Doc. Math. 31 (2026), 385–399
DOI 10.4171/DM/984

© 2025 Deutsche Mathematiker-Vereinigung
Published by EMS Press
This work is licensed under a CC BY 4.0 license

Hilbert's 13th problem in prime characteristic

Oakley Edens and Zinovy B. Reichstein

Abstract. The resolvent degree $\mathrm{rd}_{\mathbb{C}}(n)$ is the smallest integer d such that a root of the general polynomial

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

can be expressed as a composition of algebraic functions in at most d variables with complex coefficients. It is known that $\mathrm{rd}_{\mathbb{C}}(n) = 1$ when $n \leqslant 5$. Hilbert was particularly interested in the next three cases: he asked if $\mathrm{rd}_{\mathbb{C}}(6) = 2$ (Hilbert's Sextic conjecture), $\mathrm{rd}_{\mathbb{C}}(7) = 3$ (Hilbert's 13th problem) and $\mathrm{rd}_{\mathbb{C}}(8) = 4$ (Hilbert's Octic conjecture). These problems remain open. It is known that $\mathrm{rd}_{\mathbb{C}}(6) \leqslant 2$, $\mathrm{rd}_{\mathbb{C}}(7) \leqslant 3$ and $\mathrm{rd}_{\mathbb{C}}(8) \leqslant 4$. It is not known whether or not $\mathrm{rd}_{\mathbb{C}}(n)$ can be > 1 for any $n \geqslant 6$.

In this paper, we show that all three of Hilbert's conjectures can fail if we replace $\mathbb{C}$ with a base field of positive characteristic.

1. Introduction

The algebraic form of Hilbert's 13th problem asks for the resolvent degree $\mathrm{rd}_{\mathbb{C}}(n)$ of the general polynomial

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

where $a_1, \dots, a_n$ are independent variables. Here $\mathrm{rd}_{\mathbb{C}}(n)$ 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 an algebraic function in $\leqslant d$ variables at each step. For a precise definition, see [1, 6, 13, 14] or Section 2 below. It is known that $\mathrm{rd}_{\mathbb{C}}(n) = 1$ for every $n \leqslant 5$. It is not known whether or not $\mathrm{rd}_{\mathbb{C}}(n)$ is bounded from above, as n tends to infinity or even if $\mathrm{rd}_{\mathbb{C}}(n)$ can be greater than 1 for any n. Various upper bounds on $\mathrm{rd}_{\mathbb{C}}(n)$ have been proved over the past 200 years. For an overview, see [4]. These classical bounds have recently been sharpened by Wolfson [17], Sutherland [15], and Heberle–Sutherland [9]. All of them are of the form $\mathrm{rd}_{\mathbb{C}}(n) \leqslant n - \alpha(n)$, where $\alpha(n)$ is an unbounded but very slow-growing function of n. There is a wide gap between the best-known lower bound, $\mathrm{rd}_{\mathbb{C}}(n) \geqslant 1$, and the best-known upper bound, $\mathrm{rd}_{\mathbb{C}}(n) \leqslant n - \alpha(n)$. It is fair to say that after two centuries of research, we still know very little about $\mathrm{rd}_{\mathbb{C}}(n)$ for $n \geqslant 6$. Specifically, Hilbert conjectured the following values for small n.

Mathematics Subject Classification 2020: 14G17 (primary); 12E05, 14L30, 20C33 (secondary).
Keywords: resolvent degree, Hilbert's 13th problem, positive characteristic.

Conjecture 1.1. (a) $\mathrm{rd}_{\mathbb{C}}(6) = 2$, (b) $\mathrm{rd}_{\mathbb{C}}(7) = 3$, (c) $\mathrm{rd}_{\mathbb{C}}(8) = 4$.

(a) and (c) appeared in [10, p. 247]; they are known as Hilbert's sextic and octic conjectures, respectively. (b) is taken from the statement of Hilbert's 13th problem [11, p. 424]. The upper bounds,

$$\mathrm{rd}_{\mathbb{C}}(6) \leqslant 2, \mathrm{rd}_{\mathbb{C}}(7) \leqslant 3 \quad \text{and} \quad \mathrm{rd}_{\mathbb{C}}(8) \leqslant 4 \tag{1.1}$$

go back to the work of Hamilton in the 1830s [8]; for modern treatments, see [4, p. 87] or [6, Corollary 7.3]. The reverse inequalities remain out of reach.

Recently Farb and Wolfson [6] defined the resolvent degree $\mathrm{rd}_k(G)$, where G is a finite group and k is a field of characteristic 0. Setting G to be the symmetric group S_n and k to be the field $\mathbb{C}$ of complex numbers, we recover $\mathrm{rd}_{\mathbb{C}}(n)$. This definition was extended by the second author [14] to the case where k is an arbitrary field and G is an arbitrary algebraic group over k. For a fixed algebraic group G defined over the integers, $\mathrm{rd}_k(G_k)$ depends only on the characteristic of k and not on k itself; see [14, Theorem 1.2]. We will write $\mathrm{rd}_p(G)$ in place of $\mathrm{rd}_k(G)$, when k is a field of characteristic $p \geqslant 0$. Moreover, if G is an (abstract) finite group, then $\mathrm{rd}_0(G) \geqslant \mathrm{rd}_p(G)$ for any $p > 0$; see [14, Theorem 1.3].

In view of the last inequality, it is natural to ask if more can be said about Conjecture 1.1 in the case, where the base field $\mathbb{C}$ is replaced by a field k of positive characteristic. Conjecturally, one expects $\mathrm{rd}_p(G)$ to be the same as $\mathrm{rd}_0(G)$ when p does not divide the order of G. We will thus examine $\mathrm{rd}_p(\mathrm{S}_n)$ in the case when $n = 6, 7, 8$ and $2 \leqslant \mathrm{char}(k) = p \leqslant n$. Our main result is as follows.

Theorem 1.2. *Let* S_n *denote the symmetric group on n letters. Then*

(a) $\mathrm{rd}_3(\mathrm{S}_6) \leqslant 1$,

(b) $\mathrm{rd}_3(\mathrm{S}_7) \leqslant 2$,

(c) $\mathrm{rd}_5(\mathrm{S}_7) = \mathrm{rd}_5(\mathrm{S}_6) \leqslant 2$,

(d) $\mathrm{rd}_7(\mathrm{S}_7) \leqslant 2$,

(e) $\mathrm{rd}_2(\mathrm{S}_8) \leqslant 3$.

In particular, every part of Conjecture 1.1 fails if $\mathbb{C}$ is replaced by a base field of (suitable) positive characteristic.

