ON TSCHIRNHAUS TRANSFORMATIONS

JOE BUHLER AND ZINOVY REICHSTEIN

ABSTRACT. We revisit the classical problem of simplifying polynomials by means of Tschirnhaus transformations. We consider Tschirnhaus transformations involving (i) no auxiliary radicals, (ii) arbitrary radicals, (iii) odd degree radicals, and (iv) odd degree radicals and the square root of the discriminant. In [BR] we showed that by using substitutions of type (i) one cannot reduce the general polynomial of degree n to a form with less than $[n/2]$ independent coefficients. In this paper we give a new proof of this result and also extend it to transformations of types (iii) and (iv). In the last section we present alternative proofs, based on the cohomological approach shown to us by J.-P. Serre.

1. Introduction

By the end of the nineteenth century a number of techniques were known for simplifying polynomials by using Tschirnhaus transformations. "Reducing the number of parameters" was one of the central motivations of Hilbert's 13th problem, which asks whether the root of a general seventh degree polynomial can be expressed in terms of functions of fewer than three variables. Our goal here is to revisit the topic of parameter reduction via Tschirnhaus transformations from a modern point of view.

We fix the notation of this paragraph throughout. Let k be a base field, of characteristic zero. We assume that all fields mentioned in this paper are function fields over k and that all varieties and maps are defined over k. Let n be a positive integer and $a_1, \cdots, a_n$ be algebraically independent over k. The polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

The second author was partially supported by NSA grant MDA904-9610022.

is a "general" monic polynomial of degree n; it can be specialized to any polynomial of degree n with coefficients lying in a field containing k. Let $K = k(a_1, \cdots, a_n)$, and let

$$L = K[X]/f \tag{1}$$

be the root field of f over K, so that L/K is, in some sense, a general extension of degree n. We let $x = X \pmod{f}$ so that $L = K(x)$. Finally, if K' is any extension of K, we let $L' = K'[X]/f = K'(x)$.

Now we consider the problem of finding a Tschirnhaus transformation that simplifies f. A Tschirnhaus transformation is determined by an element y of L

$$y = h(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}\ , \tag{2}$$

where the b_i are in K. Denote the minimal polynomial g of y over K by

$$g(Y) = Y^n + c_1 Y^{n-1} + \cdots c_n\ ;$$

this polynomial can be explicitly computed as the resultant of $h(X) - Y$ and $f(x)$, with respect to X. Let $K_y := k(c_1, \cdots, c_n)$ be the field generated by the coefficients of g. Our goal is to minimize the "number of parameters" in g, which we interpret as minimizing the transcendence degree of K_y. This motivates us to define

$$d(n) = \min\{\operatorname{trdeg} K_y : K(y) = L\}\ .$$

We emphasize that many of our definitions depend on the ground field k, so that $d_k(n)$ would be a more proper notation that $d(n)$, but we choose to suppress this throughout for the sake of simplicity. We also remark that if g is obtained as above by a Tschirnhaus transformation from the general polynomial $f(X)$ then g is generic in the sense that any extension of fields E/F of degree n (of fields containing k) can be obtained as a root field of a specialization of g (see [BR]).

One way to minimize the transcendence degree is to make coefficients zero. Hermite [He] showed in 1861 that the general quintic could be reduced, in the above sense, to the form

$$X^5 + aX^3 + bX + c.$$

Since it is easy to make the last two coefficients equal by scaling X, we see that $d(5) \leq 2$. By similar techniques, Joubert [J] and Richmond [Ri] showed that a general sextic can be reduced to the form

$$X^6 + aX^4 + bX^2 + cX + c$$

so $d(6) \leq 3$. For an elegant treatment of the these results that uses arithmetic properties of cubic surfaces, see [C].

A theorem of Klein ([Kl]) asserts that it impossible to reduce the general quintic to one-parameter form without using auxiliary radicals, thus proving that $d(5) \geq 2$. The following result generalizes this inequality.

Theorem 1.1. ([BR])
(a) $d(n+1) \geq d(n)$.
(b) $d(n) \geq [n/2]$.

Part (b) says that at least $[n/2]$ of the coefficients of any Tschirnhaus transformation $g(Y)$ of a general polynomial $f(X)$ are algebraically independent over k. It is not clear how close $[n/2]$ is to the true value of $d(n)$; the best upper bound we know ([BR]) is $d(n) \leq n - 3$ for all $n \geq 5$. In particular, $d(5) = 2$ and $d(6) = 3$, so the above-mentioned Hermite form of the quintic and Joubert-Richmont form of the sextic do, indeed, have the smallest possible numbers of independent parameters. The first unknown value of $d(n)$ is $d(7)$ which could be equal to either 3 or 4.

Much of the 19th century work was motivated by the problem of finding roots of polynomials; consequently, the above reductions were not nearly as prominent as other normal forms, obtained by allowing auxiliary radicals. For instance, Bring and then Jerrard proved that the general quintic can be reduced to the form

$$X^5 + X + a \, .$$

One-parameter forms of the quintic were used by Klein and others to reduce the solution of the quintic to the evaluation of special functions. More recently Doyle and McMullen [DM] used this technique in their solution of the quintic by iterations.

To formalize the notion of auxiliary radicals, we consider Tschirnhaus transformations of the form

$$y' = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} \, ,$$

where the b_i lie in a solvable extension K' of K. Then we let c_i' denote the coefficients of the minimal polynomial of y' over K', set $K_y' = k(c_1', \cdots, c_n')$. We are only interested in y that generate the full extension in the sense that $K'(y) = L' = K'(x)$. Thus we define

$$d^{solv}(n) = \min\{\operatorname{trdeg} K_y' \mid K'(y) = K'(x)\}$$

where K' ranges over all solvable extensions of K. Obviously, $d^{solv}(n) \leq d(n)$. Since equations of degree ≤ 4 can be solved in radicals, we shall assume from now on that $n \geq 5$.

