comments on earlier versions of this paper.

Funding. The author was partially supported by National Sciences and Engineering Research Council of Canada Discovery grant 253424-2017.

References

[1] G. Berhuy and G. Favi, Essential dimension: a functorial point of view (after A. Merkurjev). *Doc. Math.* **8** (2003), 279–330. Zbl 1101.14324 MR 2029168

[2] R. Brauer, On the resolvent problem. *Ann. Mat. Pura Appl. (4)* **102** (1975), 45–55. Zbl 0299.12105 MR 371854

[3] M. Brion, On extensions of algebraic groups with finite quotient. *Pacific J. Math.* **279** (2015), no. 1–2, 135–153. Zbl 1332.14057 MR 3437773

[4] P. Brosnan, Z. Reichstein and A. Vistoli, Essential dimension and algebraic stacks. 2007, arXiv:math/0701903v1.

[5] P. Brosnan, Z. Reichstein and A. Vistoli, Essential dimension in mixed characteristic. *Doc. Math.* **23** (2018), 1587–1600. Zbl 1405.14002 MR 3890962

[6] F. E. Browder (ed.), *Mathematical developments arising from Hilbert problems*, Proc. Sympos. Pure Math., Vol. XXVIII, American Mathematical Society, Providence, RI, 1976. Zbl 0326.00002 MR 419125

[7] J. Buhler and Z. Reichstein, On the essential dimension of a finite group. *Compositio Math.* **106** (1997), no. 2, 159–179. Zbl 0905.12003 MR 1457337

[8] V. I. Chernousov, A remark on the (mod 5)-invariant of Serre for groups of type E_8. (in Russian) *Mat. Zametki* **56** (1994), no. 1, 116–121. MR 1309826 English translation: *Math. Notes* **56** (1994), no. 1–2, 730–733. Zbl 0835.20059

[9] V. Chernousov, The kernel of the Rost invariant, Serre's conjecture II and the Hasse principle for quasi-split groups ${}^{3,6}D_4, E_6, E_7$. *Math. Ann.* **326** (2003), no. 2, 297–330. Zbl 1036.20040 MR 1990912

[10] V. Chernousov, On the kernel of the Rost invariant for E_8 modulo 3. In *Quadratic forms, linear algebraic groups, and cohomology*, pp. 199–214, Dev. Math. 18, Springer, New York, 2010. Zbl 1231.20046 MR 2648726

[11] V. Chernousov, P. Gille and Z. Reichstein, Reduction of structure for torsors over semilocal rings. *Manuscripta Math.* **126** (2008), no. 4, 465–480. Zbl 1157.14028 MR 2425436

[12] C. Chevalley, Une démonstration d'un théorème sur les groupes algébriques. *J. Math. Pures Appl. (9)* **39** (1960), 307–317. Zbl 0115.38901 MR 126447

[13] I. S. Cohen, On the structure and ideal theory of complete local rings. *Trans. Amer. Math. Soc.* **59** (1946), no. 1, 54–106. Zbl 0060.07001 MR 16094

[14] B. Conrad, A modern proof of Chevalley's theorem on algebraic groups. *J. Ramanujan Math. Soc.* **17** (2002), no. 1, 1–18. Zbl 1007.14005 MR 1906417

[15] M. Demazure and A. Grothendieck (eds.), *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*. Doc. Math. (Paris) 7, Société Mathématique de France, Paris, 2011. Zbl 1241.14002 MR 2867621. Original volume: Lecture Notes in Math. 151, Springer, Berlin–Heidelberg, 1970. Zbl 0207.51401 MR 0274458

[16] M. Demazure and A. Grothendieck (eds.), *Schémas en groupes (SGA) 3). Tome III. Structure des schémas en groupes réductifs*. Doc. Math. (Paris) 8, Société Mathématique de France, Paris, 2011. Zbl 1241.14003 MR 2867622. Original volume: Lecture Notes in Math. 153, Springer, Berlin–Heidelberg, 1970. Zbl 0212.52810 MR 0274460

[17] J. Dixmier, Histoire du 13e problème de Hilbert. In *Analyse diophantienne et géométrie algébrique*, pp. 85–94, Cahiers Sém. Hist. Math. Sér. 2 3, Université Paris VI, Paris, 1993. Zbl 0795.01012 MR 1240756

[18] A. Duncan and Z. Reichstein, Versality of algebraic group actions and rational points on twisted varieties. *J. Algebraic Geom.* **24** (2015), no. 3, 499–530. Zbl 1327.14210 MR 3344763

[19] B. Farb, M. Kisin and J. Wolfson, Modular functions and resolvent problems. *Math. Ann.* **386** (2023), no. 1–2, 113–150. Zbl 07686079 MR 4585146

[20] B. Farb and J. Wolfson, Resolvent degree, Hilbert's 13th problem and geometry. *Enseign. Math.* **65** (2019), no. 3–4, 303–376. Zbl 1460.14104 MR 4113045

[21] R. S. Garibaldi, The Rost invariant has trivial kernel for quasi-split groups of low rank. *Comment. Math. Helv.* **76** (2001), no. 4, 684–711. Zbl 1001.20042 MR 1881703

[22] S. Garibaldi, Cohomological invariants: exceptional groups and spin groups. *Mem. Amer. Math. Soc.* **200** (2009), no. 937. Zbl 1191.11009 MR 2528487

[23] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*. Cambridge Stud. Adv. Math. 165, Cambridge University Press, Cambridge, 2017. Zbl 1373.19001 MR 3727161

[24] A. Grothendieck, Torsion homologique et sections rationnelles, exposé 5. In *Séminaire C. Chevalley; 2e année. Anneaux de Chow et applications*, Secrétariat mathématique, Paris, 1958.