Theorem 1.2 may be viewed as complementing the results of [7,9,15,17]. These papers generalize the inequalities $\mathrm{rd}_0(\mathrm{S}_6) \leqslant 2$, $\mathrm{rd}_0(\mathrm{S}_7) \leqslant 3$ and $\mathrm{rd}_0(\mathrm{S}_8) \leqslant 4$ of (1.1) by giving upper bounds on $\mathrm{rd}_0(G)$, when G is the symmetric group S_n (n arbitrary) [9, 15, 17] or when G is a sporadic finite simple group [7]. Here we stay with $G = \mathrm{S}_6, \mathrm{S}_7, \mathrm{S}_8$ and prove sharper bounds on $\mathrm{rd}_p(G)$ for suitable small primes p.

We also consider the Weyl group $W(E_6)$ of the root system of type E_6. It is shown in [6, Section 8] that this group arises naturally in connection with Conjecture 1.1 (a), and that $\mathrm{rd}_0(W(E_6)) \leqslant 3$; see also [14, Proposition 15.1]. We show that in (small) positive characteristic, this inequality can be sharpened.

Theorem 1.3. $\mathrm{rd}_p(W(E_6)) \leqslant 2$ *if* $p = 2, 3$ *or* 5.

	Characteristic				
G	0	2	3	5	7
S_6	2	2	1	2	2
S_7	3	3	2	2	2
S_8	4	3	4	4	4
$W(E_6)$	3	2	2	2	3

Table 1. $\mathrm{rd}_p(G) \leqslant d$ for d as above.

In summary, $\mathrm{rd}_p(G) \leqslant d$, where the value of d is given in Table 1.

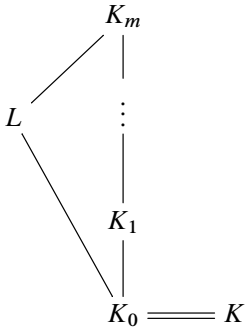
The remainder of this paper is structured as follows. In Section 2 we recall the definition of resolvent degree of a finite group and collect some of its properties for future use. We believe that part (a) of Theorem 1.2 was known classically; for lack of a reference, we include a short proof at the end of Section 2. In Section 3 we prove upper bounds on the resolvent degree of finite symplectic and unitary groups. These upper bounds play a key role in the proofs of parts (b) and (c) of Theorem 1.2 and of Theorem 1.3 in Section 4. Parts (d) and (e) of Theorem 1.2 are proved in Section 6 by a different (more geometric) argument inspired by our previous work on the essential dimension of symmetric groups [5].

2. Preliminaries

2.1. The level of a finite field extension

Let K be a field containing a base field k, and L/K be a finite extension. We say that L/K *descends to an intermediate field* $k \subset K_0 \subset K$ if $L = L_0 \otimes_{K_0} K$ for some finite extension L_0/K_0. The *essential dimension* $\mathrm{ed}_k(L/K)$ is then the smallest transcendence degree $\mathrm{trdeg}_k(K_0)$ such that L/K descends to K_0.

The level $\mathrm{lev}_k(L/K)$ of a finite extension L/K is the smallest integer d such that there exists a tower of field extensions



with $[K_i : K_{i-1}] < \infty$ and $\mathrm{ed}_k(K_i/K_{i-1}) \leqslant d$ for every $i = 1, \ldots, m$.

The *resolvent degree* $\mathrm{rd}_k(G)$ of a finite group G over a field k is defined as the maximal value of $\mathrm{lev}_k(L/K)$, where the maximum is taken over all fields K containing k and all G-Galois field extensions L/K.[1]

Lemma 2.1. *Let G be an abstract finite group and k be a field of characteristic $p \geqslant 0$. Then*

(a) $\mathrm{rd}_k(G) = \mathrm{rd}_{k'}(G)$ *for any field k' of characteristic p.*

(b) *If H is a subgroup of G, then $\mathrm{rd}_k(H) \leqslant \mathrm{rd}_k(G)$. Moreover, if $G \neq 1$, then $\mathrm{rd}_k(G) \geqslant 1$.*

(c) *If G is abelian, then $\mathrm{rd}_k(G) \leqslant 1$.*

(d) *If $1 \to A \to G \to B \to 1$ is an exact sequence of finite groups, then $\mathrm{rd}_k(G) \leqslant \max\{\mathrm{rd}_k(A), \mathrm{rd}_k(B)\}$. If additionally A is a central subgroup of G, $B \neq 1$ and $\mathrm{char}\, k \nmid |A|$, then $\mathrm{rd}_k(G) = \mathrm{rd}_k(B)$.*

Proof. Part (a) is [14, Theorem 1.2].

(b) For the inequality $\mathrm{rd}_k(H) \leqslant \mathrm{rd}_k(G)$, see [6, Lemma 3.13] or [14, Remark 10.5]. To prove the inequality $\mathrm{rd}_k(G) \geqslant 1$ we may replace k by its algebraic closure; see part (a). In the case, where k is algebraically closed, $\mathrm{lev}_k(L/K) \geqslant 1$ for every non-trivial extension L/K; see [14, Lemma 4.5]. Thus $\mathrm{rd}_k(G) \geqslant 1$ for every non-trivial group G.

For (c), see [6, Corollary 3.4] or [14, Example 10.6].[2]

For the first inequality in (d), see [6, Theorem 3.3] or [14, Proposition 10.8 (a)]. In the case, where A is central, [14, Proposition 10.8 (d)] tells us that

$$\mathrm{rd}_k(G) \leqslant \max\left\{\mathrm{rd}_k(B), 1\right\} \quad \text{and} \quad \mathrm{rd}_k(B) \leqslant \max\left\{\mathrm{rd}_k(G), 1\right\}. \tag{2.1}$$

By our assumption $B \neq 1$ and hence, $G \neq 1$. By part (b), $\mathrm{rd}_k(B) \geqslant 1$, $\mathrm{rd}_k(G) \geqslant 1$. Now the inequalities (2.1) translate to $\mathrm{rd}_k(G) = \mathrm{rd}_k(B)$. ∎

For notational simplicity, we will write $\mathrm{rd}_p(G)$ in place of $\mathrm{rd}_k(G)$, where $p = \mathrm{char}(k)$ is either 0 or a prime. This notation makes sense in view of Lemma 2.1 (a). As we mentioned in Section 1,

$$\mathrm{rd}_0(G) \geqslant \mathrm{rd}_p(G) \text{ for any } p > 0; \tag{2.2}$$

see [14, Theorem 1.3].

Corollary 2.2. $\mathrm{rd}_p(\mathrm{A}_n) = \mathrm{rd}_p(\mathrm{S}_n)$ *for every $p \geqslant 0$ and every $n \geqslant 3$.*

Proof. By part (b) of Lemma 2.1, $1 \leqslant \mathrm{rd}_p(\mathrm{A}_n) \leqslant \mathrm{rd}_p(\mathrm{S}_n)$. It remains to prove the opposite inequality, $\mathrm{rd}_p(\mathrm{S}_n) \leqslant \mathrm{rd}_p(\mathrm{A}_n)$. Indeed, applying Lemma 2.1 (d) to the natural exact sequence $1 \to \mathrm{A}_n \to \mathrm{S}_n \to \mathbb{Z}/2\mathbb{Z} \to 1$, and remembering that $\mathrm{rd}_p(\mathbb{Z}/2\mathbb{Z}) \leqslant 1$ by part (c),

[1] Note that this maximum is well defined because a G-Galois field extension L/K with $k \subset K$ exists for any finite group G. Indeed, consider the regular representation $G \hookrightarrow \mathrm{GL}(V)$, where $V = k[G]$ is the group algebra. Now set $L = k(V)$ = the field of rational functions on V, and $K = L^G$.