It is easy to show that $d^{solv}(n) \leq n - 4$ (see, e.g., [H2]); however, we know no interesting lower bounds on $d^{solv}(n)$. In an attempt to better understand how close $d^{solv}(n)$ is to $d(n)$, we will consider two related functions that lie between them:

$$d^{odd}(n) = \min\{\operatorname{trdeg}_k K_y'' \mid K''(y) = K''(x)\}$$

where K'' ranges over all solvable extensions of K of odd degree, and

$$d_{\Delta}^{odd}(n) = \min\{\operatorname{trdeg}_k K_y''' \mid K'''(y) = K'''(x)\}$$

where $\Delta \in K$ is the discriminant of $f(x)$ and K''' ranges over all solvable extensions of $K(\sqrt{\Delta})$ of odd degree. The number $d^{odd}(n)$ tells us to what extent we can simplify $f(x)$ by performing a Tschirnhaus transformations $x \longrightarrow y$, where y is in (2) and each b_i is a radical expression in $a_1, \ldots, a_n$ (with coefficients in k) involving only odd degree radicals. The number $d_{\Delta}^{odd}(n)$ answers a similar question when the α_i involve odd degree radicals and the square root of the discriminant. It is clear from the definitions that

$$d^{solv}(n) \leq d_{\Delta}^{odd}(n) \leq d^{odd}(n) \leq d(n) \ .$$

The main new results of this paper are Theorem 6.1, which says that $d^{solv}(n)$, $d^{odd}(n)$, and $d_{\Delta}^{odd}(n)$ are non-decreasing functions of n, and Theorem 7.1, which says that $d^{odd}(n) \geq [n/2]$ and $d_{\Delta}^{odd}(n) \geq 2[n/4]$. Note that Theorem 7.1 implies, in particular, that the above-mentioned Bring-Jerrard form (or any other 1-parameter form) of the quintic cannot be attained by a substitution involving only odd degree radicals and $\sqrt{\Delta}$.

The rest of this paper is organized as follows. In an attempt to understand $d(n)$ in more general terms, we will introduce the notion of "essential dimension" in the second section. Then we consider the relationship of these ideas to Hilbert's 13th problem.

In section 4 we give a new proof of the lower bound $d(n) \geq [n/2]$ that relies on Tsen-Lang theory. In section 5, 6, and 7 we study the functions $d^{solv}(n)$, $d^{odd}(n)$, and $d^{odd}_{\Delta}(n)$. In the final section we outline Serre's proof of the inequality $d(n) \geq [n/2]$, and then show how his cohomological techniques can be used to give alternative proofs of the lower bounds on $d^{odd}(n)$ and $d^{odd}_{\Delta}(n)$.

Acknowledgements: We would like to thank J.-P. Serre and B. Kahn for helpful discussions.

2. Essential Dimension

Let E/F be a field extension of degree n such that F contains k. We shall say that E is defined over a subfield F_0 of F if there is an extension E_0/F_0 of degree n such that $E_0F = E$; thus, $E = E_0 \otimes_{F_0} F$. (As always, F_0 and all other fields are function fields over k.) In other words, E is defined over F_0 if there exists an element $y \in E$ whose minimal polynomial over F is of degree n and has all of its coefficients in F_0. The *essential dimension* of the extension E/F, denoted $\mathrm{ed}(E/F)$, is defined to be the minimum value of $\mathrm{trdeg}_k F_0$, where E is defined over F_0.

Lemma 2.1. *Let $K = k(a_1, \ldots, a_n)$, $f = X^n + a_1X^{n-1} + \cdots + a_n$, and $L = K[X]/f$ be as in (1). If K'/K is a solvable extension, denote the field $K'[X]/f$ by L'. Then*
(a) $d(n) = \mathrm{ed}_k(L/K)$.
(b) $d^{solv}(n) = \min\{\mathrm{ed}_k(L'/K') \mid K'/K \text{ solvable}, \sqrt{\Delta} \in K'\}$,
(c) $d^{odd}(n) = \min\{\mathrm{ed}_k(L'/K') \mid K'/K \text{ solvable of odd degree}\}$,
(d) $d^{odd}_{\Delta}(n) = \min\{\mathrm{ed}_k(L'/K') \mid K'/K(\sqrt{\Delta}) \text{ solvable of odd degree}\}$.

Proof. The lemma follows from the definitions and discussion in the previous section; note that in part (a) we can, indeed, let K' range only over those solvable extensions of K which contains $\sqrt{\Delta}$, since making K' bigger (e.g., by adjoining $\sqrt{\Delta}$) cannot increase $\mathrm{ed}_k(L'/K')$. □

Two facts about essential dimension of fields will be useful when we consider a geometric interpretation of this concept. The first says that the essential dimension is unchanged if a further algebraically independent variable is adjoined. The second says that essential dimension is unchanged when one passes to the normal closure; therefore it suffices to consider the essential dimension of normal extensions of fields.

Lemma 2.2. *Let E/F be a finite field extension and let t be an independent variable over F. Then* $\mathrm{ed}(E(t)/F(t)) = \mathrm{ed}(E/F)$.

Proof. The inequality $\mathrm{ed}(E(t)/F(t)) \leq \mathrm{ed}(E/F)$ follows directly from the definition, and the opposite inequality follows from [Ro, Lemma 1]. □

Lemma 2.3. (*Lemma 2.3 in* [BR]) *Let E/F be a field extension and let $E^{\#}$ be the normal closure of E over F. Then*

$$\mathrm{ed}(E/F) = \mathrm{ed}(E^{\#}/F).$$

If G is a finite group and X is an irreducible algebraic variety on which G acts faithfully, then a *compression* of this action is a faithful G-variety Y together with a dominant rational map $X \longrightarrow Y$ of faithful G-varieties. The *essential dimension* of X, denoted $\mathrm{ed}(X)$, is the minimal dimension of Y, as Y ranges over all compressions of X.

The essential dimension of a G-variety is determined by the action of G on its function field. More precisely

$$\mathrm{ed}(X) = \mathrm{ed}(k(X)/k(X)^G)\ ;$$

see [BR, Lemma 2.2]. Combining this with the previous lemma shows that if $G = S_n$ and $V = k^n$ is made into an S_n-variety by using the natural action of the symmetric group on n-tuples, then

$$d(n) = \mathrm{ed}(V)\ . \tag{3}$$

Next we prove the somewhat surprising fact that $\mathrm{ed}(V)$ is independent of V, as V ranges over all faithful linear representations of G. As a first step, we consider the following lemma from [Re1].