[25] C. Heberle and A. J. Sutherland, Upper bounds on resolvent degree via Sylvester's obliteration algorithm. *New York J. Math.* **29** (2023), 107–146. Zbl 1508.14026 MR 4538037

[26] J. E. Humphreys, *Linear algebraic groups*. Grad. Texts in Math. 21, Springer, New York–Heidelberg, 1975. Zbl 0325.20039 MR 396773

[27] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The book of involutions*. Amer. Math. Soc. Colloq. Publ. 44, American Mathematical Society, Providence, RI, 1998. Zbl 0955.16001 MR 1632779

[28] S. Lang and J. Tate, Principal homogeneous spaces over abelian varieties. *Amer. J. Math.* **80** (1958), no. 3, 659–684. Zbl 0097.36203 MR 106226

[29] A. Merkurjev, Rost invariants of simply connected algebraic groups. In *Cohomological invariants in Galois cohomology*, pp. 101–158, Univ. Lecture Ser. 28, American Mathematical Society, Providence, RI, 2003. MR 1999385

[30] A. S. Merkurjev, Essential dimension: a survey. *Transform. Groups* **18** (2013), no. 2, 415–481. Zbl 1278.14066 MR 3055773

[31] J. S. Milne, *Étale cohomology*. Princeton Math. Ser. 33, Princeton University Press, Princeton, NJ, 1980. MR 559531

[32] Y. A. Nisnevich, Espaces homogènes principaux rationnellement triviaux et arithmétique des schémas en groupes réductifs sur les anneaux de Dedekind. *C. R. Acad. Sci. Paris Sér. I Math.* **299** (1984), no. 1, 5–8. Zbl 0587.14033 MR 756297

[33] Z. Reichstein, Essential dimension. In *Proc. Internat. Congr. Math. Vol. II*, pp. 162–188, Hindustan Book Agency, New Delhi, 2010. Zbl 1232.14030 MR 2827790

[34] Z. Reichstein, From Hilbert's 13th problem to essential dimension and back. *Eur. Math. Soc. Mag.* (2021), no. 122, 4–15. Zbl 1492.14085 MR 4417655

[35] Z. Reichstein and F. Scavia, The behavior of essential dimension under specialization. *Épijournal Géom. Algébrique* **6** (2022), article no. 21. Zbl 07641775 MR 4526269

[36] N. Semenov, Motivic construction of cohomological invariants. *Comment. Math. Helv.* **91** (2016), no. 1, 163–202. Zbl 1344.14005 MR 3471941

[37] J.-P. Serre, Espaces fibrés algébriques, exposé 1. In *Séminaire C. Chevalley; 2e année. Anneaux de Chow et applications*, Secrétariat mathématique, Paris, 1958.

[38] J.-P. Serre, *Local fields*. Grad. Texts in Math. 67, Springer, New York–Berlin, 1979. MR 554237

[39] J.-P. Serre, Cohomologie galoisienne: progrès et problèmes. Astérisque 227, pp. 229–257 (Exp. no. 783), Société Mathématique de France, Paris, 1995. Zbl 0837.12003 MR 1321649

[40] J.-P. Serre, *Galois cohomology*. Springer, Berlin, 1997. MR 1466966

[41] J.-P. Serre, *Exposés de séminaires (1950–1999)*. Doc. Math. (Paris) 1, Société Mathématique de France, Paris, 2001. Zbl 1005.01012 MR 1942136

[42] J. H. Silverman, *The arithmetic of elliptic curves*. Second edn., Grad. Texts in Math. 106, Springer, Dordrecht, 2009. Zbl 1194.11005 MR 2514094

[43] T. A. Springer, Regular elements of finite reflection groups. *Invent. Math.* **25** (1974), 159–198. Zbl 0287.20043 MR 354894

[44] T. A. Springer, *Linear algebraic groups*. Second edn., Progr. Math. 9, Birkhäuser, Boston, MA, 1998. Zbl 0927.20024 MR 1642713

[45] A. J. Sutherland, Upper bounds on resolvent degree and its growth rate. 2021, arXiv:2107.08139v1

[46] J. Tits, Théorie des groupes. *Ann. Collège France* **91** (1990/91), 125–138 (1992). MR 1325733

[47] J. Tits, Sur les degrés des extensions de corps déployant les groupes algébriques simples. *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), no. 11, 1131–1138. Zbl 0823.20042 MR 1194504

[48] J. Tits, *Résumés des cours au Collège de France 1973–2000*. Doc. Math. (Paris) 12, Société Mathématique de France, Paris, 2013. Zbl 1286.01001 MR 3235648

[49] D. TOSSICI, Essential dimension of group schemes over a local scheme. *J. Algebra* **492** (2017), 1–27. Zbl 1400.14120 MR 3709138

[50] B. TOTARO, Splitting fields for E_8-torsors. *Duke Math. J.* **121** (2004), no. 3, 425–455. Zbl 1048.11031 MR 2040282

[51] J. WOLFSON, Tschirnhaus transformations after Hilbert. *Enseign. Math.* **66** (2020), no. 3–4, 489–540. Zbl 1509.14055 MR 4254270

(Reçu le 30 mai 2022)

Zinovy REICHSTEIN, Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada; *e-mail:* reichst@math.ubc.ca