[2] Note that [6] assumes that $\mathrm{char}(k) = 0$. In [14], k is allowed to be of arbitrary characteristic.

we obtain

$$\mathrm{rd}_p(\mathrm{S}_n) \leqslant \max\left\{\mathrm{rd}_p(\mathrm{A}_n), \mathrm{rd}_p(\mathbb{Z}/2\mathbb{Z})\right\} = \max\left\{\mathrm{rd}_p(\mathrm{A}_n), 1\right\} = \mathrm{rd}_p(\mathrm{A}_n),$$

as desired. ∎

2.2. Generically free actions

Consider an algebraic variety X equipped with the action of a finite group G defined over a field k. We will sometimes refer to such X as a G-variety. We say that the G-action on X is *generically free* if G acts freely on a G-invariant dense open subvariety $U \subset X$ defined over k. In other words, we require that the stabilizer of every $\bar{k}$-point $u \in U$ be trivial. Here $\bar{k}$ denotes the algebraic closure of k.

Recall that the G-action on X is called *faithful* if every non-trivial element of G acts non-trivially on X. We record the following easy lemma for future reference.

Lemma 2.3. *Let G be a finite group and X be a G-variety.*

(a) *A generically free G-action on X is faithful.*

(b) *If X is irreducible, then the converse holds: A faithful G-action on X is generically free.*

Proof. Part (a) is obvious from the definition, because X has a $\bar{k}$-point with trivial stabilizer. For part (b), assume the contrary: a G-action on X is not generically free. This means that X is covered by the fixed point loci X^g, where g ranges over the non-identity elements of G. Since X is irreducible, we conclude that $X = X^{g_0}$ for some $1 \neq g_0 \in G$. The element g_0 then acts trivially on X, and thus the G-action on X is not faithful. ∎

Note that part (b) may fail if X is allowed to be reducible. For example, the natural action of S_n on a disjoint union of n points, is faithful but not generically free.

Lemma 2.4. *Let V be a finite-dimensional k-vector space of dimension $\geqslant 1$, G be a finite subgroup of* $\mathrm{PGL}(V)$ *and X be an irreducible G-invariant hypersurface of degree $d \geqslant 2$ in $\mathbb{P}(V)$. Then the G-action on X is generically free.*

Proof. We may assume without loss of generality that the base field k is algebraically closed. Assume the contrary: the G-action on X is not generically free. Then X is covered by the union of the fixed point loci $\mathbb{P}(V)^g$, as g ranges over $G \setminus \{1\}$. Since X is irreducible, $X \subset \mathbb{P}(V)^g$ for one particular $1 \neq g \in G$.

Now observe that the fixed locus $\mathbb{P}(V)^g$ is a finite union of subvarieties of the form $\mathbb{P}(V_\lambda)$, where $\tilde{g}$ is a preimage of g in $\mathrm{GL}(V)$, λ is an eigenvalue of $\tilde{g}$, and V_λ is the λ-eigenspace of $\tilde{g}$. Note that since $g \neq 1$ in $\mathrm{PGL}(V)$, $V_\lambda \subsetneq V$. Since X is irreducible, $X \subset \mathbb{P}(V_\lambda) \subsetneq \mathbb{P}(V)$ for one particular λ. Since X is a hypersurface, this is only possible if $X = \mathbb{P}(V_\lambda)$ is a hypersurface of degree 1. This contradicts our assumption that the degree d of X is $\geqslant 2$. ∎

Lemma 2.5. *Suppose G is a finite subgroup of $\mathrm{PGL}_{n+1}(k)$ and there exists a G-invariant closed subvariety X of $\mathbb{P}^n$ of degree a and dimension $b \geqslant 1$ (not necessarily smooth or irreducible). Assume further that the G-action on X is generically free. Then*

$$\mathrm{rd}_k(G) \leqslant \max\left\{b, \mathrm{rd}_k(\mathrm{S}_a)\right\},$$

where S_a denotes the symmetric group on a letters.

Proof. See [14, Proposition 14.1 (a)] or [17, Proposition 4.11]. ∎

Proof of Theorem 1.2 (a). We need to show that $\mathrm{rd}_3(\mathrm{S}_6) = 1$. In view of Corollary 2.2 and Lemma 2.1 (b) it suffices to show that $\mathrm{rd}_3(\mathrm{A}_6) \leqslant 1$. Recall that $\mathrm{A}_6 \simeq \mathrm{PSL}_2(9)$; see [3, p. 4]. Thus there exists a faithful action of A_6 on the projective line $\mathbb{P}^1$ defined over the field $k = \mathbb{F}_9$. We now apply Lemma 2.5 with $G = \mathrm{A}_6$, $n = 1$ and $X = \mathbb{P}^1$. Here we view X as a closed subvariety of $\mathbb{P}^1$ of degree $a = 1$ and dimension $b = 1$. Since X is irreducible, the (faithful) A_6-action on X is automatically generically free; see Lemma 2.3 (b). By Lemma 2.5 we conclude that

$$\mathrm{rd}_3(\mathrm{A}_6) = \mathrm{rd}_k(\mathrm{A}_6) \leqslant \max\left\{1, \mathrm{rd}_k(\mathrm{S}_1)\right\} = 1.$$

as desired. ∎

3. Resolvent degree of finite symplectic and unitary groups

Let n be a positive integer, $q = p^r$ be a prime power, and $\mathbb{F}_q$ be the finite field with q elements. Recall that $\mathrm{U}_n(q)$ is defined as the subgroup of elements of $\mathrm{GL}_n(\mathbb{F}_{q^2})$ which preserve the hermitian form h on $\mathbb{F}_{q^2}^n$ defined by the formula

$$h\big((x_1, \dots, x_n), (y_1, \dots, y_n)\big) \mapsto x_1\overline{y_1} + \cdots + x_n\overline{y_n}.$$

Here $\mathbb{F}_{q^2}/\mathbb{F}_q$ is a field extension of degree 2, and $x \mapsto \bar{x} = x^q$ is the unique non-trivial automorphism of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. The group $\mathrm{SU}_n(q)$ is the subgroup of elements of $U_n(q)$ of determinant 1.