Lemma 2.4. *Let X be a faithful G-variety, V be a linear G-variety of dimension d, and V_0 be a d-dimensional vector space, which we shall view as a G-variety with trivial G-action. Then $X \times V$ and $X \times V_0$ are birationally isomorphic (as G-varieties).*

Proof. This is a variant of the "no-name" lemma. To derive it from the "usual" form (see [EM, Prop. 1.1]), denote $k(X \times V)$ by $E = k(X)(t_1, \dots, t_d)$. It is easy to see that the embeddings $E^G \hookrightarrow E$ and $k(X) \hookrightarrow E$ induce a G-equivariant isomorphism of fields $k(X) \otimes_{k(X)^G} E^G \simeq E$. By the usual no-name lemma $E^G = k(X)^G(s_1, \ldots, s_d)$ for some $s_1, \ldots, s_d \in E^d$. Thus we have G-equivariant isomorphisms

$$E \simeq k(X) \otimes_k (X)^G E^G \simeq k(X)(s_1, \ldots, s_d) \simeq k(X \times V_0) ,$$

and the lemma follows. □

As an easy corollary, we see that $\mathrm{ed}(X \times V) = \mathrm{ed}(X)$, where X is a faithful G-variety and V is a faithful linear G-variety. Indeed, by the lemma, $\mathrm{ed}(X \times V) = \mathrm{ed}(X \times V_0)$ where V_0 is a vector space of the same dimension as V on which V acts trivially. The function field of $X \times V_0$ is obtained from $k(X)$ by adjoining independent variables, so

$$\mathrm{ed}(X \times V) = \mathrm{ed}(X \times V_0) = \mathrm{ed}(X) ,$$

by Lemma 2.2. If V and V' are faithful linear representations of G then this fact says that

$$\mathrm{ed}(V) = \mathrm{ed}(V \times V') = \mathrm{ed}(V').$$

Thus the essential dimension of a linear G-variety depends only on the finite group G, and not on the choice of V; we let $\mathrm{ed}(G)$ denote this dimension, and refer to this as the essential dimension of G.

In particular $d(n) = \mathrm{ed}(S_n)$; see (3). We remark that if H is a subgroup of G then $\mathrm{ed}(H) \leq \mathrm{ed}(G)$, from the definition. It follows, since S_n is a subgroup of S_{n+1}, that $d(n) \leq d(n+1)$, as claimed in Theorem 1.1(a).

We also remark that the concept of essential dimension can be extended to algebraic groups (see [Re1]), and that most of the basic results here extend to that context.

3. Hilbert's 13-th problem

Hilbert phrased his 13th problem in broad terms. He viewed a root x of $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ as an algebraic function of $a_1, \ldots, a_n$; the 13th problem specifically asks if this function can be expressed as compositions of continuous functions of 2 variables. Kolmogorov and Arnold answered this question by showing, roughly speaking, that every continuous function of any number of variables can be expressed in terms of continuous functions of one variables and the binary function "addition" (see [Lo] for this, as well as several further developments in this direction).

However, Hilbert also referred to expressions for x in terms of algebraic functions, and it seems that this was a central motivation for the problem. Some support for this can be seen from amount of space devoted to this version of the question in [H2], which was apparently Hilbert's last published paper. A fuller discussion of the history of algebraic versions of the problem can be found in [AS] and [Di]. Further algebraic interpretations and interesting results can be found in a recent paper of Abhyankar ([A]).

One algebraic version of the question is as follows (this is equivalent to those in [AS] and [Di]). Let $n = 7$, so that $L = K[X]/f$ is the root field of the general septic polynomial; see (1). Is L contained in the top field K_r of a tower

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

where each K_{i+1}/K_i has essential dimension at most three? More generally, for arbitrary n, we let $s(n)$ be the minimal integer such that L is contained in a tower of extensions of essential dimension at most $s(n)$.

Hilbert proves in [H2] that $s(n) \leq n-5$ for $n \geq 9$. More generally, $s(n)$ can be bounded by $n-t(n)$ where $t(n)$ is a very slowly growing function of n (see the discussion in in [Di]). It is very unclear whether this is even a rough approximation to the correct value of $s(n)$.

We do note that $s(n) \leq d^{solv}(n)$. Indeed, solvable extensions are of essential dimension one. By the definition of $d^{solv}(n)$ there is a sequence of solvable extensions followed by an extension of essential dimension $d^{solv}(n)$ that contains L. Thus $s(n) \leq d^{solv}(n)$.

4. A lower bound on $d(n)$.

Since S_n has a subgroup which is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{[n/2]}$, we have

$$d(n) = \mathrm{ed}(S_n) \geq \mathrm{ed}(\mathbf{Z}/2\mathbf{Z})^{[n/2]} .$$

Thus the lower bound on $d(n)$ given in Theorem 1.1(b) is a consequence of the following result.

Theorem 4.1. $\mathrm{ed}((\mathbf{Z}/2\mathbf{Z})^m) = m$.

The proof in [BR, Corollary 5.5] uses induction on m; the inductive step involves passing to the residue field for an appropriate valuation. Another argument, due to J.-P. Serre, can be found in Section 8. Here we give a short proof using Tsen-Lang theory.

Proof. The group $G_r = (\mathbf{Z}/2\mathbf{Z})^r$ has a faithful r-dimensional representation $V = k^r$ given by $\zeta x_i \longrightarrow (-1)^{\zeta_i} x_i$ where $\zeta = (\zeta_1, \ldots, \zeta_r) \in G_r$. Thus $\mathrm{ed}(G_r) \leq m$. To prove the opposite inequality, we may assume without loss of generality that the base field k is algebraically closed; in fact, it is clear from the definition that the essential dimension can only decrease when the base field k is enlarged.

Let $E = k(V) = k(x_1, \cdots, x_r)$ be the function field of V and let $F = E^{G_r} = k(a_1, \ldots, a_r)$, where $a_i = x_i^2$. Then $\mathrm{ed}(G_r) = \mathrm{ed}(V) = \mathrm{ed}(E/F)$. We want to show that the extension E/F is not defined over any field F_0 with $\mathrm{trdeg}_k(F_0) < r$. In order to do so, we consider the trace form $q_{E/F}(x) = \mathrm{Tr}_{E/F}(x^2)$. This is a quadratic form $E \longrightarrow F$, where E is viewed as a 2^r-dimensional vector space over F. We claim that this form is anisotropic (i.e., has no zeroes) over F. Indeed, set $x^I = x_1^{i_1} \ldots x_r^{i_r}$. The elements x^I form an F-basis of E, where $i_1, \ldots, i_r \in \{0, 1\}$. Writing $x = \sum t_I x^I$ we see that

$$q_{E/F}(x) = 2^r \sum_{I \in \{0,1\}^r} a^I t_I^2 \,,$$

where $a^I = a_1^{i_1} \ldots a_r^{i_r}$. In other words, $q_{E/F}$ is a constant multiple of the r-fold Pfister form $<< a_1, \ldots, a_r >>$, which is known to be anisotropic (see, e.g., [P, Ch. 8, Ex. 1.2(6)]). This proves our claim.

We are now ready to finish the proof of the theorem. Suppose the extension E/F is defined over a field F_0 with $\mathrm{trdeg}_k(F_0) \leq r - 1$. Since we are assuming that k is algebraically closed, and $q_{E/F}$ is a quadratic form in 2^r variables, the Tsen-Lang theorem asserts that $q_{E/F}$ has a nontrivial zero, i.e., is isotropic; see [P, Ch. 5, Cor. 1.5]. This contradiction shows that $\mathrm{ed}(E/F) = r$, thus completing the proof of Theorem 4.1. $\square$

5. Relative essential dimension

In order to study $d^{solv}(n)$, $d^{odd}(n)$, and $d^{odd}_{\Delta}(n)$, we need to relativize the notion of essential dimension.

Let G and H be finite groups, let m be an integer, and let X be a faithful G-variety. We shall say that a G-equivariant map $\pi : Y \longrightarrow X$ is an (m, H)-cover if π corresponds to a finite field extension $k(Y)/k(X)$ whose degree divides m and whose galois group $\mathrm{Gal}(k(Y), k(X))$ is isomorphic to a subgroup of H. Note that we do not require $k(Y)$ to be Galois over $k(X)$; here, as usual, $\mathrm{Gal}(k(Y), k(X))$ denotes $\mathrm{Aut}_{k(X)}(k(Y)^{\#})$, where $k(Y)^{\#}$ is the normal closure of $k(Y)$ over $k(X)$.

Definition 5.1. Let X be a faithful G-variety. The relative essential dimension $\mathrm{ed}^{m,H}(X)$ is the minimal value of $\mathrm{ed}(Y)$, as

$$\pi : Y \longrightarrow X$$

ranges over all (m, H)-covers of X.

Observe that the identity map $id_X : X \longrightarrow X$ is an (m, H)-cover for any m and H. Thus the minimum in the above definition is taken over a non-empty set and $\mathrm{ed}^{m,H}(X) \leq \mathrm{ed}(X)$ for any m and H. On the other hand, for some m and H there are no (m, H)-covers other than id_X, and, consequently, the above inequality becomes an equality by default. For example, this happens when m and $|H|$ are relatively prime.

We record an algebraic form of Definition 5.1 for future reference.

Lemma 5.2. *Let X be a G-variety with function field $E = k(X)$ and let $F = k(X)^G$. Then $\mathrm{ed}_H(X) = \min\{\mathrm{ed}(E \otimes_F F'/F')\}$, where F' ranges over all extensions F'/F such that (i) $[F' : F']$ divides m, (ii) $E \otimes_F F'$ is a field and (iii) $\mathrm{Gal}(E'/E)$ is isomorphic to a subgroup of H.*

Proof. Recall that all fields considered in this paper are function fields over k. Thus the extensions F'/F satisfying (i) and (ii) are in 1-1 correspondence with the (m, H)-covers $Y \longrightarrow X$ via $F' = k(Y)^G$ and Y is a variety with function field $E \otimes_F F'$. □

We now prove the relative form of Lemma 2.2.

Lemma 5.3. *Let X be a faithful G-variety. Then*

$$\mathrm{ed}^{m,H}(X \times \mathbf{A}^1) = \mathrm{ed}^{m,H}(X)$$

for any m and H. Here $\mathbf{A}^1$ is an affine line with trivial G-action.

Proof. Suppose $\pi : Y \longrightarrow X$ is an (m, H)-cover. Then

$$\pi \times id : Y \times \mathbf{A}^1 \longrightarrow X \times \mathbf{A}^1$$

is also an (m, H)-cover. Since $\mathrm{ed}(Y \times \mathbf{A}^1) = \mathrm{ed}(Y)$, we conclude that $\mathrm{ed}^{m,H}H(X \times \mathbf{A}^1) \leq \mathrm{ed}^{m,H}(X)$.

The opposite inequality is a consequence of the Hilbert Irreducibility Theorem. Indeed, suppose $\mathrm{ed}^{m,H}(X \times \mathbf{A}^1) = d$. Let $\pi : Y \longrightarrow X \times \mathbf{A}^1$ be an H-cover such that there exists a compression $\alpha : Y \longrightarrow Z$ with $\dim(Z) = d$. After replacing Y and Z by appropriate G-invariant open subsets, we may assume without loss of generality that α is a regular map and that G acts freely on Z (and, hence, on Y).

Given an element $f \in k(X)^G$, let X_f be the graph of the rational map $f : X \longrightarrow \mathbf{A}^1$. Note that X_f is a G-invariant subvariety of $X \times \mathbf{A}^1$; moreover, X and X_f are birationally isomorphic as G-varieties. Let $Y_f = \pi^{-1}(X_f)$. Then by the Hilbert Irreducibility Theorem we can choose f so that Y_f is irreducible and

$$\pi : Y_f \longrightarrow X_f$$

is an (m, H)-cover; see [FJ, Cor. 11.7]. Since $\alpha_{|Y_f}$ compresses Y_f to a subvariety of Z, we have $\mathrm{ed}(Y_f) \leq d$ and hence, $\mathrm{ed}^{m,H}(X) = \mathrm{ed}^{m,H}(X_f) \leq \mathrm{ed}(Y) \leq d$, as claimed. $\square$

We can now define the relative essential dimension $\mathrm{ed}^{m,H}(G)$ by mimicking the definition of $\mathrm{ed}(G)$ given in section 2. That is, we define $\mathrm{ed}^{m,H}(G)$ as $\mathrm{ed}^{m,H}(V)$, where V is a faithful representation of G. To make sure this number is well defined, we need to show that

$$\mathrm{ed}^{m,H}(V_1) = \mathrm{ed}^{m,H}(V_2)$$

for any two faithful representations V_1 and V_2 of G. Indeed, combining the above lemma with Lemma 2.4, we see that $\mathrm{ed}^{m,H}(X \times V) = \mathrm{ed}^{m,H}(X)$, where X is a faithful G-variety and V is a G-representation. Substituting $X = V_1$ and $V = V_2$, we obtain $\mathrm{ed}^{m,H}(V_1 \times V_2) = \mathrm{ed}^{m,H}(V_1)$. Similarly, $\mathrm{ed}^{m,H}(V_1 \times V_2) = \mathrm{ed}^{m,H}(V_2)$, which proves the desired equality.