The group $\mathrm{Sp}_n(q)$ is defined in a similar manner as the subgroup of elements of $\mathrm{GL}_n(\mathbb{F}_q)$ which preserve the standard symplectic form ω on $(\mathbb{F}_q)^n$. Here n is assumed to be even, $n = 2m$, and

$$\omega\big((x_1, \dots, x_{2m}), (y_1, \dots, y_{2m})\big) = (x_1y_2 - x_2y_1) + \cdots + (x_{2m-1}y_{2m} - x_{2m}y_{2m-1}).$$

Note that every non-degenerate hermitian form on $\mathbb{F}_{q^2}^n$ is equivalent to h and every symplectic form on $\mathbb{F}_q^n$ is equivalent to ω.

Proposition 3.1. *Let $q = p^r$ be a prime power. Then*

(a) $\mathrm{rd}_p(\mathrm{Sp}_n(q)) \leqslant \max\{n-2, \mathrm{rd}_p(\mathrm{S}_{q+1})\}$ *for any even integer $n \geqslant 4$, and*

(b) $\mathrm{rd}_p(\mathrm{U}_n(q)) \leqslant \max\{n-2, \mathrm{rd}_p(\mathrm{S}_{q+1})\}$ *for every integer $n \geqslant 3$.*

Proof. We will use the following notational conventions: $x_1, \dots, x_n$ will denote independent variables over $\mathbb{F}_q$, $\mathbf{x} := (x_1, \dots, x_n)$ and $\mathbf{x}^q := (x_1^q, \dots, x_n^q)$.

(a) Consider the homogeneous polynomial

$$\begin{aligned} f(\mathbf{x}) &= \omega(\mathbf{x}, \mathbf{x}^q) \\ &= (x_1 x_2^q - x_2 x_1^q) + \cdots + (x_{2m-1} x_{2m}^q - x_{2m} x_{2m-1}^q) \in \mathbb{F}_q[x_1, \dots, x_n] \end{aligned}$$

of degree $q+1$. A simple application of the Jacobian criterion shows that $f(\mathbf{x})$ cuts out a smooth hypersurface in $\mathbb{P}^{n-1}$. Denote this smooth hypersurface by X. Since $n \geqslant 3$, X has to be irreducible; otherwise, irreducible components of X would intersect non-trivially, and their intersection point would be singular on X.

We are now ready to complete the proof of part (a). Applying Lemma 2.1 (d) to the central exact sequence

$$1 \to Z \to \mathrm{Sp}_n(q) \to \mathrm{PSp}_n(q) \to 1, \tag{3.1}$$

where $Z = \{\pm 1\}$ is the subgroup of scalar matrices in $\mathrm{Sp}_n(q)$, we obtain $\mathrm{rd}_p(\mathrm{Sp}_n(q)) = \mathrm{rd}_p(\mathrm{PSp}_n(q))$. On the other hand, $\mathrm{PSp}_n(q) \subset \mathrm{PGL}_n(\mathbb{F}_q)$ acts on the irreducible hypersurface X of degree $q+1 > 2$ in $\mathbb{P}^{n-1}$. By Lemma 2.4, the $\mathrm{PSp}_n(q)$-action on X is generically free. Applying Lemma 2.5, we obtain

$$\mathrm{rd}_p\left(\mathrm{Sp}_n(q)\right) = \mathrm{rd}_{\mathbb{F}_q}(\mathrm{PSp}_n(q)) \leqslant \max\left\{n-2, \mathrm{rd}_{\mathbb{F}_q}(\mathrm{S}_{q+1})\right\}, \tag{3.2}$$

as desired.

(b) We apply a similar argument to the polynomial

$$f(\mathbf{x}) = h(\mathbf{x}, \mathbf{x}) = x_1^{q+1} + \cdots + x_n^{q+1} \in \mathbb{F}_q[x_1, \dots, x_n]$$

of degree $q+1$. Let $X \subset \mathbb{P}^{n-1}$ be the hypersurface cut out by $f(\mathbf{x})$. Once again, X is smooth by the Jacobian criterion, and since $n \geqslant 3$, this allows us to conclude that X is irreducible.

Claim. $f(\mathbf{x})$ (and hence, X) is invariant under the natural action of $\mathrm{U}_n(q)$.

Choose $g \in \mathrm{U}_n(q)$. Our goal is to prove that

$$\Delta(\mathbf{x}) := f(g \cdot \mathbf{x}) - f(\mathbf{x}) \in \mathbb{F}_{q^2}[x_1, \dots, x_n]$$

is the zero polynomial. Indeed, for every $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_{q^2}^n$, we have

$$f(g \cdot \mathbf{a}) = h(g \cdot \mathbf{a}, g \cdot \mathbf{a}) = h(\mathbf{a}, \mathbf{a}) = f(\mathbf{a}).$$

We conclude that $\Delta(\mathbf{x})$ is a homogeneous polynomial of degree $q+1$ which vanishes at every $\mathbb{F}_{q^2}$-point of $\mathbb{P}^{n-1}$. By [12, Théorème 2.1], the minimal degree of any non-zero polynomial with this property is q^2+1. This tells us that $\Delta(\mathbf{x})$ is the zero polynomial, thus completing the proof of the claim.

To finish the proof of part (b), we argue as in part (a). Consider the central exact sequence

$$1 \to Z \to \mathrm{U}_n(q) \to \mathrm{PU}_n(q) \to 1,$$

where $Z = \{\pm 1\}$ is the subgroup of scalar matrices in $\mathrm{U}_n(q)$. By Lemma 2.1 (d),

$$\mathrm{rd}_p\left(\mathrm{U}_n(q)\right) = \mathrm{rd}_p\left(\mathrm{PU}_n(q)\right) \tag{3.3}$$

On the other hand, $\mathrm{PU}_n(q) \subset \mathrm{PGL}_n(\mathbb{F}_{q^2})$ acts on the irreducible hypersurface X of degree $q+1 \geqslant 2$ cut out by $f(\mathbf{x})$ in $\mathbb{P}^{n-1}$. By Lemma 2.4, the $\mathrm{PU}_n(q)$-action on X is generically free. Thus

$$\begin{aligned}\mathrm{rd}_p\left(\mathrm{PU}_n(q)\right) &= \mathrm{rd}_{\mathbb{F}_{q^2}}\left(\mathrm{PU}_n(q)\right) \leqslant \max\left\{n-2, \mathrm{rd}_{\mathbb{F}_{q^2}}(\mathrm{S}_{q+1})\right\} \\ &= \max\left\{n-2, \mathrm{rd}_p(\mathrm{S}_{q+1})\right\}, \end{aligned} \tag{3.4}$$

where the first and the last equalities follow from Lemma 2.1 (a), and the inequality in the middle from Lemma 2.5. Combining (3.3) and (3.4), we arrive at the inequality of part (b). ∎

4. Proof of Theorems 1.2 (b)–(c) and 1.3

For the proofs of Theorems 1.2 (b-c) and 1.3 we use the classification results for maximal subgroups of finite classical groups found in [2]. Occasionally, we mention groups constructed as central products; we recall this latter definition here. Given finite groups G, H, central subgroups $Z_1 \subset Z(G)$, $Z_2 \subset Z(H)$ and an isomorphism $\varphi : Z_1 \to Z_2$, we may construct the *central product* $G \circ_\varphi H$ as the quotient $(G \times H)/N$, where N is the normal subgroup

$$\left\{(g,h) \in G \times H : g \in Z_1, h \in Z_2, \text{ and } \varphi(g)h = 1\right\}.$$

Note that the natural maps $G \to G \circ_\varphi H$ and $H \to G \circ_\varphi H$ are injective. When the subgroups Z_1, Z_2 and the isomorphism φ are clear from the context, we write the central product as $G \circ H$.