Corollary 5.4. *If G_1 is a subgroup of G then $\mathrm{ed}^{m,H}(G_1) \leq \mathrm{ed}^{m,H}(G)$ for any group H and any integer m.*

Proof. Immediate from the definition. $\square$

6. The d-functions are non-decreasing

In this section we prove the following theorem.

Theorem 6.1. *(a)* $d^{solv}(n+1) \geq d^{solv}(n)$.

(b) $d^{odd}(n+1) \geq d^{odd}(n)$.

(c) $d^{odd}_{\Delta}(n+1) \geq d^{odd}_{\Delta}(n)$.

The idea of the proof is to interpret the functions $d^{solv}(n)$, $d^{odd}(n)$, and $d^{odd}_{\Delta}(n)$ in terms of essential dimension.

Lemma 6.2. *(a)* $d^{solv}(n) = \min\{\mathrm{ed}^{m,H}(A_n) \mid H \,\text{solvable}, \ m \geq 1\}$.

(b) $d^{odd}(n) = \min\{\mathrm{ed}^{m,H}(S_n) \mid H \,\text{solvable}, \ m \text{ odd}\}$.

(c) $d^{odd}_{\Delta}(n) = \min\{\mathrm{ed}^{m,H}(A_n) \mid H \,\text{solvable}, \ m \text{ odd}\}$.

Proof. Let $V = k^n$, viewed as an S_n-variety with the natural action. Denote the function field of V by $E = k(V) = k(x_1, \dots , x_n)$ and let $K = E^{S_n} = k(a_1, \dots , a_n)$, where $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ is the minimal polynomial of x_1. Note that this is the same polynomial f and the same field K we considered in Section 1 and that the field $L = K[x]/f$ can now be identified with $K(x_1)$. Also note that $E^{A_n} = K(\sqrt{\Delta})$, where Δ is the discriminant of f.

Part (a) now follows from the characterization of $d^{solv}(n)$ in terms of essential dimension given by Lemma 2.1(b). Indeed, recall that by definition $\mathrm{ed}^{m,H}(A_n) = \mathrm{ed}^{m,H}(V)$, where V is viewed as a linear A_n-variety. Moreover, by Lemma 5.2 $\mathrm{ed}^{m,H}(V)$ is the minimum of $\mathrm{ed}(E'/K')$, where K' ranges over all extensions of $K(\sqrt{\Delta})$ such that (i) $[K' : K(\sqrt{\Delta})]$ divides m, (ii) $E' = E \otimes_{K(\sqrt{\Delta})} K'$ is a field, and (iii) $\mathrm{Gal}(K', K(\sqrt{\Delta}))$ is isomorphic to a subgroup of H. Note that if H is a solvable group then (ii) is automatic, since f remains irreducible over K'. (Recall that we are assuming throughout that $n \geq 5$.) Moreover, E' equals the splitting field of $L' = K'[x]/f$ over K' and thus, by Lemma 2.3, $\mathrm{ed}(E'/K') = \mathrm{ed}(L'/K')$. Letting m range over all positive integers and H over all solvable groups, we see that the right hand side of (a) is equal to $\min\{\mathrm{ed}(L'/K')\}$, as K' ranges over all solvable extensions of $K(\sqrt{\Delta})$. Part (a) now follows from Lemma 2.1(b). Parts (b) and (c) are proved in the same way. $\square$

Proof of Theorem 6.1 Since $A_n \subset A_{n+1}$, Corollary 5.4 implies

$$\mathrm{ed}^{m,H}(A_n) \leq \mathrm{ed}^{m,H}(A_{n+1})$$

for any group H. By the previous Lemma this translates into

$$d^{solv}(n+1) \geq d^{solv}(n) \ .$$

The other two parts of the Theorem follow similarly. □

7. Lower bounds on d^{odd} and d^{odd}_{Δ}

Our goal is to prove the following lower bounds on $d^{odd}(n)$ and $d^{odd}_{\Delta}(n)$.

Theorem 7.1. *(a) $d^{odd}(n) \geq [n/2]$.*

(b) $d^{odd}_{\Delta}(n) \geq 2[n/4]$.

We begin by generalizing Theorem 4.1 to the relative situation.

Theorem 7.2. *Let $G_r = (\mathbf{Z}/2\mathbf{Z})^r$ and let m be an odd integer. Then $\mathrm{ed}^{m,H}(G_r) = r$ for any group H.*

Proof. We mimic the proof of Theorem 4.1. Let V be the faithful r-dimensional representation of G_r given in that proof,

$$E = k(V) = k(x_1, \dots, x_r),$$

and

$$F = k(V)^{G_r} = k(a_1, \dots, a_r),$$

where $a_i = x_i^r$. Since G_r has a faithful r-dimensional representation, $\mathrm{ed}^{(m,H)}(G_r) \leq r$. It therefore remains to prove the opposite inequality. At this point we may assume without loss of generality that the base field k is algebraically closed; indeed, the essential dimension cannot decrease if the base field is enlarged. By Definition 5.1, it is sufficient to prove that $\mathrm{ed}^{m,H}(Y) \geq r$ for any (m, H)-cover $\pi : Y \longrightarrow V$. Denote $k(Y)$ by E' and $k(Y)^G$ by F'. Note that $m' = [E' : E]$ divides m and is, therefore, odd. We now consider the following diagram.

$$\begin{tikzcd}
& E' \arrow[dd, dash, "|G|"] \\
E \arrow[ur, dash, "m'"] \arrow[dd, dash, "|G|"'] & \\
& F' \\
F \arrow[ur, dash, "m'"] \arrow[dr, dash] & \\
& k
\end{tikzcd}$$