Proof of Theorems 1.2 (b). By Lemma 2.1 (a), it suffices to show that $\mathrm{rd}_{\mathbb{F}_3}(\mathrm{S}_7) \leqslant 2$. In view of Corollary 2.2, we need to show that $\mathrm{rd}_{\mathbb{F}_3}(\mathrm{A}_7) \leqslant 2$. By [2, Table 8.11] we have an inclusion $\mathbb{Z}/4\mathbb{Z} \circ (2 \cdot \mathrm{A}_7) \subset \mathrm{SU}_4(3)$, which induces an inclusion $2 \cdot \mathrm{A}_7 \subset U_4(3)$. Consequently, Proposition 3.1 (b) implies that

$$\begin{aligned}&\mathrm{rd}_{\mathbb{F}_3}(\mathrm{A}_7) \\ &= \mathrm{rd}_{\mathbb{F}_3}(2 \cdot \mathrm{A}_7) \leqslant \mathrm{rd}_{\mathbb{F}_3}\left(U_4(3)\right) \leqslant \max\left\{4-2, \mathrm{rd}_{\mathbb{F}_3}(\mathrm{S}_4)\right\} \leqslant \max\left\{2, \mathrm{rd}_{\mathbb{C}}(\mathrm{S}_4)\right\} = 2.\end{aligned}$$

Here the first equality follows from Lemma 2.1 (d), applied to the central extension $0 \to \mathbb{Z}/2\mathbb{Z} \to 2 \cdot \mathrm{A}_7 \to \mathrm{A}_7 \to 1$. The first inequality follows from Lemma 2.1 (b) with $H = 2 \cdot \mathrm{A}_7$ and $G = U_4(3)$, the second inequality from Proposition 3.1 (b), and the third inequality from (2.2). The equality on the right follows from the fact that $\mathrm{rd}_{\mathbb{C}}(\mathrm{S}_4) = 1$; see [14, Example 10.8] or [6, Corollary 3.4]. ∎

Proof of Theorems 1.2 *(c).* We need to show that $\mathrm{rd}_5(\mathrm{S}_6) = \mathrm{rd}_5(\mathrm{S}_7) \leqslant 2$. The inequality $\mathrm{rd}_5(\mathrm{S}_6) \leqslant 2$ follows from (2.2) and (1.1). Moreover, by Lemma 2.1 (b), $\mathrm{rd}_5(\mathrm{S}_6) \leqslant \mathrm{rd}_5(\mathrm{S}_7)$, while $\mathrm{rd}_5(\mathrm{S}_7) = \mathrm{rd}_5(\mathrm{A}_7)$ by Corollary 2.2. Therefore it suffices to show that $\mathrm{rd}_k(\mathrm{A}_7) \leqslant \mathrm{rd}_k(\mathrm{S}_6)$, where $k = \mathbb{F}_5$. By Table 8.6 of [2] there is an inclusion $3 \cdot \mathrm{A}_7 \subset \mathrm{SU}_3(5) \subset U_3(5)$. Thus Proposition 3.1 (b) shows that

$$\mathrm{rd}_{\mathbb{F}_5}(\mathrm{A}_7) = \mathrm{rd}_{\mathbb{F}_5}(3 \cdot \mathrm{A}_7) \leqslant \mathrm{rd}_{\mathbb{F}_3}\big(U_3(5)\big) \leqslant \max\big\{3-2, \mathrm{rd}_{\mathbb{F}_5}(\mathrm{S}_6)\big\} = \mathrm{rd}_{\mathbb{F}_5}(\mathrm{S}_6),$$

as desired. Here the first equality follows from Lemma 2.1 (d), applied to the central extension $0 \to \mathbb{Z}/3\mathbb{Z} \to 3 \cdot \mathrm{A}_7 \to \mathrm{A}_7 \to 1$. The first inequality follows from Lemma 2.1 (b) with $H = 3 \cdot \mathrm{A}_7$ and $G = U_3(5)$ and the second from Proposition 3.1 (b). The equality on the right follows the second part of Lemma 2.1 (b), which tells us that

$$\mathrm{rd}_5(\mathrm{S}_6) \geqslant 1. \qquad \blacksquare$$

Proof of Theorem 1.3. We want to show that $\mathrm{rd}_p(W(E_6)) \leqslant 2$ for $p = 2, 3, 5$. Note first that

$$\mathrm{rd}_p\big(W(E_6)\big) = \mathrm{rd}_p\big(\mathrm{SU}_4(2)\big) \tag{4.1}$$

for any $p \geqslant 0$. This follows from the exact sequence $1 \to \mathrm{SU}_4(2) \to W(E_6) \to \mathbb{Z}/2\mathbb{Z} \to 0$; see [3, p. 26]. Indeed, $\mathrm{rd}_p(\mathrm{SU}_4(2)) \leqslant \mathrm{rd}_p(W(E_6))$ by Lemma 2.1 (b). On the other hand,

$$\begin{aligned}\mathrm{rd}_p\big(W(E_6)\big) &\leqslant \max\big\{\mathrm{rd}_p\big(\mathrm{SU}_4(2)\big), \mathrm{rd}_p(\mathbb{Z}/2\mathbb{Z})\big\} \\ &= \max\big\{\mathrm{rd}_p\big(\mathrm{SU}_4(2)\big), 1\big\} = \mathrm{rd}_p\big(\mathrm{SU}_4(2)\big)\end{aligned}$$

by Lemma 2.1 (b), (c) and (d). Thus it suffices to show that $\mathrm{rd}_p(\mathrm{SU}_4(2)) \leqslant 2$ for $p = 2, 3, 5$.

Case $p = 2$. By Lemma 2.1 (b) and Proposition 3.1 (b),

$$\mathrm{rd}_2\big(\mathrm{SU}_4(2)\big) \leqslant \mathrm{rd}_2\big(\mathrm{U}_4(2)\big) \leqslant \max\big\{4-2, \mathrm{rd}_2(\mathrm{S}_3)\big\} = 2.$$

Combining this with (4.1), we obtain the desired inequality, $\mathrm{rd}_2(W(E_6)) \leqslant 2$.