In section 4 we showed that $q_{E/F}(x) = \mathrm{Tr}_{E/F}(x^2)$ is anisotropic. Thus by a theorem of Springer $q_{E'/F'}(x) = \mathrm{Tr}_{E'/F'}(x^2)$ is also anisotropic (see, e.g., [P, Thm 1.12]). The rest of the proof of Theorem 4.1 goes through unchanged. That is, assume to the contrary, that the extension E'/F' is defined over a field F_0 with $\mathrm{trdeg}_k(F_0) \leq r-1$. Then $q_{E'/F'}$ is also defined over F_0. By the Tsen-Lang Theorem F_0 is a C_{r-1}-field. Thus every quadratic form in 2^r variables defined over F_0 is isotropic, a contradiction. $\square$

Proof of Theorem 7.1 (a) Recall that S_n contains a copy of $G_r = (\mathbf{Z}/2\mathbf{Z})^r$ for $r = [n/2]$. Thus for any group H of odd order

$$\mathrm{ed}^{m,H}(S_n) \geq \mathrm{ed}^{m,H}(G_{[n/2]}) = [n/2] \; ;$$

see Corollary 5.4. Combining this with Lemma 6.2(b), we obtain the desired inequality $d^{odd}(n) \geq [n/2]$.

(b) Note that A_n contains $G_r = (\mathbf{Z}/2\mathbf{Z})^r$ for $r = 2[n/4]$. Indeed, A_n contains $(A_4)^{[n/4]}$ and each copy of A_4 contains $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$. Thus for any group H of odd order

$$\mathrm{ed}^{m,H}(A_n) \geq \mathrm{ed}^{m,H} G_{2[n/4]} = 2[n/4] \; .$$

Combining this with Lemma 6.2(c), we obtain $d^{odd}(n) \geq 2[n/4]$. $\square$

8. A cohomological approach

Throughout this section k will be assumed to be algebraically closed. Suppose F/k is a field extension of transcendence degree $\leq d$. The proofs above of Theorems 1.1(b) and 7.1 were based on the fact that such a field F is a C_d-field; see e.g., [P, Sect. 5]. An alternative proof of Theorem 1.1(b), communicated to us by J.-P. Serre, is based on the fact that the cohomological dimension of F is at most d; see [S, II.4]. In this section we present Serre's argument and use it to give an alternative proof of Theorem 7.1.

If F is a field, then we let $\overline{F}$ be its algebraic closure, and let $G_F = \mathrm{Gal}(\overline{F}, F)$ be its Galois group. We will denote the cohomology group $H^i(G_F, \mathbf{Z}/2\mathbf{Z})$ by $H^i(F)$; here $\mathbf{Z}/2\mathbf{Z}$ is viewed as a trivial G_F-module. The sum $H^*(F) = \oplus_i H^i(F)$ is a ring with the multiplication given by the cup product. Since our coefficient module is $\mathbf{Z}/2\mathbf{Z}$, this ring is, in fact, commutative. A field extension F'/F induces the restriction homomorphism

$$\mathrm{Res}_{F'/F} : H^i(F) \longrightarrow H^i(F')$$

for every i. By Kummer theory $H^1(F) \simeq F^*/F^{*2}$; we will denote the class corresponding to $x \pmod{x^2}$ by (x). If $q(x_1, \ldots, x_n) = a_1x_1^2 + \ldots + a_nx_n^2$ is a quadratic form over F then the r-th Stiefel-Whitney class $w_r(q) \in H^r(F)$ is given by

$$w_r(q) = \sum_{1 \leq i_1 < \ldots < i_r \leq n} (a_{i_1})(a_{i_2}) \ldots (a_{i_r}) \ . \tag{4}$$

By a theorem of Delzant $w_r(q)$ depends only on the equivalence class of the quadratic form $q = < a_1, \ldots, a_r >$ and not on the specific presentation of q as a sum of squares; see [De].

We shall be particularly interested in the quadratic forms which arise as trace forms of etale algebras. Recall that E is an etale algebra over F if E is a direct sum of field extensions of F of finite degree. We shall denote the trace form of such an algebra by $q_{E/F}$. That is, $q_{E/F}(x) = \mathrm{Tr}_{E/F}(x^2)$ for any $x \in E$.

Lemma 8.1. *Let k be an algebraically closed field, F be a field containing k, and E/F be a finite field extension with* $\mathrm{ed}(E/F) = d$. *Then $w_r(q_{E/F}) = 0$ for every $r > d$.*

Proof. Since $\mathrm{ed}(E/F) = d$, there exists a subfield F_0 of F and a degree n extension E_0/F_0 such that $\mathrm{trdeg}_k(F_0) = d$ and $E \simeq E_0 \otimes_{F_0}$

F. Then $w_r(q_{E/F}) = \mathrm{Res}_{E/F}(w_r(q_{E_0/F_0}))$. Since the cohomological dimension of F_0 is $\leq d$, we have $H^r(F_0) = (0)$ for all $r > d$. In particular, $w_r(q_{E_0/F_0}) = 0$, and the lemma follows. □

Lemma 8.2. *Let $F_m = k(b_1, \dots, b_m)$, where $b_1, \dots, b_m$ are independent variables over k. Then $(b_1)\dots(b_m) \neq 0$ in $H^m(F_m)$.*

Proof. We proceed by induction on m. Since b_1 is not a square in F_1, the lemma is true for $m = 1$. To prove the induction step, let F be a field and let t be an independent variable over F. (We will later set $F = F_{m-1}$ and $t = b_m$.) Let

$$G = G_{F(t)} = \mathrm{Gal}(\overline{F(t)}, F(t)),\ N = \mathrm{Gal}(\overline{F(t)}, \overline{F}(t)),$$

and thus $G/N = \mathrm{Gal}(\overline{F}(t), F(t)) \simeq \mathrm{Gal}(\overline{F}, F) = G_F$. Consider the Hochschild-Serre sequence

$$0 \longrightarrow H^m(F) \longrightarrow H^m(F(t)) \xrightarrow{\alpha} H^{m-1}(G_F, H^1(\overline{F}(t))) \longrightarrow 0\ ;$$

see [S, (1.4), p. 111]. The valuation $\overline{F}(t) \longrightarrow \mathbf{Z}$ given by the degree in t descends to

$$H^1(\overline{F}(t)) \simeq \overline{F}(t)^*/(\overline{F}(t)^*)^2 \longrightarrow \mathbf{Z}/2\mathbf{Z}\ ,$$

which in turn gives rise to

$$\beta : H^{m-1}(G/N, H^1(\overline{F}(t)) \longrightarrow H^{m-1}(G/N, \mathbf{Z}/2\mathbf{Z}) = H^{m-1}(F)\ .$$