Case $p = 3$. Here we use the exceptional isomorphism $\mathrm{SU}_4(2) \cong \mathrm{PSp}_4(3)$; see [3, p. 26]. Combining (4.1) and Proposition 3.1 (a) we obtain

$$\begin{aligned}\mathrm{rd}_3\big(W(E_6)\big) &= \mathrm{rd}_3\big(\mathrm{SU}_4(2)\big) = \mathrm{rd}_3\big(\mathrm{PSp}_4(3)\big) = \mathrm{rd}_{\mathbb{F}_3}\big(\mathrm{Sp}_4(3)\big) \\ &\leqslant \max\big\{4-2, \mathrm{rd}_{\mathbb{F}_3}(\mathrm{S}_4)\big\} \leqslant 2.\end{aligned}$$

Here, the equality

$$\mathrm{rd}_3\big(\mathrm{PSp}_4(3)\big) = \mathrm{rd}_3\big(\mathrm{Sp}_4(3)\big)$$

follows from Lemma 2.1 (d), because $\mathrm{Sp}_4(3)$ is a central extension of $\mathrm{PSp}_4(3)$.

Case $p = 5$. Table 8.11 of [2] gives an inclusion $2 \cdot \mathrm{SU}_4(2) \subset \mathrm{SU}_4(5) \subset \mathrm{U}_4(5)$. By Lemma 2.1 (d), we have $\mathrm{rd}_5(2 \cdot \mathrm{SU}_4(2)) = \mathrm{rd}_5(\mathrm{SU}_4(2))$. Combining this with (4.1) and

Proposition 3.1 (b), we obtain

$$\begin{aligned}\mathrm{rd}_5\left(W(E_6)\right) = \mathrm{rd}_5\left(2\cdot \mathrm{SU}_4(2)\right) &\leqslant \mathrm{rd}_{\mathbb{F}_5}\left(U_4(5)\right) \leqslant \max\left\{4-2, \mathrm{rd}_{\mathbb{F}_5}(\mathrm{S}_6)\right\}\\ &\leqslant \max\left\{2, \mathrm{rd}_{\mathbb{C}}(\mathrm{S}_6)\right\} \leqslant 2,\end{aligned}$$

where the inequality on the right follows from (1.1). ∎

5. The varieties Y_{123}

Let n be a positive integer. We define the closed subvariety X_{123} of $\mathbb{A}^n$ by

$$X_{123} := \left\{(x_1,\dots,x_n) \in \mathbb{A}^n \mid s_1(x_1,\dots,x_n) = s_2(x_1,\dots,x_n) = s_3(x_1,\dots,x_n) = 0\right\}.$$

Here $s_j(x_1,\dots,x_n)$ denotes the jth elementary symmetric polynomial in $x_1,\dots,x_n$. We denote by $Y_{123} \subset \mathbb{P}^{n-1}$ the projective variety cut out by the same equations. Note that X_{123} and Y_{123} depend on n, which is assumed to be fixed throughout. The symmetric group S_n acts on both X_{123} and Y_{123} by permuting the variables.

Lemma 5.1. *Let k be a field of characteristic $p \geqslant 0$ and $n \geqslant 7$ be a positive integer. Then*

(a) *the symmetric group S_n acts transitively on the irreducible components of X_{123} (respectively Y_{123}), each of which has dimension $n-3$ (respectively, $n-4$).*

(b) *The projective variety Y_{123} is of degree 6 in $\mathbb{P}^{n-1}$. It has either one or two irreducible components. If there are two components, then odd permutations in S_n interchange them, and even permutations leave each component invariant.*

(c) *The S_n-action on Y_{123} is generically free.*

(d) *If $p > 0$ and $n = p^r$ is a power of p, then the projective variety Y_{123} is a cone over the S_n-fixed point $(1:1:\cdots:1)$ in $\mathbb{P}^{n-1}$.*

Proof. (a) The ring of invariants $k[X_{123}]^{\mathrm{S}_n}$ is the free polynomial k-algebra generated by the elements $a_4, a_5, \dots, a_n$, where $a_j = s_j(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$. Hence, the geometric quotient X_{123}/S_n is isomorphic to the affine space $\mathbb{A}^{n-3}$. The natural inclusion $k[X_{123}]^{\mathrm{S}_n} \hookrightarrow k[X_{123}]$ gives rise to a (finite) geometric quotient map $\pi\colon X_{123} \to \mathbb{A}^{n-3}_k$. The assertions about X_{123} in part (a) now follow from the fact that $\mathbb{A}^{n-3}$ is an irreducible variety of dimension $n-3$. The assertions about Y_{123} follow from the fact that X_{123} is the affine cone over Y_{123}.

(b) Y_{123} is an $(n-4)$-dimensional closed subvariety of $\mathbb{P}^{n-1}$ cut out by the polynomials $s_i(x_1,\dots,x_n)$ of degree i for $i = 1, 2, 3$. Hence, the degree of Y_{123} is 6. Denote the number of irreducible components of Y_{123} by m. The group S_n acts transitively on these components. Hence, $m \leqslant \deg(Y_{123}) = 6$. The S_n-action on the m irreducible components of Y_{123} gives rise to a transitive permutation representation $\mathrm{S}_n \to \mathrm{S}_m$. Since $n \geqslant 7$, this permutation representation has a non-trivial kernel. An easy exercise in finite group theory shows that either (i) $m = 1$, i.e., Y_{123} is irreducible or (ii) $m = 2$, i.e., Y_{123} has two irreducible components, and each component is preserved by the alternating group A_n.

(c) Assume the contrary. From the description of the irreducible components of Y_{123} it follows that the action of A_n on each irreducible component is not generically free. By Lemma 2.3 (b), this implies that the action of A_n on each irreducible component of Y_{123} is not faithful. In other words, for every irreducible component of Y_{123}, there is a non-trivial normal subgroup N of A_n which acts trivially on that component. Since A_n is a simple group, $N = \mathrm{A}_n$ is the only possibility for N. In other words, A_n acts trivially on Y_{123}.

This means that for every element $(y_1 : \cdots : y_n) \subset Y_{123}$ and every $\sigma \in \mathrm{A}_n$, we have

$$(y_{\sigma(1)}, \dots, y_{\sigma(n)}) = \lambda(\sigma)(y_1, \dots, y_n),$$

in $\mathbb{A}^n$, where $\lambda(\sigma)$ is a non-zero scalar in $\bar{k}$. It is easy to see that the map $\sigma \to \lambda(\sigma)$ is a multiplicative character $\mathrm{A}_n \to \bar{k}^*$. Since A_n is a simple group, it has no non-trivial multiplicative characters. We conclude that $(y_{\sigma(1)}, \dots, y_{\sigma(n)}) = (y_1, \dots, y_n)$ in $\mathbb{A}^n$ for every $\sigma \in \mathrm{A}_n$. Since the natural action of A_n on $\{1, \dots, n\}$ is transitive, this is only possible if $y_1 = \cdots = y_n$. In other words, Y_{123} is either empty or consists of the single point $(1 : \cdots : 1)$ in $\mathbb{P}^{n-1}$. This contradicts the assertion of part (a) that $\dim(Y_{123}) = n - 4 \geqslant 3$.

(d) Suppose $y = (y_1, \dots, y_n) \in X_{123}$. We need to show that the point $y_{\alpha,\beta} = (\alpha y_1 + \beta, \dots, \alpha y_n + \beta)$ also lies in X_{123} for every $\alpha, \beta \in \bar{k}$. In other words, if $s_1(y) = s_2(y) = s_3(y) = 0$, then $s_1(y_{\alpha,\beta}) = s_2(y_{\alpha,\beta}) = s_3(y_{\alpha,\beta}) = 0$.

Indeed, $s_1(y_{\alpha,\beta}) = s_1(y)\alpha + n\beta = 0$, since we are assuming that $s_1(y) = 0$ and n is a power of $p = \mathrm{char}(k)$. Similarly,

$$s_2(y_{\alpha,\beta}) = s_2(y)\alpha^2 + (n-1)s_1(y)\alpha\beta + \binom{n}{2}\beta^2 = 0$$

in k (recall that we are assuming that $n \geqslant 7$ is a power of p). Finally,

$$s_3(y_{\alpha,\beta}) = s_3(y)\alpha^3 + \alpha^2\beta(n-2)s_2(y) + \alpha\beta^2\binom{n-1}{2}s_1(y) + \binom{n}{3} = 0,$$

again because $s_1(y) = s_2(y) = s_3(y)$ and $\binom{n}{3} = 0$ in k under our assumptions on n and $\mathrm{char}(k)$. ∎

Remark 5.2. The condition on n and $\mathrm{char}(k)$ in part (d) can be weakened: our proof goes through whenever

$$\binom{n}{1} = \binom{n}{2} = \binom{n}{3} = 0$$

in k. In the next section, we will only need the special case, where $n = p^r \geqslant 7$, considered above.

Remark 5.3. The variety Y_{123} is, in fact, irreducible. This can be deduced from [16, Corollary 2]. We chose to go with the weaker assertion of Lemma 5.1 (b) because its proof is short and self-contained, and because it suffices for the purpose of establishing Theorem 1.2 (d) and (e) in the next section.

6. Proof of Theorem 1.2 (d)–(e)

We continue with the notational conventions introduced in the previous section. Recall that Y_{123} in the closed subvariety of $\mathbb{P}^{n-1}$ given by

$$s_1(x_1, \dots, x_n) = s_2(x_1, \dots, x_n) = s_3(x_1, \dots, x_n) = 0,$$

where s_1, s_2 and s_3 are the first three elementary symmetric polynomials. Lemma 5.1 (d) asserts that when $\operatorname{char}(k) = p > 0$ and $n \geqslant 7$ is a power of p, Y_{123} is a cone over the point $(1 : \cdots : 1)$ in $\mathbb{P}^{n-1}$. Let us denote the "base" of this cone by $Z_{123} \subset \mathbb{P}(V) \simeq \mathbb{P}^{n-2}$, where $V = k^n/\Delta$. Here Δ denotes the small diagonal $\operatorname{Span}_k\{(1, 1, \dots, 1)\}$ in k^n. In other words, points of Z_{123} are in bijective correspondence with lines in $\mathbb{P}^{n-1}$ passing through $(1 : 1 : \cdots : 1)$ and contained in Y_{123}.

Proposition 6.1. *Suppose $p > 0$ and $n = p^r \geqslant 7$.*

(a) *Z_{123} is a variety of dimension $n - 5$ and degree 6 in $\mathbb{P}^{n-2}$.*

(b) *The S_n-action on Y_{123} descends to a generically free action on Z_{123}.*

(c) $\operatorname{rd}_p(\mathrm{S}_n) \leqslant n - 5$.

The inequalities of Theorem 1.2 (d) and (e) are immediate consequences of Proposition 6.1 (c). Indeed, setting $n = p = 7$, we obtain $\operatorname{rd}_7(\mathrm{S}_7) \leqslant 2$ and setting $n = 8$ and $p = 2$, we obtain $\operatorname{rd}_2(\mathrm{S}_8) \leqslant 3$. It thus remains to prove Proposition 6.1.

Proof of Proposition 6.1. (a) By Lemma 5.1 (a), $\dim(Y_{123}) = n - 4$. Since Y_{123} is a cone over Z_{123}, we conclude that $\dim(Z_{123}) = \dim(Y_{123}) - 1 = n - 5$.

To find the degree of Z_{123}, note that Z_{123} is isomorphic to the intersection of the cone Y_{123} in $\mathbb{P}^{n-1}$ with a hyperplane $H \simeq \mathbb{P}^{n-2}$ not passing through the vertex $(1 : \cdots : 1)$. More precisely, the closed embedding $Z_{123} \hookrightarrow \mathbb{P}^{n-2}$ is isomorphic to the closed embedding $(Y_{123} \cap H) \hookrightarrow H$. It is clear from this description that the degree of Z_{123} in $\mathbb{P}^{n-2}$ is the same as the degree of Y_{123} in $\mathbb{P}^{n-1}$. By Lemma 5.1 (b) the degree of Y_{123} in $\mathbb{P}^{n-1}$ is 6, and part (a) follows.

As an aside, we remark that the isomorphism between Z_{123} and $Y_{123} \cap H$ is not S_n-equivariant, since H may not be invariant under S_n. We can still use this isomorphism because the S_n-action plays no role in part (a).

(b) The fact that the S_n-action on Y_{123} descends to Z_{123} is clear from our construction. To show that this action is generically free, we argue by contradiction. Assume the contrary.

Claim. A_n acts trivially on Z_{123}.

To prove the claim, recall that by Lemma 5.1 (b) either (i) Y_{123} is irreducible or (ii) Y_{123} has exactly two irreducible components. In case (i), Z_{123} is also irreducible (since Y_{123} is a cone over Z_{123}). By Lemma 2.3 (b) the S_n-action on Z_{123} is not faithful. The kernel of this action is a non-trivial normal subgroup of S_n, i.e., either the alternating group A_n or all of S_n. Either way, A_n acts trivially on Z_{123}. In case (ii), each irreducible