These maps are described in some detail in [S, II, Appendix 1 and II.4.2]. Tracing through the definitions, we see that $\gamma(a.(t)) = a$; where

$$\gamma = \beta \circ \alpha : H^m(F(t)) \longrightarrow H^{m-1}(F)$$

and $a.(t)$ denotes the cup product of a and (t). In particular, $a.(t)$ is nonzero if a is nonzero. Setting $F = F_{m-1}$, $t = b_m$, and $a = (b_1)\dots(b_{m-1})$, yields the desired induction step. □

Now let E be an etale algebra of dimension n over F and let Σ be the set of F-homomorphisms $E \longrightarrow \overline{F}$. Then Σ is a set of n elements. The group $G_F = \mathrm{Gal}(\overline{F}, F)$ acts on Σ; this action is given by a (continuous) homomorphism $\phi : G_F \longrightarrow S_n$. This map is uniquely determined by E up to an inner automorphisms of S_n. We shall refer to the image of ϕ as the Galois group of E over F and denote it by $\mathrm{Gal}(E, F)$. Note that if E is a finite field extension of F then this definition coincides with the usual one, i.e., $\mathrm{Gal}(E,F) = \mathrm{Aut}_F(E^{\#})$, where $E^{\#}$ is the normal closure of E over F.

Proposition 8.3. *Let L/K be the general field extension, as in (1). Let F be a field extension of k, E be an n-dimensional an etale algebra over F, and $t = (t_1, \dots, t_n)$ be an n-tuple of algebraically independent variables over F. Then*

(a) there is an inclusion of fields $K \hookrightarrow F(t)$ such that $E(t) \simeq L \otimes_K F(t)$. Moreover,

(b) if $Gal(E,F) \subset A_n$ then there exists an inclusion of fields $K(\sqrt{\Delta}) \hookrightarrow F(t)$ such that $E(t) \simeq L(\sqrt{\Delta}) \otimes_{K(\sqrt{\Delta})} F(t)$.

Proof. (a) It is sufficient to find an element y of $E(t) = E \otimes_F F(t)$ such that (i) $E = F[y]$ and (ii) the minimal polynomial $g(t) = t^n + b_1 t^{n-1} + \ldots + b_n$ of y over $F(t)$ has algebraically independent coefficients. Indeed, if such an element can be found then the desired inclusion $K \hookrightarrow F$ is given by $a_i \longrightarrow b_i$. If $e_1, \dots, e_n$ is a basis for E as an F-vector space then $y = t_1 e_1 + \ldots + t_n e_n$ satisfies (i) and (ii); this is proved in [Re2].

(b) Suppose $y \in F$ satisfies conditions (i) and (ii) above. Denote the discriminant of g by Δ_y. Then, since $\mathrm{Gal}(E,F) \subset A_n$, $\Delta_y = z^2$ for some $z \in F$. Now the desired embedding $K(\sqrt{\Delta}) \hookrightarrow F$ is given by $a_i \longrightarrow b_i$ and $\sqrt{\Delta} \longrightarrow z$. □

Theorem 8.4. *(a) Let $K = k(a_1, \dots, a_n)$, $f(X)$, and $L = K[x]/f$ be as in (1). Then*

(a) $w_{[n/2]}(q_{L/K}) \neq 0$.

(b) $w_{2[n/4]}(q_{L(\sqrt{\Delta})/K(\sqrt{\Delta})}) \neq 0$.

Proof. (a) Assume, to the contrary, that $w_{[n/2]}(q_{L/K}) = 0$. Let E be an n-dimensional etale algebra over F and let $t = (t_1, \dots, t_n)$ be an n-tuple of independent variables over F. Then by Proposition 8.3(a), $w_{[n/2]}(q_{E(t)/F(t)}) = 0$, since it is the image of $w_{[n/2]}(q_{L/K}) = 0$ under the restriction map $\mathrm{Res}_{F(t)/K}$. On the other hand, since $\mathrm{Res}_{F(t)/F}$ is injective (see [S, I.4.3]), $w_{[n/2]}(q_{E(t)/F(t)}) = 0$ implies $w_{[n/2]}(q_{E/F}) = 0$. Thus, in order to obtain a contradiction, it is sufficient to construct a field F containing k and an n-dimensional etale F-algebra E such that $w_{[n/2]}(q_{E/F}) \neq 0$.

First suppose $n = 2m$ is even. Let $b_1, \dots, b_m$ be independent variables over F, $F = k(b_1, \dots, b_m)$, and $E = E_1 \oplus \ldots \oplus E_m$, where

$E_i = F(\sqrt{b_i})$. Then the elements $1_{E_1}, \sqrt{b_1}, 1_{E_2}, \sqrt{b_2}, \dots, 1_{E_m}, \sqrt{b_m}$ form a basis for E over F. Writing out $q_{E/F}$ in the basis, we see that $q_{E/F} =< 2, 2b_1, \dots, 2, 2b_m >$ and, hence, $w_{2m}(q_{E/F}) = (b_1)(b_2)\dots(b_m)$. By Lemma 8.2 this class is non-zero in $H^m(F)$, as claimed.

If $n = 2m+1$ is odd, we repeat the same argument with

$$E_1 = F \oplus E.$$

Then $q_{E_1/F} =< 1 > \oplus q_{E/F}$ and $w_{2m}(q_{E_1/F}) = (b_1)(b_2)\cdots(b_m)$, which is again non-zero by Lemma 8.2.

(b) Arguing as in part (a) (but using Proposition 8.3(b) in place of 8.3(a)), we see that it is sufficient to construct an n-dimensional etale algebra E over a field F with $w_{2[n/4]}(q_{E/F}) \neq 0$ and $\mathrm{Gal}(E, F) \subset A_n$.