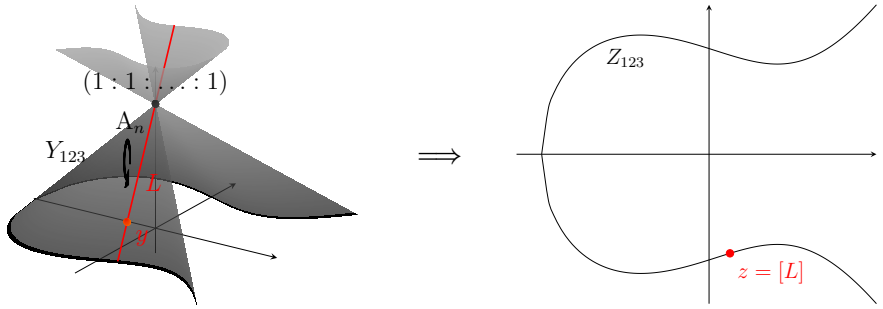


Figure 1. The picture on the left shows the variety Y_{123} in P^{n-1} and the line $L \subset Y_{123}$, which has a faithful action of A_n. The picture on the right shows the variety Z_{123} in P^{n-2} with the A_n-fixed point $z = [L] \in Z_{123}$.

component Y'_{123} and Y''_{123} of Y_{123} is a cone with the vertex $(1 : \cdots : 1)$. Thus Z_{123} has two irreducible components Z'_{123} and Z''_{123}, where Y'_{123} (respectively, Y''_{123}) is a cone over Z'_{123} (respectively, of Z''_{123}). Recall from Lemma 5.1 (b) that odd permutations in S_n interchange Y'_{123} and Y''_{123}; hence, they also interchange Z'_{123} and Z''_{123}. Thus the stabilizer of any point of Z_{123} away from the intersection of the two components lies in the alternating group A_n. We conclude that the action of A_n on either of the components Z'_{123} and Z''_{123} is not generically free. Now the same argument as in case (i) shows that A_n acts trivially on both Z'_{123} and Z''_{123}. This proves the Claim.

Continuing with the proof of part (b), recall that by Lemma 5.1 (c), S_n acts generically freely on Y_{123}. Choose a $\bar{k}$-point $y \in Y_{123}$ whose stabilizer in S_n is trivial. Note that $y \neq (1 : \cdots : 1)$, because the stabilizer of $(1 : \cdots : 1)$ is all of S_n. Let z be the point of Z_{123} corresponding to the line L joining y to the vertex $(1 : \cdots : 1)$; see Figure 1. By our assumption A_n fixes z and hence acts on the line $L \simeq \mathbb{P}^1$. Since L passes through the point y with trivial stabilizer in A_n, we conclude that this action is faithful. On the other hand, A_n fixes the point $(1 : \cdots : 1)$ on L. This means that A_n embeds into the subgroup $B \subset \mathrm{Aut}(L) \simeq \mathrm{PGL}_2(\bar{k})$, where B consists of automorphisms of $L \simeq \mathbb{P}^1$ fixing the point $(1 : \cdots : 1)$. This group is isomorphic to the subgroup of upper-triangular matrices of the form $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{PGL}_2(\bar{k})$. Note that B decomposes as a semidirect product $\mathbb{G}_a(\bar{k}) \rtimes \mathbb{G}_m(\bar{k})$, where $\mathbb{G}_a$ is the additive group of strictly upper-triangular matrices, with $\alpha = 1$, and $\mathbb{G}_m$ is the multiplicative group of diagonal matrices, with $\beta = 0$. This semidirect product decomposition shows that B is solvable. On the other hand, A_n is not solvable; hence, it cannot embed into B. This contradiction completes the proof of part (b).

(c) Parts (a) and (b) allow us to apply Lemma 2.5 with $G = S_n$, $X = Z_{123}$, $a = 6$ and $b = n - 5$. We conclude that

$$\mathrm{rd}_p(S_n) \leqslant \max\left\{n-5, \mathrm{rd}_p(S_6)\right\} \leqslant \max\left\{n-5, \mathrm{rd}_0(S_6)\right\} \leqslant \max\{n-5, 2\} = n-5.$$

Here the first inequality follows from Lemma 2.5, the second from (2.2), and the third from (1.1). The last equality follows from our assumption that $n \geqslant 7$. ∎

Acknowledgments. We are grateful to Alexander Duncan, Jesse Wolfson and the anonymous referee for helpful comments.

Funding. Oakley Edens was partially supported by an Undergraduate Student Research Award (USRA) from the National Sciences and Engineering Research Council of Canada. Zinovy Reichstein was partially supported by a Discovery Grant RGPIN-2023-03353 from the National Sciences and Engineering Research Council of Canada.

References

[1] R. Brauer, On the resolvent problem. *Ann. Mat. Pura Appl. (4)* **102** (1975), 45–55 Zbl 0299.12105 MR 0371854

[2] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*. London Math. Soc. Lecture Note Ser. 407, Cambridge University Press, Cambridge, 2013 Zbl 1303.20053 MR 3098485

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, $\mathbb{ATLAS}$ *of finite groups. Maximal subgroups and ordinary characters for simple groups*. Oxford University Press, Eynsham, 1985 Zbl 0568.20001 MR 0827219

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

[5] O. Edens and Z. Reichstein, Essential dimension of symmetric groups in prime characteristic. *C. R. Math. Acad. Sci. Paris* **362** (2024), 639–647 Zbl 07887264 MR 4773747

[6] 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

[7] C. Gómez-Gonzáles, A. J. Sutherland, and J. Wolfson, Generalized versality, special points, and resolvent degree for the sporadic groups. *J. Algebra* **647** (2024), 758–793 Zbl 07828259 MR 4719199

[8] W. Hamilton, Inquiry into the validity of a method recently proposed by George B. Jerrard, Esq. for transforming and resolving equations of elevated degrees. In *Report of the sixth meeting of the british association for the advancement of science*, pp. 295–348, Bristish Association Report, Bristol, 1836

[9] 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

[10] D. Hilbert, Über die Gleichung neunten Grades. *Math. Ann.* **97** (1927), no. 1, 243–250 Zbl 52.0103.02 MR 1512361

[11] D. Hilbert, Mathematical problems. *Bull. Amer. Math. Soc. (N.S.)* **37** (2000), no. 4, 407–436; reprinted from *Bull. Amer. Math. Soc.* **8** (1902), 437–479 Zbl 33.0976.07 MR 1779412

[12] D.-J. Mercier and R. Rolland, Polynômes homogènes qui s'annulent sur l'espace projectif $\mathrm{P}^m(\mathbf{F}_q)$. *J. Pure Appl. Algebra* **124** (1998), no. 1-3, 227–240 Zbl 0899.13028 MR 1600301

[13] 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

[14] Z. Reichstein, Hilbert's 13th problem for algebraic groups. *Enseign. Math.* **71** (2025), no. 1-2, 139–192 Zbl 08016334 MR 4861787

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

[16] K. Uchida, Galois group of an equation $X^n - aX + b = 0$. *Tohoku Math. J. (2)* **22** (1970), 670–678 Zbl 0211.37104 MR 0277505

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

Communicated by Nikita A. Karpenko

Received 5 July 2024; revised 29 July 2024.

Oakley Edens
Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA; oedens@math.harvard.edu

Zinovy B. Reichstein
Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver, BC V6T 1Z2, Canada; reichst@math.ubc.ca