First consider the case $n = 4m$. Let $F = k(b_1, \dots, b_{2m})$, as before, and let $E = E_1 \oplus \dots \oplus E_m$, with $E_i = F(\sqrt{b_{2i-1}}, \sqrt{b_{2i}})$. Note that each E_i is Galois over F and $\mathrm{Gal}(E_j, F) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \subset S_4$. Moreover, since E_i is a field, this subgroup is transitive. The group S_4 has only one such subgroup, namely, the normal subgroup of order 4; in particular, this group is contained in A_4. Consequently,

$$\mathrm{Gal}(E, F) \subset A_4 \times \dots \times A_4 \ \ (m \ \text{ times}) \subset A_n \ .$$

To show that $w_{2m}(q_{E/F}) \neq 0$, we write $q_{E/F}$ in the basis $z_1, \dots, z_{4m}$, where

$$z_{4i-3} = 1_{E_i}, z_{4i-2} = \sqrt{b_{2i-1}}, z_{4i-1} = \sqrt{b_{2i-2}}, z_{4i} = \sqrt{b_{2i-1}b_{2i-2}}$$

for every $i = 1, \dots, m$. In this basis

$$q = \oplus_{i=1}^{m} < 4, 4b_{2i-1}, 4b_{2i}, 4b_{2i-1}b_{2i} > \ .$$

Now formula (4) yields $w_{2m}(q_{E/F}) = (b_1)(b_2)\dots(b_{2m})$. By Lemma 8.2 this class is non-zero in $H^{2m}(F)$, as claimed.

This proves part (b) in the case $n = 4m$. If $n = 4m+s$, where $s = 0, 1, 2, 3$ then we replace E by $F^s \oplus E$; the rest of the argument goes through unchanged. $\square$

We are now ready to give alternative proofs of Theorems 1.1(b) and 7.1. Note that in both cases we may assume without loss of generality that the base field k is algebraically closed.

Cohomological proof of Theorem 1.1(b) (a) Assume the contrary: $d(n) < [n/2]$. That is, $\mathrm{ed}(L/K) < [n/2]$; see Lemma 2.1(a). By Lemma 8.1 this implies $w_{[n/2]}(q_{L/K}) = 0$ and thus contradicts Theorem 8.4(a). $\square$

Cohomological proof of Theorem 7.1 (a) Assume the contrary: $d^{odd}(n) < [n/2]$. Then by Lemma 2.1(c) there exists a solvable odd degree extension K'/K such that $\mathrm{ed}(L'/K') < [n/2]$. Hence, $w_{[n/2]}(q_{L'/K'}) = 0$ in $H^{[n/2]}(K')$ by Lemma 8.1. On the other hand, since K'/K is an odd degree extension, the restriction map $\mathrm{Res}_{F'/F} : H^i(F) \longrightarrow H^i(F')$ as injective for every i; see [S, Sect. 2.4]. Thus $w_{[n/2]}(q_{L/K})$, being the preimage of $w_{[n/2]}(q_{L'/K'})$ under this map, is also 0, contradicting Proposition 8.3(a).

(b) Assume the contrary: $d^{odd}(n) < 2[n/4]$. Then there exists a solvable odd degree extension $K'/K(\sqrt{\Delta})$ such that

$$\mathrm{ed}(L'/K') < [n/2].$$

Hence, $w_{2[n/4]}(q_{L'/K'}) = 0$ in $H^{2[n/4]}(K')$. Reasoning as in part (a), we see that this implies $w_{2[n/4]}(q_{L(\sqrt{\Delta})/K(\sqrt{\Delta})}) = 0$, contradicting Proposition 8.3(b). $\square$

References

[A] S. Abhyankar, *Hilbert's Thirteenth Problem*, Société Mathématique de France, Seminaires et Congres, Mémoire **67**, 1997.

[AS] V. Arnold, and G. Shimura, *Superposition of algebraic functions*, Proc. Symposia in pure math., **28** (1976), AMS, Providence, 45-46.

[BR] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math., **106** (1997), 159-179.

[C] D. Coray, *Cubic hypersurfaces and a result of Hermite*, Duke J. Math. **54** (1987), 657-670.

[De] A. Delzant, *Définition des classes de Stiefel-Whitney d'un module quadratique sur un corps de caractéristique différente de 2*, C. R. Acad. Sci. Paris **255** (1962), 1366-1368.

[Di] J. Dixmier, *Histoire du 13e probleme de Hilbert*, Cahiers Sém. Hist. Math. S/'er. 2, 3, 85-94 Univ. Paris VI, Paris, 1993.

[DM] P. Doyle and C. McMullen, *Solving the quintic by iteration*, Acta Math. **163** (1989), 151-180.

[EM] S. Edno and T. Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan, **25** (1973), no. 1, 7-26.

[FJ] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, Heidelberg and New York, 1986.

[He] C. Hermite, *Sur l'invariant du dix-huitième ordre des formes du cinquième degré*, J. Crelle **59** (1861), 304–305.

[H1] D. Hilbert, Mathematical problems. Lecture delivered before the international congress of mathematicians at Paris in 1900, in *Mathematical developments arising from Hilbert Problems*, Proceedings of Symposia in Pure Mathematics **28**, American Mathematical Society, 1976.

[H2] D. Hilbert, *Über die Gleichung neunten Grades*, Mathematische Annalen **97** (1927), 243–250.

[J] P. Joubert, *Sur l'equation du sixième degré*, C-R. Acad. Sc. Paris **64** (1867), 1025–1029.

[Kl] F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig, 1884. English translation: *Lectures on the icosahedron and solution of equations of the fifth degree*, translated by G.G. Morrice, 2nd and rev. edition, New York, Dover Publications, 1956.

[Lo] G. G. Lorentz, The 13-th problem of Hilbert, Proc. Symposia in pure math., **28** (1976) AMS, Providence, 419-430.

[P] A. Pfister, *Quadratic Forms with Applications to Geometry and Topology*, Cambridge University Press, 1995.

[Re1] Z. Reichstein, *On the essential dimension of an algebraic group*, preprint.

[Re2] Z. Reichstein, *On a theorem of Hermite and Joubert*, submitted for publication; preprint on `www.orst.edu/~reichtsz/pub.html`.

[Ri] H. W. Richmond, *Note on the invariants of a binary sextic*, Quarterly J. of Math. **31** (1900), 57–59.

[Ro] P. Roquette, *Isomorphisms of generic splitting fields of simple algebras*, J. Reine Angew. Math. **214/215** (1964), 207–226.

[S] J-P. Serre, Galois Cohomology, Springer, 1997.

Department of Mathematics, Reed College, Portland, OR 97202, USA

E-mail address: `jpb@reed.edu`

Department of Mathematics, Oregon State University, Corvallis, OR 97331, USA

E-mail address: `zinovy@math.orst.edu`